Common Messages

For Radio Bridge Sensors

VERSION 1.12

JANUARY 2020

TABLE OF CONTENTS

1. QUICK START

To start using your sensor, simply go to:

https://console.radiobridge.com

From here you can register your device and immediately start receiving messages.

The sensor configuration, message monitoring, and setting up alerts is usually self-explanatory through the user interface. For further explanations of any sensor features, you may refer to this user guide

2. OVERVIEW

2.1. Common Messages Overview

The wireless sensors designed and manufactured by Radio Bridge provide full sensor to cloud solutions for Internet of Things (IoT) applications. This document describes the messages common to all wireless sensors. For messages specific to each sensor, please refer to the corresponding user guide.

2.2. Revision History

Table 1 Revision History

Revision	Date	Description
1.0	April 2018	Initial release of the document
1.1	November 2018	Global downlink config definitions
1.2	December 2018	Supervisory period configuration
1.3	December 2018	Fixed byte definitions for supervisory message
1.4	February 2019	Fixed ADR definition
1.5	April 2019	Added extended sensor states
1.6	June 2019	Added global config for sampling rate
1.7	July 2019	Added accumulator for supervisory

1.8	August 2019	Unconfirmed repeat limited to 1
1.9	September 2019	Added link quality message
1.10	October 2019	Added Firmware Version Definition, new Custom Sensor Type to Appendix A
1.11	December 2019	Added link quality messages
1.12	January 2020	Depreciated rate limit feature

2.3. Document Conventions

Table 2 Document Conventions

Font / Icon	Meaning
	Important notes
	Warnings and cautions

3. COMMON MESSAGE PROTOCOL

This section defines the protocol and message definitions common to all wireless sensors. Common messages include basic error messages, tamper, supervisory, link quality, and downlink acknowledgements but do not include sensor specific data.

3.1. Uplink Messages

The uplink messages (sensor to web application) have the structure defined in the following table.

Table 3 Message Structure for Wireless Sensors

Protocol Version	Packet Count	Message Type	Message Payload
4 bits	4 bits	1 byte	0-7 bytes

The Protocol Version (currently a constant 1) is used to provide extensibility to the specific format of a Message Type. It is not expected there will be more than 1 format for each Message Type.

The Sequence Number starts at 0 for the first message sent from the Sensor to the Cloud. It is incremented by 1 for each subsequent message. When it reaches 0xF (15 decimal), it wraps back to 0. Its purpose is to help identify when a Message is lost. For example, if the Sequence Number goes from 2 to 4, instead of 3, this would indicate that a Message has been lost. (It can also help identify out-of-order or duplicate Messages, although this should be much less likely.)

The Message Type byte format is 8 bits where all combinations (256 different Message Types) are possible; although for a given Sensor, there are generally much fewer Message Types. There are two kinds of Message Types, those that are Common to all Sensors, and those that are Unique to a specific sensor. The Common Message Types are described in this document, while the Unique Message Types are described in each individual sensor document

Each Message Type has between 0 and 8 bytes of payload data that is specific to the sensor. The common message types are defined in the following table.

Table 4 Common Message Types for Wireless Sensors

Message	Payload	Description
0x00	5-byte reset code	Device has Reset. The cause of reset is represented in the 5-byte reset code payload.
0x01	3-byte status	Daily Supervisory message (1-2 per day). The 3-byte payload contains status (current) of the sensor. See the Supervisor section for detail on the payload.
0x02	1-byte event	A Tamper event has occurred. This includes enclosure or wall mount tampers. See the tamper section for detail on the tamper payload.
(see datasheets)	Sensor event	Sensor events are defined in their individual datasheets
0xfb	Link Quality	Sent after each DOWNLINK configuration (see Link Quality Message below) or to periodically ping the network server (see Link Quality Check Period below).

0xfc	Current rate limit	DEPRECIATED. Rate limit exceeded. See the Rate Limit section for more detail.
0xfd	Sensor state	Test message with current sensor state
0xfe		Reserved
0xff	1-byte status	Downlink message ack. See the Downlink section for more detail.

3.1.1. Reset Message 0x00

The Reset Message is sent to the Cloud every time that the Sensor is Reset. The Reset Code has to do with the nature of the reset and is used by the factory for diagnostic purposes.

The reset message payload is defined in the following table.

Table 5 Reset Payload

Bytes	Description
0	Sensor type code
1	Hardware version
2-3	Firmware version (see decode below)
4-5	Reset code (used for factory diagnostics)

The sensor type codes are enumerated in Appendix A.

