Anybus® Wireless Bridge

Ethernet–WLAN

USER MANUAL

HMSI-27-205 2.5 ENGLISH

HMS Connecting Devices™

Important User Information

Liability

Every care has been taken in the preparation of this document. Please inform HMS Industrial Networks AB of any inaccuracies or omissions. The data and illustrations found in this document are not binding. We, HMS Industrial Networks AB, reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be considered as a commitment by HMS Industrial Networks AB. HMS Industrial Networks AB assumes no responsibility for any errors that may appear in this document.

There are many applications of this product. Those responsible for the use of this device must ensure that all the necessary steps have been taken to verify that the applications meet all performance and safety requirements including any applicable laws, regulations, codes, and standards.

HMS Industrial Networks AB will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features, timing, or functional side effects found outside the documented scope of this 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.

The examples and illustrations in this document are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks AB cannot assume responsibility for actual use based on these examples and illustrations.

Intellectual Property Rights

HMS Industrial Networks AB has intellectual property rights relating to technology embodied in the product described in this document. These intellectual property rights may include patents and pending patent applications in the USA and other countries.

Trademark Acknowledgements

Anybus® is a registered trademark of HMS Industrial Networks AB. All other trademarks are the property of their respective holders.

Table of Contents

Page

This page intentionally left blank

1 About This Document

This manual describes how to install and configure the Anybus Wireless Bridge Ethernet to WLAN 2.4 GHz, 5 GHz, and Dual-band models.

For additional related documentation and file downloads, please visit the support website at www.anybus.com/support.

1.1 Document history

Summary of recent changes

Change	Where (section no.)
Added info about Telnet access	*4.1*
Fixed typos etc.	—

Revision list

Version	Date	Author	Description
1.00	2011-03-22	KaD	First released version
1.10	2012-04-20	KaD	Converted to FrameMaker, minor updates and corrections
1.20	2013-10-09	SDa	Added safety warnings
1.30	2015-02-19	KeL	Removed section 3.13
2.0, 2.1	2016-01-25	ThN	Not released
2.2	2016-03-07	ThN	Major rewrite, new structure and layout
2.3	2016-05-02	ThN	Updated compliance information
2.4	2016-06-15	ThN	Minor corrections Updated compliance information
2.5	2016-07-14	ThN	Minor update

1.2 Conventions

Unordered (bulleted) lists are used for:

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

Ordered (numbered or alphabetized) lists are used for instructions that must be carried out in sequence:

1. First do this,
2. Then open this dialog, and
   a. set this option...
   b. ...and then this one.

Bold typeface indicates interactive parts such as connectors and switches on the hardware, or menus and buttons in a graphical user interface.

```
Monospaced text is used to indicate program code and other
kinds of data input/output such as configuration scripts.
```

This is a cross-reference within this document: *Conventions, p. 4*

This is an external link (URL): www.hms-networks.com

This is additional information which may facilitate installation and/or operation.

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

Caution
This instruction must be followed to avoid a risk of personal injury.

WARNING
This instruction must be followed to avoid a risk of death or serious injury.

2 Product Description

2.1 LED Indicators

2.1.1 Status LED Indicators

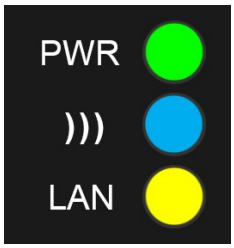

Fig. 1 Status LED indicators

LED Indication		Meaning
PWR	OFF	No power or no application running
	Steady Green	Unit has power and application is running
)))	OFF	No wireless activity
	Steady Blue	A wireless connection has been established
	Flashing Blue	Wireless data activity
	Steady Purple	Attempting to establish a wireless connection
	Steady Red	Wireless connection error
LAN	OFF	No Ethernet connection
	Steady Yellow	Ethernet link is present
	Flashing Yellow	Ethernet data activity

2.1.2 A-B-C-D LED Indicators

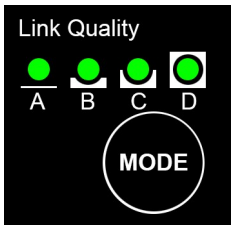

Fig. 2 A-B-C-D LED indicators

When the Anybus Wireless Bridge is operating in infrastructure mode, pressing **MODE** briefly will make the Link Quality LEDs indicate the quality of the wireless signal. In ad-hoc mode, link quality is not indicated. All 4 LEDs lit = excellent signal quality.

Keeping the MODE button pressed for more than 5 seconds will reboot the unit.

2.2 WLAN Network Modes

WLAN networking can be set up in two basic connection modes:

Infrastructure (managed) mode

Used when wireless devices connect through a WLAN access point.

In infrastructure mode, all transmission speeds and encryption and authentication methods supported by the hardware can be used, i.e. the maximum throughput will be 14 Mbit/s.

Ad-hoc mode

Used when wireless devices connect directly to each other without a WLAN access point.

Ad-hoc mode only allows 802.11b transmission, i.e. the maximum throughput will be 11 Mbit/s. Only WEP encryption is supported.

> **!** Ad-hoc connections between a Wireless Bridge and a Windows computer may be unstable and are normally not recommended.

2.3 Wireless Bridge Operating Modes

The Anybus Wireless Bridge has three main operating modes:

UDP Tunnel Mode

In this mode, which is supported only between two Wireless Bridges, the Ethernet packages are encapsulated in UDP packages and transferred transparently between the two units. Devices on both sides of the wireless link are completely unaware of the wireless connection.

UDP Tunnel mode will introduce an extra overhead because of the encapsulation and will therefore have a significantly lower throughput than the other modes.

Single Client Mode

In this mode the Wireless Bridge acts as a wireless interface for the Ethernet device it is connected to. The Wireless Bridge is configured to take over (clone) the MAC address of the connected device. This means that only a single Ethernet device can be connected to each Wireless Bridge – not an Ethernet network with multiple devices connected through a switch or hub.

In Single Client Mode, the Wireless Bridge cannot be accessed over the WLAN interface. However, if the Ethernet link is lost, the unit will temporarily enter *Multiclient Mode* and can then be accessed again. When the Ethernet link is re-established, the Wireless Bridge will revert to Single Client Mode.

Multiclient Mode

Same as Single Client mode but allowing multiple devices to communicate on the IP layer.

2.4 WLAN Security

The following combinations of authentication and encryption methods are supported:

	Open Connection	Shared Secret	WPA/WPA2 PSK	LEAP	PEAP
No encryption	x				
WEP 64	x	x			
WEP 128	x	x		x	
TKIP			x (WPA)	x	x
AES/CCMP			x (WPA2)	x	x

- WPA/WPA2 PSK with TKIP encryption is considered a WPA connection.
- WPA/WPA2 PSK with AES/CCMP is considered a WPA2 connection.
- WPA with AES/CCMP encryption is not possible.
- Not all access points will support LEAP or PEAP as the authentication algorithm.
- Neither LEAP, PEAP nor WPA/WPA2 PSK will work in ad-hoc mode.

Some access points have support for a combination of WPA and WPA2, as well as AES/CCMP and TKIP. These options are not supported by the Wireless Bridge.

2.4.1 Key Management

For WEP 64 and WEP 128, shared keys can be entered in all four possible slots made available by the `AT*AGFPWI` Write Encryption/Authentication Key (with Index) command. However, for LEAP, PEAP and WPA/WPA2 PSK, the password or PSK must be entered in the key slot with index 1 (one). This key must also be the one currently set as active by the `AT*AGAFP` Active Encryption/Authentication Key command.

If using LEAP or PEAP, the username for the Radius server should be entered with the command `AT*AGUN`, and the domain with command `AT*AGDN`. For PEAP, the certificate must also be considered. When receiving the certificate from the Radius server, the SHA-1 fingerprint is calculated and stored in the WEPA for future comparisons. If the certificate changes, or if a different Radius server is to be used, the new fingerprint must be entered, or the old must be cleared with the command `AT*AGCFP`.

If using WPA/WPA2 PSK, it is possible to enter either the pre-shared key (hexadecimal string) or the password (plain-text), commonly referred to as “WPA-PSK” or “WPA-PWD”. If a plain-text password is entered, the next connection attempt will take somewhat longer as the real key has to be calculated from the password. The Wireless Bridge will be unresponsive while the key is calculated.

By default, the key is entered as an ASCII string. To enter a hexadecimal key, each byte must be escaped with a backslash (\).

Example: To enter the string “12345” as hexadecimal, enter: `\31\32\33\34\35`.

