ENGLISH

Anybus® Wireless Bridge II Serial™

USER MANUAL

SCM-1202-185
Version 2.0
Publication date 2022-02-23

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.

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

1. Preface

1.1. About This Document

This document describes how to install and configure Anybus® Wireless Bridge II Serial™.

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

1.2. Document Conventions

Lists

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

User Interaction Elements

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

Program Code and Scripts

```
Program code and script examples
```

Cross-References and Links

Cross-reference within this document: Document Conventions (page 1)

External link (URL): www.anybus.com

Safety Symbols

DANGER
Instructions that must be followed to avoid an imminently hazardous situation which, if not avoided, will result in death or serious injury.

WARNING
Instructions that must be followed to avoid a potential hazardous situation that, if not avoided, could result in death or serious injury.

CAUTION
Instruction that must be followed to avoid a potential hazardous situation that, if not avoided, could result in minor or moderate injury.

IMPORTANT
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.

Information Symbols

NOTE
Additional information which may facilitate installation and/or operation.

TIP
Helpful advice and suggestions.

1.3. Trademarks

Anybus® is a registered trademark and Wireless Bridge II Serial™ is a trademark of HMS Networks AB.

All other trademarks are the property of their respective holders.

2. Safety

2.1. General Safety

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

CAUTION
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.

2.2. External Antenna Restrictions

For models with external antenna, only use antennas that are certified for use with this equipment.

Using external antennas that are not certified for use with this equipment will invalidate its certifications and make it non-compliant with the regulations for radio equipment.

A list of certified antennas can be found at www.anybus.com/support.

2.3. 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. Support and Resources

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

TIP
Have the product article number available, to search for the product specific support web page. You find the product article number on the product cover.

3.2. Optional Equipment

Bridge II Serial can be mounted on a standard DIN rail using the optional DIN mounting kit.

The DIN mounting kit is not included with the Bridge II Serial. For information about ordering the DIN mounting kit, please visit www.anybus.com.

3.3. Network Environment

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

3.4. Placement

Antenna Considerations

For models with internal antenna the characteristics of the antenna should be considered when choosing the placement and orientation of the Bridge II Serial.

See also Internal Antenna Characteristics (page 65).

Required Distance Between Devices

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

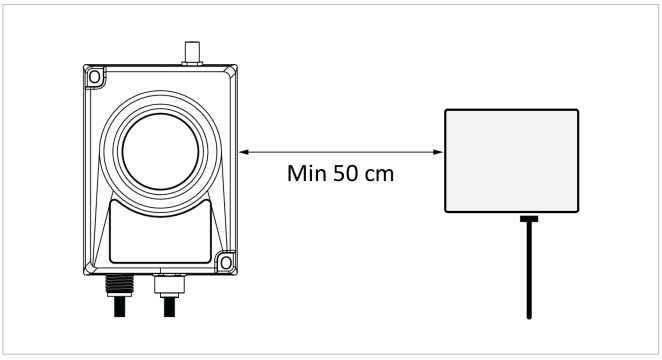


Figure 1. Required minimum distance between devices

See Wireless Technology Basics (page 64).

3.5. When to Use Bluetooth or WLAN

Use Bluetooth when:

- The wireless link has an Anybus Wireless Bolt or Anybus Wireless Bridge II 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.

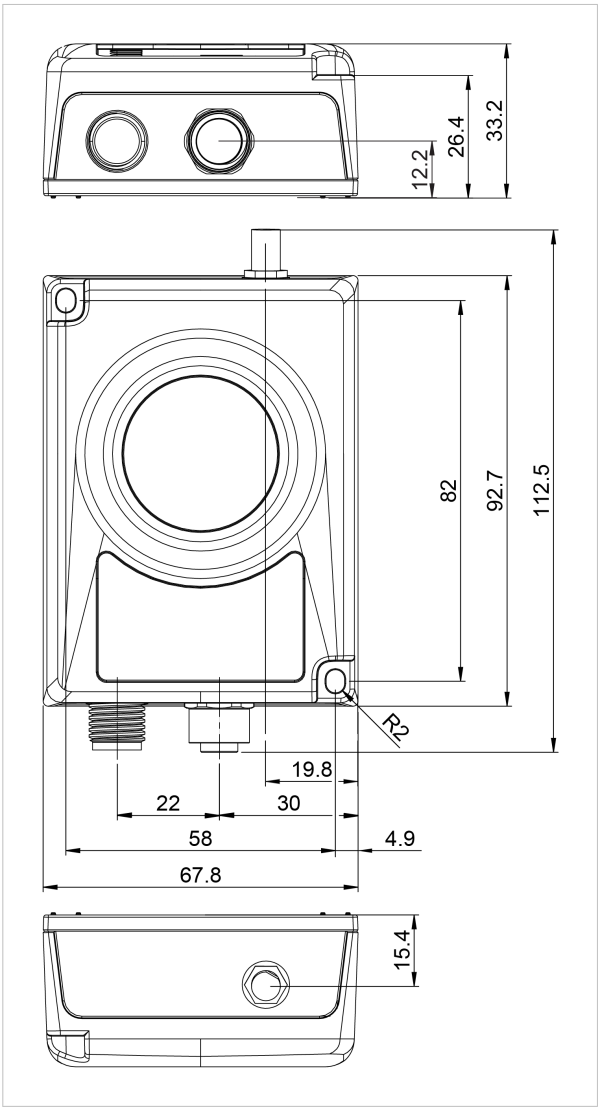
3.6. Bluetooth Limitations

Due to different implementations of Bluetooth by different manufacturers, Bluetooth PAN (Personal Area Network) may not work with some devices.

WLAN 5 GHz cannot be used at the same time as WLAN 2.4 GHz or Bluetooth.

4. Installation

4.1. Installation Drawing



All measurements are in mm.

Figure 2. Bridge II Serial Installation drawing

4.2. Surface Mounting

Bridge II Serial can be screw-mounted directly onto a flat surface.

Before You Begin

NOTE
To avoid signal interference, a minimum distance of 50 cm between the devices should be observed.
See also Wireless Technology Basics (page 64).

Procedure

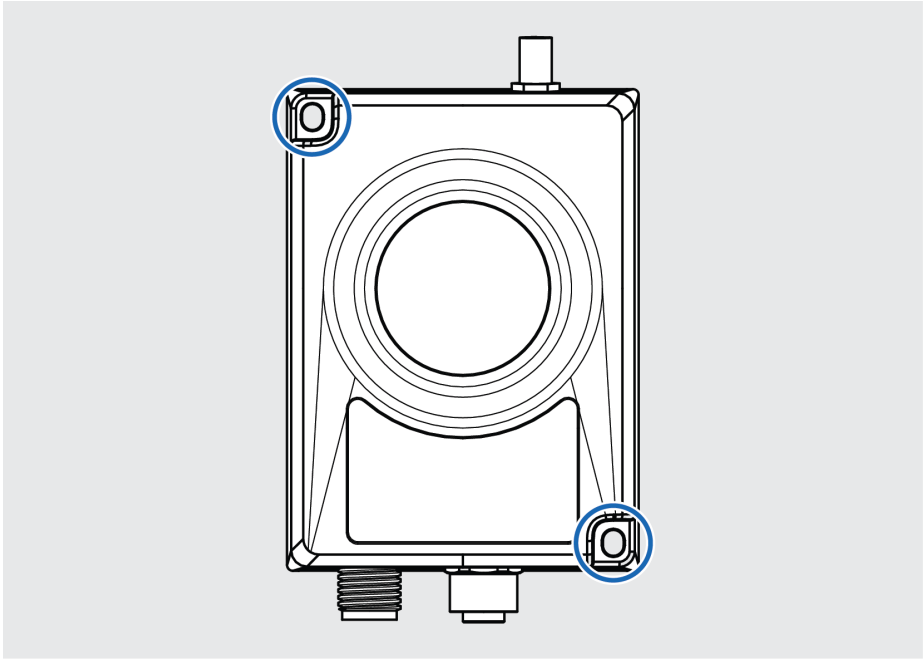


Figure 3. Surface mounting holes

- To screw-mount the Bridge II Serial on a surface, use the two holes (Ø 4 mm) at the corners of the Bridge II Serial.

4.3. DIN Rail Mounting

Using the optional DIN mounting kit, Bridge II Serial can be mounted on a standard DIN rail. See Optional Equipment (page 4).

Before You Begin

NOTE
To avoid signal interference, a minimum distance of 50 cm between the devices should be observed. See also Wireless Technology Basics (page 64).

Procedure

To attach the Bridge II Serial on the DIN rail

1. Fasten the DIN clip with the 2 included screws on the rear side of the Bridge II Serial.

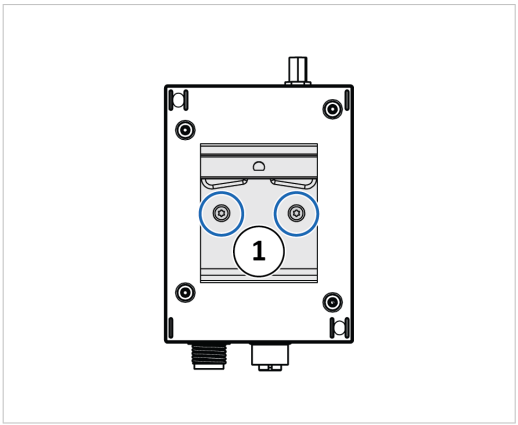


Figure 4. DIN clip on Bridge II Serial

2. Insert the upper end of the DIN rail clip into the DIN rail.
3. Push the bottom of the DIN rail clip into the DIN rail.

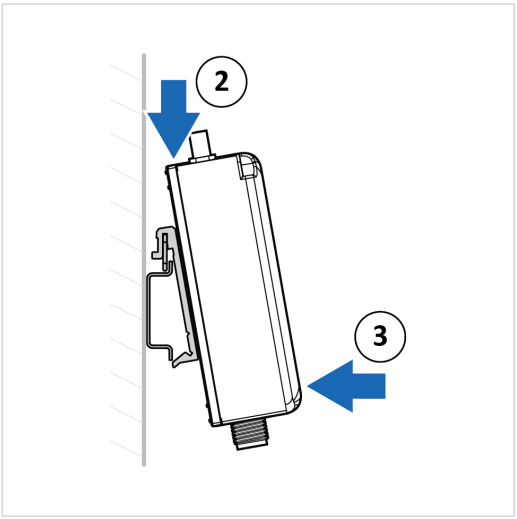


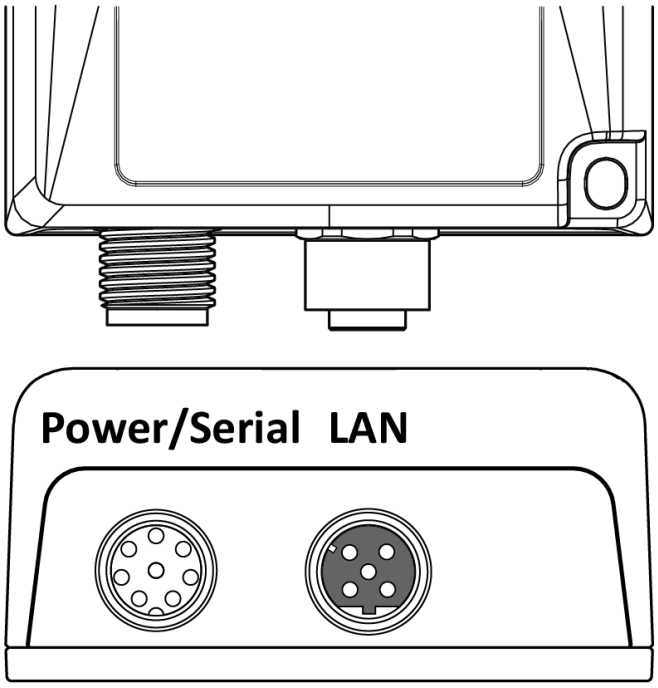
Figure 5. Attach Bridge II Serialon DIN rail

4.4. Connect to LAN, Serial and Power

Before You Begin

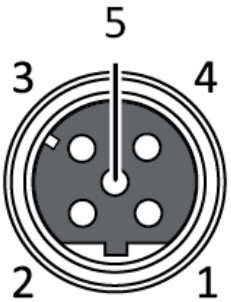
CAUTION
This equipment is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be used if a shielded Ethernet cable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

Procedure



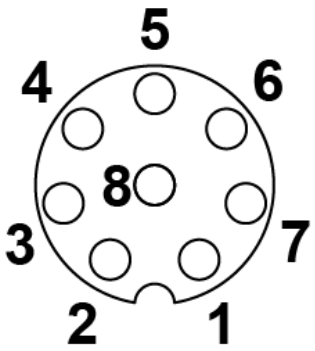
1. Connect the Bridge II Serial to LAN network.

Table 1. LAN connector pinout

LAN Connector	Pin	Function
	1	Transmit +
	2	Receive +
	3	Transmit -
	4	Receive -
	5	N/C

2. Connect the Bridge II Serial a serial network and Power.

Table 2. Shielded 8-pos A-coded M12 female connector

Serial and Power Connector	Pin	Wire Color		Function
	1	WH (White)	BU (Blue)	RS-232 TX
	2	WH (White)	BN (Brown)	Power 24 V
	3	BN (Brown)		Power GND
	4	OG (Orange)		RS-422_TX_A, RS485_A
	5	WH (White)	GN (Green)	RS-422_RX_B
	6	WH (White)	OG (Orange)	RS-422_TX_B, RS485_B
	7	BU (Blue)		Signal GND
	8	GN (Green)		RS-422_RX_A, RS-232_RX
	Housing	N/A		Acts as product FE (Functional Earth) when the cable shield is connected to FE.

5. Configuration

5.1. Bridge II Serial Built-In Web Interface

The Bridge II Serial built-in web interface is used to configure, maintain and troubleshoot the Bridge II Serial. Parameters can be set individually or using pre-configured Easy Config modes.

The web interface is accessed by pointing a web browser to the IP address of the unit.

The default address is 192.168.0.99.

See also Access the Built-In Web Interface (page 12).

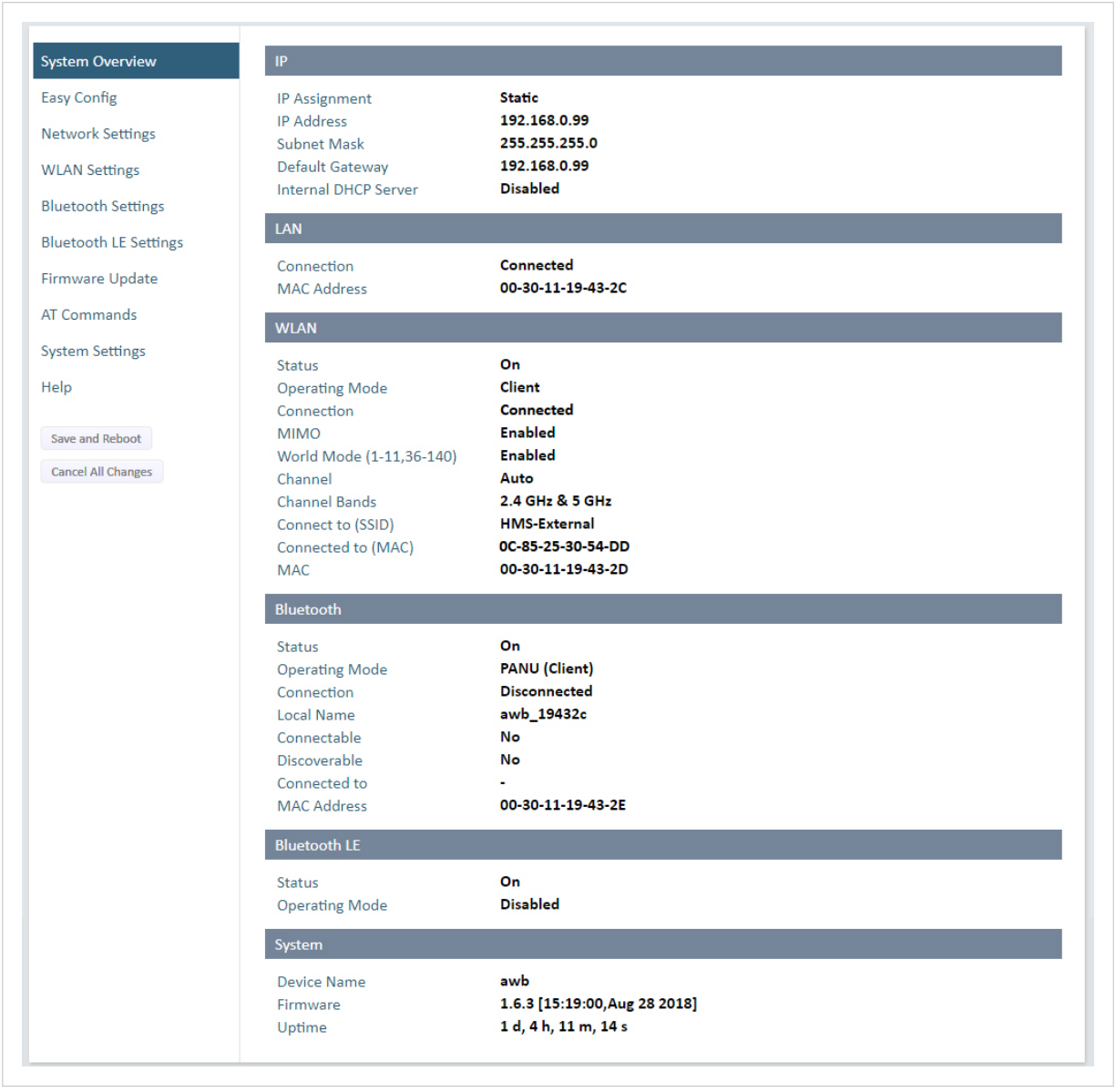


Figure 6. System Overview page example

The **System Overview** page shows current settings and network connection status.

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

5.2. Access the Built-In Web Interface

5.2.1. Required IP Address Settings

To be able to access the Bridge II Serial built-in web interface you may need to adjust the IP settings, choose one of the following methods.

The Bridge II Serial default IP address is 192.168.0.99.

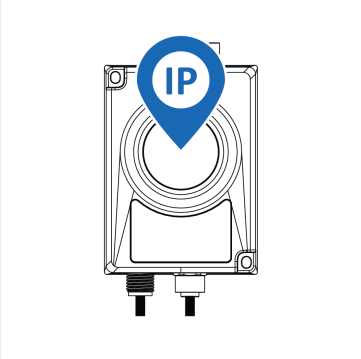
Option 1 - Set a Static IP Address on Your PC

On the PC accessing the Bridge II Serial built-in web interface, set a static IP address within the same IP address range as the Bridge II Serial IP address.

To access the Bridge II Serial built-in web interface, ensure that Port 80 TCP is open in your PC Windows Firewall.

Note that when you change to a static IP address on your PC, internet access is lost.

Option 2 - Change the IP Address on the Bridge II Serial Ethernet port



Use the software application HMS IPconfig to find and change the IP address on the Bridge II Serial Ethernet port, to one within the same IP address range as the PC accessing the Bridge II Serial built-in web interface.

To download the installation files, please visit www.anybus.com/support and enter the product article number to search for the Bridge II Serial support web page. You find the product article number on the product cover.

