Anybus® Wireless Bolt CAN™

USER MANUAL

scm-1202-175 1.11 en-US ENGLISH

HMS Connecting Devices™

Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Table of Contents

Page

1 Preface 3

1.1 About This Document 3

1.2 Document Conventions 3

1.3 Trademarks 3

2 Safety 4

2.1 General Safety Instructions 4

2.2 Intended Use 4

3 Preparation 5

3.1 General Information 5

3.2 When to Use Bluetooth and WLAN 5

4 Installation 6

4.1 Mechanical Installation 6

4.2 Connector 7

4.3 Cabling 8

4.4 Digital Input 9

4.5 RESET Button 9

5 Configuration 10

5.1 Web Interface 11

5.2 Use Cases 33

5.3 Set Up a Wireless Infrastructure 35

5.4 Factory Restore 39

6 Technical Data 40

6.1 Technical Specifications 40

A CAN Electrical Connection 41

A.1 CAN Termination 41

B Wireless Technology Basics 42

C Radio Antenna Patterns 43

C.1 Azimuth (Horizontal) View 43

C.2 Vertical Views 44

C.3 Throughput Diagram 45

This page intentionally left blank

1 Preface

1.1 About This Document

This manual describes how to install and configure Anybus Wireless Bolt CAN.

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.anybus.com/support.

1.2 Document Conventions

Numbered lists indicate tasks that should be carried out in sequence:

1. First do this
2. Then do this

Bulleted lists are used for:

- Tasks that can be carried out in any order
- Itemized information

► An action

→ and a result

User interaction elements (buttons etc.) are indicated with bold text.

```
Program code and script examples
```

Cross-reference within this document: *Document Conventions, p. 3*

External link (URL): www.hms-networks.com

WARNING
Instruction that must be followed to avoid a risk of death or serious injury.

Caution
Instruction that must be followed to avoid a risk of personal injury.

Instruction that must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

Additional information which may facilitate installation and/or operation.

1.3 Trademarks

Anybus® is a registered trademark and Wireless Bolt CAN™ is a trademark of HMS Networks AB. All other trademarks mentioned in this document are the property of their respective holders.

2 Safety

2.1 General Safety Instructions

Caution
This equipment emits RF energy in the ISM (Industrial, Scientific, Medical) band. Make sure that all medical devices used in proximity to this equipment meet appropriate susceptibility specifications for this type of RF energy.

Caution
Minimum temperature rating of the cable to be connected to the field wiring terminals, 90 °C.

Caution
Use copper wire only for field wiring terminals.

This equipment is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be used if a shielded Ethernet cable is used, in order to meet emission requirements.

This equipment contains parts that can be damaged by electrostatic discharge (ESD). Use ESD prevention measures to avoid damage.

2.2 Intended Use

The intended use of this equipment is as a communication interface and gateway. The equipment receives and transmits data on various physical levels and connection types.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

3 Preparation

3.1 General Information

Make sure that you have all the necessary information about the capabilities and restrictions of your local network environment before installation.

The characteristics of the internal antenna should be considered when choosing the placement and orientation of the unit.

For optimal reception, wireless devices require a zone between them clear of objects that could otherwise obstruct or reflect the signal. A minimum distance of 50 cm between the devices should also be observed to avoid interference.

See also *Wireless Technology Basics, p. 42*.

3.2 When to Use Bluetooth and WLAN

Use Bluetooth when:

- The wireless link has an Wireless Bolt CAN at both ends.
- An interruption-free connection is more important than data throughput speed.
- Interference robustness is important – e.g. in an industrial environment.

Use WLAN when:

- Connecting to other types of wireless devices or a WLAN infrastructure.
- High data throughput speed is more important than connection reliability.
- Large file transfers are expected.
- WLAN channel frequency planning is possible.

4 Installation

4.1 Mechanical Installation

The device is intended to be mounted through an M50 (50.5 mm) hole using the included sealing ring and nut.

The top mounting surface (in contact with the sealing) must be flat with a finish equivalent to Ra 3.2 or finer and cleaned and free from oils and greases.

Tightening torque: 5 Nm ±10 %.

> **!** Make sure that the sealing ring is correctly placed in the circular groove in the top part of the housing before tightening the nut.

> **!** Always hold the BOTTOM part of the unit when untightening the nut, not the top part (the cap).

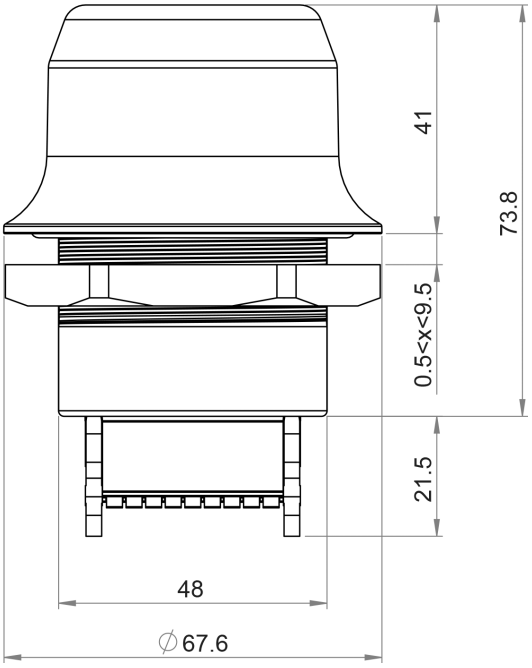


Fig. 1 Installation drawing

All measurements are in mm.

4.2 Connector

The 18-pin connector is common for several models of the Anybus Wireless Bolt. Some pins may have a different function depending on model. Unused pins should not be connected.

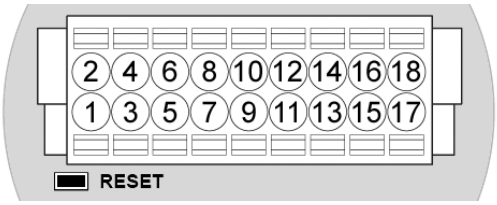


Fig. 2 Connector

The location of the **RESET** button can be used as a reference for the pin numbering when the connector is attached to the Wireless Bolt CAN. Pin 1 will be the pin closest to the button.

The Ethernet interface is intended for configuration purposes only. Wireless Bolt CAN is not designed for permanent Ethernet communication.

For information about the correct connection type and termination, refer to *CAN Electrical Connection, p. 41*.

Pin	Name	Description	
1	VIN	Power + (9–30 V)	
2	GND	Power Ground	
3	DI	Digital input + (9–30 V)	
4	DI_GND	Digital input ground	
5	ETN_RD+	Ethernet receive + (white/orange)	
6	ETN_RD-	Ethernet receive - (orange)	
7	ETN_TD-	Ethernet transmit - (green)	
8	ETN_TD+	Ethernet transmit + (white/green)	
9	RS485_B	RS-485 B Line	Not used for Wireless Bolt CAN.
10	FE/Shield	Ethernet: Serial and CAN:	Functional Earth Functional Earth and Shield
11	RS232_TXD	RS-232 Transmit	Not used for Wireless Bolt CAN.
12	RS485_A/RS232_RXD	RS-485 A Line / RS-232 Receive	Not used for Wireless Bolt CAN.
13	RS232_RTS	RS-232 Request To Send	Not used for Wireless Bolt CAN.
14	RS232_CTS	RS-232 Clear To Send	Not used for Wireless Bolt CAN.
15	ISO_5V	Isolated 5 V for serial interface	Not used for Wireless Bolt CAN.
16	CAN_GND	Isolated Ground for CAN interface	
17	CAN_L	CAN Low	
18	CAN_H	CAN High	

Note:

- The Ethernet wire colors refer to the **T568A** standard.
- If using a shielded Ethernet cable the shield must be unconnected.
- Use termination for CAN when required.

4.3 Cabling

*When using **Easy Config Modes**, the Wireless Bolt CAN that is to be configured as a Client does not need to be connected to the Ethernet wires. Only power and CAN wiring are used.*

To make an Ethernet, CAN and power connector cable for Anybus Wireless Bolt CAN:

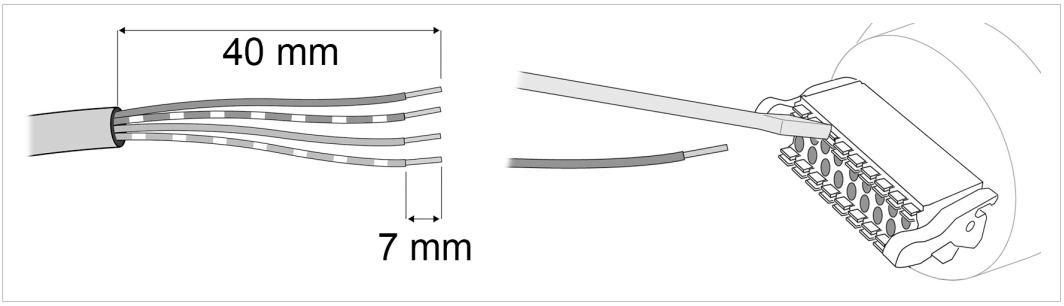


Fig. 3

To maintain signal integrity, low emission and high immunity to EMI, untwist the twisted pair cable as little as possible.

1. Cut off one of the connectors on a standard Cat5e or Cat6 Ethernet cable.
2. Strip off about 40 mm (1½ inch) of the cable jacket, from the orange, orange/white, green and green/white wires.

   The shield and the other wires are not used.
3. Strip off about 7 mm (¼ inch) of the isolation on each wire.
4. Push the pin spring release next to each socket on the connector and insert the correct wire end according to *Connector, p. 7*.
5. Connect the wires from the power supply to the connector in the same way as the Ethernet wiring. **Make sure that polarity is not reversed.**

4.4 Digital Input

The digital input can be used to control roaming between Bluetooth access points (NAP). For more information, refer to the AT Reference Guide at www.anybus.com/support.

> **!** If voltage is applied to the digital input for more that 10 seconds the unit will be reset to factory defaults.

4.5 RESET Button

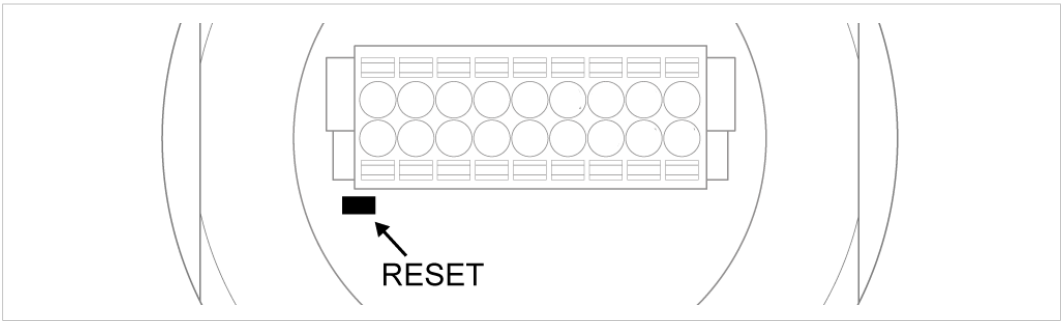


Fig. 4 RESET button

The **RESET** button is located on the bottom of the unit.

When the unit is powered on, press and hold **RESET** for >10 seconds and then release it to reset to the factory default settings.

Recovery Mode

If the web interface cannot be accessed, the unit can be reset by starting in *Recovery Mode* and reinstalling the firmware using Anybus Firmware Manager II, which can be downloaded from www.anybus.com/support.

To enter Recovery Mode, press and hold **RESET** during startup.

> **!** Firmware updates should normally be carried out through the web interface. Recovery Mode should only be used if the unit is unresponsive and the web interface cannot be accessed.

5 Configuration

Anybus Wireless Bolt CAN should normally be configured via the web interface. Parameters can be set individually or using one of the pre-configured **Easy Config** modes.

The web interface is accessed by pointing a web browser to the IP address of the Wireless Bolt CAN. The default address is **192.168.0.99**. The computer accessing the web interface must be in the same IP subnet as the Wireless Bolt CAN.