3 Installation

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

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

Make sure that you have all the necessary information about the capabilities and restrictions of your local network environment before installing the Anybus Wireless Bridge. Contact your network administrator if in doubt.

For optimal reception between units they should be oriented front-to-front with the line of sight between them clear of obstructions. A minimum distance of 50 cm between the devices should be observed to avoid interference.

See also *Wireless Technology Basics, p. 31* and *Internal Antenna Characteristics, p. 33*.

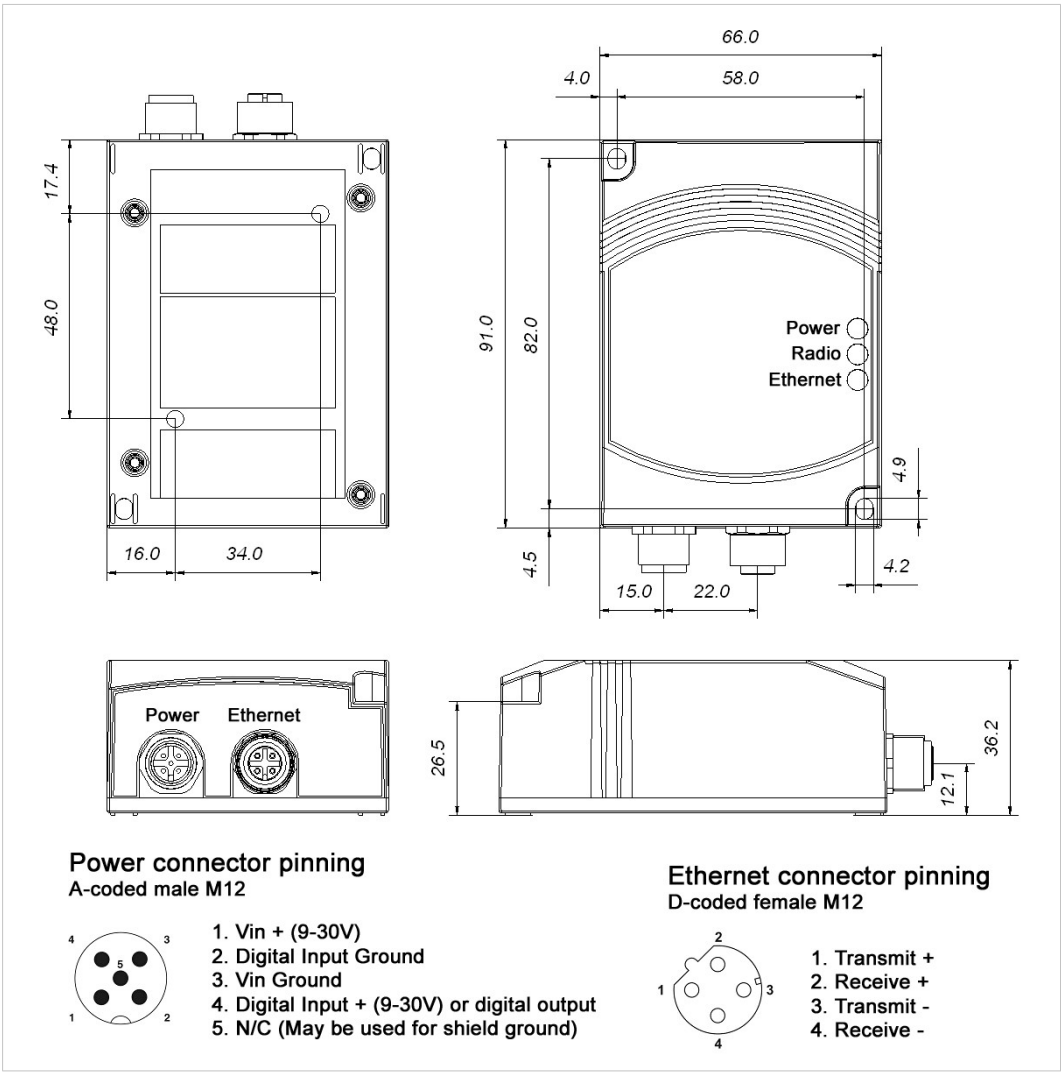

Fig. 3 Installation drawing

4 Startup and Configuration

4.1 Options for Device Configuration

SMART Configuration

Basic use cases can be set up quickly using the **MODE** button and the **A-B-C-D** LEDs to select one of the SMART configuration modes.

See *SMART Configuration, p. 10*.

Web Configuration

The built-in web server gives access to status information and configuration settings via a graphical user interface.

See *Web Configuration, p. 11*.

AT Commands

Advanced configuration can be carried out by issuing AT (Hayes) commands in the **Advanced** section of the web interface or using a Telnet connection to the Wireless Bridge on port 8080.

A list of supported AT commands can be found at www.anybus.com/support.

4.2 Factory Reset

Anybus Wireless Bridge can be reset to the factory default settings in one of the following ways:

- Keeping the **MODE** button pressed while the unit is starting up
- Executing SMART Mode 2 (see *SMART Configuration, p. 10*)
- Issuing the AT command **AT&F** (see *Settings – Advanced View, p. 17*)

Factory Default Settings	
IP Assignment:	Static
IP Address:	192.168.0.98
Subnet Mask:	255.255.0.0
Default Gateway:	192.168.0.98
Web configuration password:	(no password)

See *Web Configuration, p. 11* for information about the default settings of all parameters.

> **!** Do not reset the Anybus Wireless Bridge while a firmware update is in progress.

> **!** As the default password setting is empty (no password), setting a secure password when first configuring the unit is strongly recommended.

4.3 SMART Configuration

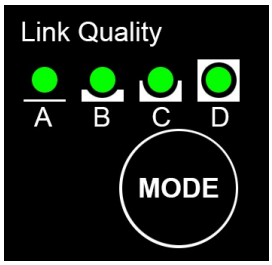

Fig. 4 MODE button and LED indicators

1. Power on the Wireless Bridge, then immediately press and release **MODE**.
2. Press **MODE** repeatedly to cycle through the configuration modes until the desired mode is indicated by the LED combination.
3. Press and hold **MODE** until the LEDs go out or blink, then release the button. The unit will restart with the selected configuration.

If the unit is not restarted within 20 seconds of selecting a configuration mode it will exit SMART configuration and return to the previous settings.

SMART Configuration Modes and LED Indication

SMART	WLAN Mode	Client Mode	Description	LED			
				A	B	C	D
1	—	—	Enable internal DHCP server	●			
2	—	—	Reset to factory defaults		●		
3	—	—	Reset IP settings only	●	●		
4	Ad-hoc	UDP Tunnel	Wait for auto configuration			●	
5	Ad-hoc	UDP Tunnel	Initiate auto configuration	●		●	
6	Ad-hoc	UDP Tunnel	Wait for auto configuration (PROFINET prioritized)		●	●	
7	Ad-hoc	UDP Tunnel	Initiate auto configuration (PROFINET prioritized)	●	●	●	
8	Infrastructure	UDP Tunnel	Wait for auto configuration				●
9	Infrastructure	UDP Tunnel	Initiate auto configuration	●			●
10	Infrastructure	UDP Tunnel	Initiate auto configuration (wired)		●		●
11	Ad-hoc	Single Client	Wait for MAC address	●	●		●
12	Ad-hoc	Multiclient	Initiate automatic configuration			●	●
13			(reserved)	●		●	●
14			(reserved)		●	●	●
15			(reserved)	●	●	●	●

Enable DHCP Server (Mode 1) activates a built-in DHCP server, which makes it possible to access the Wireless Bridge without manually configuring the IP address of the connecting computer. The computer must be set up for DHCP and be connected directly to the unit, not through a network. The DHCP server will stay enabled until the Wireless Bridge is restarted.

4.4 Web Configuration

The web configuration interface can be accessed by entering the IP address of the Anybus Wireless Bridge in any web browser that supports HTML5. The computer used for configuration must be in the same subnet as the Wireless Bridge.

The default IP address is 192.168.0.98.

The initial page (Info page) shows the status and basic settings of the Wireless Bridge. The colors of the **LAN Status** and **WLAN Status** entries correspond to the LED indicators.

Click on **Update Status** to refresh the values once, or on **Auto Update** to make the values refresh every second.

To access the configuration page, click on **Settings** and enter the password to login.

The default password setting is empty (no password). Setting a secure password when first configuring the unit is strongly recommended.