Result

Now you can enter the Bridge II Serial IP address in your web browser and search to access the built-in web interface login page.

See Log In to the Built-In Web Interface (page 13).

5.2.2. Log In to the Built-In Web Interface

The Bridge II Serial built-in web interface can be accessed from a standard web browsers.

Before You Begin

IMPORTANT
Before installing Bridge II Serial on a network, change the default administrator password.

IMPORTANT
Before installing the Bridge II Serial on a network, change the Bridge II Serial default username and password.

NOTE
The Bridge II Serial comes with a default password. You find the default password on the Bridge II Serial product housing.

NOTE
The Bridge II Serial default IP address is 192.168.0.99.

Procedure

Login to the Bridge II Serial built-in web interface

1. Open a web browser.
2. Click to select the **Address bar** and enter the Bridge II Serial IP address.

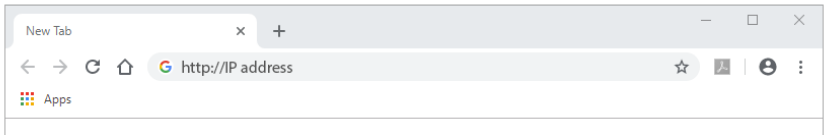


Figure 7. Enter IP address in web browser

3. Press **Enter**.
   The built-in web interface login screen appears.
4. Enter the **Password** and click **Sign in**.

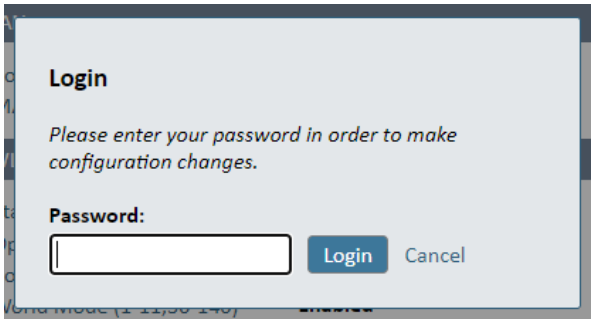


Figure 8. Built-in web interface login screen

Result

You are logged in to the **System Overiew** page.

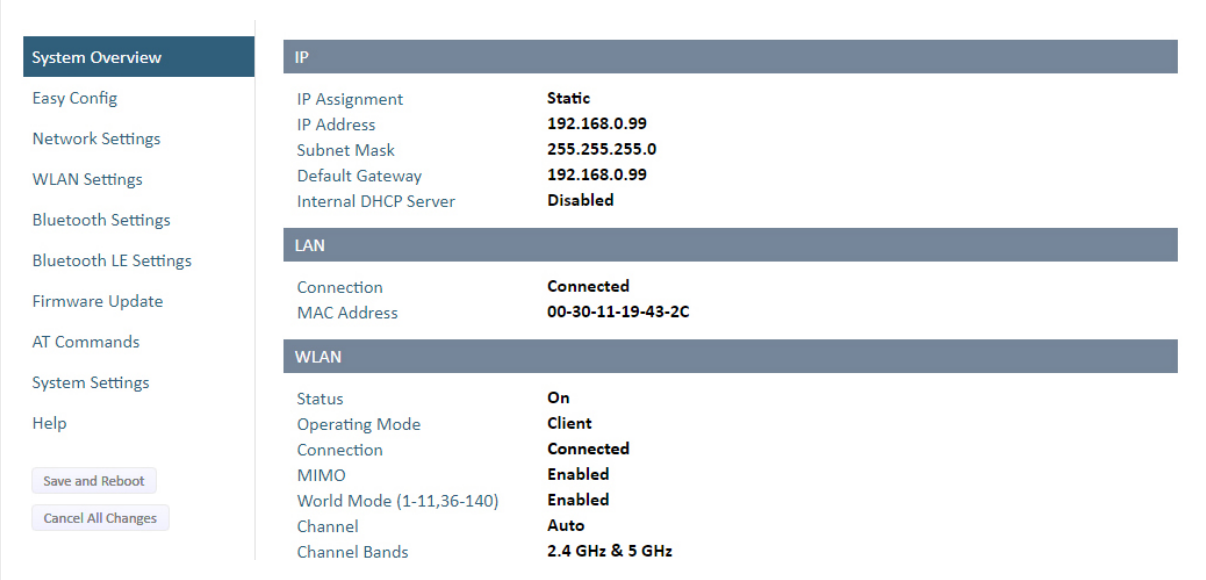
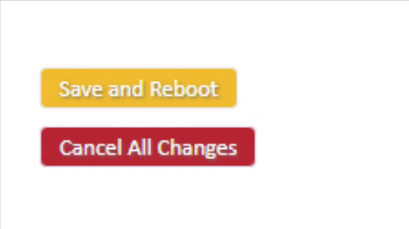


Figure 9. **System Overiew** page

5.3. To Save and Reboot



Cancel Changes

To cancel changes you have made to the settings:

- In the left sidebar menu, click **Cancel All Changes**.

To restore settings, see Restore Settings From Backup File (page 56).

Apply Changes

- To apply changes, click **Save and Reboot** in the left sidebar menu.
  Bridge II Serial restarts for the changes to take effect.

5.4. Factory Default Settings

The Bridge II Serial comes with the following factory default settings.

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 WLAN Settings	
Operating Mode	Client
Channel Bands	2.4 GHz & 5 GHz
Authentication Mode	WPA/WPA2–PSK
Channel	Auto
Bridge Mode	Layer 3 IP forward

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 Serial Settings	
Operating Mode	RS232
Baud Rate	57600 bits/s
Data Bits	8
Stop Bits	1
Parity	No parity
Modbus Optimization	Off
TCP Mode	Server
Modbus Gateway Mode	Disabled
TCP Port	5005

5.5. Configuration Methods

There are different methods available for configuring the Bridge II Serial.

Built-In Web Interface Settings

Bridge II Serial can be configured via the settings in the built-in web interface.

See Configure Settings in the Built-In Web Interface (page 29).

Easy Config Modes

Bridge II Serial can be configured using one of the pre-configured Easy Config modes.

See Configuration with Easy Config (page 17).

AT Commands

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.

For more information about how to use the AT commands, navigate to the built-in web interface **Help** page or see the AT Commands Reference Guide.

See also Configuration with AT Commands (page 25).

5.6. Wireless Configuration via Access Point Unit

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

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.

5.7. Configuration with Easy Config

5.7.1. Available Easy Config Modes

Bridge II Serial may be configured using one of the pre-configured Easy Config modes.

NOTE

By default, the unit starts in **Easy Config Mode 4**. The unit awaits automatic configuration during 120 seconds or until receiving a configuration.

NOTE

To cancel Easy Config mode 11, the unit must be reset to factory default settings. See Reset to Factory Default (page 58)

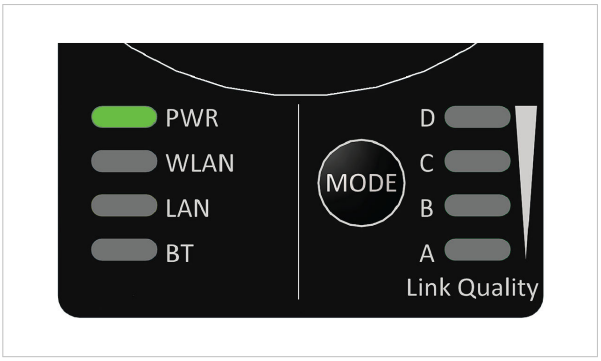


Figure 10. Easy Config A-B-C-D LED indicators

Table 3. Easy Config modes

EC	Active LED				Role	Description
1	A				Bluetooth PANU	Used for setting up point-to-point communication. The unit scans for another unit in Config Mode 4. The unit listens for 40 seconds or until a configuration is established. When a unit in mode 4 is detected: The scanning unit configures itself as a Bluetooth PANU Client, sends a connection configuration to the detected unit, and restarts. The detected unit restarts and attempt to connect to the first unit as a PANU Client.
2		B			N/A	Reset configuration to factory defaults.
3	A	B			N/A	Reset IP settings to factory defaults.
4			C		Client	Configure units in mode 4 as Clients. Wait for automatic configuration. The unit listens for 120 seconds or until receiving a configuration. When mode 4 is used with mode 1, 5 or 6, Serial Settings TCP Mode Client is activated automatically.
5	A		C		WLAN AP	The unit scans for other units in Config Mode 4 and configure them as Clients. Timeout occur after 120 seconds. Restart as Access Point and connect Clients.
6		B	C		Bluetooth NAP	
11	A	B		D	(any)	Enable PROFIsafe mode. The unit is locked in PROFIsafe mode. No other configuration settings are changed.

The Easy Config modes are also described when selected in the built-in web interface. See How to Activate an Easy Config Mode (page 18).

5.7.2. Easy Config Modes Time Considerations

Table 4. Easy Config modes time considerations

Mode	Timeout
1 and 9	The unit listens for 40 seconds or until a configuration is established.
4	The unit listens for 120 seconds or until receiving a configuration.
5, 6, 7 and 8	The unit scans for 120 seconds, then timeout occur.

5.7.3. How to Activate an Easy Config Mode

Activate an Easy Config Mode in the Built-In Web Interface

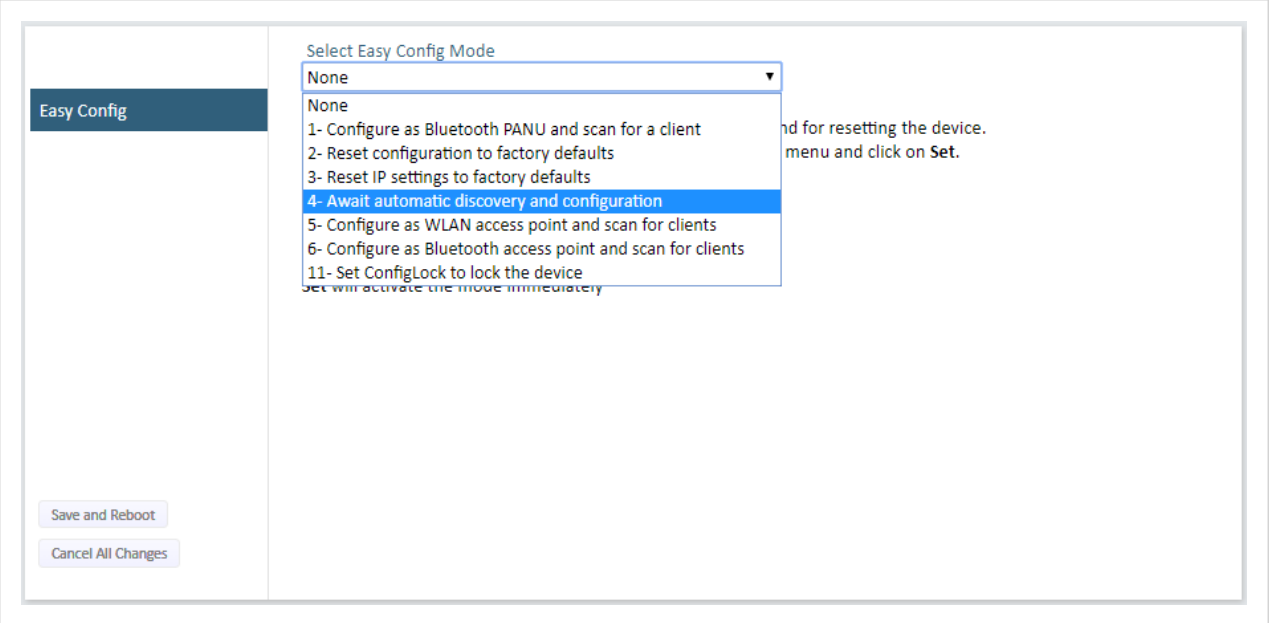


Figure 11. Built-in web interface Easy Config menu

1. In the built-in web interface, navigate to the **Easy Config** page.
2. To activate an Easy Config mode, select it from the drop-down menu and click **Set**.
   See also Available Easy Config Modes (page 17).
   The selected mode is activated immediately.

Activate an Easy Config Mode with the MODE Button

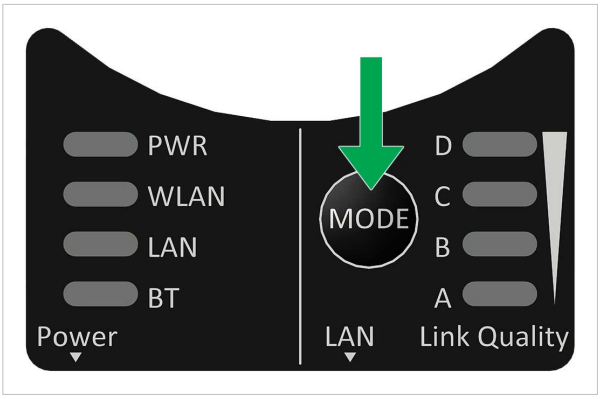


Figure 12. Easy Config using the MODE button

1. Power on the unit and wait for the Link Quality LEDs to light up and go out again, then immediately press and release the **MODE** button.
2. Press **MODE** repeatedly to cycle through the Easy Config modes until the desired mode is indicated by the A-B-C-D LEDs.
3. Within 20 seconds of step 2, press and hold **MODE** for 2 seconds.
   When the button is released the unit restart in the selected mode.

See also Easy Config Using the MODE Button (page 20).

5.7.4. Easy Config Using the MODE Button

In this topic we describe the general procedure for configuring units using the **MODE** button and Easy Config modes. For specific use case examples, see Use Cases (page 47).

Before You Begin

NOTE
By default, the unit starts in **Easy Config Mode 4**. The unit awaits automatic configuration during 120 seconds or until receiving a configuration.

Default IP address settings

- The default address to Access Point unit 1 is 192.168.0.99.
- The default IP address to Client unit 1 is 192.168.0.100.

Procedure

Configuration steps

1. Power on the first Unit.
   The power PWR LED light is lit.

2. When the Link Quality LEDs lights up and goes out again, immediately press and release **MODE**.

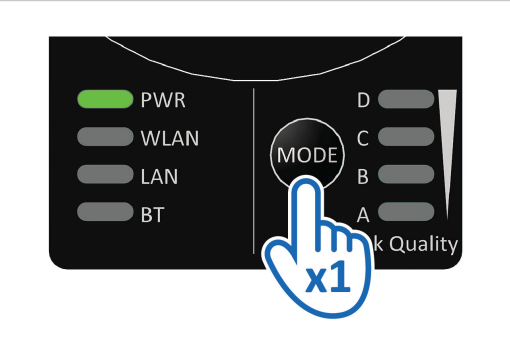


Figure 13. Press and release **MODE**

3. To select an Easy Config mode:
   a. Press **MODE** repeatedly, to cycle through the Easy Config modes.

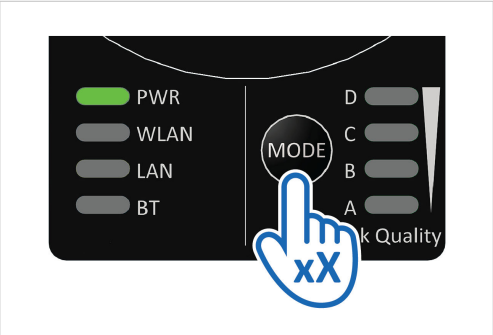


Figure 14. Select the desired mode

   b. When the A-B-C-D LED lights indicate the desired Easy Config mode, release the **MODE** button.

Table 5. Easy Config modes and LED indications

EC	LED				Role	Description
1	**A**				Bluetooth PANU	Configure as a Client and scan for another Client (PANU to PANU). Used for setting up point-to-point communication. Timeout after 40 seconds.
4			**C**		Client	Wait for automatic configuration. Timeout occur after 120 seconds.
5	**A**		**C**		WLAN AP	Configure units in mode 4 as clients. Restart as Access Point and connect Clients. Timeout occur after 120 seconds.
6		**B**	**C**		Bluetooth NAP	

4. To confirm the Easy Config mode, press and hold **MODE** for 2 seconds and then release it.

> **NOTE**
> You must confirm the Easy Config mode within 20 seconds.

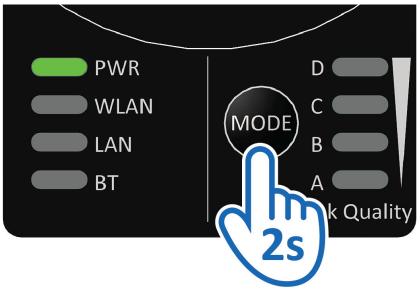


Figure 15. Confirm Easy Config mode

5. The LED lights indicating the active Easy Config mode flashes while the unit is scanning for a second unit to configure.
   Depending on the selected Easy Config mode, the following happens:

   - Easy Config mode 1: The unit restarts as a Client and starts scanning for a second unit to configure.
   - Easy Config mode 4: The unit listens for 120 seconds for receiving a configuration.
   - Easy Config mode 5 or 6: The unit restarts as an Access Point and starts scanning for a second unit to configure.

To add additional units

When using Easy Config Mode 5 or 6, up to seven additional Units can be added.

NOTE
When using Easy Config mode 4, the next unit to be added must be set up within 120 seconds after the first unit was restarted.

- To add a Unit, repeat the configuration steps, see Configuration steps (page 20).
  Each new Client unit will be assigned the next free IP address in the current Ethernet subnet.

Verify operation

See LED Indicators (page 44).

- On Units configured with Bluetooth, verify that the BT LED is lit.
- On Units configured with Easy Config Mode 4, the A-B-C-D LED lights indicates the Bluetooth link quality.
- On Units configured with WLAN, verify that the WLAN LED is lit.

To configure additional settings

- To configure additional settings, log in to the built-in web interface for each unit you want to configure.
  See Configure Settings in the Built-In Web Interface (page 29)

5.7.5. Easy Config via the Built-In Web Interface

In this topic we describe the general procedure for configuring units using the **MODE** button and Easy Config modes. For specific use case examples, see Use Cases (page 47).

Before You Begin

NOTE
By default, the unit starts in **Easy Config Mode 4**. The unit awaits automatic configuration during 120 seconds or until receiving a configuration.

Procedure

Configuration steps

1. Power on the Unit.
   The power PWR LED light is lit.

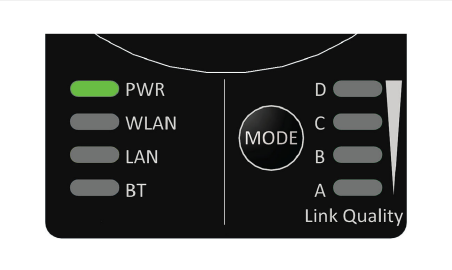


Figure 16. PWR LED

2. On the **Easy Config** page, select the desired Easy Config mode from the **Select Easy Config** drop-down menu.

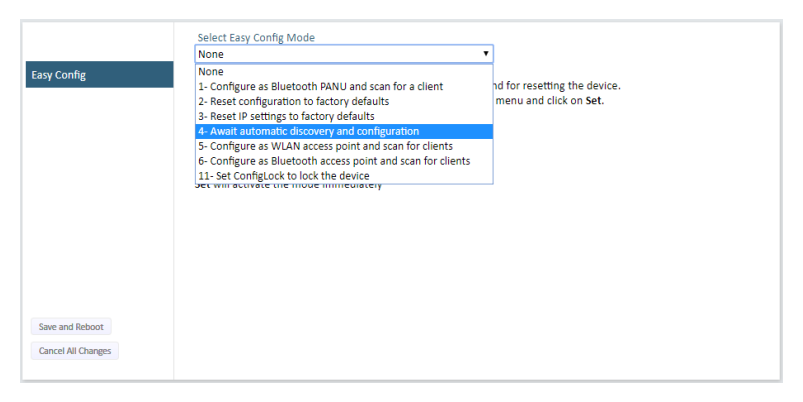


Figure 17. Easy Config Modes menu

Table 6. Available Easy Config Modes

EC	Role	Description
1	Bluetooth PANU	Configure as Bluetooth Client and scan for another Client (PANU–PANU). Timeout occur after 40 seconds.
2	–	Reset configuration to factory defaults.
3	–	Reset IP settings to factory defaults.
4	Client	Wait for automatic configuration. Configure units in Mode 4 as Clients.
5	WLAN AP	Configure units in mode 4 as clients. Restart as Access Point and connect Clients. Timeout occur after 120 seconds.
6	Bluetooth NAP	
11	(any)	Enable PROFIsafe mode.