3.1.1.1. Firmware Version

The 16-bit Firmware Version is constructed from Bytes 2-3 of the Reset Payload where Byte 2 is the Most Significant Byte. Beginning in Firmware Version 2.0 and later, the format has been enhanced as follows. Both formats are now supported and the original format is still compatible by redefining the reserved most significant bit (bit 15)

Table: Firmware Version (before 2.0) Format 0 (16-bit) Definition

Bits	Description
15	Format (bit == 0)
14:8	Major number (7 bits)
7:0	Minor number (8 bits)

Table: Firmware Version (2.0.0 and beyond) Format 1 (16-bit) Definition

Bits	Description
15	Format (bit == 1)
14:10	Major number (5 bits)
9:5	Minor number (5 bits)
4:0	Build number (5 bits)

For example, if the 16-bit Firmware Version is 0x0103, then that would be decoded as Firmware Version 1.3.

If the 16-bit Firmware Version is 0x8823, then that would be decoded as Firmware Version 2.1.3.

3.1.2. Supervisory Message 0x01

The wireless sensors will send a periodic supervisory message so that a backend system can verify that the device is still alive and to report error conditions. The supervisory message also contains a payload that contains the status (current) of the sensor.

The supervisory message payload is defined in the following table.

Table 6 Supervisory Payload

Bytes	Description
0	Supervisory error codes
1	Sensor state

2	Battery level
3-6	Extended sensor state (firmware v2.0 and later)
7-8	Event accumulation count

The bit definitions of the supervisory error codes are shown in the following table.

Table 7 Supervisory Error Code Bit Definitions

Bits	Description
7:5	Not used
4	Tamper detected since last reset
3	Current tamper state
2	Error with last downlink
1	Battery Low (under 2.8V)
0	Radio Comm Error. Communication with the integrated radio has failed and device has been reset.

The current sensor state (byte 1 of the supervisory message) is defined by the individual data sheets.

The battery level (byte 2 of the supervisory message) is a two-digit battery voltage. For example, if the battery voltage is 2.9V, byte 2 would be 0x29.

The extended sensor state is a 4-byte field added in firmware version 2.0. This allows sensors that have higher precision or multiple values to be reported during a supervisory event.

Applying a magnet to a sensor that has test message capability will force a supervisory message to allow the user to query the current state, battery level, etc. This feature is available in firmware v2.0 and beyond.

The event accumulation count in bytes 7-8 represent the number of sensor events since the last supervisory message. This can be used in conjunction with the “disable all sensor events” setting so that only an event total is reported during a supervisory message, but the individual events themselves are not reported as they occur which can serve to greatly improve battery life. This feature is available in firmware v2.0 and beyond.

3.1.3. Tamper Message 0x02

The sensor will send a message when the tamper switch has been either opened or closed through either an enclosure tamper or a wall mount tamper. The tamper message contains a 1-byte payload as shown in the following table.

Table 8 Tamper Payload

Payload	Description
0x00	Tamper switch opened
0x01	Tamper switch closed

Not all sensors support the tamper feature. See the individual datasheets for more information.

3.1.4. Link Quality Message 0xfb

The link quality message provides a signal strength and signal to noise measurement at the device itself. The payload of the link quality message is shown in the following table.

Table 9 Link Quality Message Payload

Bytes	Description
0	Current Sub-Band
1	RSSI of last DOWNLINK received, signed integer format
2	SNR of last DOWNLINK received, signed integer format

The sub-band is the frequency sub-band we have successfully joined and are using for communication to the gateway and network server. This value ranges from 1-8 for US915 and can be different for other regions depending on available channels.

The RSSI and SNR values in bytes 1 and 2 are signed integer values in two's complement format.

3.1.5. Rate Limit Exceeded Message 0xfc

Note that this feature has been depreciated and is not available on firmware v2.1 and beyond. There is also a known bug in versions 2.0 and earlier. Do not use.

The sensors have a rate limiting feature as a protection mechanism to ensure the sensors do not flood the wireless network with messages. This may happen if a particular configuration, environment, or a combination thereof creates an unexpected scenario where event messages are generated continuously.

The default rate limit is 100 and is measured between supervisory messages. In other words, if more than 100 event messages are sent between two supervisory messages (18 hours apart), the sensor will send the 0xfc message and will not send new events until the next supervisory event.

The rate limiter is configurable through the 0xfc downlink command, and if it is set to 0 then rate limiting is disabled. The maximum value of the rate limit is 0xfe (0xff is reserved).