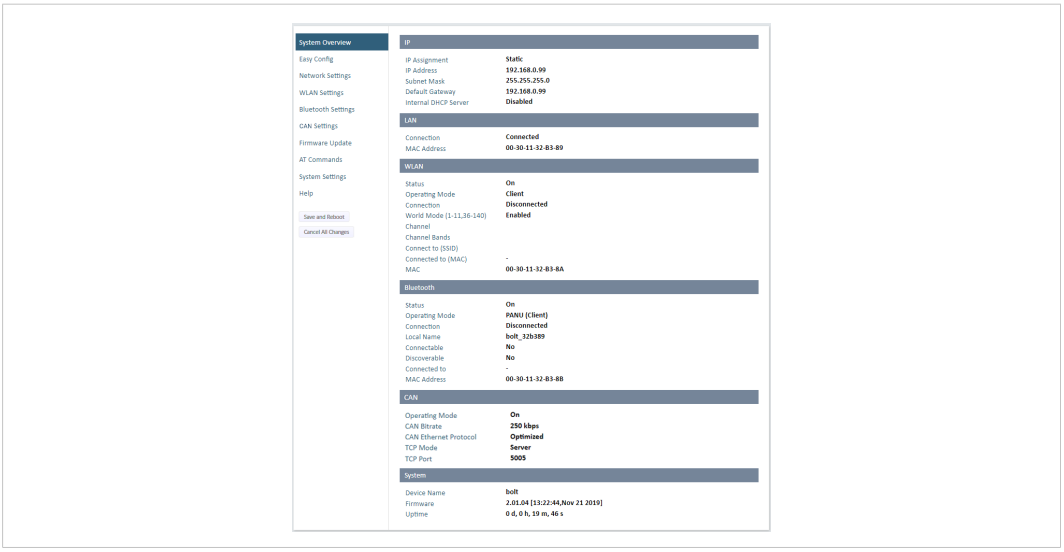


Fig. 5 Web interface

Advanced configuration can be carried out by issuing AT (modem) commands through the web interface or over a Telnet or RAW TCP connection to port 8080. See the *AT Commands Reference Guide* or the **Help** page in the web interface for more information.

5.1 Web Interface

5.1.1 System Overview

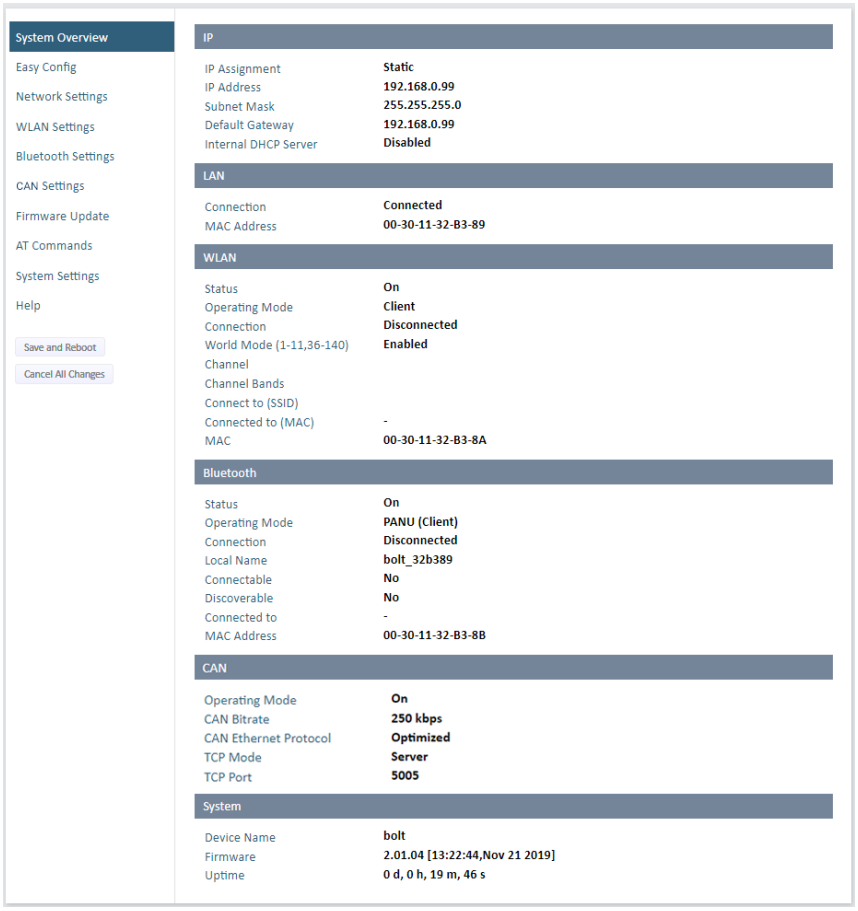


Fig. 6 System Overview page

The **System Overview** page shows the current settings and connection status for the wired and wireless interfaces. The different parameters are explained in the descriptions of each settings page in this manual.

The **Help** page describes AT commands that can be used for advanced configuration.

Save and Reboot	This button will be enabled if the unit must be restarted to apply a change.
Cancel All Changes	Resets parameter changes that have not been applied.

5.1.2 Easy Config

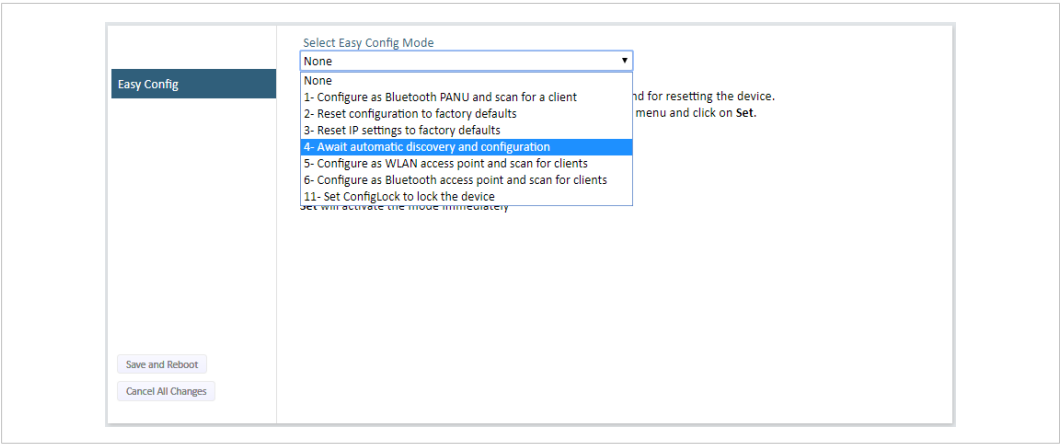


Fig. 7 Easy Config page

To activate an Easy Config mode, select it from the dropdown menu and click on **Set**. The mode will be activated immediately.

Easy Config Modes

EC	Role	Description
1	Bluetooth PANU	Configure as Bluetooth client and scan for another client (PANU–PANU). Recommended setting for Bluetooth point-to-point communication. Listens for 40 seconds or until a configuration is established. Mode 1 will scan for units in mode 4. When a unit in mode 4 is detected, the scanning unit will configure itself as a Bluetooth PANU client, send a connection configuration to the detected unit, and restart. The detected unit will also restart and attempt to connect to the first unit as a PANU client.
2	–	Reset configuration to factory defaults.
3	–	Reset IP settings to factory defaults.
4	Client	Wait for automatic configuration. Listens for 120 seconds or until receiving a configuration. Configure units in mode 4 as clients. When mode 4 is used with mode 1, 5 or 6, CAN Settings TCP Mode Client is activated automatically.
5	WLAN AP	Restart as access point and connect clients. Mode 5 and 6 will time out after 120 seconds. Modes 5 and 6 will scan for units in mode 4. The detected units will be reconfigured as clients and the scanning unit will restart as an access point. The clients will then restart and connect to the access point.
6	Bluetooth NAP	
11	(any)	Activate ConfigLock mode. Mode 7 will be added to the configuration without changing any other settings. Mode 7 locks the unit in ConfigLock mode, where the configuration cannot be changed without physical access. To cancel this mode the unit must be restored to factory defaults by pressing and holding the RESETMODE button.

Default Easy Config Mode

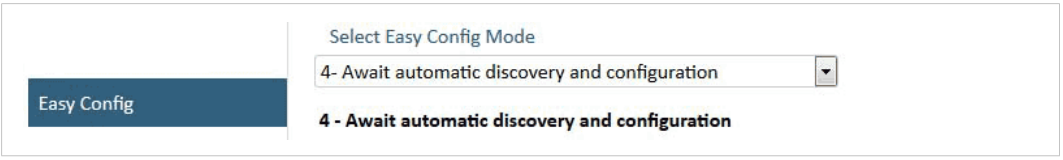


Fig. 8 The default mode is Easy Config Mode 4

By default Wireless Bolt and Bridge starts in **Easy Config Mode 4**.

Configuration of Wireless Bolt and Bridge Clients can be performed wirelessly, via a PC connected to the Wireless Bolt or Bridge Access Point.

After factory reset, Wireless Bolt will by default start in Easy Config Mode 4, if there is no Ethernet connection.

When connection is established via the wireless interface, the Wireless Bolt or Bridge Client does not need to be connected with an Ethernet cable during configuration.

5.1.3 Network Settings

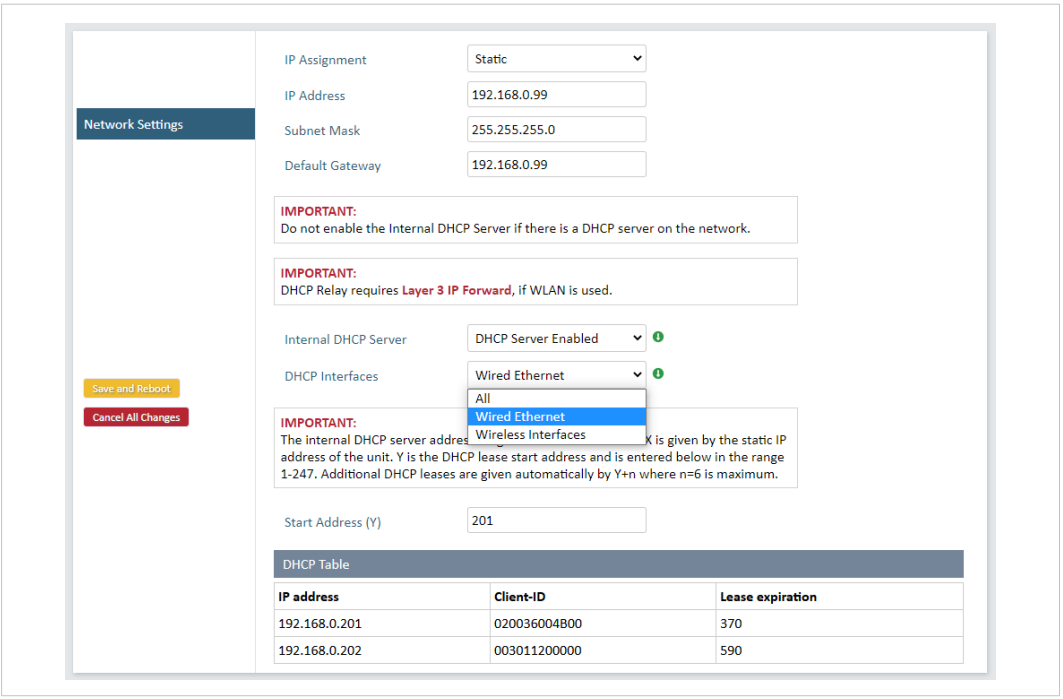


Fig. 9 Network Settings page

IP Assignment	Select static or dynamic IP addressing (DHCP)
IP Address	Static IP address for the unit The browser should automatically be redirected to the new address after clicking on **Save and Reboot** (not supported by all browsers).
Subnet Mask	Subnet mask when using static IP
Default Gateway	Default gateway when using static IP
Internal DHCP Server	**Disabled:** No internal DHCP functionality **DHCP Relay Enabled:** The unit can receive a DHCP request on one interface and resend it to a DHCP server located on one of the other interfaces. Only a single DHCP server can be active for all the connected interfaces. If WLAN is used, the forwarding mode must be set to Layer 3 IP Forward. **DHCP Server Enabled:** Activates an internal DHCP server. This option is only available when IP Assignment is set to Static. To avoid IP address conflict if a DHCP server is already active on the network, use the **DHCP Interfaces** setting to limit the internal DHCP server to the correct interface.

DHCP Interfaces

The **DHCP Interfaces** function is available when **Internal DHCP Server** > **DHCP Server Enabled** is selected.