3. Click **Set**.
   The Easy Config mode is activated immediately.

To add additional units

When using Easy Config Mode 5 or 6, up to seven additional Units can be added.

> **NOTE**
> When using Easy Config mode 4, the next unit to be added must be set up within 120 seconds after the first unit was restarted.

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

- To add a Unit, repeat the configuration steps, see Configuration steps (page 20).

Verify operation

See LED Indicators (page 44).

- On Units configured with Bluetooth, verify that the BT LED is lit.
- On Units configured with Easy Config Mode 4, the A-B-C-D LED lights indicates the Bluetooth link quality.
- On Units configured with WLAN, verify that the WLAN LED is lit.

To configure additional settings

- To configure additional settings, log in to the built-in web interface for each unit you want to configure.
  See Configure Settings in the Built-In Web Interface (page 29)

5.8. Configuration with AT Commands

Advanced configuration can be carried out by issuing AT commands via the web interface or over a Telnet or RAW TCP connection to port 8080 or over serial interface.

Use AT commands to setting advanced parameters, that are not accessible in the Bridge II Serial built-in web interface.

AT commands can be used to read out parameters in text format and for batch configuration using command scripts.

For a complete list of supported AT commands, click **Help** in the built-in web interface. See also the AT Commands Reference Guide at www.anybus.com/support.

Procedure

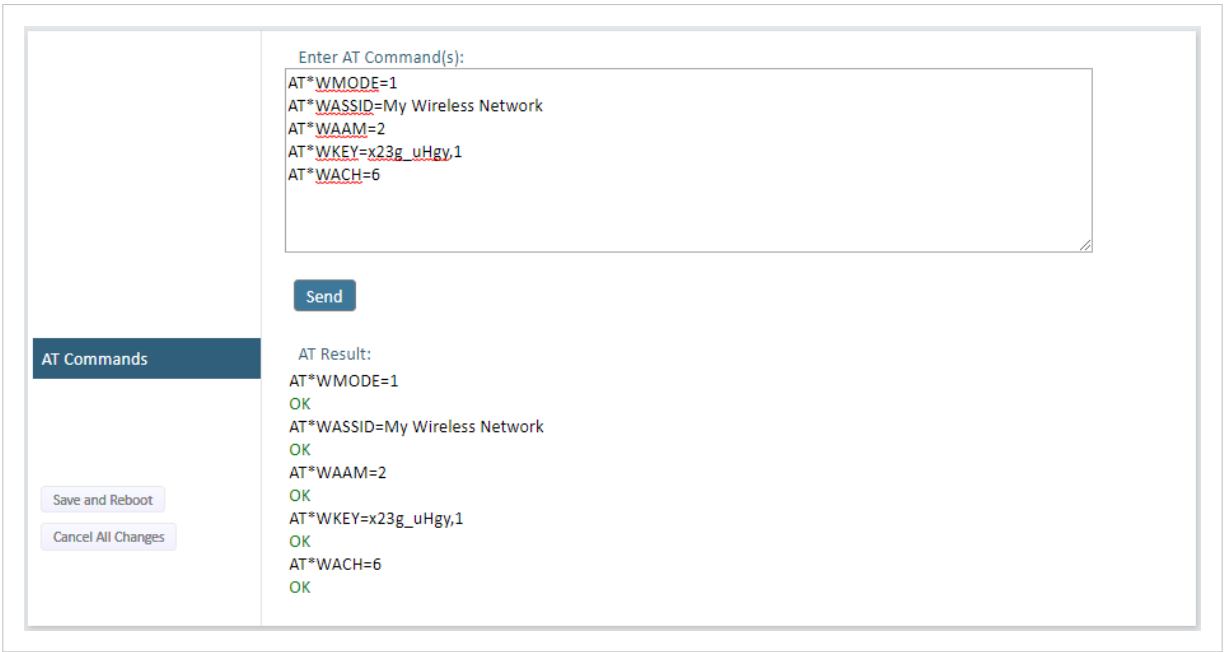


Figure 18. AT Commands and AT Results

1. Enter or paste the AT commands into the **Enter AT Command(s)** text field.
2. Click **Send**.
3. The result codes are displayed in the **AT Result** panel.

5.8.1. Enable Fast Roaming with AT Commands

Fast Roaming is only used for Client Mode.

Fast Roaming is enabled as default but can be permanently disabled using AT commands.

Procedure

Enable or Disable Fast Roaming.

1. To Enable or Disable Fast Roaming, change the value of register **4004**.
   - Enable Fast Roaming:

     ```
     ATS4004=1
     ```

   - Disable Fast Roaming:

     ```
     ATS4004=0
     ```

2. For the command to take effect, reboot the Bridge II Serial.
   Send the Reboot device AT Command:

   ```
   AT*AMREBOOT
   ```

For more information about how to set up WLAN roaming, see the AT Commands Reference Guide or the **Help** page in the built-in web interface.

5.8.2. Add Additional WLAN Channels with AT Commands

WLAN Channels and World Mode is only used for Client Mode.

World Mode can be disabled and additional channels added using AT commands.

NOTE
When World Mode is disabled and additional channels are used, WLAN communication may take a longer time to establish during startup.

When using additional channels:

- The unit will 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.

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

For information on possible channels to include, see WLAN Channels and World Mode (page 33).

Procedure

Enable or Disable World Mode and add WLAN channels.

1. To Enable or Disable World Mode.
   - Enable World Mode

     ```
     AT*WMM=1
     ```

   - Disable World Mode:

     ```
     AT*WWM=0
     ```

2. To include WLAN channels for connection and roaming, use the AT Command **AT*WSCHL=<channel_list>,<store>**.

   Example 1. Add 2.4 GHz channels

   2.4 GHz system with Access Points in channel 1, 6 and 11. There is no 5 GHz channels.

   ```
   AT*WSCHL=1,6,11,1
   ```

   Example 2. Add both 2.4 GHz and 5 GHz channels

   2.4 GHz channels: 1, 6 and 11

   5 GHz channels: 36, 40, 44, 48

   ```
   AT*WSCHL=1,6,11,36,40,44,48,1
   ```

3. For the change to take effect, reboot the Bridge II Serial.
   Send the Reboot device AT Command:

```
AT*AMREBOOT
```

5.9. Configure Settings in the Built-In Web Interface

5.9.1. Network Settings

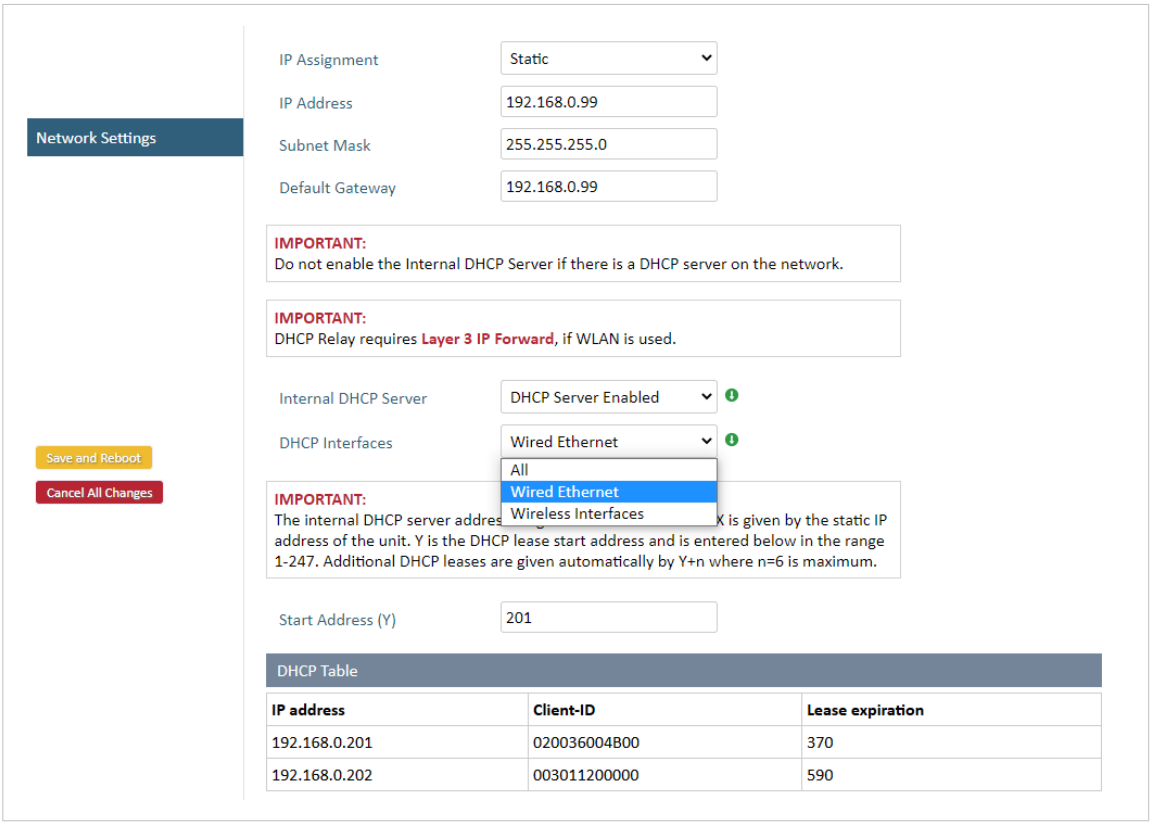


Figure 19. Network Settings page

Setting	Description
IP Assignment	Select static or dynamic IP addressing (DHCP).
IP Address	Static IP address for the unit. When you click **Save and Reboot**, the browser is redirected to the new address (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**. **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 is ignored.

Setting	Description
	Example 3. Start address 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.

5.9.2. Layer 3 IP Forward Connectivity Considerations

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.

5.9.3. WLAN Settings General

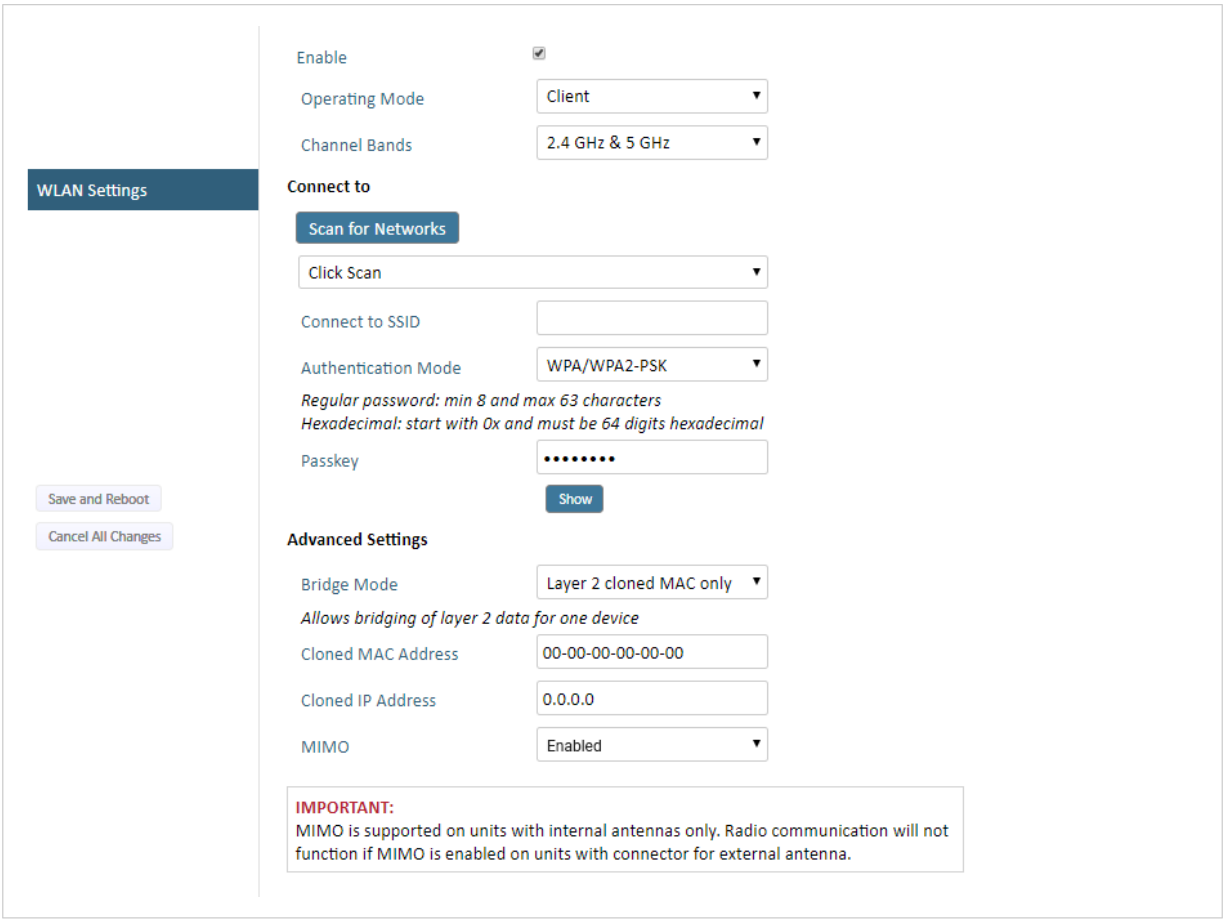


Figure 20. WLAN Settings page

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

5.9.4. WLAN Settings for Client

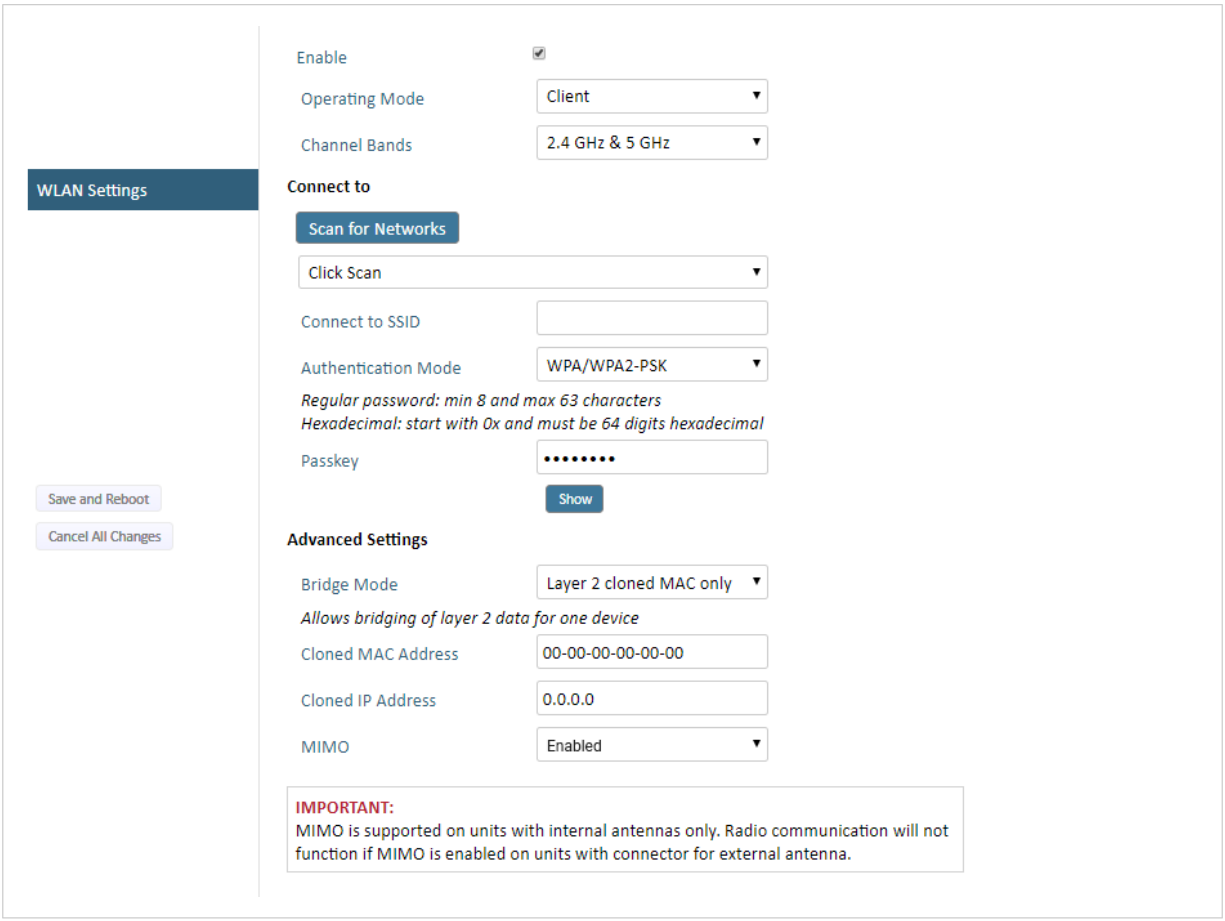


Figure 21. WLAN Settings page

Connect to settings for Client

Setting	Description
Scan for Networks	To scan the selected frequency band(s) for discoverable WLAN networks, click **Scan for Networks**. Select a network from the drop-down 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. When **Open** is selected there is no encryption or authentication.
Passkey	When using WPA/WPA2-PSK or WEP64/128, enter the passkey.
Username, Domain, Passphrase	Authentication details when using LEAP or PEAP (WPA2 Enterprise).

5.9.5. WLAN Roaming

Bridge II Serial 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.

See also Enable Fast Roaming with AT Commands (page 26).

5.9.6. WLAN Channels and World Mode

WLAN Channels and World Mode is only used for Client Mode.

NOTE
The maximum output power will be reduced on some channels depending on regulatory requirements.

Which channels are available for WLAN communication is restricted by the regulatory domain where the unit is operating.

Bridge II Serial 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.

Table 7. Regulatory domains and WLAN channels

Domain	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, 149, 153, 157, 161, 165
FCC	1-11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140

See also Add Additional WLAN Channels with AT Commands (page 27).