3.1.6. Test Message 0xfd (Removed in v2.0 and later)

The test message is initiated when a magnet is applied to the side of the sensor (see user guides for support on individual sensors). When the magnetic reed switch is tripped, a test message 0xfd is sent with the current state of the sensor. This can be used to test connectivity in a particular area or used to calibrate sensors that require specific thresholds.

Table 10 Test Message 0xFD

Bytes	Description
0	Sensor state

Note that the test message 0xFD is eliminated in v2.0 and beyond. Applying the magnet will now send a supervisory message.

3.2. Downlink Messages

A downlink message is one that is sent to the sensor from the cloud and is used to configure the sensor itself. Messages cannot be initiated from the cloud since the sensor is typically sleeping and the radio is turned off, so the sensor itself must initiate a downlink message.

For Sigfox devices, the supervisory, reset, and tamper-open (not tamper close) messages all request a downlink message as a response, and the response must be received within 30 seconds of the request. For LoRaWAN devices, a downlink can be received after any uplink within the receive windows.

The messages that can be sent back to the sensor upon a downlink request are shown in the following table.

Table 11 Downlink Messages

Command	Payload	Description
0x00	Not used	Not used
0x01	4 bytes	General configuration
(see datasheets)	0-7 bytes	Sensor configuration, see individual datasheets
0xfc	3 bytes	Advanced configuration

3.2.1. General Configuration

The general configuration command is used for configuration parameters that apply to all sensor types. This command is defined in the following table.

Table 12 General Configuration Command 0x01

Byte	Description
0x00	Disable sensor events
0x01	Radio config
0x02	Supervisory period. Default 19 hours.
0x03	Sampling rate

3.2.1.1. Disable Sensor Events

The Disable sensor events byte is defined in the following table.

Table 13 Disable Sensor Events Bit Definitions

Bit	Description
7:1	Not used
0	Disable all sensor events

When the sensor events are disabled (bit 0 in the above table), supervisory and tamper-open will still initiate messages but the sensor events will not. Setting bit 0 (set to 1) will disable new event messages and clearing bit 0 (set to 0) will re-enable the event messages.

3.2.1.2. Radio Config

The Radio config byte is defined in the following table.

Table 14 Radio Config Bit Definitions

Bits	Description
7:6	Not used (reserved)
5:2	Uplink retries (LoRaWAN only)
1	Use unconfirmed messages (LoRaWAN only)
0	Disable Adaptive Data Rate (LoRaWAN only)

The range for uplink retries is 1-8 for confirmed messages (ack required) and does not apply to unconfirmed messages. Default 0 (leave unchanged). Available in firmware v1.4 and above.

If the use unconfirmed messages bit is set, the sensor will not look for an ack from the network server. Default is 1 (unconfirmed messages, no acks required). EU sensors cannot use confirmed messages, and thus setting this bit to 0 on an EU device will result in an error. Available in firmware v1.4 and above.

Set the disable adaptive data rate bit to disable ADR, clear to enable ADR. Default is 0 (enabled). Available in firmware v1.3 and above.

Note that the radio config described in the above table is **only available in firmware version 1.4 or later**.

3.2.1.3. Supervisory Period

The supervisory period from the general configuration command controls the time between supervisory messages as defined in the following table.

Table 15 Supervisory Period Bit Definitions

Bit 7	Bits 6:0
0	Period defined in hours (1-127 hours). Available in firmware v1.3 and above.
1	Period defined in minutes (1-127 minutes) Available in firmware v1.3 and above.

For example, to receive a report every 4 hours, byte 1 would be set to 0x04. To receive a periodic report every 15 minutes, byte 1 would be set to 0x8f.

3.2.1.4. Sampling Rate

The sampling rate controls the frequency at which the devices wakes up out of low power sleep mode to check the state of the sensor. Some sensors require very little power to check the state and need to react quickly, whereas other samples can be sampled at a much lower rate, say 30 second or even 30 minute intervals. By increasing the time between samples, the battery life can be greatly increased.

See the Battery Estimator on the Radio Bridge site for battery life estimates relative to sampling rate:

https://radiobridge.com/documents/Sensor Battery Estimator.xlsx

A value of 0 in this field leaves the sampling rate at the current value and for any non-zero value the sampling rate can be determined by the following table:

Table 16 Sampling Period Bit Definitions

Bit 7:6	Bits 5:0
00	Sampling period defined in increments of 250ms (0.25-15 seconds)
01	Sampling period defined in increments of seconds (1-63 seconds)
10	Sampling period defined in increments of minutes (1-63 minutes)
11	Sampling period defined in increments of hours (1-63 hours)

Note that the sampling period only applies to sensors that take measurements like temperature and tilt, whereas it is not applied to sensors with binary inputs such as door/window sensors or push buttons.