All: By default, the DHCP Interfaces function is set to use all interfaces.

Wired Ethernet: The internal DHCP server only listens for clients on the wired Ethernet interface.

Wireless Interfaces: The internal DHCP server listens for clients on all supported wireless interfaces (WLAN/Bluetooth).

Start Address (Y)

The internal DHCP server will assign up to 7 IP addresses starting from **X.X.X.Y**, where **X** is taken from the current static IP address setting, and **Y** is the value in **Start Address**. Already allocated addresses will be skipped, including the address of the unit itself. The subnet mask setting will be ignored.

Examples:
IP Address: 192.168.0.99, Start Address: 101
DHCP range = 192.168.0.101 – 192.168.0.107

IP Address: 192.168.0.103, Start Address: 101
DHCP range = 192.168.0.101 – 192.168.0.108
7 addresses are allocated but the address of the unit is skipped.

5.1.4 WLAN Settings - Client

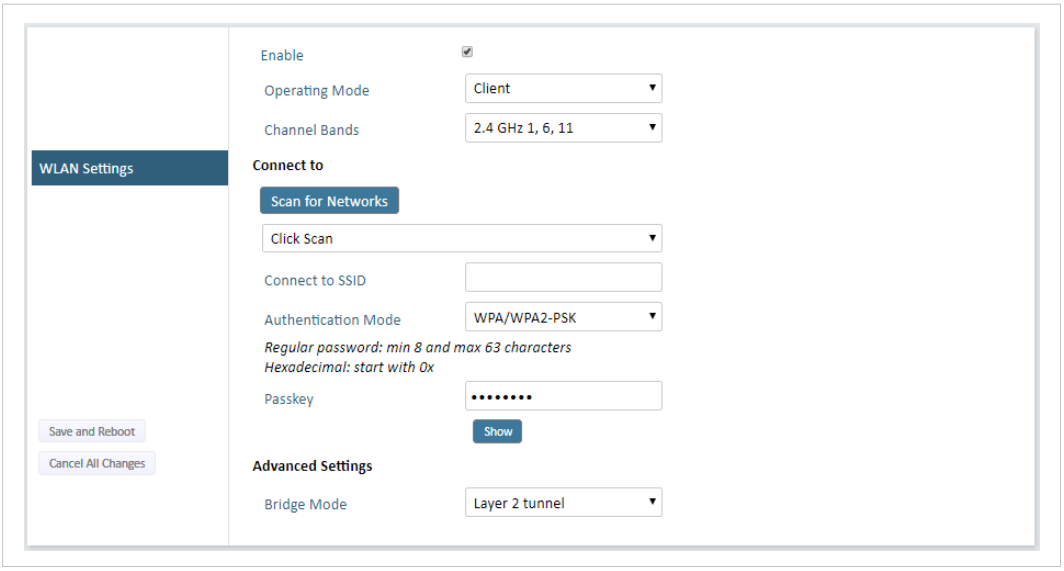


Fig. 10 WLAN Settings - Client

Enable	Enable/disable the WLAN interface.
Operating Mode	Choose operation as WLAN Client or Access Point. If Access Point is selected, additional settings will be available.
Channel Bands	Choose to scan only the 2.4 GHz or 5 GHz channel band, or both (default).

The unit can be configured to scan on both the 2.4 GHz and 5 GHz channel bands but can only communicate on one band at a time.

Scan for Networks	Click to scan the selected frequency band(s) for discoverable WLAN networks. Select a network from the dropdown menu to connect to it.
Connect to SSID	To connect manually to a network, enter its SSID (network name) here. This can be used if the network does not broadcast its SSID.
Authentication Mode	Select the authentication/encryption mode required by the network. **Open** = No encryption or authentication
Passkey	Enter the passkey when using WPA/WPA2-PSK or WEP64/128.
Username, Domain, Passphrase	Authentication details when using LEAP or PEAP (WPA2 Enterprise).

Advanced Settings	
Bridge Mode	**Layer 2 tunnel** = All layer 2 data will be bridged over WLAN. Use when multiple devices on both sides of an Ethernet network bridge must be able to communicate via WLAN (many-to-many). Only works between Anybus Wireless Bolt or Wireless Bridge II devices. **Layer 2 cloned MAC only** = Layer 2 data from only a single MAC address (specified below) will be bridged over WLAN (many-to-one). **Layer 3 IP forward** (default) = IP data from all devices will be bridged over WLAN. This mode must be used when using the DHCP Relay function. When using Layer 3 IP forward in an enterprise network, such as a Cisco Wireless LAN Controller, the connectivity may be reduced. The cause may be: • Multiple devices sharing a single wireless interface is not typically supported without special configuration. • The network cannot enforce a 1-to-1 mapping of IP to MAC addresses and must allow propagation of broadcasted ARP messages over the wireless segment in order to route traffic to the bridged devices. If this for security or performance reasons is not acceptable, a setup with a single Ethernet node connected to the Wireless Bridge is recommended.
Cloned MAC Address	The MAC address to use with **Layer 2 cloned MAC only** (see above).
Cloned IP Address	The IP address to use with **Layer 2 cloned MAC only** (see above).

WLAN Roaming

Anybus Wireless Bolt CAN supports Fast Roaming according to IEEE 802.11r. This enables a WLAN client to roam quicker between WLAN Access Points that have the same SSID and support IEEE 802.11r. Fast Roaming is enabled as default but can be permanently disabled using AT commands.

See the *AT Commands Reference Guide* or the **Help** page in the web interface for more information about how to set up WLAN roaming.

WLAN Channels and World Mode (Client Mode only)

Which channels are available for WLAN communication is restricted by the regulatory domain where the unit is operating. Anybus Wireless Bolt CAN supports regulatory domain detection according to the IEEE 802.11d specification.

The unit is initially set in *World Mode* which enables only the universally allowed channels in the 2.4 GHz and 5 GHz bands (see the table below). World Mode can be disabled and additional channels added using AT commands. The unit will then search for country information during the scan. If the scan indicates that the unit is operating within either the European (ETSI) or North American (FCC) regulatory domains, the additional channels will be enabled. A new scan will be performed every hour to update the regulatory domain.

If no country information or conflicting information is detected, the unit will revert to World Mode. The unit must then be restarted to update the regulatory domain.

See the *AT Commands Reference Guide* or the **Help** page in the web interface for more information about how to use AT commands.

Regulatory domains and WLAN channels

	2.4 GHz	5 GHz
WORLD	1–11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140
ETSI	1–11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
FCC	1–11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140

Notes

- The maximum output power will be reduced on some channels depending on regulatory requirements.
- WLAN communication may take a longer time to establish during startup if World Mode is disabled and additional channels are used.

5.1.5 WLAN Settings - Access Point

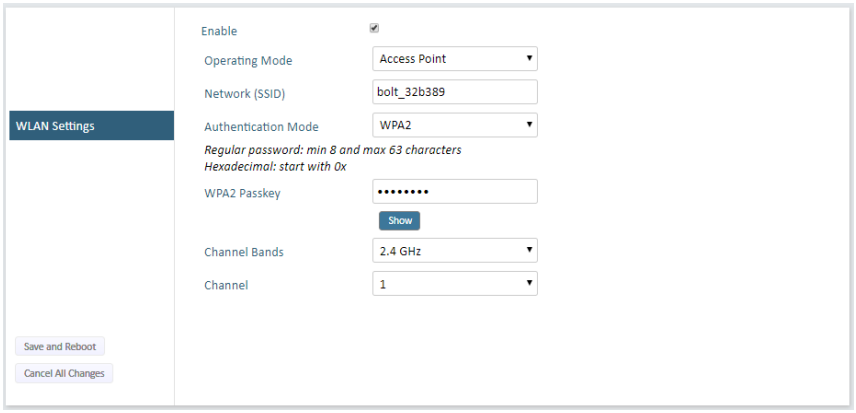


Fig. 11 WLAN Settings - Access Point

The following settings are specific for Access Point mode:

Network (SSID)	Enter an SSID (network name) for the Wireless Bolt CAN. If this entry is left blank, the unit will generate an SSID which includes the last 6 characters of the MAC ID.
Authentication Mode	Select the authentication/encryption mode to use for the access point. **Open** = No encryption or authentication **WPA2** = WPA2 PSK authentication with AES/CCMP encryption
WPA2 Passkey	Enter a string in plain text or hexadecimal format to use for authentication. Regular (plain text) passwords must be between 8 and 63 characters. All characters in the ASCII printable range (32–126) are allowed, except " (double quote) , (comma) and \ (backslash). Hexadecimal passwords must start with `0x` and be **exactly** 64 characters. See also the example passwords below.
Channel Bands, Channel	Select the WLAN channel band and channel to use for the access point. Valid channels are 1 to 11 for the 2.4 GHz band and 36, 40, 44, 48 for the 5 GHz band.

Password examples

For plain text passwords a combination of upper and lower case letters, numbers, and special characters is recommended.

Example of a strong plain text password:
`uS78_xpa&43`

Example of hexadecimal password:
`0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f`

> **!** Do not use the example passwords above in a live environment!

5.1.6 Bluetooth Settings – General

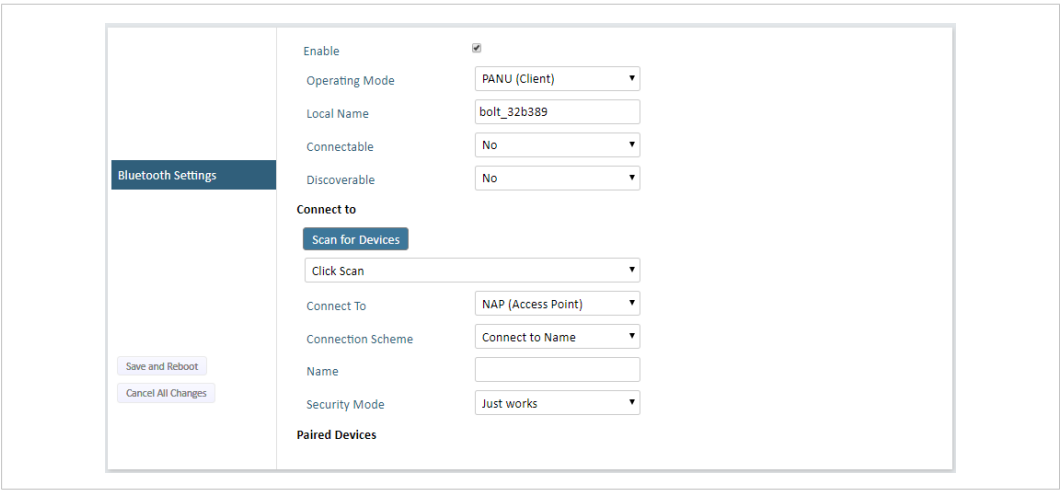


Fig. 12 Bluetooth Settings

Enable	Enable/disable the Bluetooth interface.
Operating Mode	**PANU (Client)** = The unit will operate as a Bluetooth PAN (Personal Area Network) User device. It can connect to another single Bluetooth PANU device or to a Bluetooth Network Access Point. **NAP (Access Point)** = The unit will operate as a Bluetooth Network Access Point. It can connect to up to 7 Bluetooth PANU devices.
Local Name	Identifies the unit to other Bluetooth devices. If left blank, the unit will use a default name including the last 6 characters of the MAC ID.
Connectable	Enable to make the unit accept connections initiated by other Bluetooth devices.
Discoverable	Enable to make the unit visible to other Bluetooth devices.
Security Mode	**Disabled** = No encryption or authentication. **PIN** = Encrypted connection with PIN code security. This mode only works between two units of this type and brand (not with third-party devices). PIN codes must consist of 4 to 6 digits. **Just Works** = Encrypted connection without PIN code.
Paired Devices	Lists the currently connected Bluetooth devices.