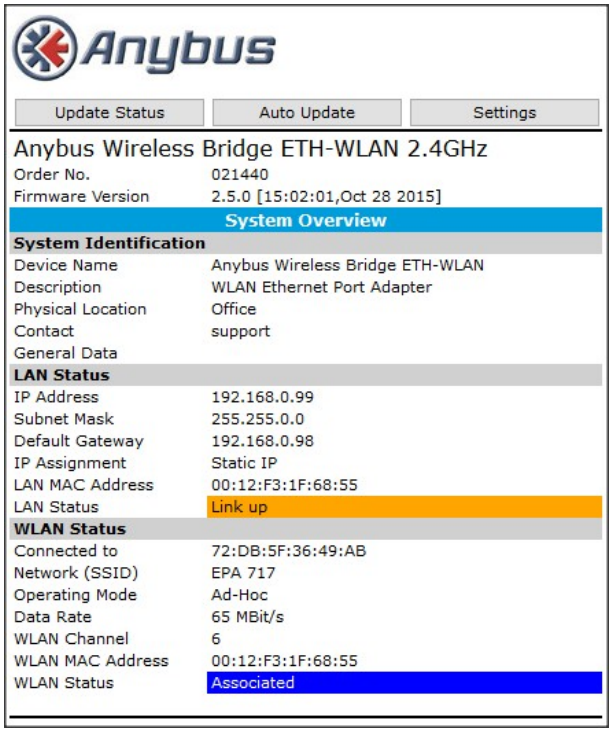

Fig. 5 Status page

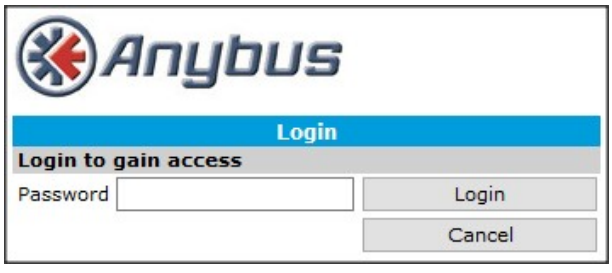

Fig. 6 Login page

4.4.1 Settings – Standard View

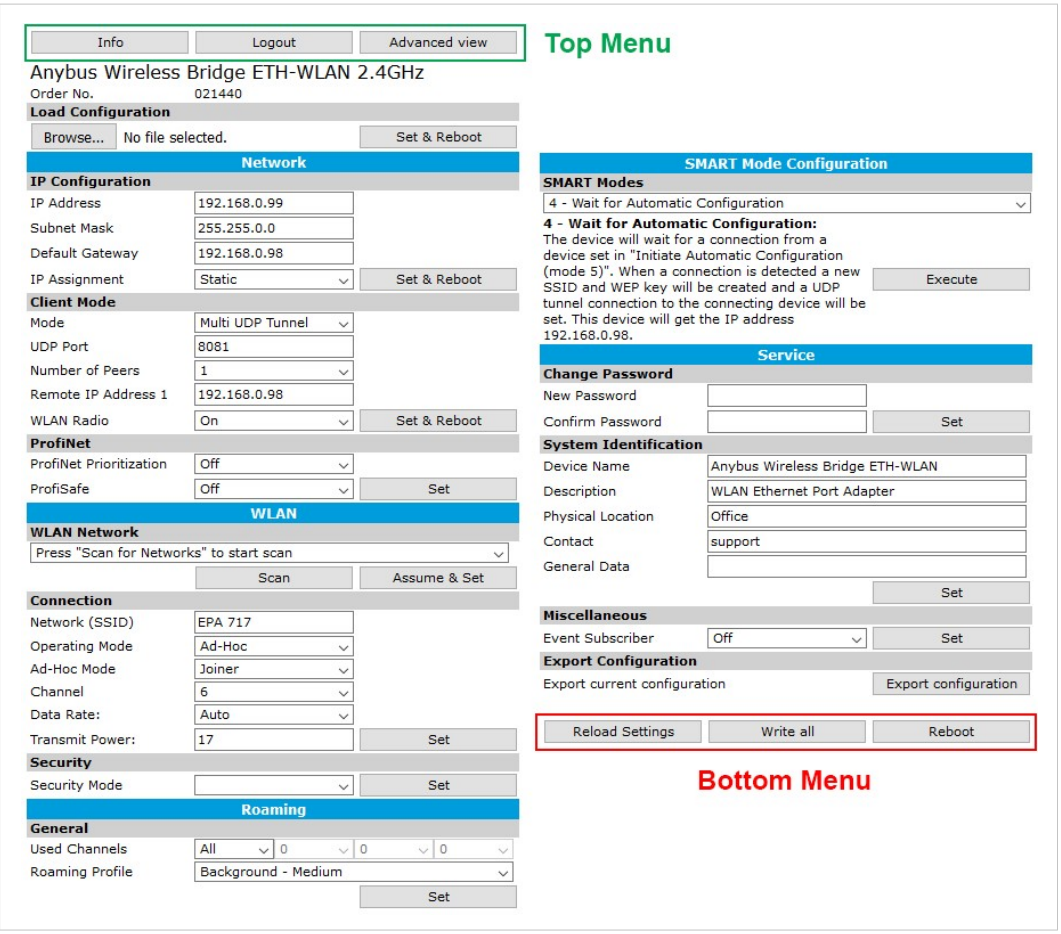

Fig. 7 Standard view

Top Menu	
Info	Return to the Info page but stay logged in.
Logout	Return to the Info page and log out.
Advanced view	Open the Advanced view (see *Settings – Advanced View, p. 17*).

Load Configuration	
Browse	Select a saved configuration file.
Set & Reboot	Apply the configuration and reboot.

Bottom Menu	
Reload Settings	Cancel all changes and reload the current configuration.
Write All	Apply all changed settings to the Anybus Wireless Bridge. This has the same function as clicking on **Set** in each of the different settings sections.
Reboot	Restart the Anybus Wireless Bridge (without applying changes).

Network – IP Configuration

IP Address	The IP address of the Anybus Wireless Bridge. Default: 192.168.0.98
Subnet Mask	Subnet mask. Default: 255.255.0.0
Default Gateway	IP address of the transition point to other network segments. Must also be set when DHCP addressing is used. Default: 192.168.0.98
IP Assignment	**Static** (default): The unit is assigned the IP address set above. **DHCP**: IP configuration settings are retrieved from a DHCP server. **Static & DHCP Server**: The unit is assigned the IP address set in the IP Address field and operates as DHCP server for devices connected to the LAN port.
Set & Reboot	Apply the changes and reboot.

Network – Client Mode

Mode	Operating mode for the LAN connection **Single Client**: Connection with layer 2 transparency – only one device can be connected to the Wireless Bridge. **Multi Client** (default): One device can be connected with layer 2 transparency, the other devices with IP transparency. **UDP/Multi UDP Tunnel**: Connection with layer 2 transparency to multiple devices between two Wireless Bridges.
DHCP Relay (Multi Client)	When acting as DHCP relay, the Anybus Wireless Bridge can process DHCP requests of devices connected on the LAN side via the wireless interface, even if it is in (multi) client mode and uses the MAC address of a connected device.
Device MAC (Single/Multi Client)	Sets the layer 2 device address (MAC) of the WLAN interface. Click on **Scan** to list the MAC addresses of all identifiable devices connected on the LAN side. **EPA MAC** = use the original MAC address of the Anybus Wireless Bridge.
UDP Port (UDP/Multi UDP Tunnel)	Port number for UDP tunnel. Usually, the port number can be used unchanged. All the devices can use the same port number.
Remote IP Address (UDP/Multi UDP Tunnel)	The IP address(es) of the remote peer(s) of the UDP tunnel.
Number of Peers (Multi UDP Tunnel)	The number of UDP connections.
WLAN Radio (Multi UDP Tunnel)	Enable/disable the internal wireless module for operation on an existing WLAN network (tunnel starting point).
Set & Reboot	Apply the changes and reboot.