5.9.7. WLAN Settings for Access Point

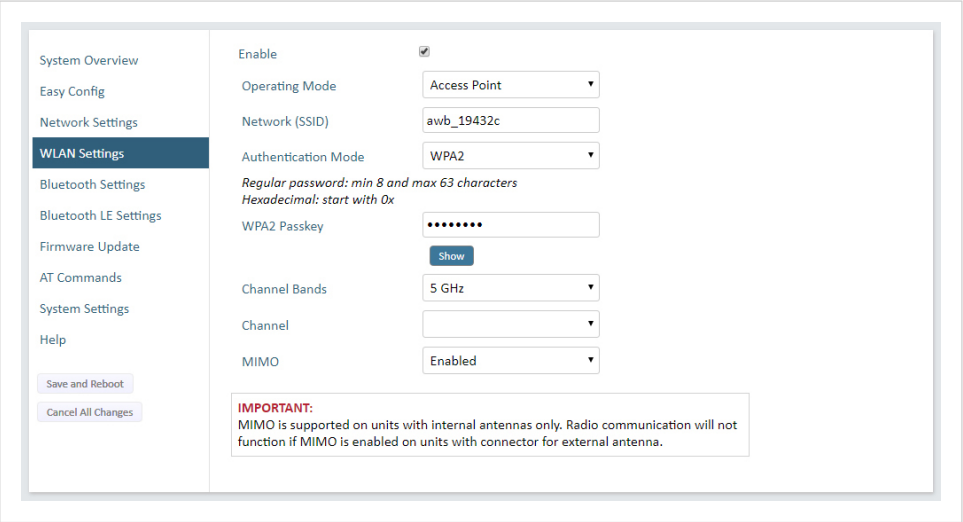


Figure 22. WLAN Settings page

Connect to settings for Access Point

The following settings are specific for Access Point mode:

Setting	Description
Network (SSID)	Enter an SSID (network name) for the Bridge II Serial. 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. When **Open** is selected there is no encryption or authentication. When **WPA2** is selected WPA2 PSK authentication with AES/CCMP encryption is used.
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 WPA2 Password Examples (page 34).
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.

WPA2 Password Examples

IMPORTANT
Do not use the example passwords in a live environment!

Example 4. Plain text password

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 5. Hexadecimal password example

0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f

5.9.8. WLAN Advanced Settings

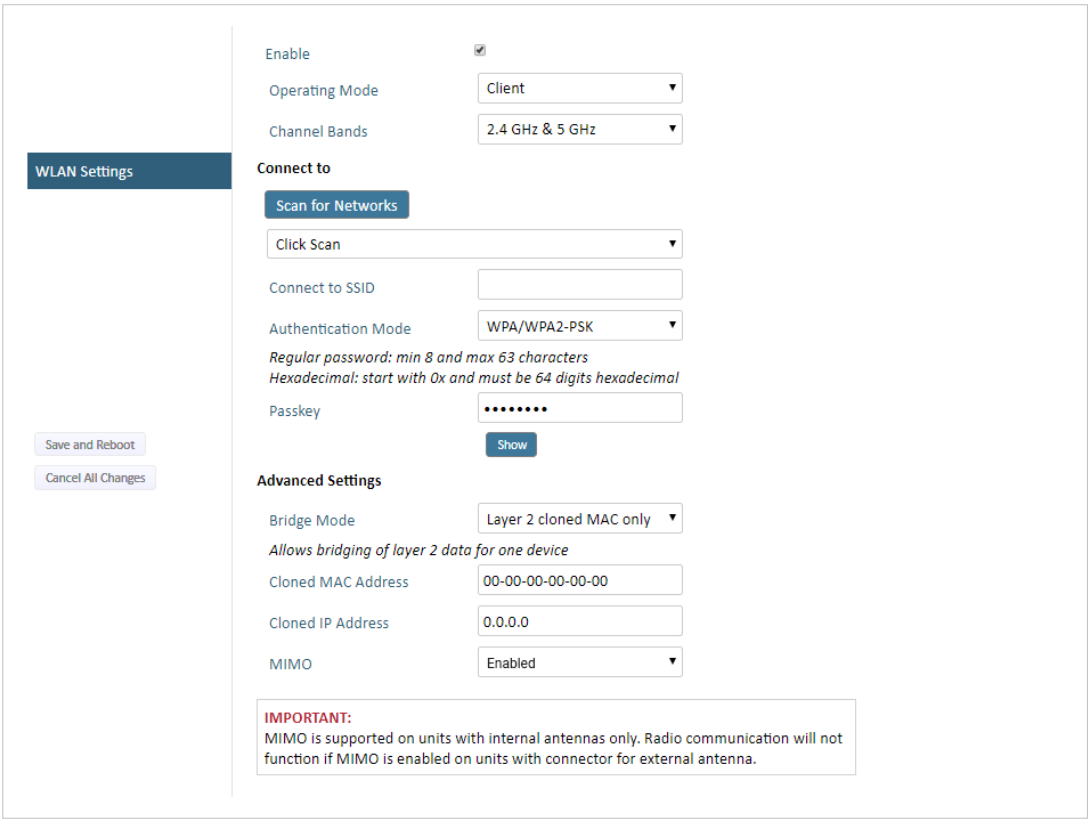


Figure 23. WLAN Settings page

Advanced Settings

Setting	Description
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 setting. IP data from all devices will be bridged over WLAN. This mode must be used when using the DHCP Relay function. See Layer 3 IP Forward Connectivity Considerations (page 30).
Cloned MAC Address	The MAC address to use with **Layer 2 cloned MAC only**.
Cloned IP Address	The IP address to use with **Layer 2 cloned MAC only**.
MIMO	MIMO (multiple input, multiple output) antenna technology uses multiple antennas for wireless communication in 802.11n. **IMPORTANT** MIMO is supported on units with internal antennas only. Radio communication will not function if MIMO is enabled on units with connector for external antenna.

5.9.9. Bluetooth Settings General

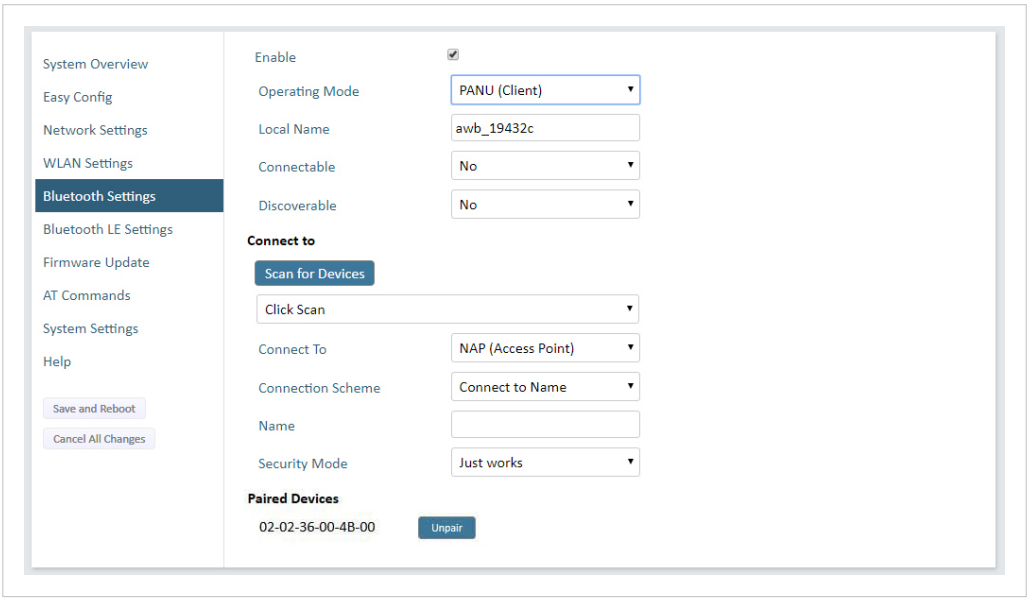


Figure 24. Bluetooth Settings page

General settings

Setting	Description
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.

Connect to settings

Setting	Description
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

The currently connected Bluetooth devices DHCP Client-ID are listed in the **Paired devices** panel.

To unpaire a devices, click **Unpaire**.

5.9.10. Bluetooth Settings for PANU Mode

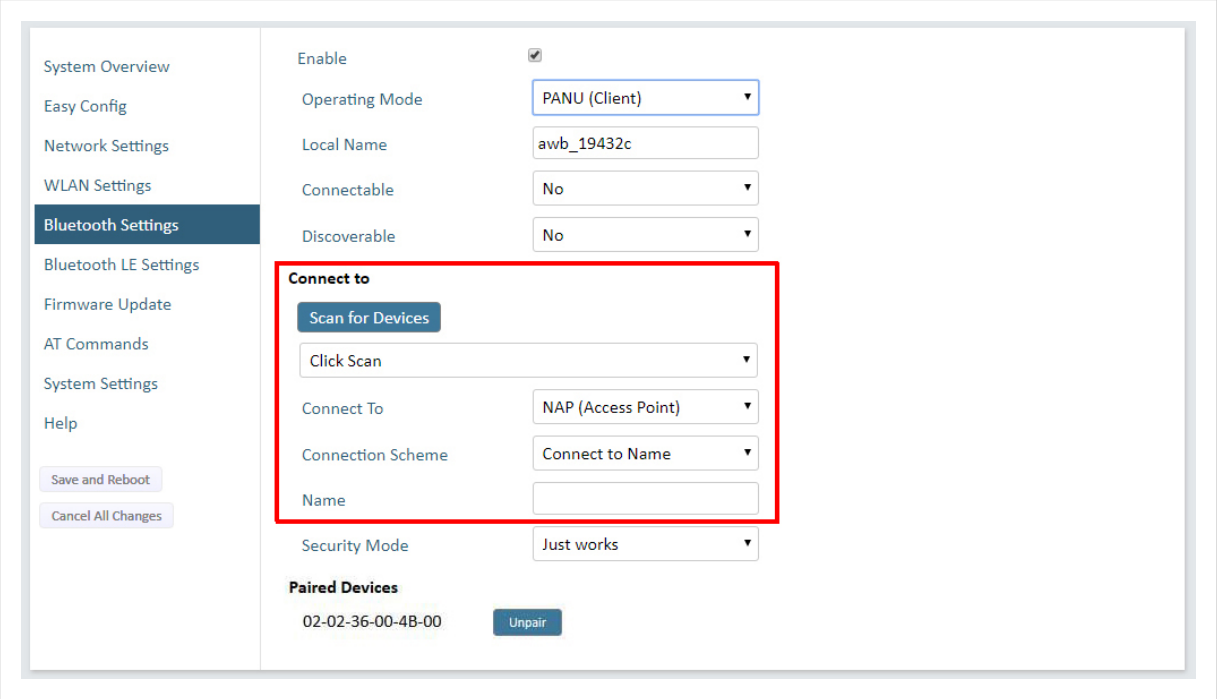


Figure 25. Bluetooth Settings page

Connect to settings for PANU Mode

Setting	Description
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.

5.9.11. Bluetooth Settings for NAP Mode

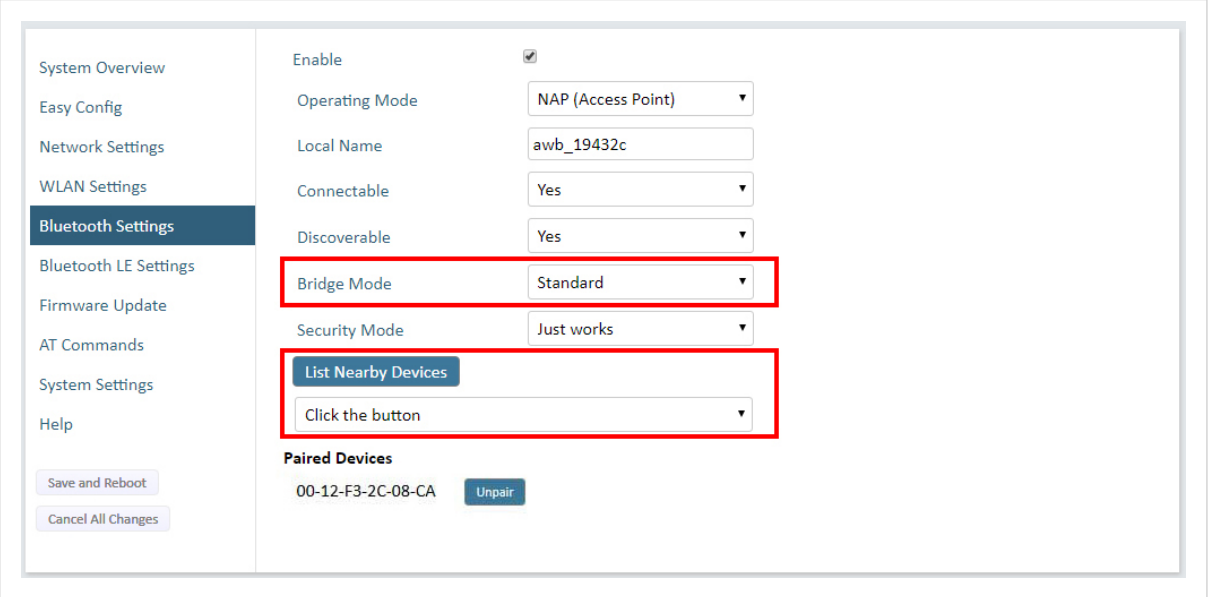
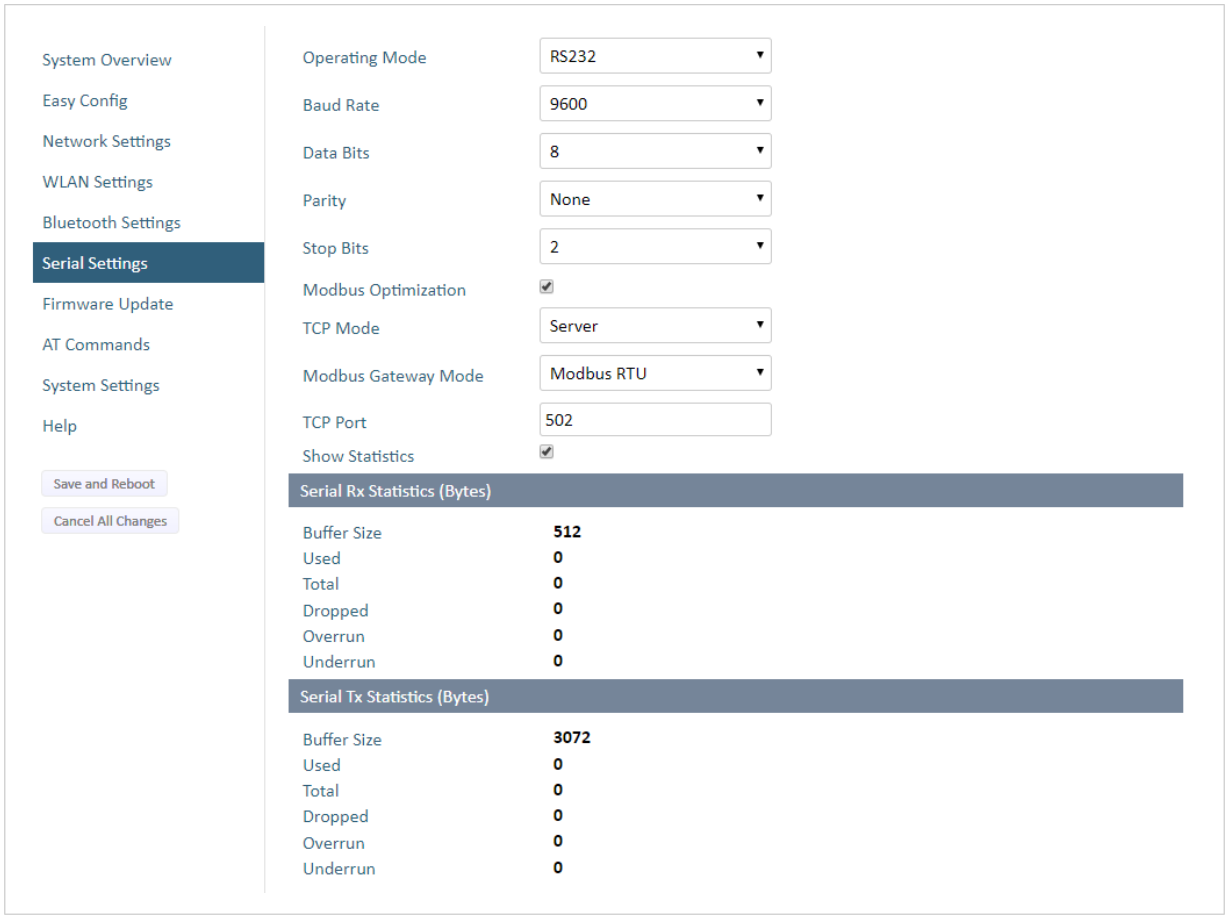


Figure 26. Bluetooth Settings page

Bluetooth Settings for NAP Mode

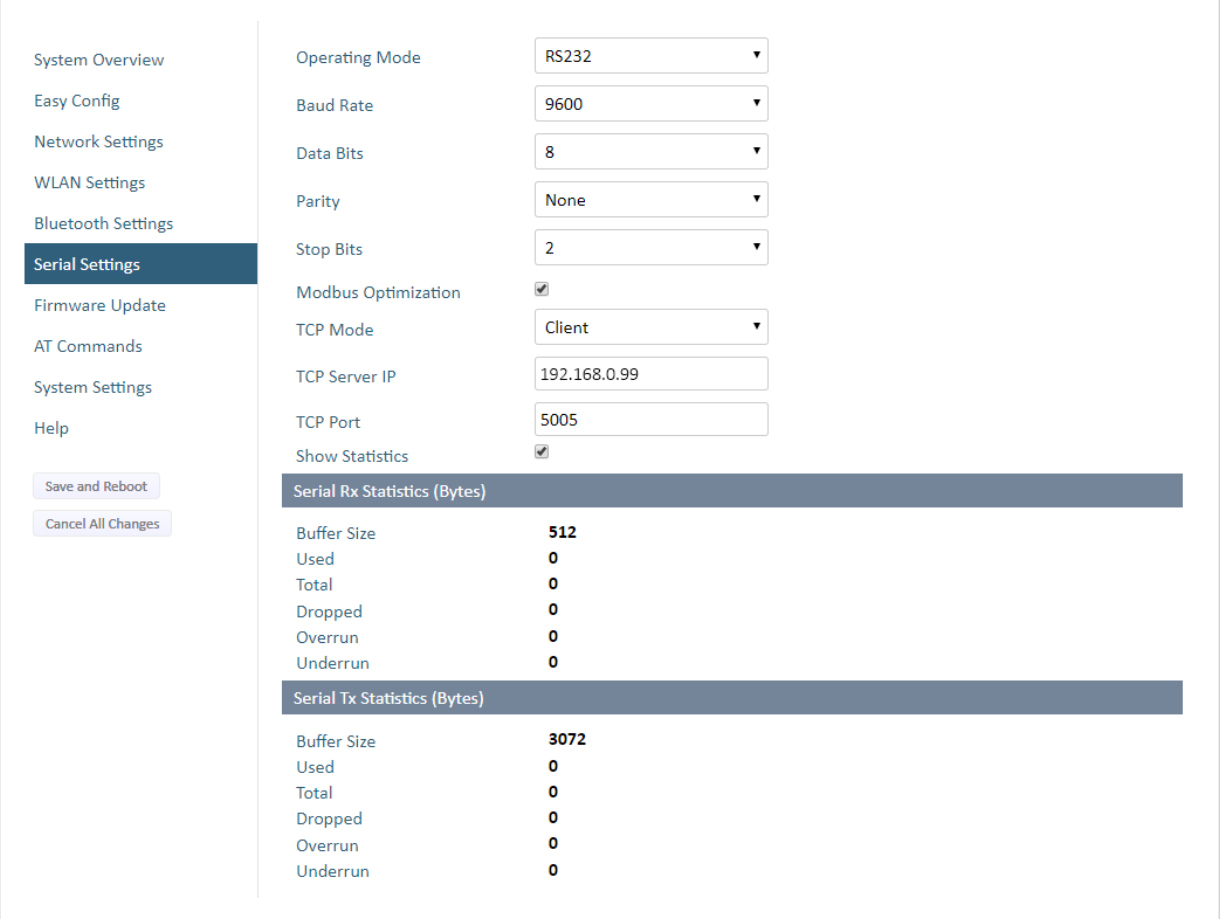
Setting	Description
Bridge Mode	**Standard**: Default mode. Layer 3 IP forward = IP data will be bridged over Bluetooth. This mode must be used when connecting to an Android device over Bluetooth. The network must have an active DHCP server.
List Nearby Devices	Scans the network and lists discoverable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

5.9.12. Set Up Serial Communication



Serial Settings example, TCP Mode Server with Modbus TCP to Modbus RTU Gateway function enabled

Figure 27. Serial Settings page, TCP Mode Server



Serial Settings example, TCP Mode Client enabled

Figure 28. Serial Settings page, TCP Mode Client

Serial Settings

NOTE
To avoid timing problems when different baud rates are set on the Master and the Slaves, set the lowest baud rate on the Master.