5.1.7 Bluetooth Settings – PANU Mode

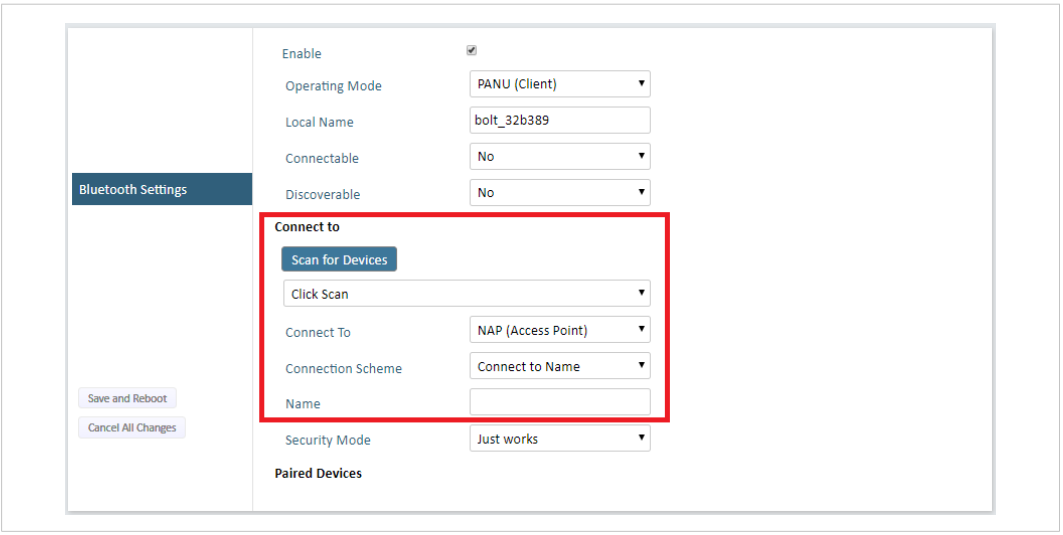


Fig. 13 Bluetooth Settings – PANU

PANU mode only	
Scan for Devices	Scans the network for discoverable Bluetooth devices. To connect to a device, select it from the dropdown menu when the scan has completed.
Connect To	Used when connecting manually to a NAP or PANU device.
Connection Scheme	Choose whether to select a Bluetooth device by MAC address (default) or Name when connecting manually. Connecting to MAC will lock the connection to a specific hardware while connecting to Name allows for more flexibility.
MAC/Name	MAC address or Name of the Bluetooth device to connect to.

5.1.8 Bluetooth Settings – NAP Mode

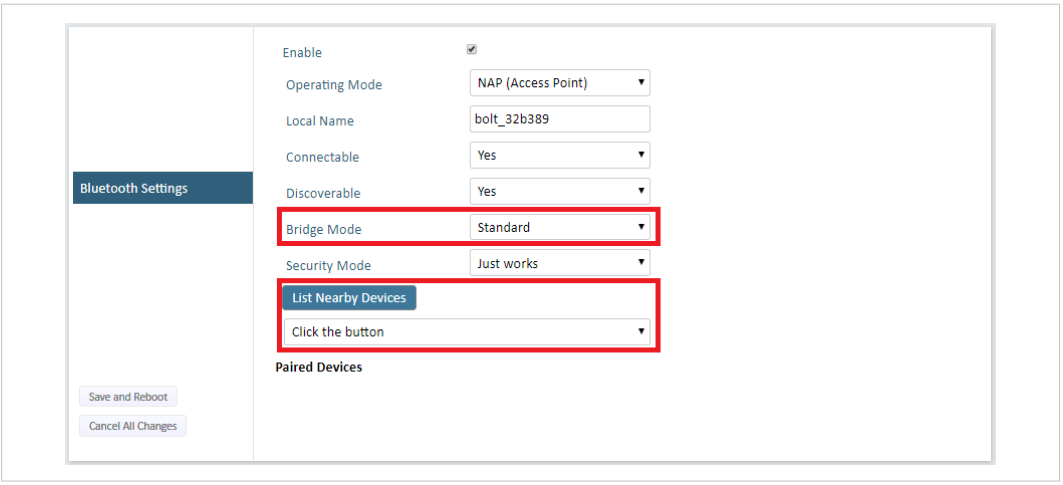


Fig. 14 Bluetooth settings – NAP

NAP mode only	
Bridge Mode	**Standard** = Default mode. **Layer 3 IP forward** = IP data will be bridged over Bluetooth. This mode must be used when connecting to an Android device over Bluetooth. The network must have an active DHCP server.
List Nearby Devices	Scans the network and lists discoverable Bluetooth devices. Pairing cannot be initiated in NAP mode.

5.1.9 Bluetooth LE Settings

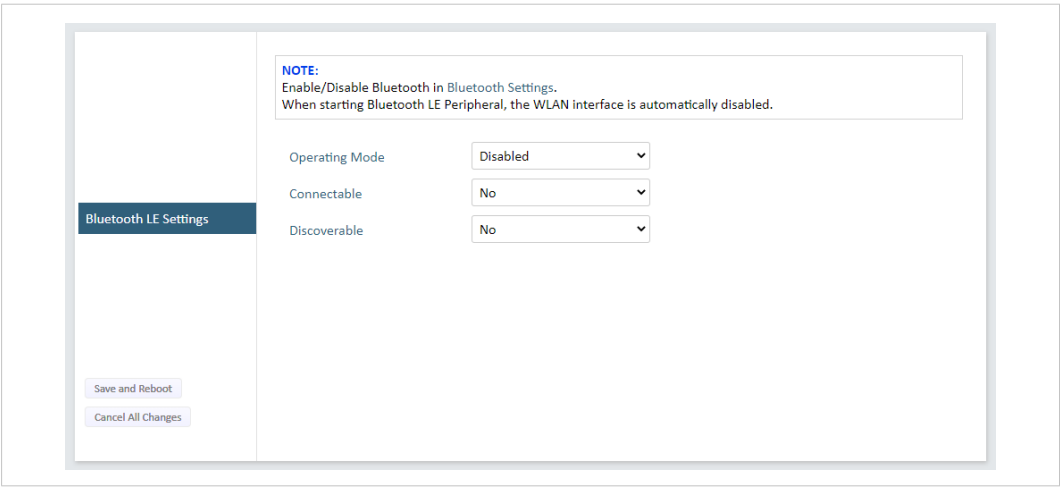


Fig. 15 Bluetooth LE settings

Bluetooth LE Settings	
Operating Mode	**Disabled** = Bluetooth LE disabled (default) **Central** = Bluetooth LE Central operating mode enabled **Peripheral** = Bluetooth LE Peripheral operating mode enabled. This requires that the WLAN interface is disabled.
Connectable	**No** = Connectable is disabled (default) **Yes** = Enables the Wireless Bolt CAN to search, connect and transfer data with another Bluetooth-capable device.
Discoverable	**No** = Discoverable is disabled (default) **Yes** = Enables the Wireless Bolt CAN to pair with another Bluetooth-capable device.

Please refer to the *AT Commands Reference Guide* or select **Help** in the main menu for more information about using Bluetooth LE.

*Bluetooth must be enabled on the **Bluetooth Settings** page to use Bluetooth LE.*

5.1.10 CAN Settings

Setting Up CAN Communication

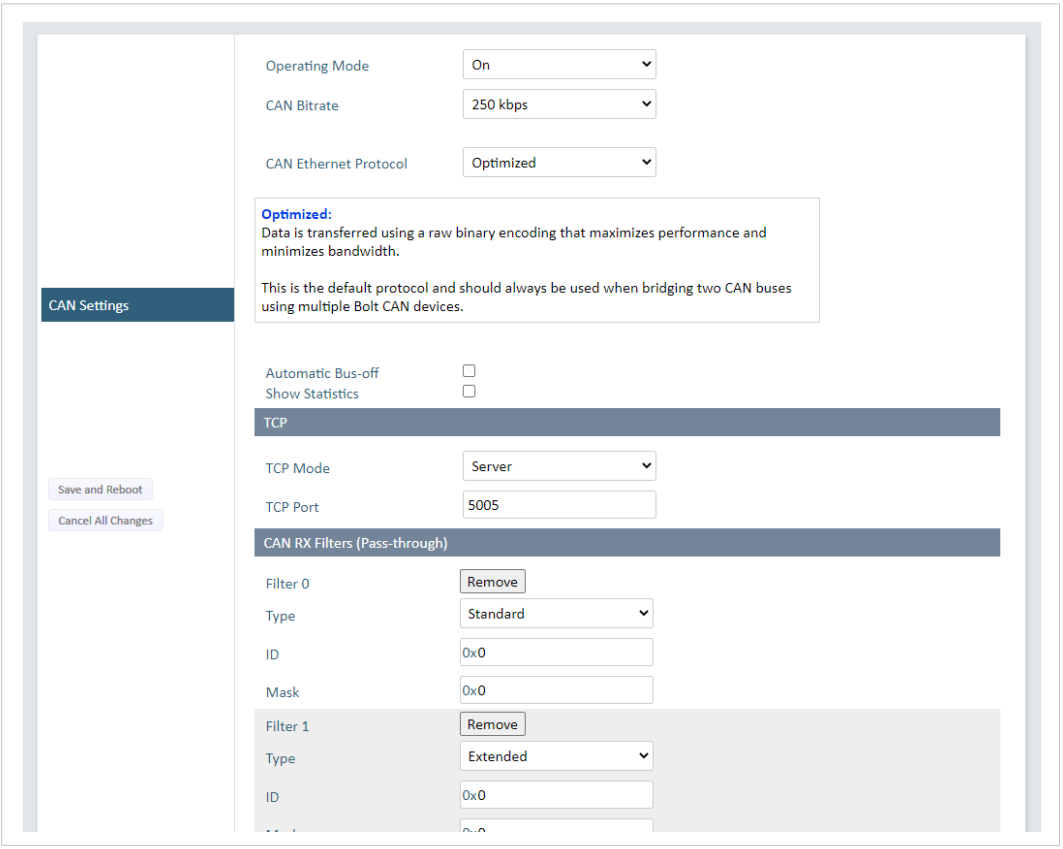
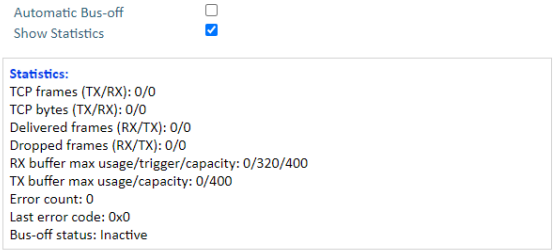


Fig. 16

CAN Settings	
Operating Mode	Select Operation Mode **On** (Default) or **Off**.
CAN Bitrate	Select a CAN Bitrate: **10 kbps**, **20 kbps**, **50 kbps**, **100 kbps**, **125 kbps**, **250 kbps** (Default), **500 kbps**, **1000 kbps** or **Custom**. For information about Custom bitrate, refer to *Calculate Custom CAN Bitrate, p. 26*.
CAN Ethernet Protocol	**Optimized** (Default): Use this protocol when bridging two CAN buses using multiple Bolt CAN devices. Data is transferred using a raw binary encoding that maximizes the performance and minimizes the bandwidth. **SLCAN**: Use the ASCII based SLCAN protocol to bridge CAN traffic to a custom endpoint. CAN frames can be sent and received via a TCP/IP socket using basic commands. The command starts with a letter followed by a number of hexadecimal digits and ends with a carriage return (character code 0x0D). Refer to *SLCAN Protocol, p. 27*. **Simple**: In this mode the raw bytes of any incoming TCP payload will be transparently copied into the data segment of one or multiple CAN frames. The frame ID can be specified in the CAN Simple ID field. Only the data segment of any incoming CAN frames will be transparently copied to the outgoing TCP stream, with no markers indicating where contents of one frame ends and the next one begins. Incoming frames will still be subject to the CAN RX filter. Refer to *Simple Protocol, p. 29*.
CAN Simple ID	Active when the Simple CAN Ethernet Protocol is selected. Specify the frame ID to use.
Extended Frame	Active when the Simple CAN Ethernet Protocol is selected. Extended Frame defines if the CAN Simple ID should be standard or extended. By default, Standard Frame is used. Select the checkbox to enable Extended Frame.
Automatic Bus-off	By default, Automatic Bus-off is off, the checkbox is unselected.