Network – PROFINET

PROFINET Prioritization	Enable/disable prioritization for PROFINET
PROFIsafe	Enable/disable PROFIsafe functionality
Set	Apply the changes (no reboot required)

WLAN – WLAN Network	
Scan	Search for available WLAN networks. The networks will be listed in the drop-down menu with their corresponding SSID and security modes.
Assume & Set	Confirm the WLAN network/SSID/security mode selection.
WLAN Band (Dual-mode model only)	Select either 2.4 or 5 GHz, or **Auto** (default) to scan both frequency bands. Selecting a single band will speed up the search for a suitable network.
Set	Apply the changes (no reboot required)

WLAN – Connection	
Network (SSID)	Enter the wireless network ID (SSID). Clients may perform roaming between access points that have the same SSID.
Operating Mode	Select WLAN operating mode. **Infrastructure**: Operating as a client in a WLAN network. **Ad hoc**: Direct connection between the Wireless Bridge and another device.
Ad-hoc Mode	**Creator**: The Wireless Bridge is the initiator of the ad-hoc network. **Joiner**: The Wireless Bridge is connecting to an existing ad-hoc network.
Channel	Select wireless channel for ad-hoc connections. (In infrastructure mode, the access point determines the channel.)
Data Rate	Select data rate (modulation). **Auto** (default) automatically selects the maximum possible data rate.
Transmit Power	Transmission power in dBm. Default = 17 dBm (max). Can be reduced down to -17 dBm to limit the range. The value refers to the electronics, the gain of the internal antenna of ~5 dBi is not taken into account. Setting the value to e.g. “15” will result in a radiated power of approximately 20 dBm.
Set	Apply the changes (no reboot required).

WLAN – Security	
Security Mode	Select security profile. The security settings must be identical to those of the wireless network. Use **Other** to implement more unusual combinations of encryption and authentication. The settings are automatically taken from the network scan.
Passkey Format	Interprets the passkey as text (ASCII) or hexadecimal characters (0…F).
Passkey	Enter passkey for encrypted connections. The possible characters depend on the encryption method used. WEP 64: 5 (ASCII) or 10 (HEX) WEP 128: 13 (ASCII) or 26 (HEX) WPA/WPA2: 8 - 63 characters (ASCII 32 to 126 except “\”).
Authentication	Select method for secure encryption initialization. This setting limits the encryption selection to matching combinations. Therefore, select authentication before encryption.
Encryption	Select encryption method for securing the data transmission.
User Name	Enter user name for authentication via LEAP or PEAP.
Domain	Enter authentication domain for LEAP or PEAP.
Certificate Fingerprint	Certificate for authentication via PEAP.
Set	Apply the changes (no reboot required).

Roaming – General	
Used Channels	Select possible wireless channels. Channel limitation is used for optimizing the roaming time.
Roaming Profile	Select typical setting for roaming optimization. **Hold connection**: No roaming **Background**: Search for better access point in short (high), medium or long (low) distance. **Individual**: Enables loading individual, adapted parameter records (templates) for special cases.
Set	Apply the changes (no reboot required).

SMART Mode Configuration	
SMART Modes	See *SMART Configuration, p. 10*.
Execute	Apply the selected SMART configuration mode and reboot.

Service – Change Password	
New Password	Enter a new password for the web configuration interface.
Confirm Password	Enter the new password again.
Set	Confirm the new password (it will be required on the next login attempt).

Service – System Identification	
Device Name	A name for the device.
Description	A short description of the device.
Physical Location	The location of installation.
Device Contact	Contact person (including e-mail, phone number, etc.).
General Data	Additional information about the device.
Set	Apply the changes (no reboot required).

Miscellaneous	
Event Subscriber	Activate sending of system events via TCP or Syslog.
Value	Select which values to send: Receive quality (RSSI), Connection, or both
IP Address (Syslog only)	The IP address of the Syslog server.
Set	Apply the changes (no reboot required).

Export Configuration	
Export configuration	Save the current configuration settings as AT commands in a text file.

4.4.2 Settings – Advanced View

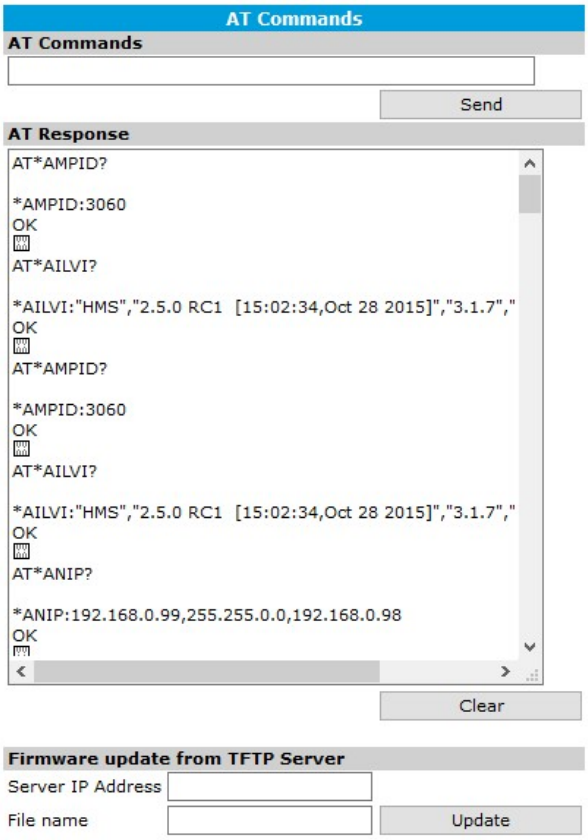

Fig. 8 Advanced view

AT Commands	
AT Commands	Enter AT commands into the field, then click on **Set** to upload them to the Anybus Wireless Bridge.
AT Response	Shows a log of the latest AT commands and their responses.
Clear	Clears the log window.

Firmware update from TFTP Server	
Server IP Address	Enter the IP address of the TFTP server that provides the firmware file.
File name	Enter the filename of the firmware file.
Update	Click on **Update** to upload the firmware to the Anybus Wireless Bridge. Make sure that TFTP traffic (UDP port 69) is not blocked by a firewall.

> **!** Do not reset the Anybus Wireless Bridge during a firmware update.

5 Configuration Examples

The following configuration examples require a basic understanding of how to install and power up Anybus Wireless Bridge and how to access and use SMART configuration modes. Read sections *Product Description* and *Startup and Configuration* before you continue.

- All the examples start out from the factory default settings.
- Settings not mentioned in the examples should normally be left at their default values.
- The Ethernet networks in the examples use static IP addressing within the default subnet range of the Wireless Bridge.
- The computer used for web configuration must be in the same subnet as the Wireless Bridge being configured.

5.1 UDP Tunnel via Ad-Hoc Network

5.1.1 Overview

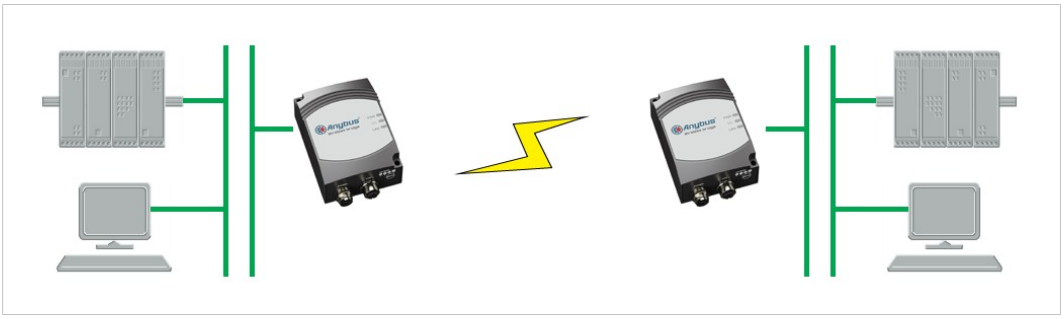

Fig. 9 UDP Tunnel via Ad-Hoc Network

This example describes two Wireless Bridges using UDP tunneling in an ad-hoc network to connect two Ethernet network segments.

5.1.2 SMART Configuration

Provided that the default IP addresses (192.168.0.98/99) can be used, this configuration can be set up using only the MODE button. See *SMART Configuration, p. 10*.

1. Reset both Wireless Bridges to the factory default settings.
2. On the first Wireless Bridge, activate SMART configuration mode 4 (LED C).
   The LED will blink while the unit is waiting for a connection.

   

3. On the second Wireless Bridge, activate SMART configuration mode 5 (LED A+C).
   The LEDs will blink until the units have connected.

   

4. When the Wireless Bridges have connected, the first unit will have IP address 192.168.0.98 and the second 192.168.0.99. The units will be operating in ad-hoc mode.

5.1.3 Manual Configuration

If any of the predefined IP addresses 192.168.0.98 and 192.168.0.99 are already in use on your network, or if the network uses DHCP addressing, the setup must be configured manually in the web interface for each unit.

In the following example, static addressing is used and the two units are assigned IP addresses 192.168.0.101 and 192.168.0.102.