Some features described above such as the Enable Adaptive Data Rate and Supervisory Period are **only available in firmware version 1.3 or later**. The firmware version is supplied in the sensor's reset message and is displayed on the Radio Bridge Console

This feature is available in firmware v2.0 and above.

3.2.2. Advanced Configuration

The advanced configuration command is used for advanced configuration parameters that apply to all sensor types. This command is defined in the following table.

Table 17 Advanced Configuration Command 0xFC

Byte	Description
0x00	Rate limit (range 0-255)
0x01	Port number (LoRaWAN only)
0x02	Link quality check period (LoRaWAN only)

3.2.2.1. Rate Limit

The sensors have a rate limiting feature as a protection mechanism to ensure the sensors do not flood the wireless network with messages (see the section Rate Limit Exceeded Message 0xfc). If the rate limit is set to 0, rate limiting is disabled. The rate limiter is reset with every supervisory message (typically once per day).

The default for the rate limit is 100 for Sigfox and 0 for LoRa.

Disabling the rate limiter may cause unrecoverable failures in the field.

3.2.2.2. Port Number

Byte 0x01 of the advanced configuration command changes the uplink port per the LoRaWAN protocol. Note that this is only available in LoRaWAN devices.

The default port is 2, and a value of 0 in this field means to leave it at the default. This feature is available in firmware v1.4 and above.

3.2.2.3. Link Quality Check Period

Setting this register causes the device to “ping” the network server on a periodic basis with a requested ack to ensure the device is still connected. This is implemented as a confirmed message containing connectivity info, and is typically used in conjunction with unconfirmed messages.

In other words, while running with *unconfirmed* messages, this feature will create a periodic *confirmed* message and look for the ack to ensure connectivity. This feature is available for LoRaWAN devices only.

See Table for the encoded bit definitions of this byte. A value of 0x00 means disable the connectivity period feature. Available in firmware v2.0 and above.

The Link Quality period in byte 2 is defined in the following table.

Table 18 Link Quality Period Bit Definitions

Bit 7	Bits 6:0
0	Period defined in hours (1-127 hours). Available in firmware v2.0 and above.
1	Period defined in minutes (1-127 minutes) Available in firmware v2.0 and above.

3.3. Downlink Ack

The sensor will reply to the downlink data with a 0xFF message (downlink ack) with a payload shown in the following table.

Table 19 Downlink Ack Messages

Command	Payload
0x00	Not used
0x01	Message was invalid or undefined
0x02	Message was valid

This downlink ack message is used by the cloud app to verify that the downlink message was received by the sensor and that it was considered valid.

4. APPENDIX A: SENSOR TYPE CODES

The sensor type codes in the table below are provided as product identifiers and sent as part of the reset message.

Table 20 Sensor Type Codes

Sensor	Code
Door/Window	0x01
Door/Window High Security	0x02
Contact	0x03
Temperature No-Probe	0x04
Temperature External Probe	0x05
Single Push Button	0x06
Dual Push Button	0x07
Acceleration-Based Movement	0x08
Tilt	0x09
Water	0x0a
Tank Level Float	0x0b
Glass Break	0x0c
Ambient Light	0x0d
Air Temperature and Humidity	0x0e
High-Precision Tilt	0x0f
Ultrasonic Level	0x10
4-20mA Loop	0x11
Air Temp and Humidity – External Probe	0x12
Thermocouple	0x13
Voltmeter	0x14
Custom (for customized sensors)	0x15
GPS	0x16

Honeywell 5800 bridge	0x17

5. CUSTOMER SUPPORT

Radio Bridge offers free technical support at:

https://support.radiobridge.com

Radio Bridge also offers technical support plans and service packages to help our customers get the most out of their Radio Bridge products.

6. DISCLAIMERS

Information in this document is subject to change without notice and does not represent a commitment on the part of Radio Bridge. Radio Bridge provides this document "as is," without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Radio Bridge may make improvements and/or changes in this manual or in the product(s) and/or the software described in this manual at any time.

7. LEGAL NOTICES

See the Legal Notices section of the website for up to date information on Radio Bridge's warranty, returns policy, privacy statement, terms of sale, and terms of service.

8. TRADEMARKS AND COPYRIGHT

Radio Bridge™, SubGig®, Armored Sensor™ and BridgeBee® are trademarks of Radio Bridge Inc in the United States.

© 2019 Radio Bridge Inc. All rights reserved