CAN Settings (continued)

	When a Bus-off condition is detected, the Wireless Bolt CAN stays in Bus-off until it is restarted; via a power-cycle or via a remote reboot from the built-in web interface. In the Wireless Bolt CAN built-in web interface, an error banner appears prompting you to reboot the system.  To enable Automatic Bus-off, select the checkbox. When Automatic Bus-off is enabled, the recovering sequence automatically starts when the Wireless Bolt CAN enters the Bus-off state.
Show Statistics	When Show Statistics is selected, current statistics from the CAN bus are displayed below the checkbox. The values are updated every two seconds. Examples of statistics displayed: The number of sent/received CAN frames, buffer usage and error information. 
TCP Mode	Select a TCP Mode from the dropdown menu: **Client**: The Wireless Bolt CAN acts as a client and establishes a connection to the TCP server. **Server**: The Wireless Bolt CAN acts as a server and listens for incoming connections from the TCP client.
TCP Port	Enter the TCP Port number. Default port: 5005
TCP Server IP	When TCP Mode Client is selected, enter the TCP Server IP address.
CAN RX Filters	With CAN RX filters, you can configure Bolt CAN to forward only a subset of the messages. Example: CAN RX filters can be used to reduce bandwidth requirements, avoid sending sensitive information or minimize sending unnecessary information. You can add up to 28 CAN RX Filters. **Type**: Select **Standard** (Identifier length: 11 bits) or **Extended Frame** (Identifier length: 29 bits). **ID**: Enter the ID for the CAN frames that the CAN RX Filter should receive. **Mask**: The mask specifies which bits of the incoming frame ID match the ID configured in the filter. Example: A filter with ID 0x123 and mask 0x00F will match an incoming frame with ID 0x123 or 0x333, but not with ID 0x120. **Factory Reset** When the Wireless Bolt CAN is factory reset, two filters will be defined; one for Standard frames and one for Extended frames. Both filters with mask set to the value 0x0. This will result in all frames passing through the filter.

Calculate Custom CAN Bitrate

When none of the pre-defined bitrates match the connected CAN bus, you can use the **Custom** CAN bitrate and calculate a bitrate.

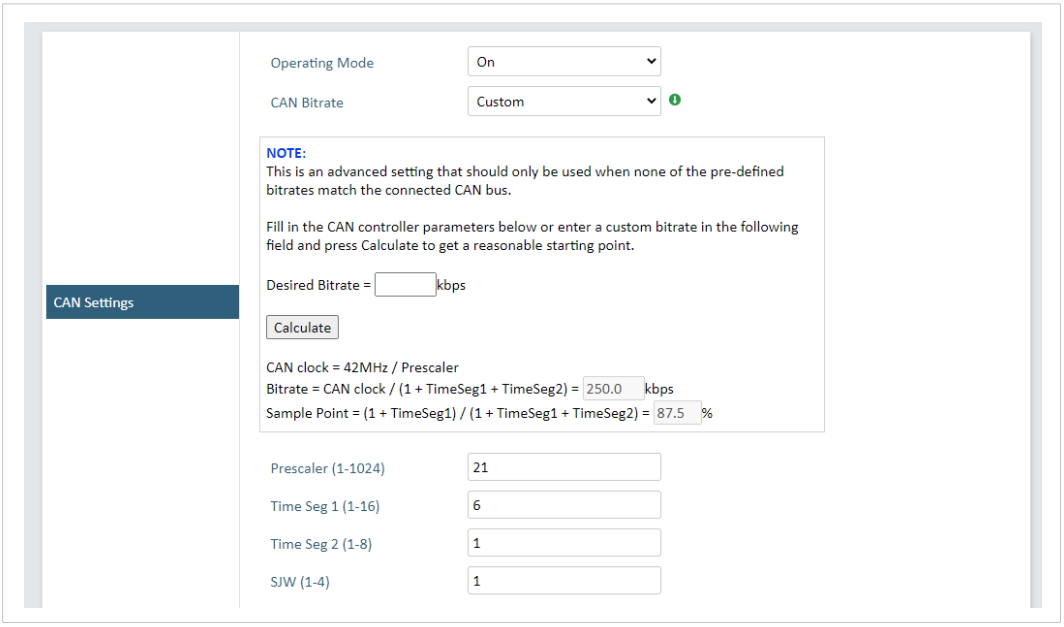


Fig. 17

To calculate a bitrate

1. Select **Custom** in the CAN Bitrate dropdown menu.
2. Enter the **Desired Bitrate**.
3. Press **Calculate**.

   → The following values are calculated:

Prescaler (1-1024)	The CAN clock prescaler value. A numerical value from 1 to 1024.
Time Seg 1 (1-16)	Time Segment 1 A numerical value from 1 to 16. The number of quanta before the sampling point.
Time Seg 2 (1-8)	Time Segment 2 A numerical value from 1 to 8. The number of quanta after the sampling point.
SJW (1-4)	SJW (Synchronization Jump Width) A numerical value from 1 to 4. The maximum phase error that can be corrected by one synchronization.

4. If needed, you can edit the calculated values.

CAN Ethernet Protocols

SLCAN Protocol

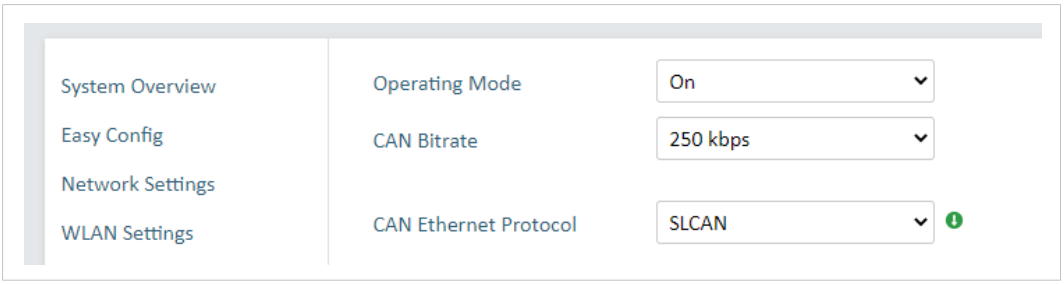


Fig. 18

SLCAN is an ASCII-based protocol.

Each frame follows the following format: [type][id][length][data]\r

[type]	Type of CAN frame:	
	t	Standard frame
	T	Extended frame
	r	Standard remote frame
	R	Extended remote frame
[id]	CAN frame identifier. Length of field depends on frame type. Standard frame: 3 hex digits (000 to 7FF) Extended frame: 8 hex digits (00000000 to 1FFFFFFF)	
[length]	A digit (0 to 8) specifying the length of the data field (DLC in CAN terminology).	
[data]	One pair of (case-insensitive) hex digits for every data byte.	
\r	A carriage return character (ASCII code 13 or 0x0D).	

Frame examples

- t1234aabbccdd\r

  Standard frame with identifier 0x123 and data 0xAA 0xBB 0xCC 0xDD.

- R02468ace8\r

  Extended remote frame with identifier 0x02468ACE and length set to 8.

CAN Ethernet Protocol SLCAN example

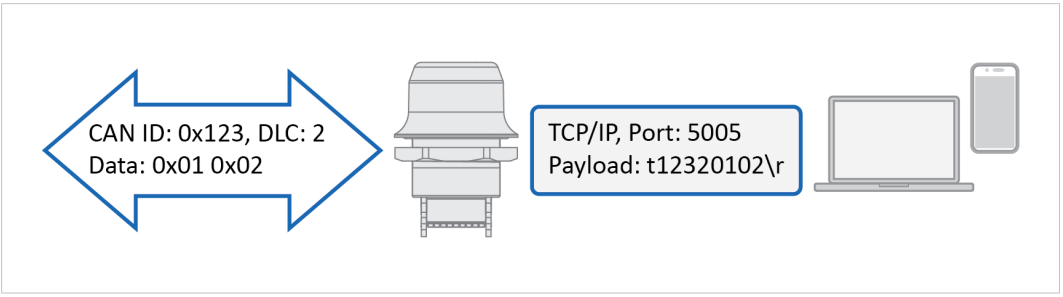


Fig. 19

Python-can library

The python-can library supports the SLCAN protocol.

The python-can library provides a set of utilities for sending and receiving messages on a CAN bus.

For information about the python-can library, refer to https://python-can.readthedocs.io.

Example 1: SLCAN using the python-can library

```
import can

slcan = can.interface.Bus(
    bustype = 'slcan',
    channel = 'socket://192.168.0.99:5005')

msg = can.Message(
    arbitration_id = 0x123,
    is_extended_id = False,
    data = [0x01, 0x02, 0x03, 0x04])
slcan.send(msg)

rmsg = slcan.recv(timeout = 5)
print("Received CAN message 0x{:X} with data {}".format(
    rmsg.arbitration_id,
    rmsg.data))

slcan.shutdown()
```

Simple Protocol

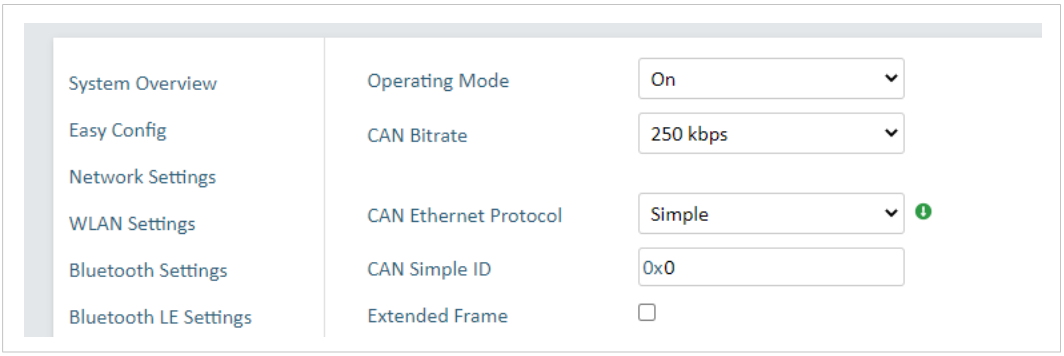


Fig. 20

When using the simple protocol each incoming TCP packet payload will be transparently copied into the data portion of one or more CAN frames.

The setting **CAN Simple ID** is used to configure the identifier used for all sent frames.

As CAN frames are received only their data bytes will be transparently copied into the outgoing TCP stream.

*If the **CAN RX Filters** are configured to accept CAN frames with different identifiers, it will not be possible to determine what CAN frame the payload originated from.*

CAN Ethernet Protocol Simple example

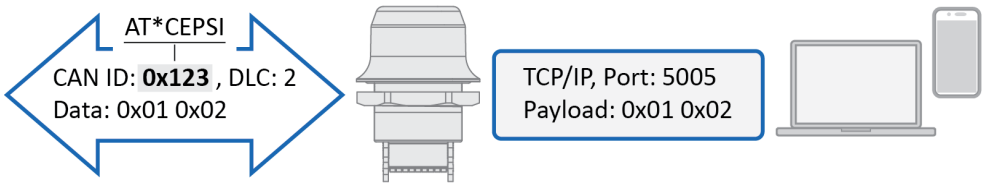


Fig. 21

5.1.11 Firmware Update

To update the firmware in the unit, click on **Browse** to select a downloaded firmware file, then click on **Send** to send it to the unit.

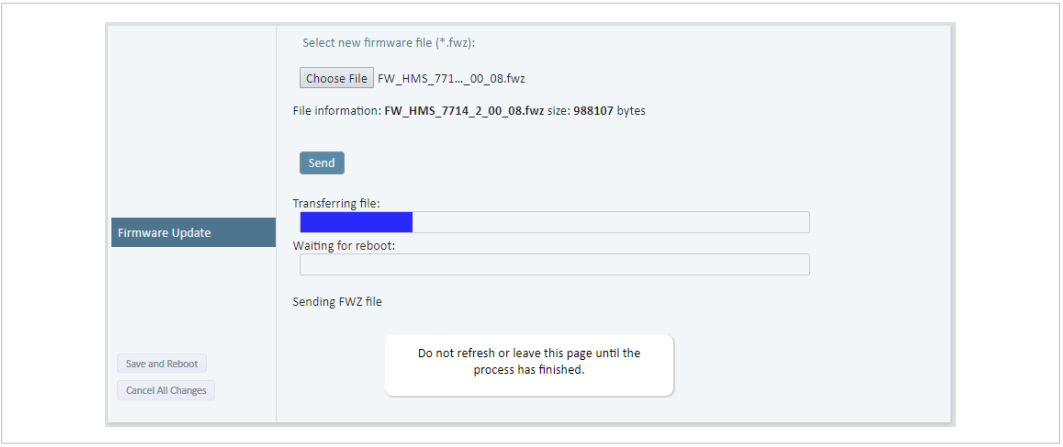


Fig. 22 Firmware update in progress

Both progress bars will turn green when the firmware update has been completed. The unit will then reboot automatically.