> **!** Make sure that the IP addresses are not already allocated on the local network.

1. Reset both Wireless Bridges to the factory default settings.
2. Open the web interface of each Wireless Bridge and set up the following configuration:

Parameter	Wireless Bridge 1	Wireless Bridge 2
Network		
IP Address	**192.168.0.101**	**192.168.0.102**
Subnet Mask	255.255.0.0	255.255.0.0
Default Gateway	192.168.0.101	192.168.0.101
IP Assignment	Static	Static
Client Mode		
Mode	UDP Tunnel	UDP Tunnel
UDP Port	2000	2000
Remote IP Address	**192.168.0.102**	**192.168.0.101**
WLAN		
Network (SSID)	Create a new SSID	Same SSID as first unit
Operating Mode	Ad-Hoc	Ad-Hoc
Ad-hoc Mode	**Creator**	**Joiner**
Channel	Auto (Default)	Auto (Default)

   Make sure that all settings except **IP Address**, **Remote IP Address**, and **Ad-hoc mode** are exactly the same in both units. Settings not mentioned in this example should normally be left at their default values.

3. Click on the **Write all** button to save the configuration for each Wireless Bridge. The units will automatically restart and connect.

5.2 UDP Tunnel via WLAN Access Point

5.2.1 Overview

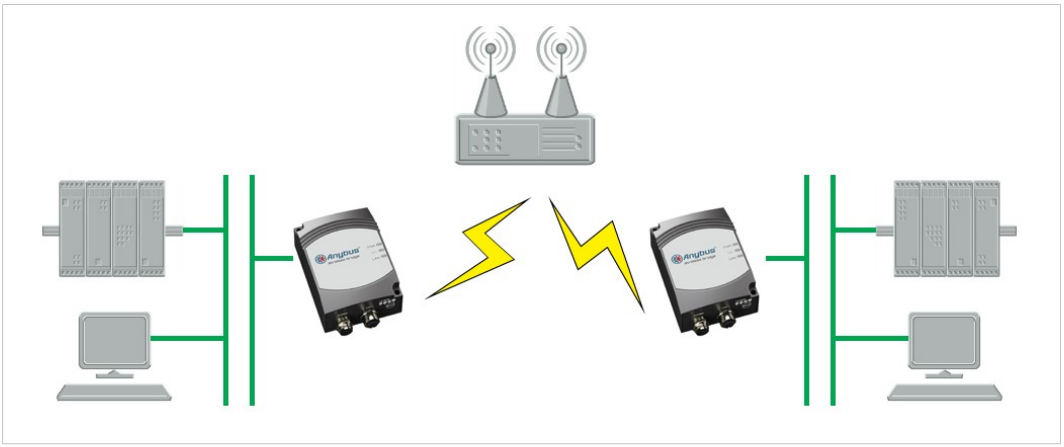

Fig. 10 UDP Tunnel via WLAN Access Point

This example describes two Wireless Bridges using UDP tunneling to connect two Ethernet network segments via a WLAN access point.

Using an access point and infrastructure mode will result in higher performance than when connecting directly in ad-hoc mode.

5.2.2 SMART Configuration

Basic configuration can be carried out using SMART configuration, but the SSID and security parameters must be configured through the web interface.

1. Reset both Wireless Bridges to the factory default settings.
2. On the first Wireless Bridge, activate SMART configuration mode 8 (LED D).

   

3. On the second Wireless Bridge, activate SMART configuration mode 9 (LED A+D).

   

4. When the Wireless Bridges have connected, the first unit will have IP address 192.168.0.98 and the second 192.168.0.99. The units will be operating in infrastructure mode but are still not associated with the WLAN.
5. Open the web configuration interface for each Wireless Bridge and set the SSID and the security settings as required by the access point that you are connecting to. After saving the settings, the units will restart and connect to the access point.

   See also *Settings – Standard View, p. 12*.

5.2.3 Manual Configuration

If any of the predefined IP addresses 192.168.0.98 and 192.168.0.99 are already in use on your network, the setup must be configured manually in the web interface for each unit. In the following example, IP addresses 192.168.0.101 and 192.168.0.102 are used.

> **!** Make sure that the IP addresses are not already allocated on the local network.

1. Reset both Wireless Bridges to the factory default settings.
2. Open the web interface of each Wireless Bridge and set up the following configuration:

Parameter	Wireless Bridge 1	Wireless Bridge 2
Network		
IP Address	**192.168.0.101**	**192.168.0.102**
Subnet Mask	255.255.0.0	255.255.0.0
Default Gateway	192.168.0.101	192.168.0.101
IP Assignment	Static	Static
Client Mode		
Mode	UDP Tunnel	UDP Tunnel
UDP Port	2000	2000
Remote IP Address	**192.168.0.102**	**192.168.0.101**
WLAN		
Network (SSID)	SSID of the access point	SSID of the access point
Operating Mode	Infrastructure	Infrastructure
Security Mode	As required	As required

   Make sure that all settings except **IP Address** and **Remote IP Address** are exactly the same in both units. Settings not mentioned in this example should normally be left at their default values.

3. Click on the **Write all** button to save the configuration for each Wireless Bridge. The units will automatically restart and connect.

5.3 Two Single Clients Connected via Ad-Hoc Network

5.3.1 Overview

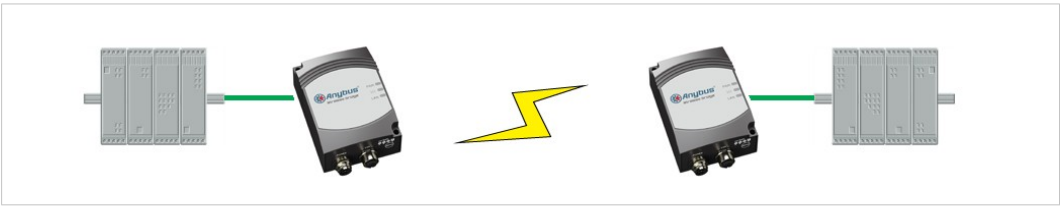

Fig. 11 Two Single Clients Connected via Ad-Hoc Network

This example describes two Ethernet devices connecting via two Wireless Bridges in Single Client mode using an ad-hoc network. Single Client mode has higher performance than UDP Tunneling since no encapsulation of the Ethernet packages is required. Only one Ethernet device can be connected to each Wireless Bridge.

5.3.2 SMART Configuration

This configuration can be set up using only the MODE button. See *SMART Configuration, p. 10*.

1. Reset both Wireless Bridges to the factory default settings.
2. On the first Wireless Bridge, activate SMART configuration mode 4 (LED C).
   The LED will blink while the unit is waiting for a connection.

   

3. On the second Wireless Bridge, activate SMART configuration mode 5 (LED A+C).
   The LEDs will blink until the units have connected.

   

4. When the Wireless Bridges have established a connection, activate SMART configuration mode 11 (LED A+B+D) on the first unit.

   

5. Activate SMART configuration mode 11 on the second Wireless Bridge. The LEDs will blink while the unit enters client mode and retrieves the MAC address of the other unit.

   

6. The first unit will now have IP address 192.168.0.98 and the second 192.168.0.99. The units will be operating in ad-hoc mode.

5.3.3 Manual Configuration

Automatic configuration requires that a Wireless Bridge can send spontaneous ARP requests to retrieve the MAC address of the device at the other end. If this is not possible, the setup must be configured manually in the web interface for each unit.

Device MAC should be set to the MAC address of the device connected to the Wireless Bridge.

1. Reset both Wireless Bridges to the factory default settings.
2. Open the web interface of each Wireless Bridge and set up the following configuration:

Parameter	Wireless Bridge 1	Wireless Bridge 2
Client Mode		
Mode	Single Client	Single Client
Device MAC	**MAC address of the connected device**	**MAC address of the connected device**
WLAN		
Network (SSID)	Create a new SSID	Same SSID as first unit
Operating Mode	Ad-hoc	Ad-hoc
Ad-hoc mode	**Creator**	**Joiner**
Security Mode	As required	As required

   Make sure that all settings except **Device MAC** and **Ad-hoc mode** are exactly the same in both units. Settings not mentioned in this example should normally be left at their default values.

3. Click on the **Write all** button to save the configuration for each Wireless Bridge. The units will automatically restart and connect.