Setting	Description
Operating Mode	Select a physical serial communication interface, **RS232**, **RS422** , **RS485** or **Off**.
Baud Rate	Specify the rate at which information is transferred in a communication channel. Select a baud rate. At baud rates up to 115200 baud, the module is ready to receive data within one bit after last bit is sent. At baud rates higher than 115200 baud, the module will be ready to receive data 7 micro seconds after the last bit is sent.
Data Bits	Specify the number of data bits to transmit. Select **5**, **6**, **7** or **8** bits. To transmit binary data, select 8 data bits.
Parity	Specify if parity should be used to detect code errors. **No parity**: No parity checking, parity bit is not transmitted. **Odd parity**: The parity bit is asserted or unasserted to obtain an odd number of mark bits. **Even**: Even parity checking.
Stop Bits	Specify the number of stop bits used to indicate the end of data transmission. Select stop bit **1** or **2**.
Modbus Optimization	When Modbus Optimization is selected, the communication is optimized to keep all Modbus packets together in one frame. This mode should only be enabled when communicating with MODBUS RTU devices.

Setting	Description
TCP Mode	Select a TCP Mode from the dropdown menu: Client: The Bolt Serial acts as a Client and establishes a connection to the TCP server. Server: The Bolt Serial acts as a server and listens for incoming connections from the TCP Client.
TCP Server IP	When TCP Mode Client is selected, enter the TCP Server IP address.
Modbus Gateway Mode	When TCP Mode Server is enabled, select Modbus Gateway Mode to enable Modbus TCP to Modbus RTU gateway functionality.
TCP Port	When TCP Mode is active, enter the TCP Port number. Default port: 5005 When Modbus Gateway Mode is active, the port automatically changes to Modbus TCP port 502.
Show Statistics	Select Show Statistics to view Serial Rx and Tx statistics. Buffer Size: The bytes in the queue, handled with in the order they were received. Used: Part of the buffer used. Total: Total size of the buffer. Dropped: The number of dropped data packets. Overrun: Occur when the buffer is full, but still tries to handle incoming data traffic. Underrun: Occur when the incoming data traffic is at a lower speed than the outgoing data traffic.

5.9.13. Serial Communication

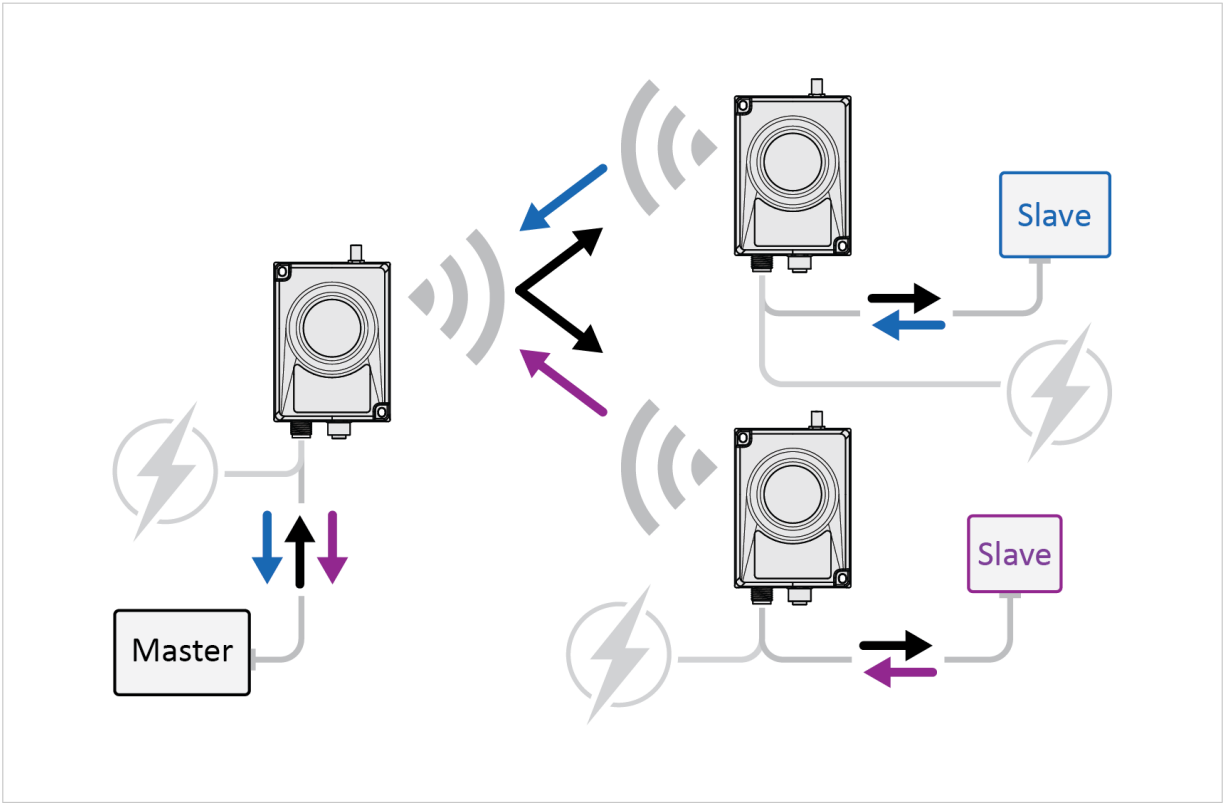
The serial functionality is used to transfer serial data from one point on a wireless link to another.

The connection can be set up as a point-to-point link or a point-to-multipoint link.

A message sent from a master to a Bolt Serial is forwarded to all the connected slaves.

The slave response sent to the Bolt Serial is forwarded to the master but not to the other slaves.

Example 6. Point-to-multipoint link



Message sent from Master and response sent from Slaves

5.9.14. System Settings

NOTE
Setting a secure password for the unit is strongly recommended.

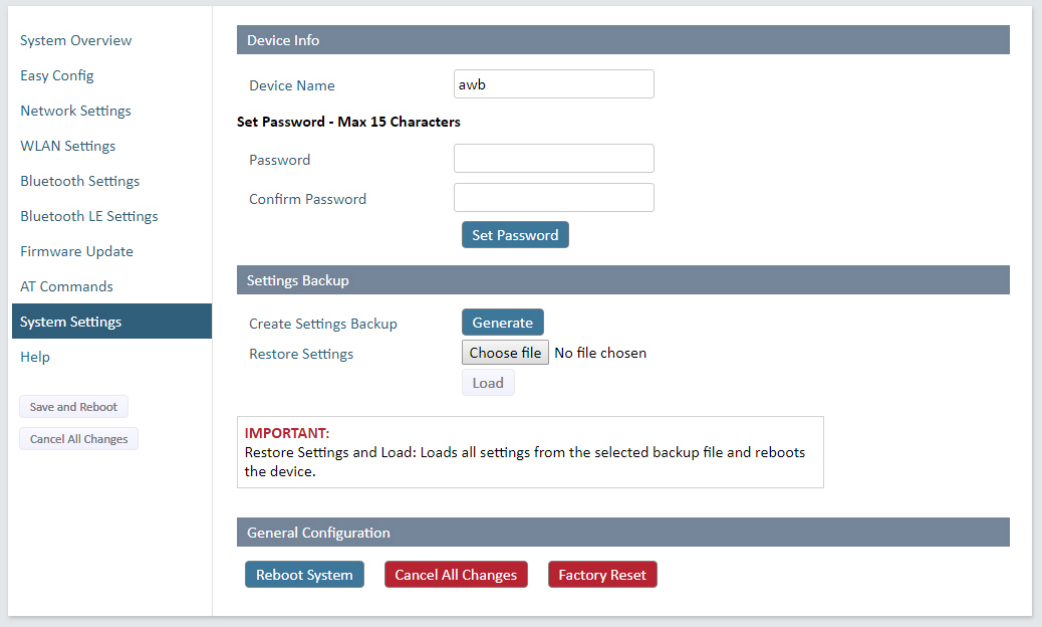


Figure 29. System Settings page

Device Info

Setting	Description
Device Name	Enter a descriptive name for the unit.
Password	Enter a password for accessing the web interface.

Settings Backup

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

General Configuration

Setting	Description
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.

6. Verify Operation

6.1. LED Indicators

Status Indicators

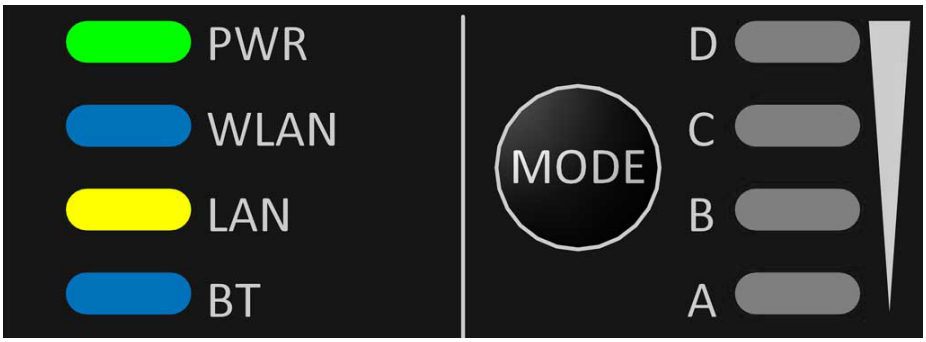


Figure 30. Status LED indicators

LED Indication		Description
PWR	Off	No power
	Green	Normal operation
WLAN	Off	WLAN disabled or no power
	Blue, blinking	Access Point: No clients, awaiting connections
	Blue	Access Point: Connected to at least one Client Client: Connected to Access Point
	Blue, flickering	WLAN data activity (when connected)
	Purple, blinking	Client: Scanning for access points
	Purple	Client: Connecting to a detected Access Point
	Red	Unrecoverable error
LAN	Off	No Ethernet connection
	Yellow	Ethernet link present
	Yellow, flickering	Ethernet data activity (when connected)
BT	Off	Bluetooth disabled or no power
	Blue, blinking	NAP: No clients, awaiting connections
	Blue	NAP: Connected to at least one PANU Client PANU: Connected to NAP
	Blue, flickering	Bluetooth data activity (when connected)
	Purple	PANU: Trying to connect to NAP
	Red	Unrecoverable error

Link Quality/Mode Indicators

The Link Quality/Mode Indicators are used to indicate Bluetooth quality, selected Easy Config mode and update status in Recovery Mode.

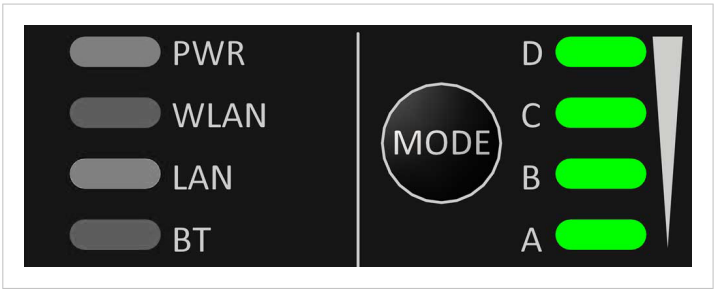


Figure 31. Link Quality/Mode indicators

Table 8. RSSI (WLAN Client) / Link Quality (Bluetooth PANU)

LED				Description
LED is off	LED is off	LED is off	LED is off	No connection
A, Green	LED is off	LED is off	LED is off	RSSI/Link Quality < 25 %
A, Green	**B**, Green	LED is off	LED is off	RSSI/Link Quality 25–50 %
A, Green	**B**, Green	**C**, Green	LED is off	RSSI/Link Quality 50–75 %
A, Green	**B**, Green	**C**, Green	**D**, Green	RSSI/Link Quality > 75 %

Recovery Mode LED Indications

Table 9. In Recovery Mode the Status LEDs indicate the firmware update status

LED	Indication	Description
PWR	Green	Firmware update in progress
	Green, blinking	Waiting for valid firmware
WLAN + **BT**	Alternating red/blue	Firmware update in progress

6.2. Network Connection Status

The **System Overview** page shows current settings and network connection status.

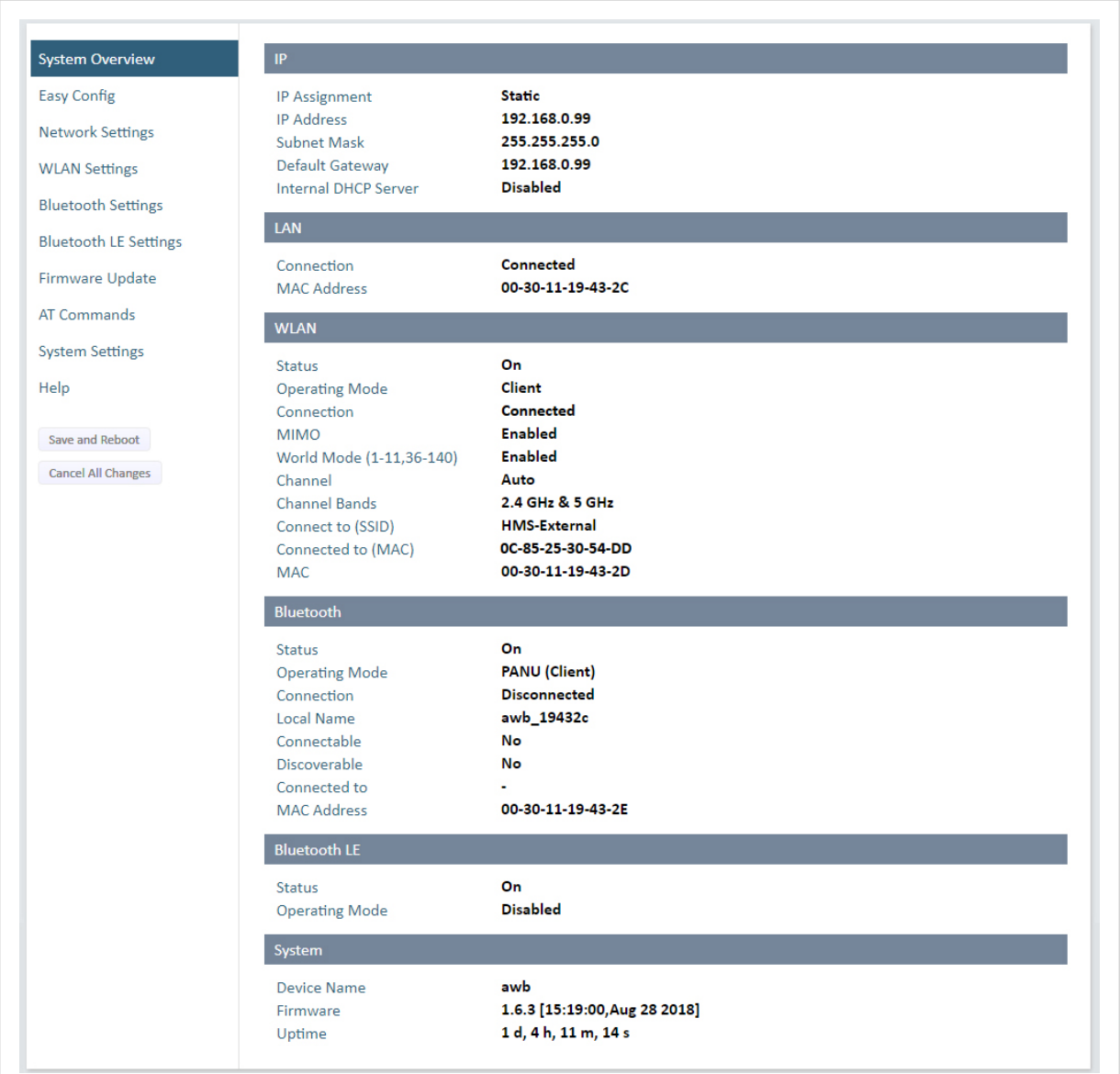
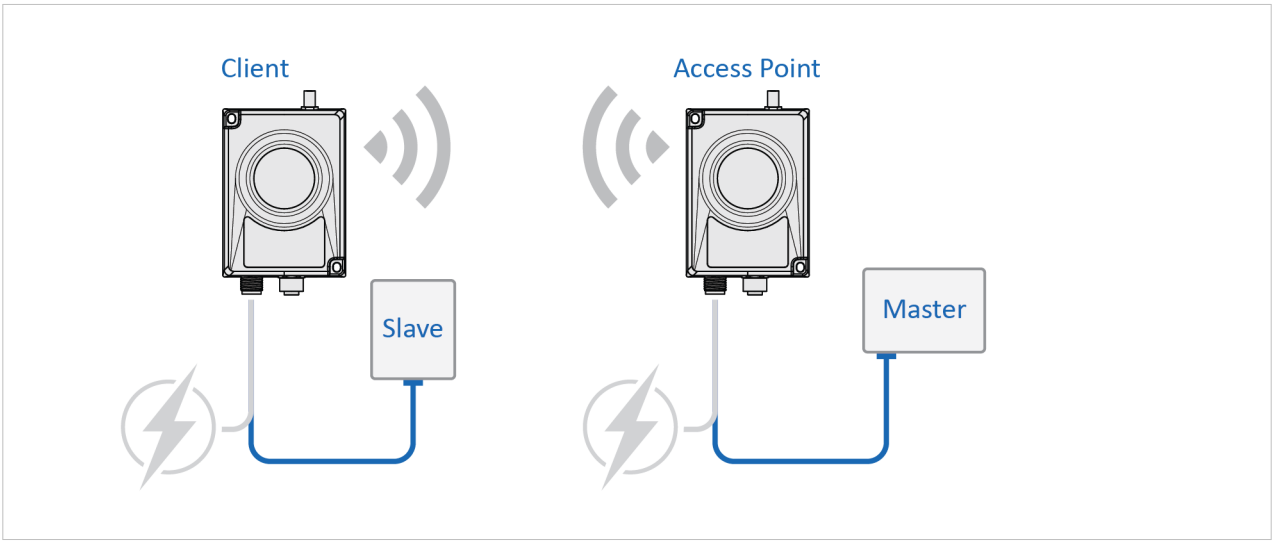


Figure 32. System Overview page example

7. Use Cases

7.1. Bridge II Serial Point-to-Point Installation



Serial cable replacement is enabled by using two pieces of Bridge II Serial which creates a wireless bridge for the Serial communication.