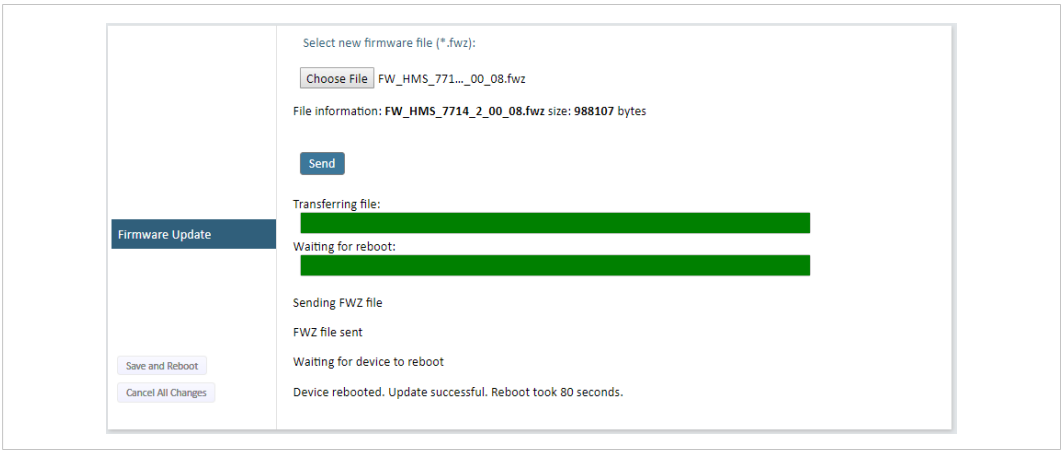


Fig. 23 Firmware update completed

Updating the firmware will not change the configuration settings.

5.1.12 AT Commands

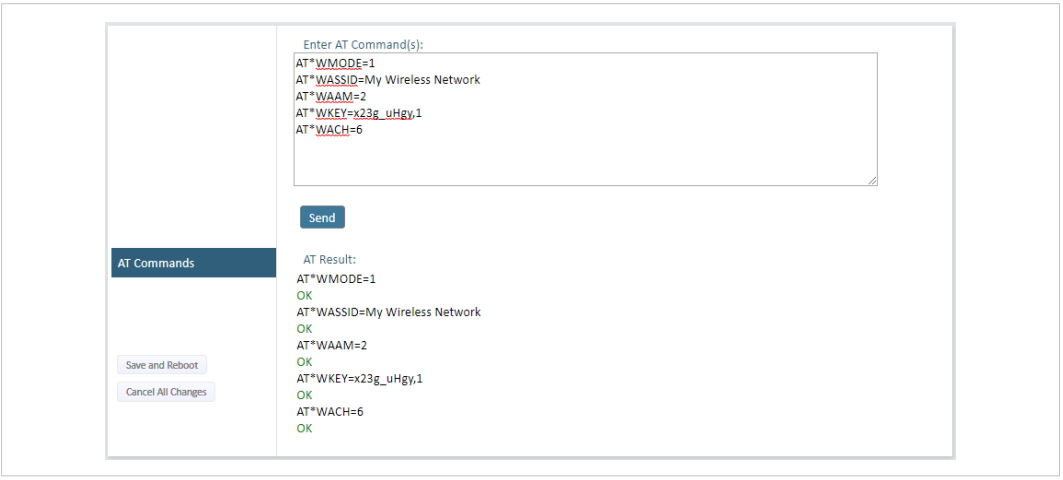


Fig. 24 AT Commands

AT commands can be used for setting advanced parameters that are not accessible in the web interface, to read out parameters in text format, and for batch configuration using command scripts.

Enter or paste the commands into the text box, then click on **Send**. The result codes will be displayed below the text box.

Click on **Help** for a complete list of supported AT commands.

5.1.13 System Settings

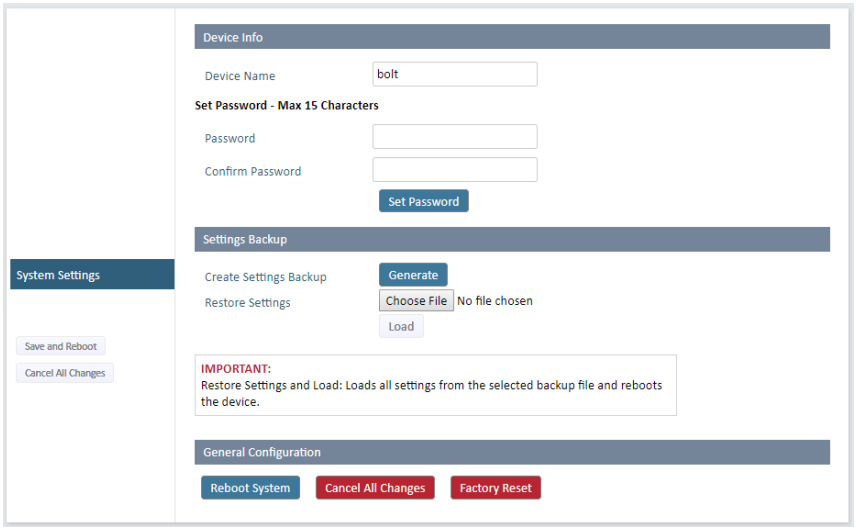


Fig. 25 System Settings

Device Info	
Device Name	Enter a descriptive name for the unit.
Password	Enter a password for accessing the web interface.
Reboot System	Reboots the system without applying changes.
Cancel All Changes	Restores all parameters in the web interface to the currently active values.
Factory Reset	Resets the unit to the factory default settings and reboots.

> **!** Setting a secure password for the unit is strongly recommended.

Settings Backup	
Create Settings Backup	Click on **Generate** to save the current configuration to a file on your computer.
Restore Settings	Click on **Choose file** and select a previously saved configuration, then click on **Load**. The settings in the saved configuration will be applied and the unit will reboot.

General Configuration	
Reboot System	Reboots the system without applying changes.
Cancel All Changes	Restores all parameters in the web interface to the currently active values.
Factory Reset	Resets the unit to the factory default settings and reboots.

5.2 Use Cases

5.2.1 Wireless Bolt CAN Point-to-Point Installation

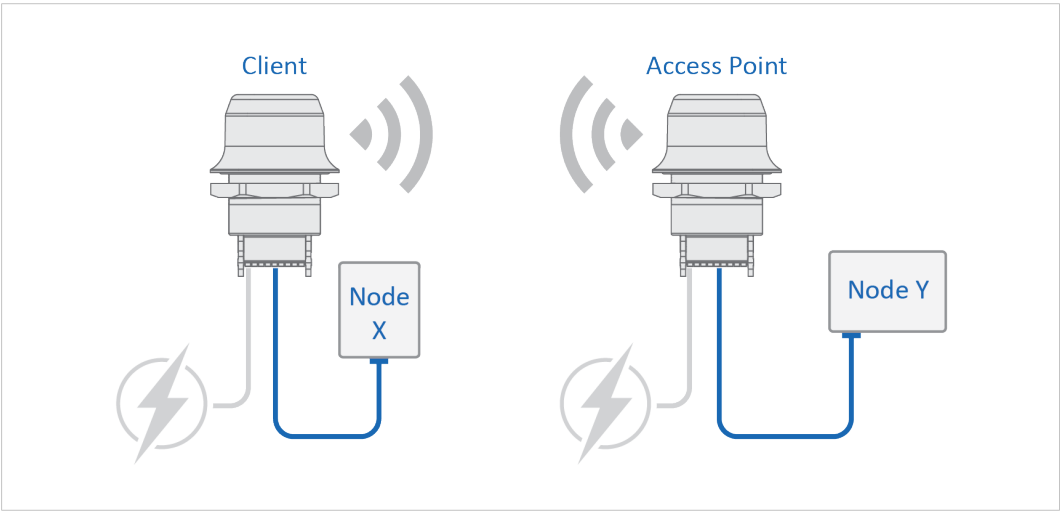


Fig. 26

CAN cable replacement is enabled by using two pieces of Wireless Bolt CAN which creates a wireless bridge for the CAN communication.

5.2.2 Installing Multiple Wireless Bolt CAN

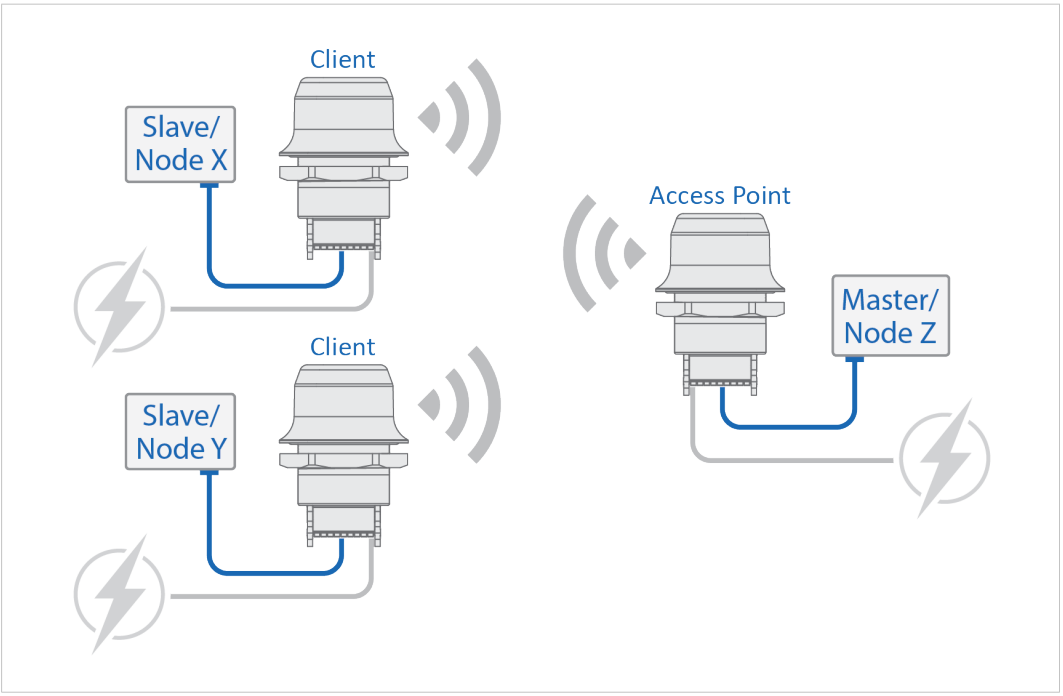


Fig. 27

When the protocol is Master/Slave oriented and more than one Wireless Bolt CAN will be installed in the bridge, the following applies.

Configure the Wireless Bolt CAN connected to the:

- *Node Z* as the *Access Point (AP)*.
- *Node (X, Y, etc.)* as a *Client*.

5.2.3 Wireless Bolt CAN TCP/IP Socket Protocol Description

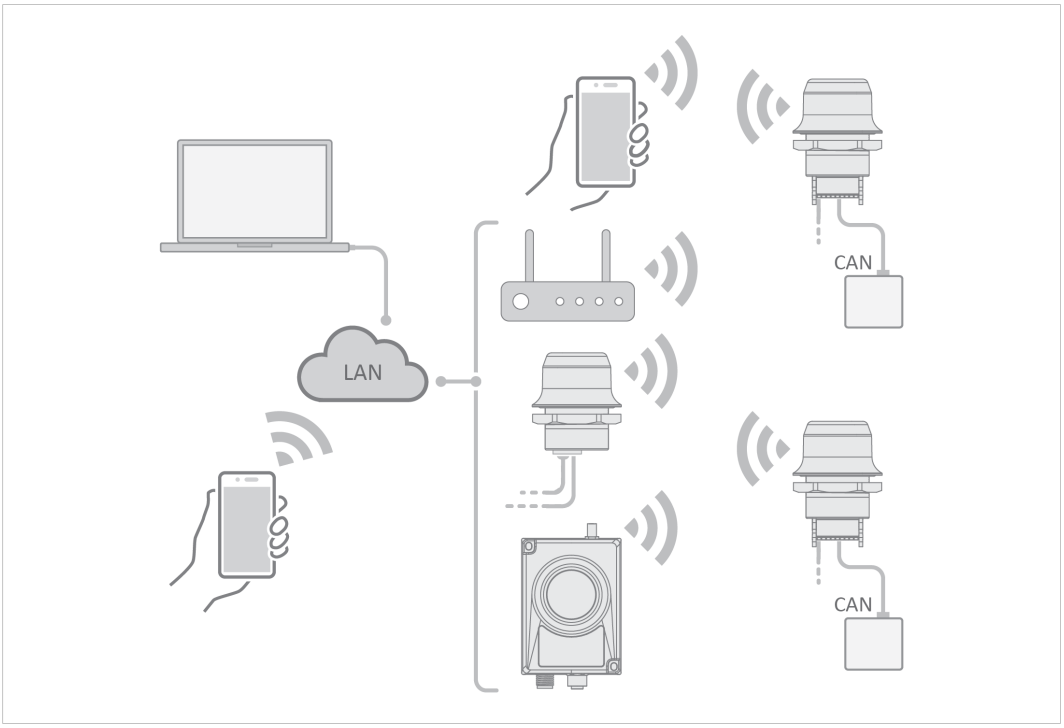


Fig. 28

The Wireless Bolt CAN may communicate with raw TCP/IP traffic and bridge the data to CAN on the CAN port.