5.4 Multiple Single Clients Connecting via Ad-Hoc Network

5.4.1 Overview

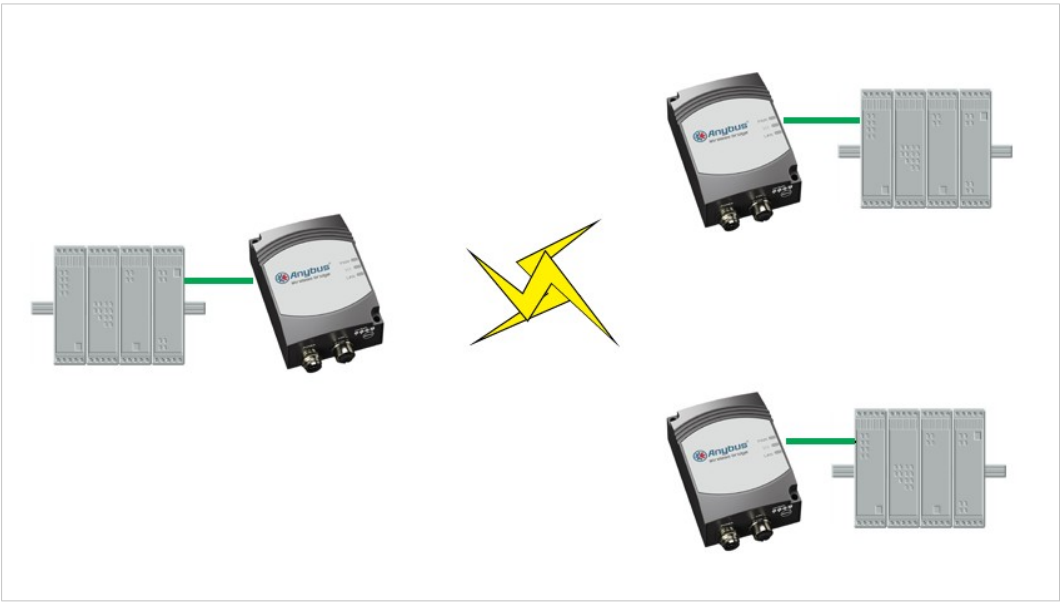

Fig. 12 Multiple Single Clients Connecting via Ad-Hoc Network

This example describes three Ethernet devices connecting via Wireless Bridges in Single Client mode using an ad-hoc network. Only one Ethernet device can be connected to each Wireless Bridge.

5.4.2 Configuration

This is basically the same as *Two Single Clients Connected via Ad-Hoc Network, p. 22* but with a third Wireless Bridge and Ethernet device added to the ad-hoc network. Configuration must in this case be done manually in the web interface of each Wireless Bridge.

1. Reset the Wireless Bridges to the factory default settings.
2. Open the web interface of the Wireless Bridges and set up the following configuration:

Parameter	Wireless Bridge 1	Wireless Bridge 2	Wireless Bridge 3
Client Mode			
Mode	Single Client	Single Client	Single Client
Device MAC	MAC address of the connected device	MAC address of the connected device	MAC address of the connected device
WLAN			
Network (SSID)	Create a new SSID	Same SSID as first unit	Same SSID as first unit
Operating Mode	Ad-Hoc	Ad-Hoc	Ad-Hoc
Ad-hoc Mode	**Creator**	**Joiner**	**Joiner**
Security Mode	As required	As required	As required

   Make sure that all settings except **Device MAC** and **Ad-hoc mode** are exactly the same in all three units. Settings not mentioned in this example should normally be left at their default values.

3. Click on **Write all** to save the configuration for each Wireless Bridge. The units will automatically restart with the new settings.

5.5 Single Clients Connected via WLAN Access Point

5.5.1 Overview

Fig. 13 Single Clients Connected via WLAN Access Point

This example describes two Ethernet devices connecting using Wireless Bridges connected in Single Client mode via an access point. Only one Ethernet device can be connected to each Wireless Bridge.

Using an access point and infrastructure mode will result in higher performance than when connecting directly in ad-hoc mode.

5.5.2 Configuration

1. Reset both Wireless Bridges to the factory default settings.
2. Open the web interface of each Wireless Bridge and set up the following configuration:

Parameter	Wireless Bridge 1	Wireless Bridge 2
Client Mode		
Mode	Single Client	Single Client
Device MAC	**MAC address of the connected device**	**MAC address of the connected device**
WLAN		
Network (SSID)	SSID of the access point	SSID of the access point
Operating Mode	Infrastructure	Infrastructure
Security Mode	As required	As required

   Additional Wireless Bridges can be added in the same way. Make sure that all settings except **Device MAC** are exactly the same in the units. Settings not mentioned in this example should normally be left at their default values.

3. Click on the **Write all** button to save the configuration for each Wireless Bridge. The units will automatically restart and connect.

5.6 PC Connected to Single Client via Ad-Hoc Network

5.6.1 Overview

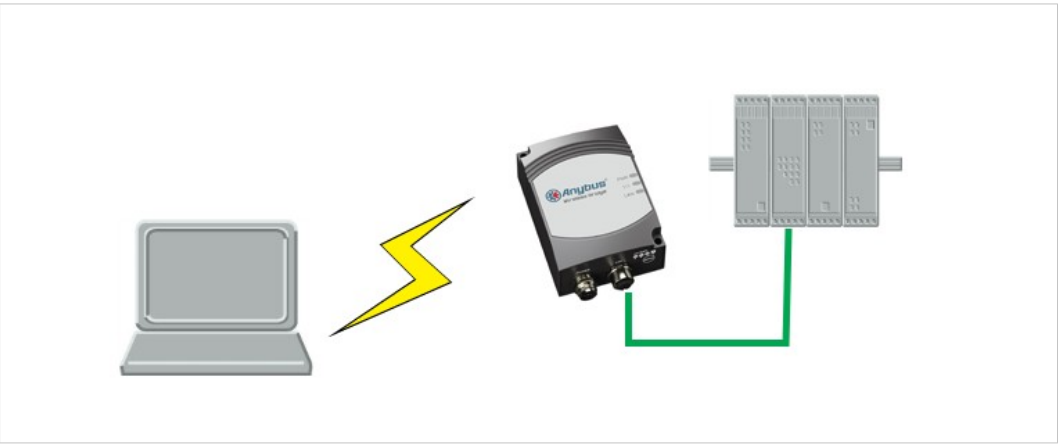

Fig. 14 PC Connected to Single Client via Ad-Hoc Network

This example describes a computer connecting to an Ethernet device via an ad-hoc network connection to a Wireless Bridge operating in single client mode.

> **!** Ad-hoc connections between a Wireless Bridge and a Windows computer may be unstable and are normally not recommended.

5.6.2 Configuration

1. Set up a new ad-hoc wireless network on the computer (refer to the documentation for the operating system of the computer for instructions).
2. Reset the Wireless Bridge to the factory default settings.
3. Open the web interface of the Wireless Bridge and set up the following configuration:

Parameter	Value
Client Mode	
Mode	Single Client
Device MAC	MAC address of the connected device
WLAN	
Network (SSID)	SSID of the ad-hoc network
Operating Mode	Ad-Hoc
Ad-hoc Mode	Joiner
Security Mode	As required

4. Click on **Write all** to save the configuration for the Wireless Bridge. The unit will automatically restart with the new settings.

5.7 PC Connected to Single Client via WLAN Access Point

5.7.1 Overview

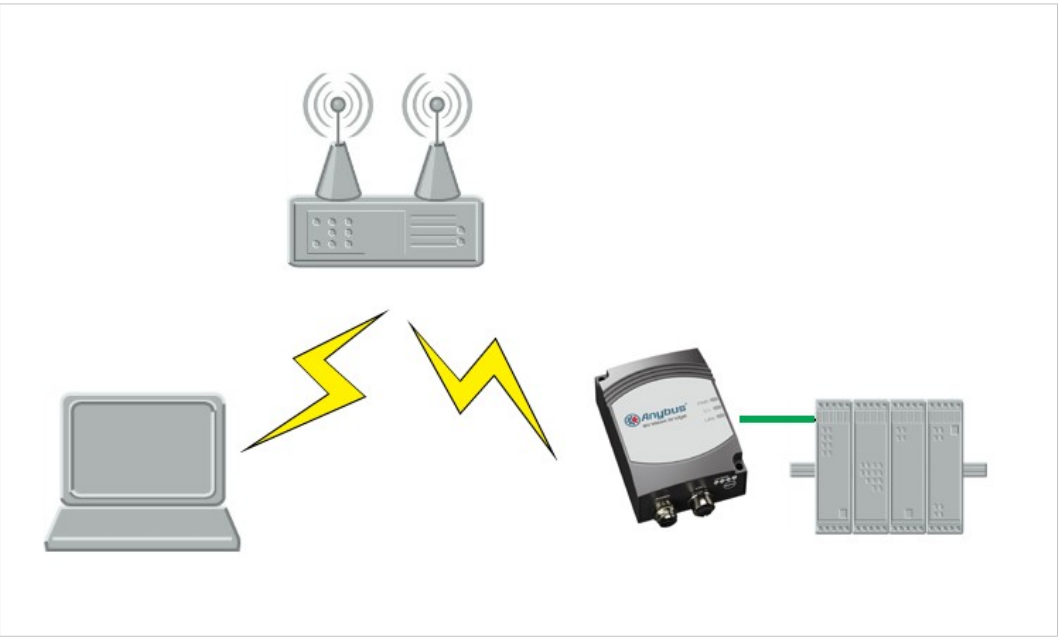

Fig. 15 PC Connected to Single Client via WLAN Access Point

This example describes a computer connecting to a single Ethernet device via a WLAN access point and a Wireless Bridge operating in single client mode.