Figure 33. Bridge II Serial Point-to-Point Installation

7.2. Installing Multiple Bridge II Serial Units

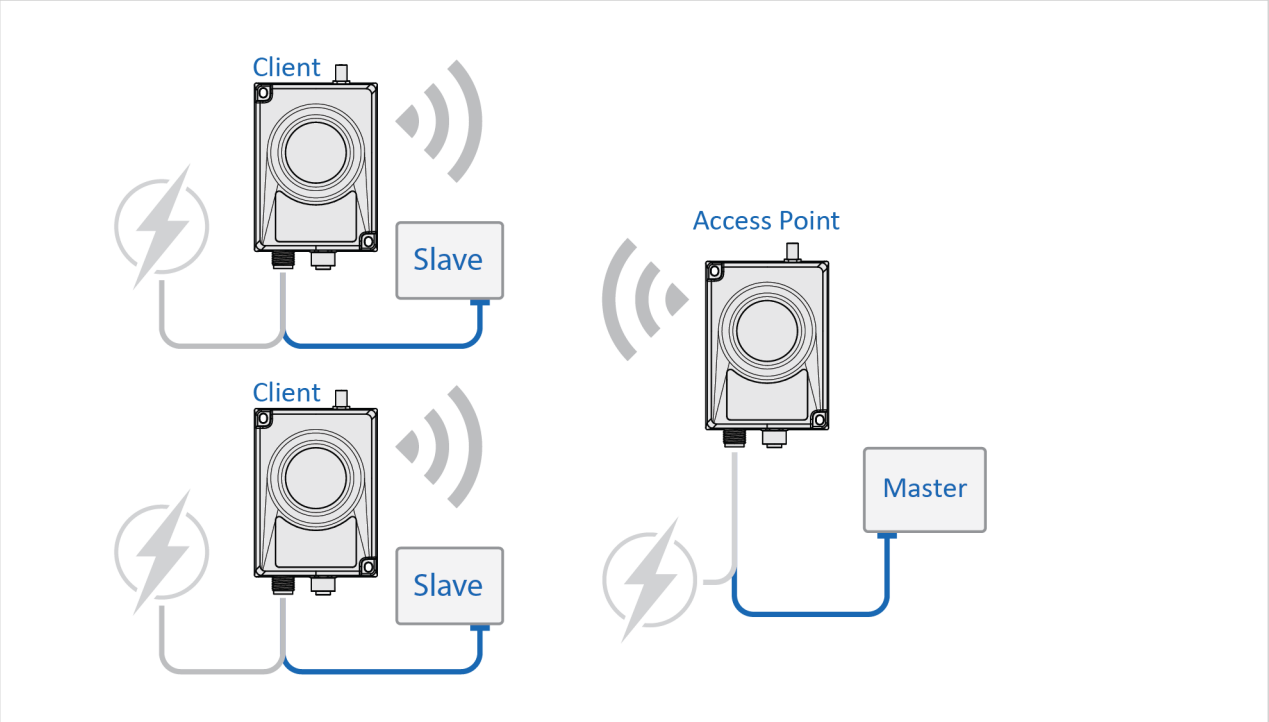


Figure 34. Installing Multiple Bridge II Serial

When installing more than one Bridge II Serial in the network infrastructure, configure the unit connected to the:

- Master device as the Access Point (AP).
- Slave as a Client.

7.3. Set Up Wireless Infrastructure

Connect two or more Bridge II Serial units via WLAN or Bluetooth using Easy Config.

Procedure

Connecting the Devices

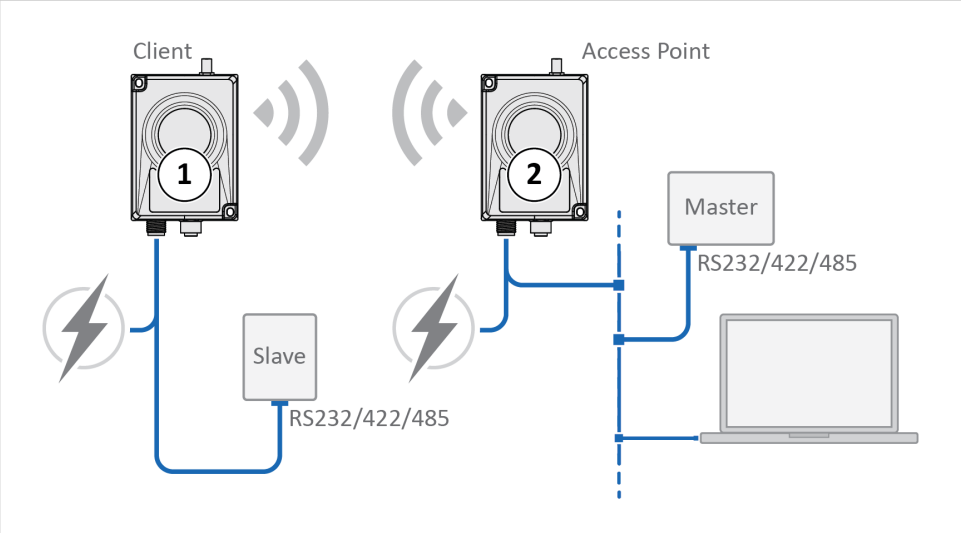


Figure 35. Serial bridge

1. Connect Client 1 to a Slave serial device. See also Connect to LAN, Serial and Power (page 9).
2. Connect Access Point 2 to the Master device.
3. Connect Access Point 2 to your PC, with an Ethernet cable.
4. Connect Access Point 2 to power.

Activate Easy Config

1. Navigate to the web interface of Access Point 2.
   The default address to Access Point unit 2 is 192.168.0.99.
2. Activate one of the following Easy Config Modes:

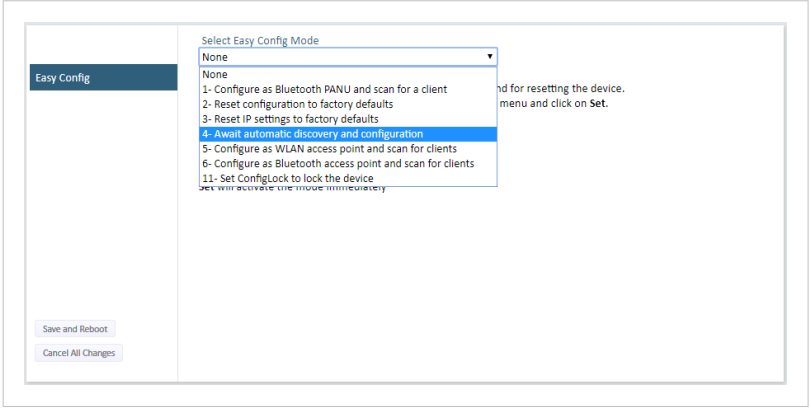


Figure 36. Easy Config modes menu

- 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 1 to power.
4. Automatic configuration of the units starts:
   - Client 1 starts up in Easy Config Mode 4 and is open for automatic configuration during 120 seconds.
   - Access Point 2 will discover and configure Client 1 as a Client and configure itself as an Access Point.
   - Client 1 will be assigned the first free IP address in the same Ethernet subnet as Access Point 2. The default address to Client 1 is 192.168.0.100.

Troubleshooting if no connection is established during Easy Config Mode

- Ensure that Client 1 is disconnected from Ethernet.
- Disconnect Client 1 from power and repeat the steps to activate Easy Config.

Add Additional Bridge II Serial Clients

Option when using Easy Config Mode 1: Continue with the configuration, see Serial Configuration (page 51).

Option when using Easy Config Mode 5 or 6: You can add up to 6 additional Bridge II Serial Clients to the serial bridge.

To add additional Clients:

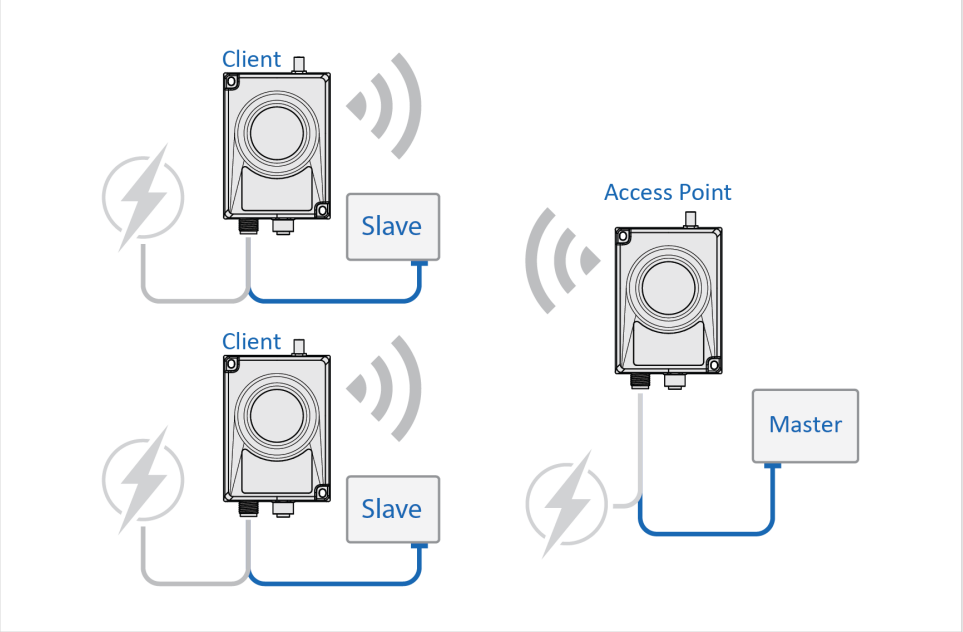


Figure 37. Serial bridge

1. Connect the Client to a serial device.
2. Automatic configuration of the Client starts.
   The Client will be assigned the next free IP address in the current Ethernet subnet.
3. To add more Clients, repeat step 1 and 2.

Serial Configuration

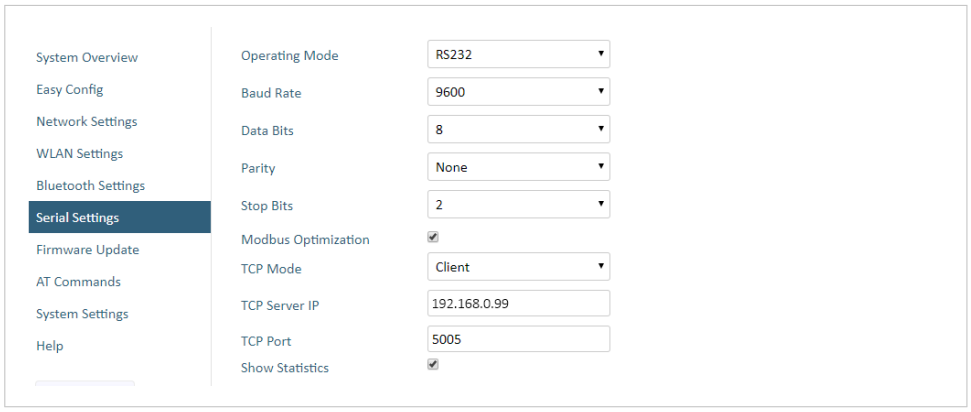


Figure 38. Serial port settings example

1. From the PC connected to Access Point 2, navigate to the built-in web interface of each Bridge II Serial Client.
2. Select the **Serial Settings** tab.
3. Configure the serial port settings, see Set Up Serial Communication (page 39).

7.4. Installing on a Modbus Network

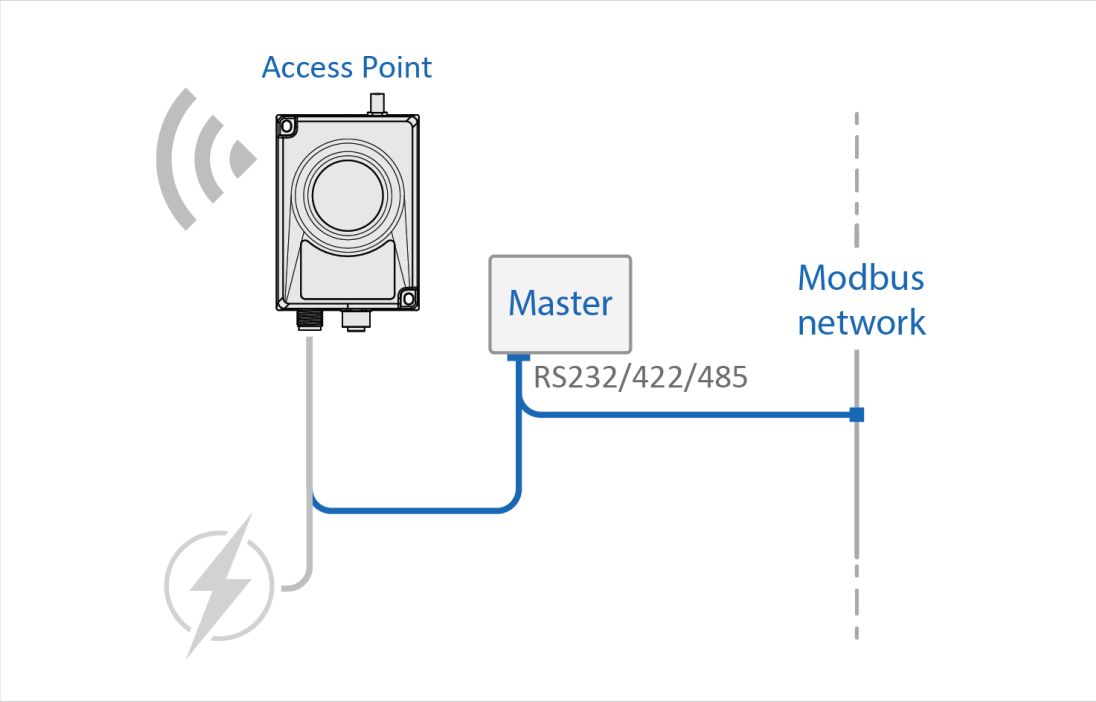


Figure 39. Access Point on Modbus network

When installing on a Modbus network, configure the Bridge II Serial connected to the:

- Master device as the Wireless Access point (AP).
- Slave as a Wireless Client.

Modbus Optimization:

- In the Bridge II Serial Access Point built-in web interface **Serial Settings** page, select the **Modbus Optimization** checkbox.

7.5. Installing Using the Modbus TCP to RTU Gateway Function

The gateway function is transparent. When a command is sent on Modbus TCP it is translated to Modbus RTU. The response is translated back to Modbus TCP and delivered to the Modbus TCP Client.

It is possible to connect Bridge II Serial to a pre-existing wireless infrastructure, such as the wireless network in a production facility.

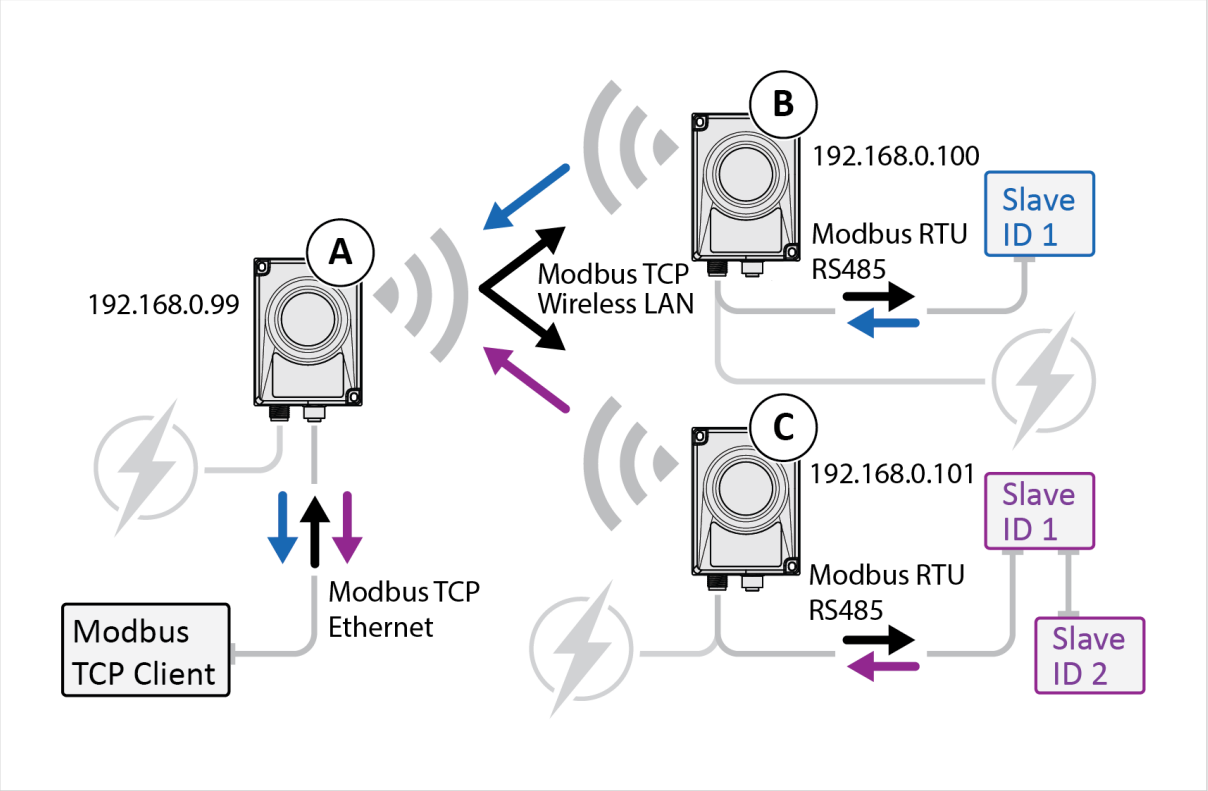


Figure 40. Serial bridge, Modbus RTU to RTU Gateway function

Bridge II Serial Access Point Unit

- Configure **Bridge II Serial A**, with IP address 192.168.0.99, connected to the Modbus TCP Client as the Access Point (AP) or Network Access Point (NAP).

Connect the Modbus RTU Slaves

The Modbus RTU Slaves are all Modbus Servers.

- One of the Modbus RTU Slaves is connected to **Bridge II Serial B** with IP address 192.168.0.100.
- The other Modbus RTU Slaves are connected to **Bridge II Serial C** with IP address 192.168.0.101.

Modbus TCP Client Configuration

Configure the **Modbus TCP Client** to access the correct Modbus Slave:

- **Slave ID 1** connected to **Bridge II Serial B**:
  IP address 192.168.0.100 and unit identifier 1.
- **Slave ID 1** connected to **Bridge II Serial C**:
  IP address 192.168.0.101 and unit identifier 1.
- **Slave ID 2** connected to **Bridge II Serial C**:
  IP address 192.168.0.101 and unit identifier 2.