The Wireless Bolt CAN act as one of the endpoints in the TCP/IP communication. The other endpoint can be a PC program, tablet or phone application, PLC, controller or similar.

For information about the available CAN Ethernet protocols and how to set up CAN communication, refer to *CAN Ethernet Protocols, p. 27* and *Setting Up CAN Communication, p. 24*.

Procedure

To set up TCP/IP communication:

1. Establish IP connectivity between the devices using either WLAN or Bluetooth (PAN profile).
2. Do one of the following:
   - Open a TCP/IP socket towards the Wireless Bolt CAN.

     Use the configured TCP port number (default 5005).

     Up to 7 active sockets are supported simultaneously.
   - Configure the Wireless Bolt CAN as a TCP client to connect to a specific IP.

Result

CAN frames can now be sent via the TCP socket to the Wireless Bolt CAN and forwarded to the CAN bus.

Incoming frames from the CAN bus are forwarded to all open TCP sockets.

The format of the CAN frames, in the TCP stream payload, depends on how the CAN Ethernet Protocol settings are configured.

5.3 Set Up a Wireless Infrastructure

Connect two or more Wireless Bolt CAN units via WLAN or Bluetooth using Easy Config.

5.3.1 Connecting the Devices

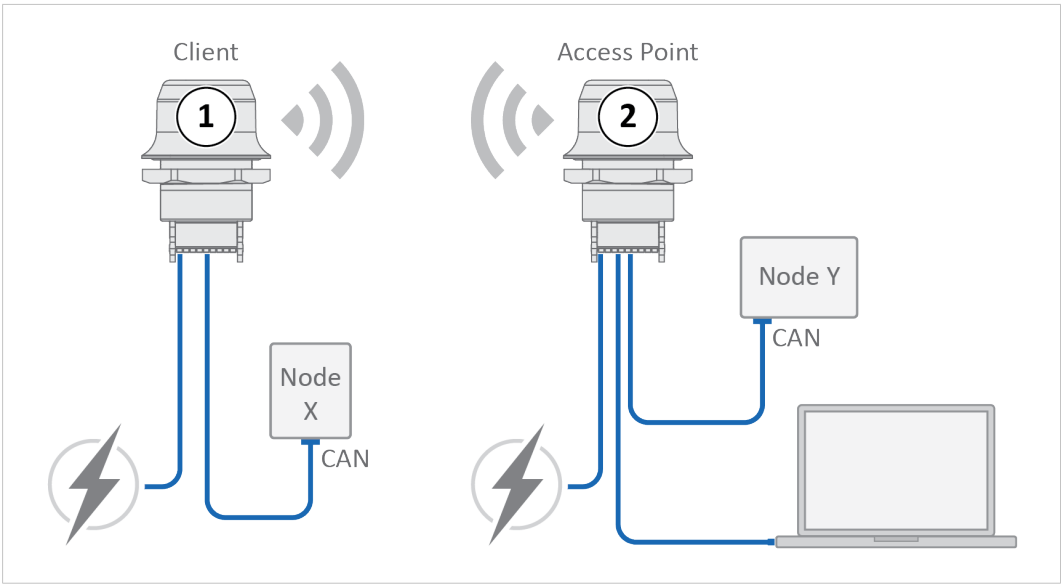


Fig. 29 CAN bridge example

1. Connect *Client unit 1* to a CAN device.
2. Connect *Access Point unit 2* to the master device.
3. Connect *Access Point unit 2* to your PC, with an Ethernet cable.
4. Connect *Access Point unit 2* to power.

5.3.2 Activate Easy Config

1. Navigate to the web interface of *Access Point unit 2*.

   The default address to *Access Point unit 2* is **192.168.0.99**.

2. Activate one of the following Easy Config Modes:

   – **Easy Config Mode 1** for Bluetooth PANU-PANU. Used for setting up point-to-point communication.

   – **Easy Config Mode 5** for WLAN

   – **Easy Config Mode 6** for Bluetooth

3. Connect *Client unit 1* to power.

→ *Client unit 1* starts up in **Easy Config Mode 4** and is open for automatic configuration during 120 seconds.

→ *Access Point unit 2* will discover and configure *Client unit 1* as a *Client* and configure itself as an *Access Point*.

→ *Client unit 1* will be assigned the first free IP address in the same Ethernet subnet as *Access Point unit 2*.

The default address to the first *Client unit* is **192.168.0.100**.

→ If no connection is established during Easy Config Mode:

– Ensure that *Client unit 1* is disconnected from Ethernet.

– Disconnect *Client unit 1* from power and repeat Activate Easy Config step 5 and 6.

5.3.3 Adding More Wireless Bolt CAN Clients

When using **Easy Config Mode 1**, continue with CAN Configuration.

When using **Easy Config Mode 5** or **Easy Config Mode 6**, up to 6 additional Wireless Bolt CAN Clients can be added to the CAN bridge.

1. To add more *Client units*, repeat Connecting the Devices step 1 and the Activate Easy Config steps.

→ Each new *Client unit* will be assigned the next free IP address in the current Ethernet subnet.

5.3.4 CAN Configuration

From the PC connected to *Access Point unit 2*:

1. Navigate to the web interface of each Wireless Bolt CAN unit.
2. Select the **CAN Settings** tab.
3. Configure the CAN port settings:

CAN Settings	
Operating Mode	Select Operation Mode **On** (Default) or **Off**.
CAN Bitrate	Select a CAN Bitrate. For information about Custom bitrate, refer to *Calculate Custom CAN Bitrate, p. 26*.
CAN Ethernet Protocol	**Optimized** (Default): Use this protocol when bridging two CAN buses using multiple Bolt CAN devices. Data is transferred using a raw binary encoding that maximizes the performance and minimizes the bandwidth. **SLCAN**: Use the ASCII based SLCAN protocol to bridge CAN traffic to a custom endpoint. CAN frames can be sent and received via a TCP/IP socket using basic commands. The command starts with a letter followed by a number of hexadecimal digits and ends with a carriage return (character code 0x0D). **Simple**: In this mode the raw bytes of any incoming TCP payload will be transparently copied into the data segment of one or multiple CAN frames. The frame ID can be specified in the CAN Simple ID field. Only the data segment of any incoming CAN frames will be transparently copied to the outgoing TCP stream, with no markers indicating where contents of one frame ends and the next one begins. Incoming frames will still be subject to the CAN RX filter.
CAN Simple ID	Active when the Simple CAN Ethernet Protocol is selected. Specify the frame ID to use.
Extended Frame	Active when the Simple CAN Ethernet Protocol is selected. Extended Frame defines if the CAN Simple ID should be standard or extended. By default, Standard Frame is used. Select the checkbox to enable Extended Frame.
Automatic Bus-off	By default, Automatic Bus-off is off, the checkbox is unselected. To enable Automatic Bus-off, select the checkbox. When Automatic Bus-off is enabled, the recovering sequence automatically starts when the Wireless Bolt CAN has entered Bus-off state.
Show Statistics	When Show Statistics is selected, current statistics from the CAN bus are displayed below the checkbox. The values are updated every two seconds. Examples of statistics displayed: The number of sent/received CAN frames, buffer usage and error information.
TCP Mode	Select a TCP Mode from the dropdown menu: **Client**: The Wireless Bolt CAN acts as a client and establishes a connection to the TCP server. **Server**: The Wireless Bolt CAN acts as a server and listens for incoming connections from the TCP client.
TCP Port	Enter the TCP Port number. Default port: 5005
TCP Server IP	When TCP Mode Client is selected, enter the TCP Server IP address.
CAN RX Filters	With CAN RX filters, you can configure Bolt CAN to forward only a subset of the messages. Example: CAN RX filters can be used to reduce bandwidth requirements, avoid sending sensitive information or minimize sending unnecessary information. You can add up to 28 CAN RX Filters. **Type**: Select **Standard** (Identifier length: 11 bits) or **Extended Frame** (Identifier length: 29 bits). **ID**: Enter the ID for the CAN frames that the CAN RX Filter should receive. **Mask**: The mask specifies which bits of the incoming frame ID match the ID configured in the filter. Example: A filter with ID 0x123 and mask 0x00F will match an incoming frame with ID 0x123 or 0x333, but not with ID 0x120.

5.3.5 CAN Installation

1. Connect each Wireless Bolt CAN unit to a device or machine equipped with a CAN port.

   For more information, refer to *Connector, p. 7* and *Cabling, p. 8*.

5.4 Factory Restore

Any one of these actions will restore the factory default settings:

- Clicking on **Factory Restore** on the **System Settings** page
- Executing **Easy Config Mode 2**
- Issuing the AT command **AT&F** and then restarting the unit
- Holding pressed for >10 seconds and then releasing it

Default Network Settings	
IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99
Internal DHCP Server	Disabled
DHCP Interfaces	All

Default Bluetooth Settings	
Operating Mode	PANU (Client)
Local Name	[generated from MAC address]
Connectable	No
Discoverable	No
Security Mode	Just works
Bluetooth LE	Operating Mode: Disabled Connectable: No Discoverable: No

Default CAN Settings	
Operating Mode	On
Bitrate	250 kbps
Ethernet protocol	Optimized
Automatic Bus-off	Off
TCP Mode	Server
TCP Port	5005
RX Filter	Standard, ID 0x0, Mask 0x0 + Extended, ID 0x0, Mask 0x0

6 Technical Data

For complete technical specifications and regulatory compliance information please visit www.anybus.com/support.