5.7.2 Configuration

1. Make sure that the computer is connected to the WLAN access point.
2. Reset the Wireless Bridge to the factory default settings.
3. Open the web interface of the Wireless Bridge and set up the following configuration:

Parameter	Value
Client Mode	
Mode	Single Client
Device MAC	MAC address of the connected device
WLAN	
Network (SSID)	SSID of the access point
Operating Mode	Infrastructure
Security Mode	As required

4. Click on **Write all** to save the configuration for the Wireless Bridge. The unit will automatically restart with the new settings.

5.8 Single Clients Connected via WLAN to a Wired Network

5.8.1 Overview

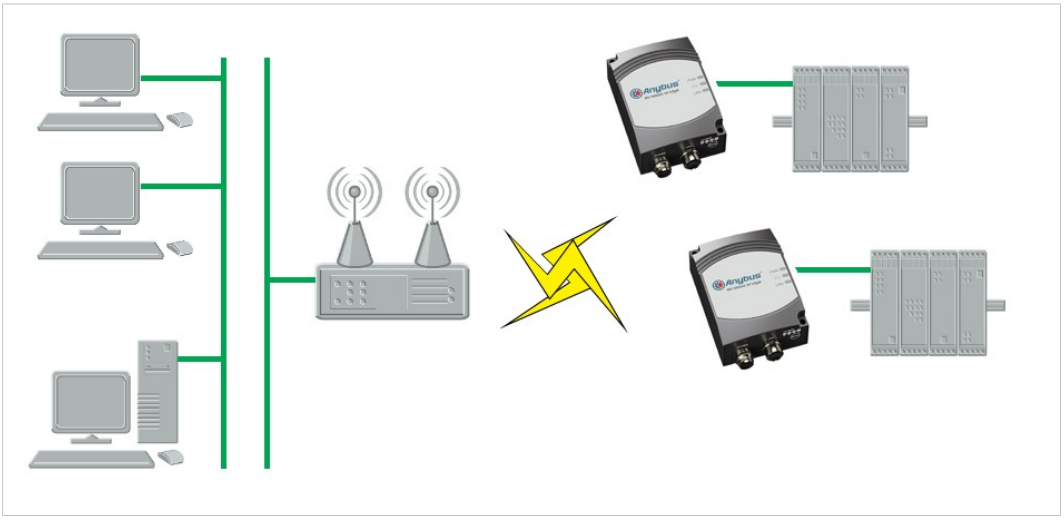

Fig. 16 Single Clients Connected via WLAN to a Wired Network

This example describes two Ethernet devices connected via two Wireless Bridges and a WLAN access point to a wired network.

5.8.2 Configuration

1. Reset both Wireless Bridges to the factory default settings.
2. Open the web interface of each Wireless Bridge and set up the following configuration:

Parameter	Wireless Bridge 1	Wireless Bridge 2
Client Mode		
Mode	Single Client	Single Client
Device MAC	**MAC address of the connected device**	**MAC address of the connected device**
WLAN		
Network (SSID)	SSID of the access point	SSID of the access point
Operating Mode	Infrastructure	Infrastructure
Security Mode	As required	As required

   Additional Wireless Bridges can be added in the same way. Make sure that all settings except **Device MAC** are exactly the same in the units. Settings not mentioned in this example should normally be left at their default values.

3. Click on the **Write all** button to save the configuration for each Wireless Bridge. The units will automatically restart and connect.

5.9 Multiple Clients Connected via WLAN Access Point

5.9.1 Overview

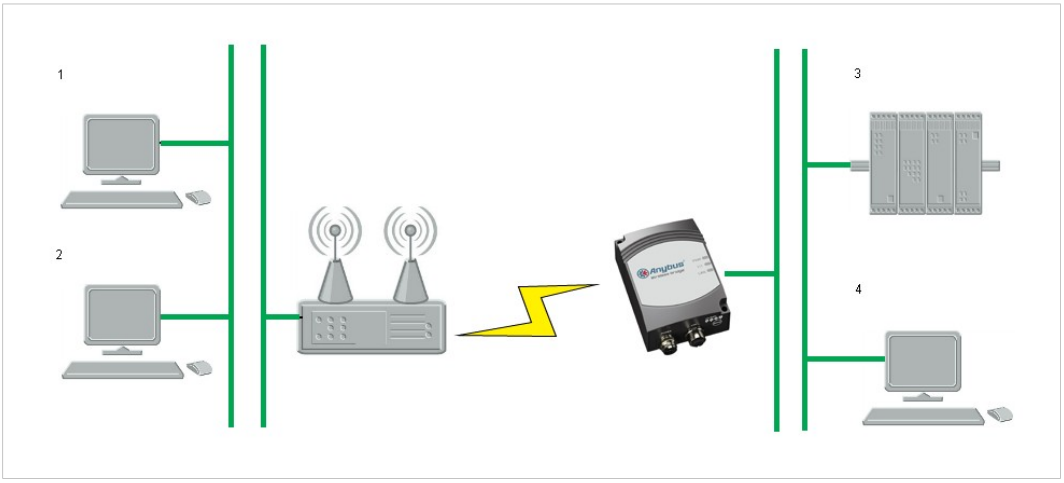

Fig. 17 Multiple Clients Connected via a Wireless Bridge and a WLAN Access Point

In the following example, two network segments are connected via a Wireless Bridge operating in Multiclient mode. The network contains a DHCP server for dynamic addressing.

Layer 2 communication is only possible for one of the devices connected to the Wireless Bridge, other devices need to use the IP layer. This means that if a device requires communication over layer 2, only one can be used in this setup.

All connected devices including the Wireless Bridge must be in the same IP subnet.

5.9.2 Configuration

1. Reset the Wireless Bridge to the factory default settings.
2. Open the web interface of the Wireless Bridge and set up the following configuration:

Parameter	Value
Default Gateway	IP address of the access point
IP Assignment	DHCP
Client Mode	
Mode	Multiclient
Device MAC	MAC address of the device that requires layer 2 communication. If none, leave as default (EPA MAC).
WLAN	
Network (SSID)	SSID of the access point
Operating Mode	Infrastructure
Security Mode	As required

3. Click on **Write all** to save the configuration for the Wireless Bridge. The unit will automatically restart with the new settings.

When the Anybus Wireless Bridge has rebooted it may have been assigned a new IP address by the DHCP server on the network. To access the web interface again you may need to also change the IP settings of the computer.

This page intentionally left blank

A 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.

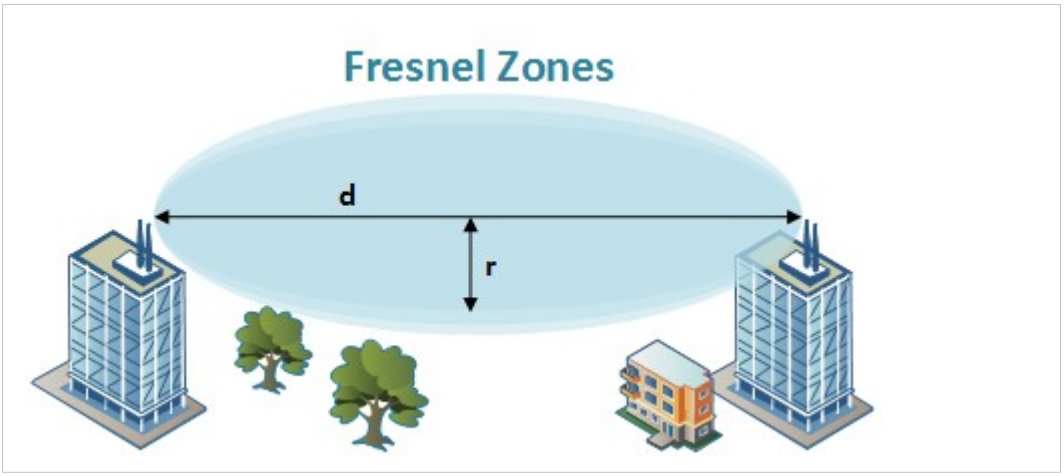

Fig. 18 Fresnel zones

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 range may also need to be limited by reducing the transmission power. For determining the optimal configuration and placement of wireless devices it is therefore recommended to use a wireless signal analysis tool.