7.6. Bridge II Serial TCP/IP Socket Protocol Description

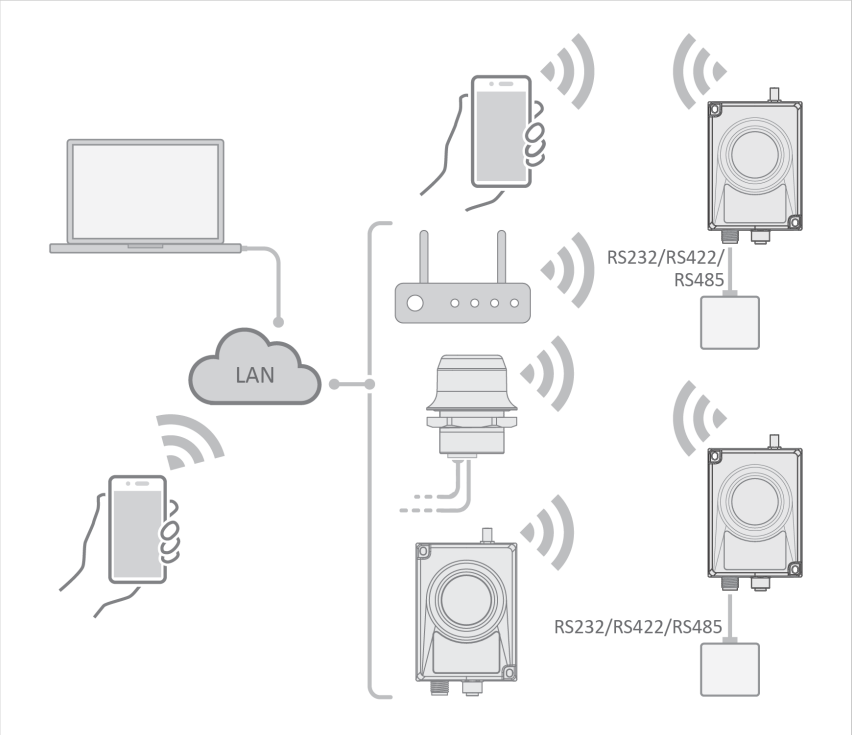


Figure 41. Bridge data to the Bridge II Serial port

The Bridge II Serial may communicate with raw TCP/IP traffic and bridge the data to RS232, RS422 or RS485 on the serial port.

The Bridge II Serial 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.

Using a virtual COM port (VCP) driver is also supported. Use a COM port redirector software that supports raw TCP/IP to enable wireless access to the devices over the network.

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 Bridge II Serial.
     Use the configured TCP port number (default 5005).
     Up to 7 active sockets are supported simultaneously.
   - Configure the Bridge II Serial as a TCP Client to connect to a specific IP.

Result

- Serial payload data can now be sent as is via the TCP socket to the Bridge II Serial and transparently forwarded to the serial port.
- Incoming data from the serial port is forwarded transparently to all open TCP sockets.

8. Maintenance

8.1. Settings Backup

8.1.1. Create Settings Backup File

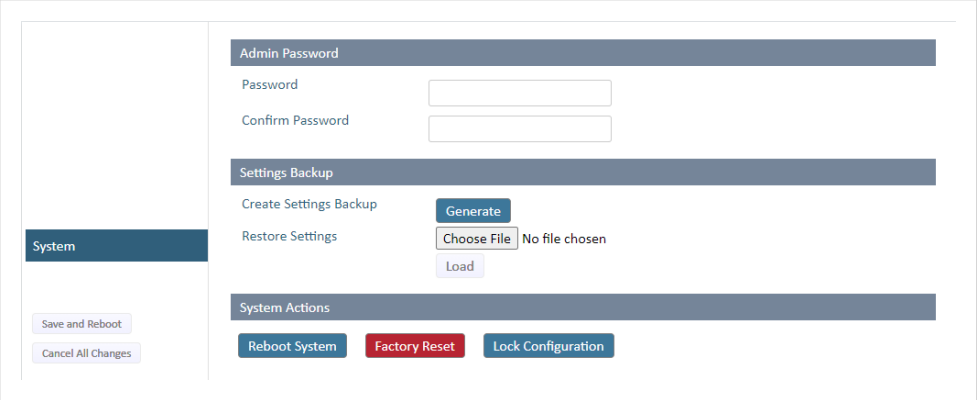


Figure 42. System page

Create Settings Backup

- To save the current configuration in a backup file, click **Generate**.
  A backup file is automatically downloaded and saved in the Downloads folder on your PC.

8.1.2. Restore Settings From Backup File

IMPORTANT
When you restore settings from a backup file, all the current settings are overwritten by the settings loaded from the backup file.

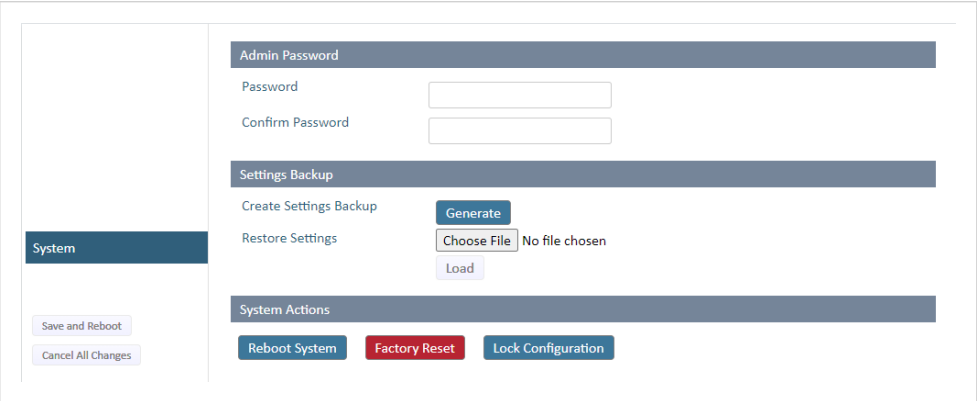


Figure 43. Restore Settings from a backup file

Restore settings from a backup file

1. Click **Choose** file.
2. Browse to and select your backup file.
3. Click **Load**.
   The Bridge II Serial reboot automatically, for the settings loaded from the backup file to take effect.

9. Troubleshooting

9.1. Recovery Mode

If the built-in web interface cannot be accessed, the unit can be reset by starting in Recovery Mode and reinstalling the firmware.

Before You Begin

IMPORTANT
Use Recovery Mode only when the unit is unresponsive and the built-in web interface cannot be accessed. Firmware updates should normally be carried out through the built-in web interface.

Procedure

To enter Recovery Mode

1. Press and hold **MODE** button during startup.

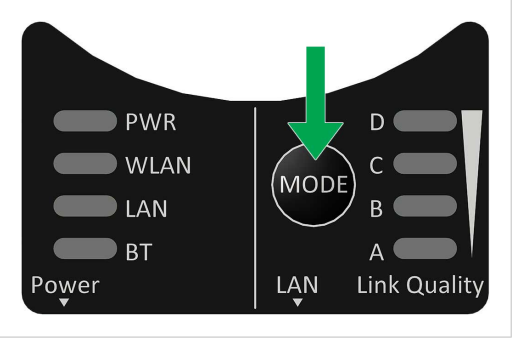


Figure 44. **MODE** button

2. Bridge II Serial enters Recovery Mode.

Table 10. In Recovery Mode the Status LEDs indicate the firmware update status

LED	Indication	Description
PWR	Green	Firmware update in progress
	Green, blinking	Waiting for valid firmware
WLAN + **BT**	Alternating red/blue	Firmware update in progress

To Reinstalling the Firmware

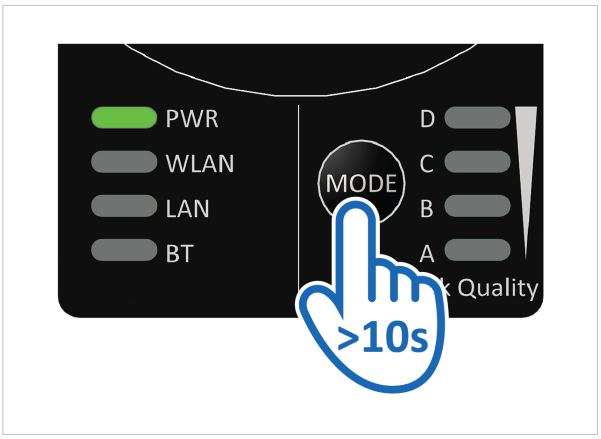
1. To reinstalling the firmware, you need Anybus Firmware Manager II.
   Download Anybus Firmware Manager II from www.anybus.com/support.
2. Install Anybus Firmware Manager II on your PC.
3. Launch Anybus Firmware Manager II and follow the instructions to reinstall the firmware.

9.2. Reset to Factory Default

IMPORTANT
If there is no Ethernet connection available after a factory reset, the Bridge II Serial starts in the default Easy Config Mode 4.

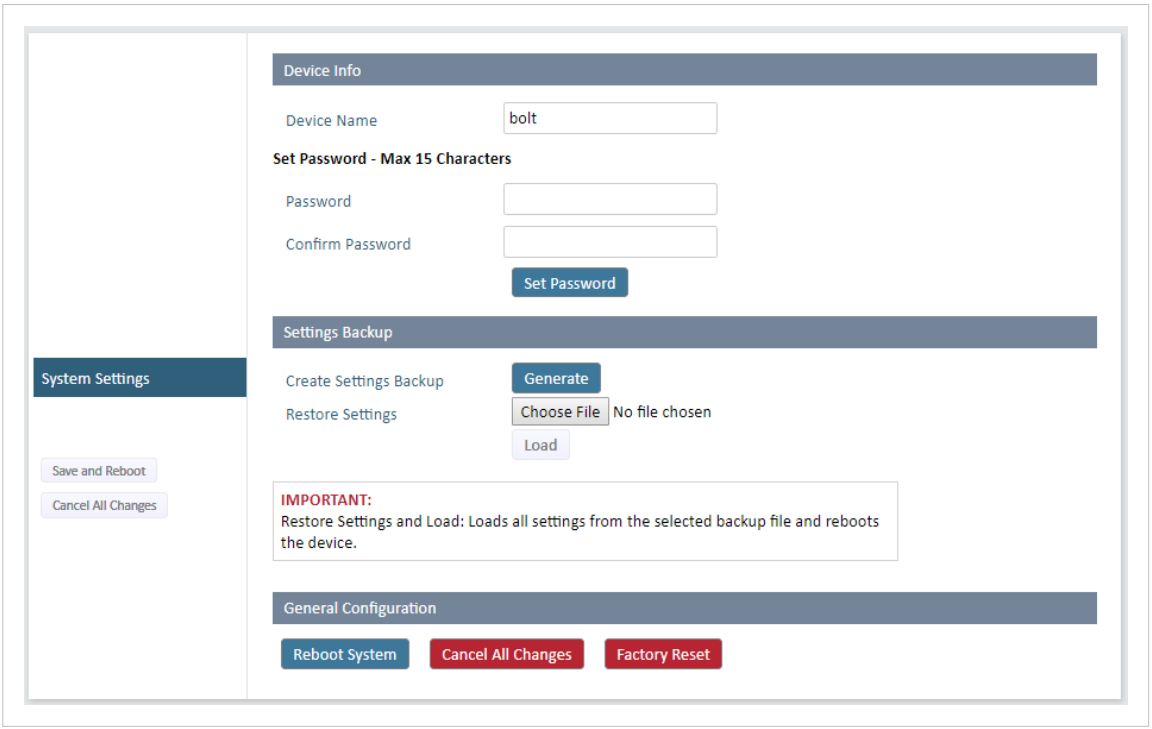
Any one of these actions will restore the unit to factory default settings.

Reset Using the MODE Button



To reset Bridge II Serial to factory default, press and hold **MODE** for >10 seconds and then release it.

Reset Via the Built-In Web Interface



Launch the built-in web interface > On the **System Settings** page, click **Factory Restore**.

Reset Using Easy Config

To reset Bridge II Serial to factory default, execute Easy Config Mode 2.

See Activate an Easy Config Mode in the Built-In Web Interface (page 18).

Reset Using AT Command

To reset Bridge II Serial to factory default, issue the AT command **AT&F** and then restart the unit.

See Configuration with AT Commands (page 25).

10. Technical Data

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

10.1. Technical Specifications

Order Code	AWB3005	AWB3015
Serial interface	Serial: RS232/RS422/RS485 Baud rate: 2400 - 921600 bit/s Data bits 5-8, stop bits 1-2, parity None, Odd, Even. Transparent serial protocol transfer including support for Modbus-RTU and Modbus-TCP to Modbus-RTU transparent routing.	
Ethernet interface	Ethernet: 10/100BASE-T with automatic MDI/MDIX auto cross-over detection. For configuration only.	
WiFi interface	Wireless standards: IEEE 802.11 a, b, g, n, d. Operation modes: Access Point or Client Wireless LAN bands: 2.4 GHz and 5 GHz RF output power: 18 dBm EIRP (including antenna gain 3 dBi) Max number of Clients 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.	
Bluetooth interface	Wireless standards (profiles): PANU & NAP Operation modes: Access Point or Client RF output power: 14 dBm EIRP (including antenna gain 3 dBi) Bluetooth conducted sensitivity: -90 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	
Dimensions	93 x 68 x 33 mm (H•W•D)	
Weight	120 g or 0,26 lbs	
Temperature	Operating: -30 to +65 °C (-22 to +149 °F) Storage: -40 to +85 °C (-40 to +185°F)	
Output power	WiFi 18 dBm EIRP - Bluetooth 14 dBm EIRP - Bluetooth Low Energy 10 dBm EIRP All including antenna gain 3dBi	
Power supply	9-30 VDC (-5% +20%), Cranking 12 V (ISO 7637-2:2011 pulse 4). Reverse polarity protection.	
Power consumption	0.7 W idle, 1.7 W max (54mA@24VDC with Wireless LAN and 36mA@24VDC with Bluetooth)	
Enclosure material	Plastic PC/ABS (Bayblend FR3010)	
Mechanical rating	IP65	
Mounting	Two screws (Ø 4 mm) on flat surface. DIN rail mount option available (optional accessory).	
Max range	400 meters	
Antennas	Three internal antennas: 1. 2.4 GHz 2. 2,4 GHz MIMO 3. 5 GHz	One external antenna: 1. 2,4/5 GHz dual band
	The external antenna does not provide better range but allows connectivity if the Wireless Bridge needs to be placed inside a radio-secure environment such as a steel cabinet. When mounting inside a steel cabinet antenna cables with magnetic foot or screw mount should also be considered.	
Connectors	1x M12 for Ethernet (4-pin, D-coded) 1x M12 for Power + Serial 5-pin, A-coded	1x M12 for Ethernet (4-pin, D-coded) 1x M12 for Power + Serial 5-pin, A-coded

Order Code	AWB3005	AWB3015
		RP-SMA antenna connector for external antenna variant
Vibration compatibility	Sinusoidal 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 axis, Velocity: 1 oct/min, Mode: in operation, Frequency: 5-500 Hz. 5-8,4Hz=±3.5mm; 8,4-40,7Hz=1g; 40,7-57Hz=±0,15mm;57-500Hz=2g. Shock test according to IEC 60068-2-27:2008 and with extra severities; Wave shape: half sine, Number of shocks: ±3 in each axis, Mode: In operation, Axes ± X,Y,Z, Acceleration: 30 m/s2 , Duration: 11 ms.	

Region	Certifications
Europe	CE, 2014/53/EU Radio Equipment Directive (RED)
USA	FCC 47 CFR part 15, subpart B. UL: Ind. Cont. Eq. UL file: E214107
Canada	ICES-003
Japan	MIC

11. Reference Guides

11.1. RS232/RS422/RS485 Electrical Connection

NOTE
A and B marking differs between different devices, in this product A is TX-/RX- or D- and B is TX+/RX+ or D+.

RS232 Typical Connection

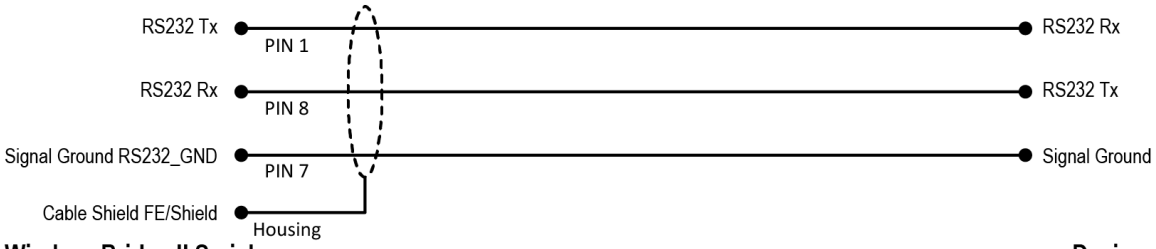


Figure 45. RS232 Typical Connection

RS422 Typical Connection

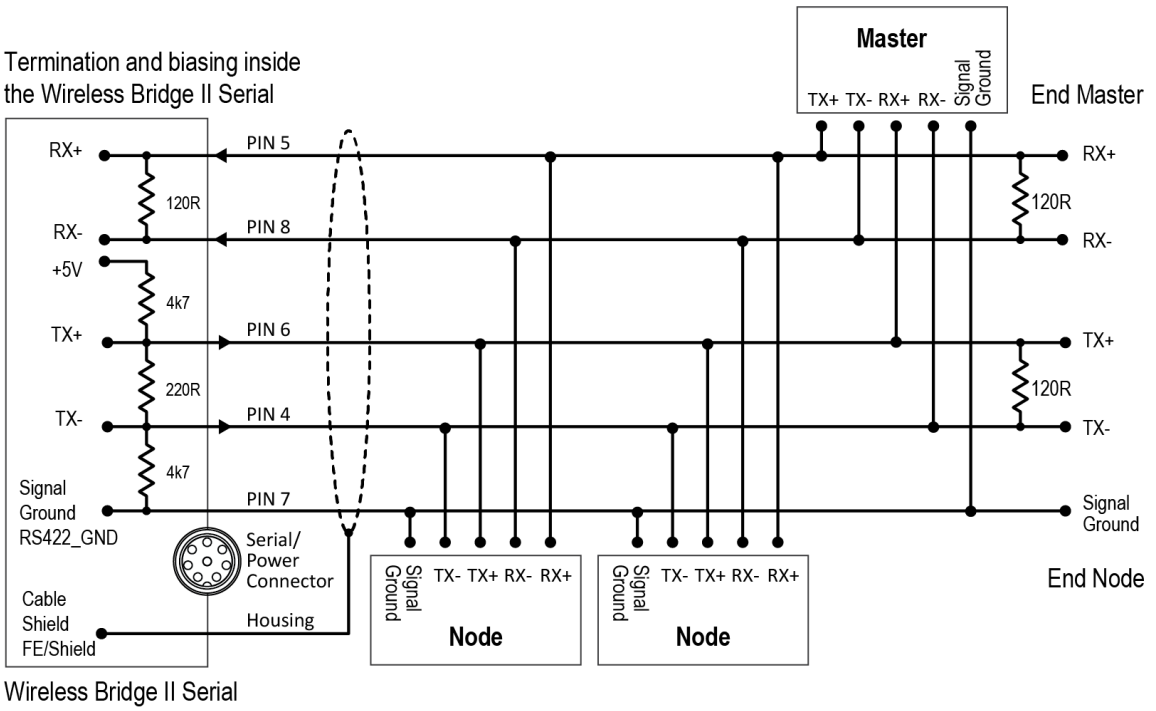


Figure 46. RS422 Typical Connection

RS485 Typical Connection

NOTE
The resistors on the Bridge II Serial side are termination resistors which form an active termination of the RS485 line.