6.1 Technical Specifications

Order code	AWB2020	AWB2021
Color	Black	White top and black base
Connector	Included plug connector (2x9p; 3.5mm, Phoenix DFMC 1.5/9-ST-3.5, push-in spring connection).	
Range	Up to 100 meters free line of sight	
Antenna	One internal antenna. Dual-band 2,4GHz and 5GHz.	
Temperature compatibility	Operating: Shadow black and white: -40 to +65 °C Direct sunlight: Black -40 to +45 °C, White -40 to +65 °C Storage temperature: -40 to +85 °C	
Weight	81 g	
Housing material	Top: Valox 357X(f1) PBT/PC. Suitable for outdoor use with respect to exposure to ultraviolet light, water exposure and immersion in accordance with UL 746C. Bottom: Celanex: XFR 6840 GF15. PBT glass reinforced plastic.	
IP protection class	IP66, IP67 and UL Type 4X for top (outside the host), IP21 for bottom (inside the host).	
Dimensions	Diameter: 68 mm. Height: 75 mm (95 mm including connector). Outside height: 41 mm.	
Mounting	M50 screw and nut (50.5 mm hole needed).	
Power	9-30 VDC (-5% +20%), Cranking 12V (ISO 7637-2:2011 pulse 4). Reverse polarity protection. (Consumption: 0.7W idle, 1.7W max.)	
Configuration	Three different methods: 1. Accessing the built-in web pages in the product 2. Sending AT-commands via Telnet/Raw TCP 3. Using Easy Config modes.	
Vibration compatibility	Sinusodial vibration test according to IEC 60068-2-6:2007 and with extra severities; Number of axes: 3 mutually perpendicular (X:Y:Z), Duration: 10 sweep cycles in each axes, Velocity: 1 oct/min, Mode: in operation, Frequency: 5-500 Hz, Displacement ±3.5 mm, Acceleration: 2g. Shock test according to IEC 60068-2-27:2008 and with extra severities; Wave shape: half sine, Number of shocks: ±3 in each axes, Mode: In operation, Axes ± X,Y,Z, Acceleration: 30 g, Duration: 11 ms.	
Humidity compatibility	EN 600068-2-78: Damp heat, +40°C, 93% humidity for 4 days.	
Digital input	Usage: To control roaming between Bluetooth access points (NAP)	
Wired interface	CAN 2.0A/B (11/29 bit identifier). CAN Bitrate 10 kbps to 1000 kbps freely selectable. Up to 28 freely customizable CAN receive pass-through filters. Advanced settings for Prescaler, Time Seg 1+2, SJW. Transparent transfer of any CAN based protocol including e.g. J1939 and CANopen. Ethernet: 10/100BASE-T with automatic MDI/MDIX auto cross-over detection. For configuration only.	
Wireless LAN	**Wireless standards:** WLAN 802.11 a, b, g, n, d, r (fast roaming). **Operation modes:** Access point or Client **WiFi channels**: 2.4 GHz, channel 1-11 + 12-13 depending on regulatory domain scan. 5 GHz Access Point: 36-48 (U-NII-1), 5 GHz Client: 100-116 + 132-140 and 120-128 depending on regulatory domain scan. (U-NII-1, U-NII-2, U-NII-2e). **RF output power**: 13.75 dBm **Max number of slaves for access point:** 7 **Power consumption:** 54mA@24VDC **Net data throughput**: 20 Mbps. Link speed: max 65 Mbps (802.11n SISO) **Security:** WEP 64/128, WPA, WPA-PSK and WPA2, TKIP and AES/CCMP, LEAP, PEAP including MS-CHAP.	
Classic Bluetooth	**Wireless standards (profiles):** PANU & NAP **Operation modes:** Access point or Client **RF output power:** 9.75 dBm **Max number of slaves for access point:** 7 **Power consumption:** 36 mA@24VDC **Net data throughput**: ~1 Mbps **Bluetooth version support:** Classic Bluetooth v2.1 **Security:** Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved	

A CAN Electrical Connection

A.1 CAN Termination

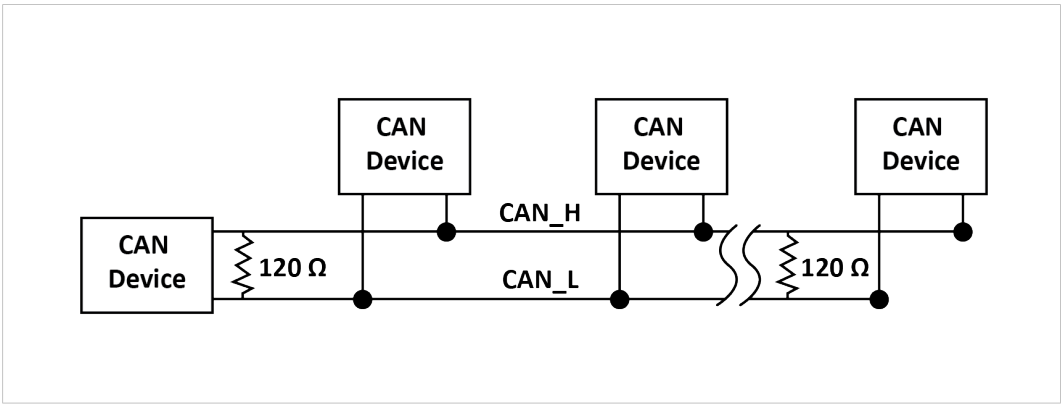


Fig. 30 CAN Termination

B Wireless Technology Basics

Wireless technology is based on the propagation and reception of electromagnetic waves. These waves respond in different ways in terms of propagation, dispersion, diffraction and reflection depending on their frequency and the medium in which they are travelling.

To enable communication there should optimally be an unobstructed line of sight between the antennas of the devices. However, the so called *Fresnel Zones* should also be kept clear from obstacles, as radio waves reflected from objects within these zones may reach the receiver out of phase, reducing the strength of the original signal (also known as phase cancelling).

Fresnel zones can be thought of as ellipsoid three-dimensional shapes between two wireless devices. The size and shape of the zones depend on the distance between the devices and on the signal wave length. As a rule of thumb, at least 60 % of the first (innermost) Fresnel zone must be free of obstacles to maintain good reception.

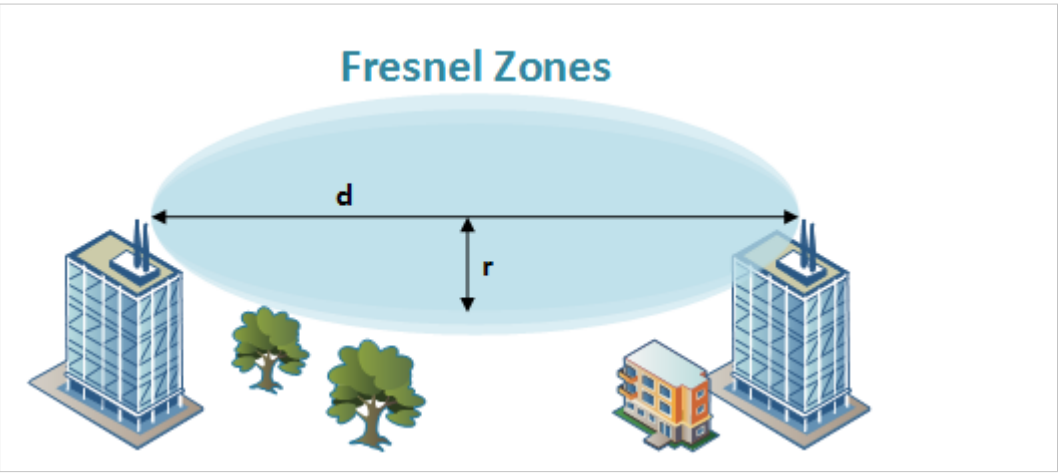


Fig. 31 Fresnel zones

Area to keep clear of obstacles (first Fresnel zone)		
Distance (d)	**Fresnel zone radius (r)**	
	2.4 GHz (WLAN or Bluetooth)	**5 GHz (WLAN)**
100 m	1.7 m	1.2 m
200 m	2.5 m	1.7 m
300 m	3.0 m	2.1 m
400 m	3.5 m	2.4 m

The wireless signal may be adequate even if there are obstacles within the Fresnel zones, as it always depends on the number and size of the obstacles and where they are located. This is especially true indoors, where reflections on metal objects may actually help the propagation of radio waves. To reduce interference and phase cancelling, the transmission power of the unit may in some cases have to be reduced to limit the range.

It is therefore recommended to use a wireless signal analysis tool for determining the optimal placement and configuration of a wireless device.

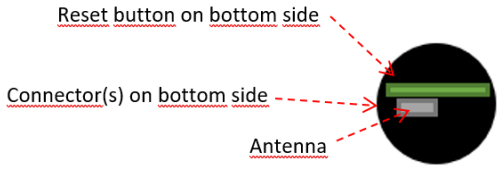
C Radio Antenna Patterns

This section presents information about the radio antenna patterns for the Anybus Wireless Bolt.

The diagram scale shows relative RSSI values, where the outer ring represents maximum radio power and is labelled 0 dB. The inner rings represent the increasing attenuation in dB measured in different angles around the Bolt, while maintaining the same distance.

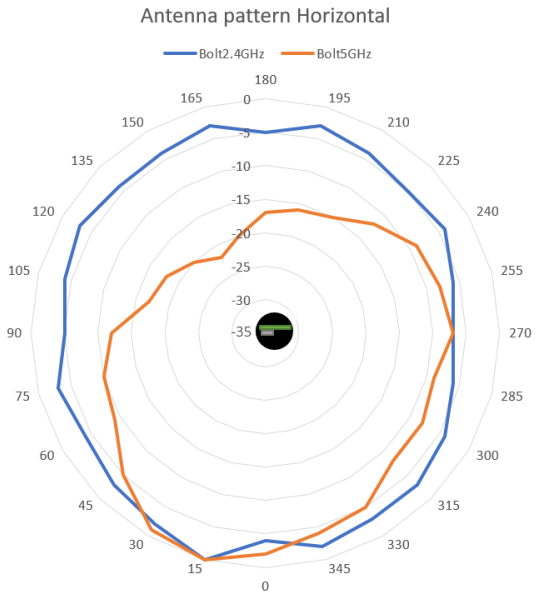
C.1 Azimuth (Horizontal) View

This diagram shows the horizontal antenna pattern when looking at the Bolt from above, i.e. looking at the top logo from above.



(Bolt viewed from above, looking at the top logo)

Diagram analysis: the diagram displays an omnidirectional antenna gain regarding 2.4 GHz (blue line) which is used for Bluetooth and Wireless LAN 2.4 GHz. However, it also shows that Wireless LAN 5 GHz (orange line) has a limited antenna gain in the approximate directions 105° to 190°, i. e. the 5 GHz range will be limited in this direction.



!	Limited gain for 5 GHz between 105° to 190°.

C.2 Vertical Views

These diagrams show the antenna pattern when looking at the Bolt from the side in two different rotations, 0° and 90°. The Bolt is mounted in a metal cabinet illustrated by the yellow box below the Bolt.

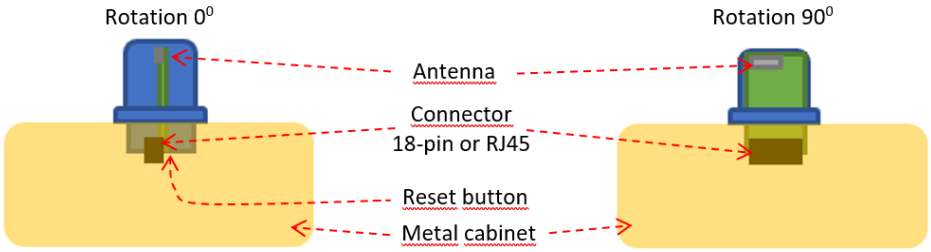
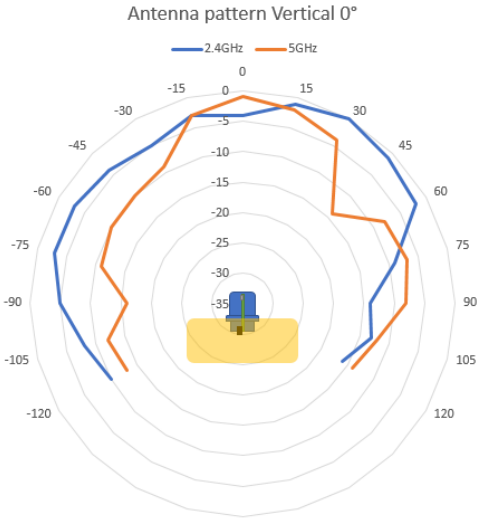
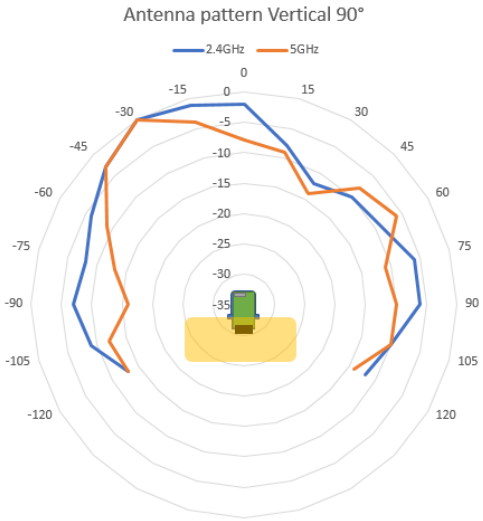


Diagram analysis: The vertical antenna gain is fairly omnidirectional for both frequencies. It is also clear to see that the metal cabinet where the Bolt is mounted will increase the gain “upwards” in reference to the surface where the Bolt is mounted. Thus the gain “downwards” is limited as expected.

C.2.1 Front View – Vertical 0°



C.2.2 Side View – Vertical 90°



C.3 Throughput Diagram

This diagram shows how data throughput decreases when distance increases. Note the huge difference between using a backshield to focus the radio energy, and not using a backshield. Using a backshield can greatly increase radio coverage if used correctly.

The diagram covers both the Anybus Wireless Bolt and the Anybus Wireless Bridge when using Wi-Fi (WLAN) 2.4 GHz.