NOTE
Termination and biasing are inside the Bridge II Serial.

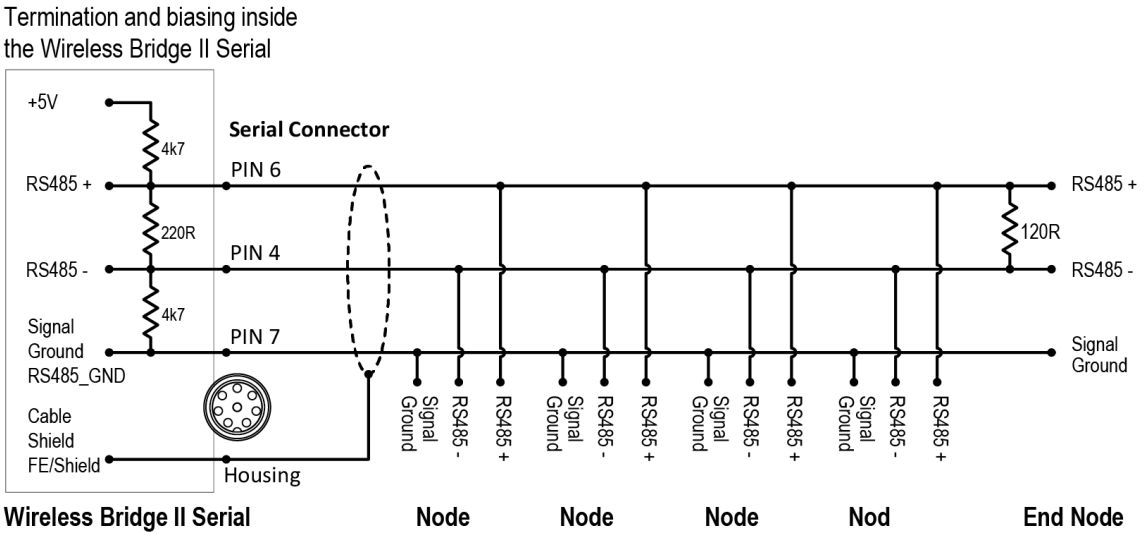


Figure 47. RS485 Typical Connection

11.2. 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.

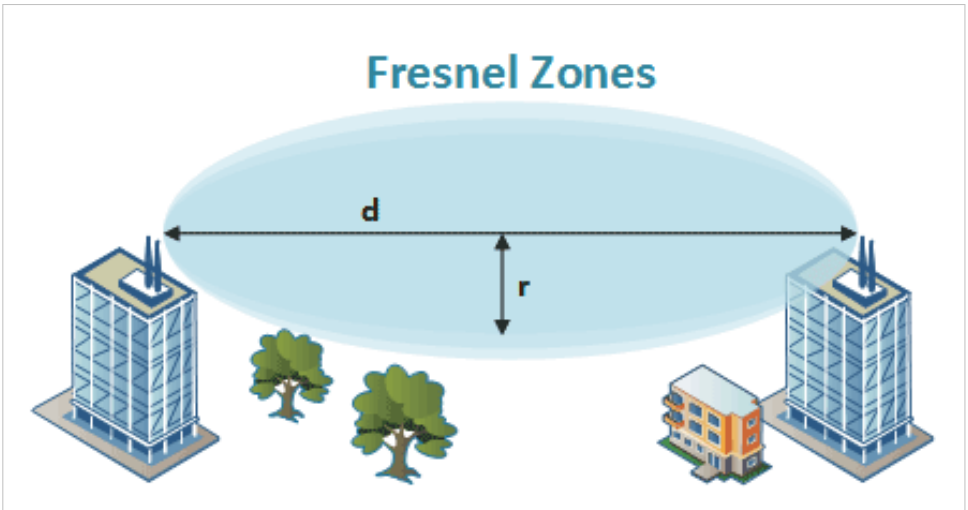


Figure 48. Fresnel zones

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.

11.3. Internal Antenna Characteristics

11.3.1. Internal Antenna Positions

Bridge II Serial has three independent quarter wave monopole antennas:

- 2.4 GHz MIMO
- 5 GHz
- 2.4 GHz

If using the unit in Bluetooth mode, the 2.4 GHz antenna is used.

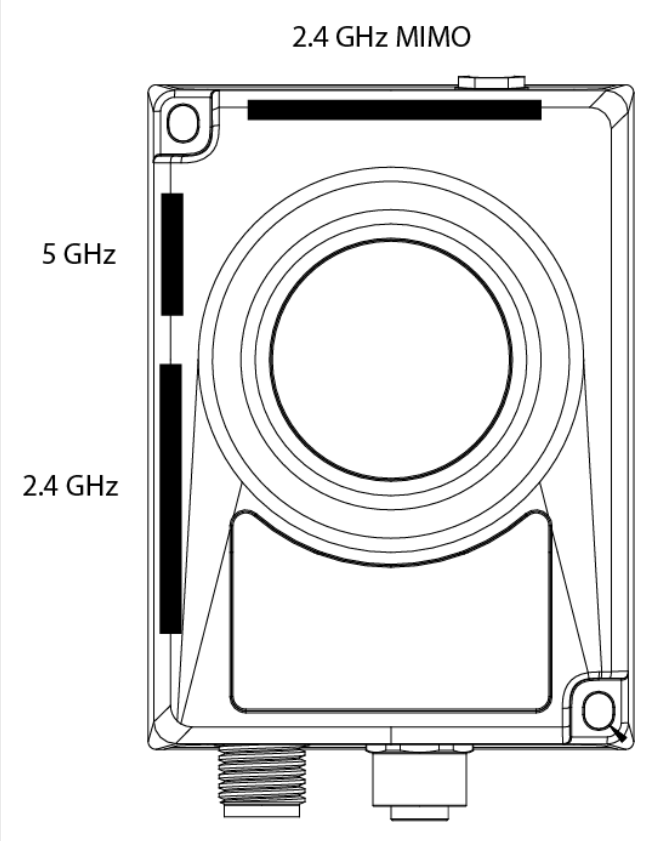
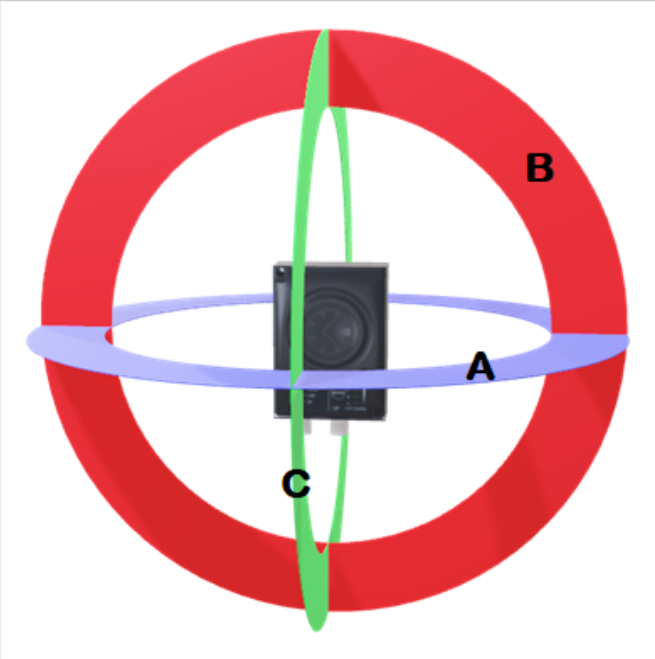


Figure 49. Placement of the three antennas in the unit

11.3.2. Lab Environment Diagrams

This topic describe the radiation measurements in different angles.



A. Azimuth plane is the horizontal spread of the radiation
B. Elevation 90° is the vertical expansion
C. Elevation 0° is the front to back expansion

The radiation diagrams show the characteristics of the different antennas as measured under laboratory test conditions.

Use the diagrams as a general guide for finding the optimal placement and orientation of the units.

The diagrams show decibel (dB) relative to the Bridge II Serial theoretical maximum signal strength.

The 2.4 MIMO diagrams show the WLAN usage using both the 2.4 GHz antennas simultaneously (the 2.4 GHz antenna and the 2.4 GHz MIMO antenna).

Azimuth (Horisontal) View

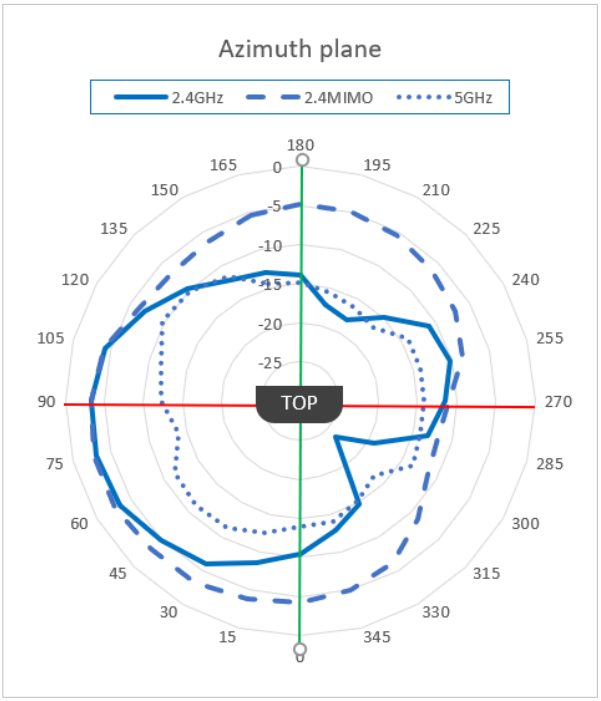


Figure 50. Azimuth plane

Front View – Elevation (Vertical)

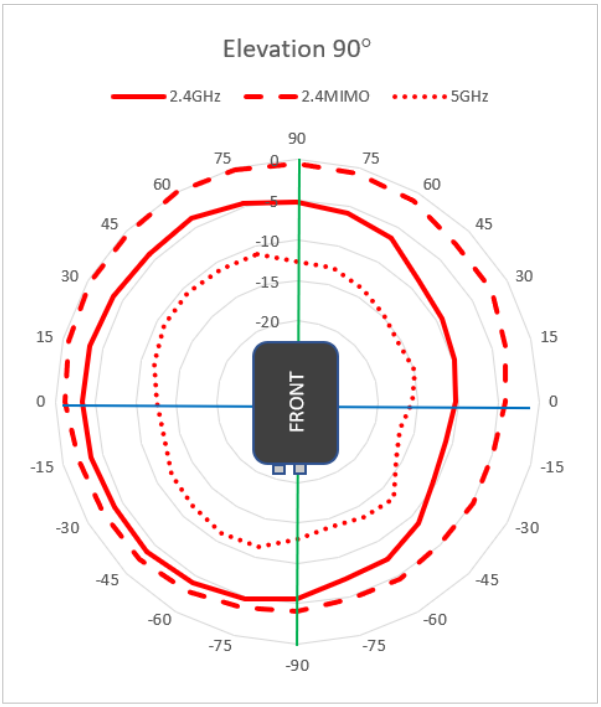


Figure 51. Elevation 90°

Side View – Elevation (Vertical)

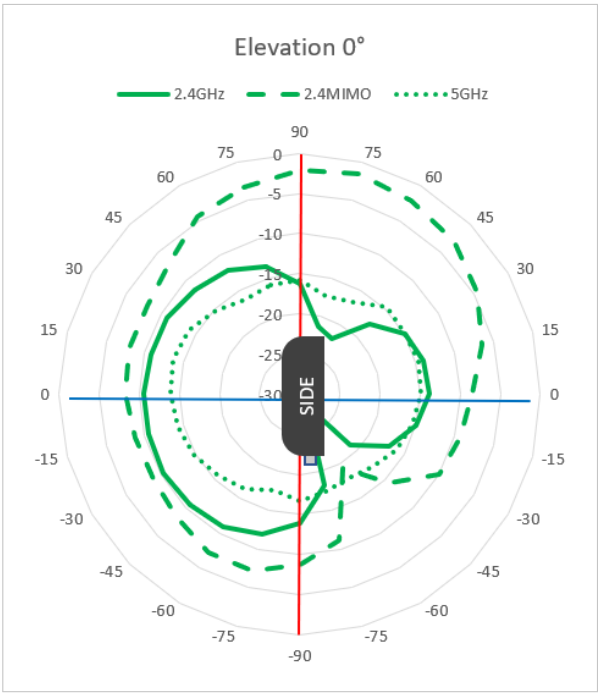


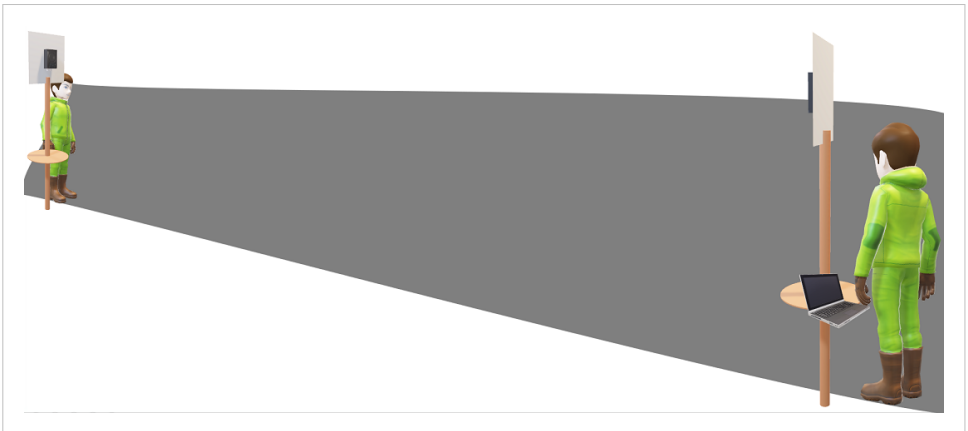
Figure 52. Elevation 0°

11.3.3. Real World Measurements

Azimuth (Horisontal) View with and without Back Shield

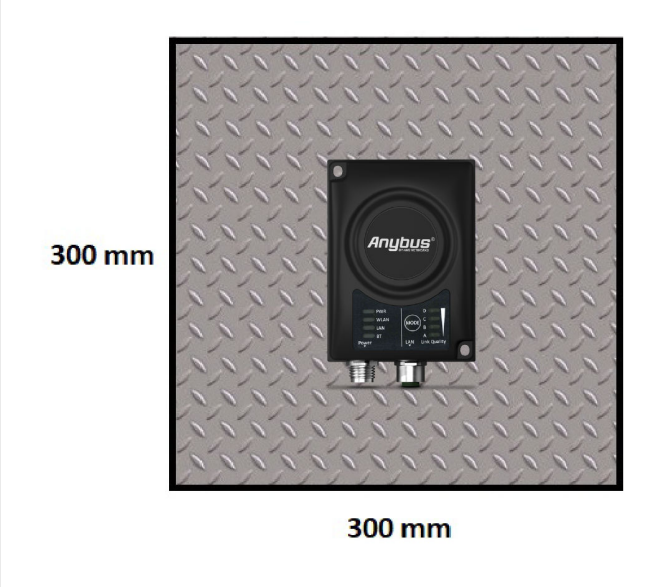
This pattern was measured in an outdoor environment, on an open field with no disturbing equipment or radiation.

As such it describes how the radio coverage can vary in a real world application.



The measurements were set up according to the graphic

Figure 53. Measurements set up



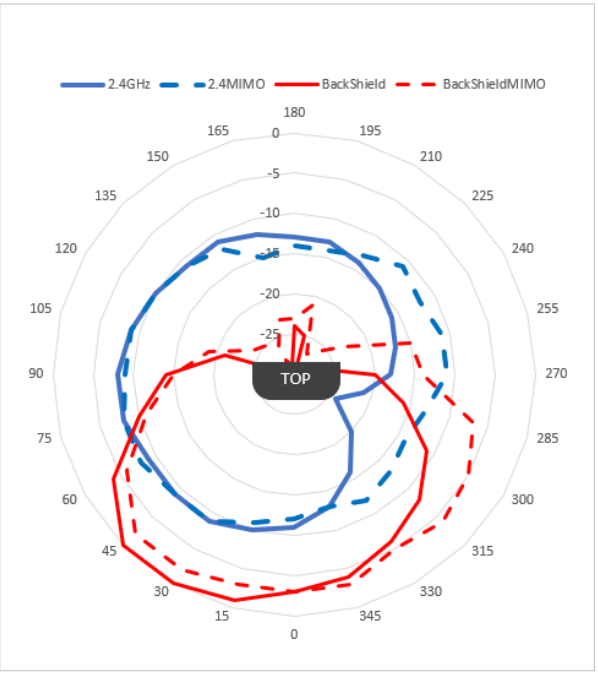
In this example, the measurements are made both with and without back shield.

A back shield is a metal surface of at least 300x300 mm.

The Bridge II Serial is placed in the center of the back shield.

The back shield could be any flat metal surface, like a metal plate or a metal cabinet.

Figure 54. Back shield



The measurements with back shield clearly shows that the back shield makes it possible to focus the radio energy in any desired direction (away from the back shield).

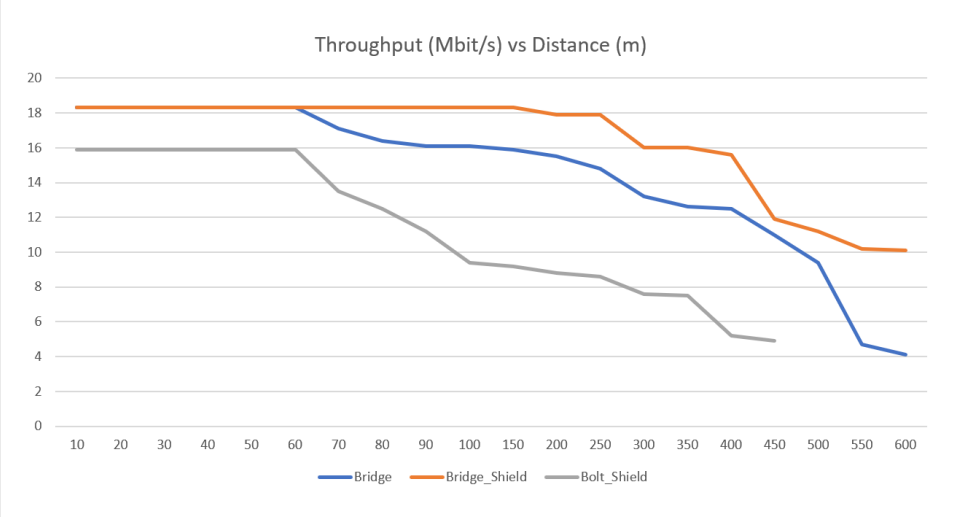
Figure 55. Measurements with and without back shield

Throughput Diagram

The diagram shows how data throughput decreases as the distance increases.

Note the huge difference between using a back shield to focus the radio energy, and not using a back shield.

Used properly, a back shield can significantly increase radio coverage.



The diagram covers both the Anybus Wireless Bridge and the Anybus Wireless Bolt.

Figure 56. Throughput diagram

This page is intentionally left blank.

This page is intentionally left blank.