B Technical Data

B.1 Technical Specifications

Model	2.4 GHz	5 GHz	Dual-band
Order code	021440	021450	024120
Dimensions (L x W x H)	91 x 66 x 36.2 mm		
Weight	120 g		130 g
Operating temperature	-30 to +65 °C		
Storage Temperature	-40 to +85 °C		
Humidity	RH 5–90 % non-condensing		
Input voltage	9–30 V DC (SELV)		
Power consumption	1.8 W (typical) — see also *Typical current consumption at 24 VDC*		
Enclosure material	Plastic		
Mechanical rating	IP65		
Power connector	M12, male, A-coded		
Ethernet connector	M12, female, D-coded		
Mounting	Screw holes for wall mounting		
Antenna	Internal		External (RPSMA)
Receiver sensitivity	-94 dBm max.	-87 dBm max.	-94/-87 dBm max.
Maximum range	400 m	200 m	400/200 m
Ethernet interface	10/100BASE-T with automatic MDI/MDIX cross-over		
Ethernet protocols	IP, TCP, UDP, LLDP, HTTP, ARP, DHCP client/server, DNS support, SNMP user management and access control		
Default IP address	192.168.0.98		
WLAN interface	802.11b/g/n	802.11n	802.11b/g/n (2.4 GHz) 802.11n (5 GHz)
WLAN security	WEP 64, WEP 128, WPA-PSK, WPA2-PSK, TKIP, CCMP (AES), LEAP, PEAP		
Wireless certifications	Europe (ETSI, R&TTE), Canada (IC, RSS), Japan (MIC) (2.4 GHz only), USA (FCC/CFR 47 part 15 unlicensed modular transmitter approval)		
Environm. certifications	CE, $_{C}UL_{US}$, Haz.Loc Class 1 Div. 2		

Typical current consumption at 24 VDC

Operation	Mean (mA)	Max (mA)
Startup	—	58.8
Idle	58.7	58.8
Idle, Ethernet	69.0	69.1
Idle + 4 x Mode LEDs	74.2	74.3
Connecting	63.2	63.9
Connected, Data	63.2	64.8
Connected, Data, Ethernet	73.4	75.5
Connected, Data, Ethernet, 4 x Mode LEDs	78.6	80.7

B.2 Internal Antenna Characteristics

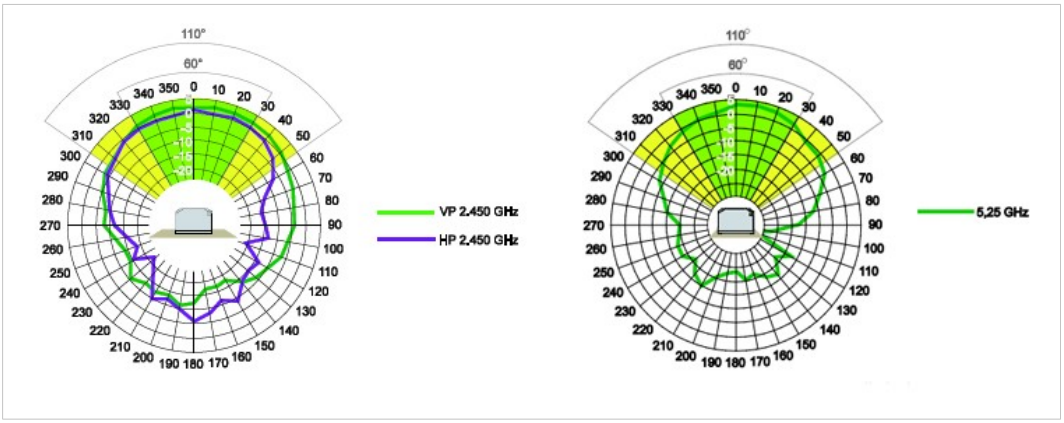

Fig. 19 Longitudinal Axis

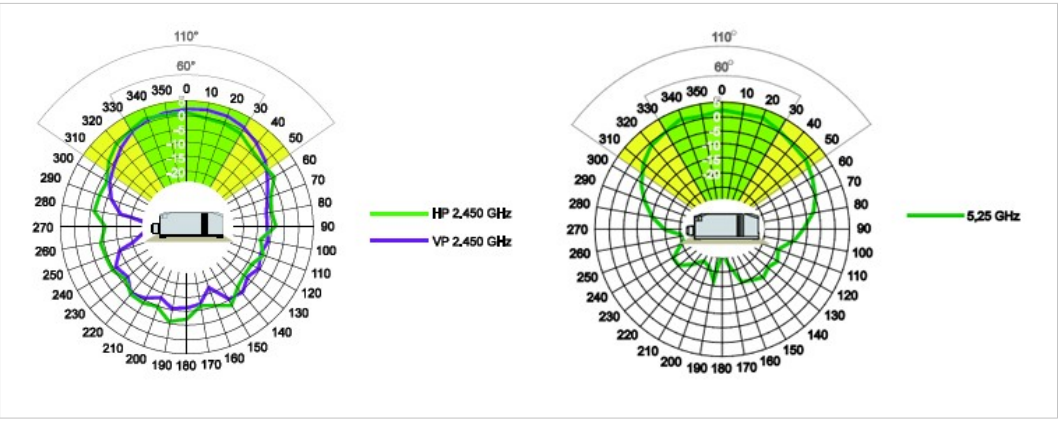

Fig. 20 Transverse Axis

B.3 Regulatory Compliance

EMC Compliance (CE)

The Anybus Wireless Bridge models 021440-B, 021450-B and 024120-B are in compliance with the RED Directive 2014/53/EU through conformance with the following standards:

Effective use of frequency spectrum	**EMC**
EN 300 328 V1.9.1 (2015-02)	EN 301 489-1 V1.9.2 (2011-09)
EN 301 893 V1.8.1 (2015-03)	EN 301 489-17 V2.2.1 (2012-09)
Safety	EN 61000-6-2:2005
EN 62479:2010	EN 61000-6-3:2007 + A1:2011
EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013	
IEC 60950-1:2005 + A1:2009 + A2:2013	

The Declaration of Conformity is available at www.anybus.com/support.

Disposal and Recycling

You must dispose of this product properly according to local laws and regulations. Because this product contains electronic components, it must be disposed of separately from household waste. When this product reaches its end of life, contact local authorities to learn about disposal and recycling options, or simply drop it off at your local HMS office or return it to HMS.
For more information, see www.hms-networks.com.

UL Certification

c UL us LISTED
IND: CONT. EQ. FOR HAZ LOC. CL I, DIV 2 GP A,B,C,D TEMP CODE T4
E203225

LISTED 67AM

This equipment is suitable only for use in Class I, Division 2, Groups A, B, C and D OR non-hazardous locations only. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.

WARNING
EXPLOSION HAZARD - SUBSTITUTION OF ANY COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2.

EXPLOSION HAZARD - DO NOT DISCONNECT EQUIPMENT UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NONHAZARDOUS.

AVERTISSEMENT
RISQUE D'EXPLOSION – LE REMPLACEMENT DE TOUT COMPOSANTS INVALIDE LA CERTIFICATION CLASS I, DIVISION 2.

RISQUE D'EXPLOSION – NE PAS DÉCONNECTER L'ÉQUIPEMENT TANT QUE L'ALIMENTATION EST TOUJOURS PRÉSENTE OU QUE LE PRODUIT EST TOUJOURS EN ZONE EXPLOSIVE ACTIVE.

FCC Compliance Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

This equipment contains FCC ID: **PVH0941**

> **!** Any changes or modifications not explicitly approved by HMS Industrial Networks AB could cause the module to cease to comply with FCC rules part 15, and thus void the user's authority to operate the equipment.

Industry Canada Statement

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Operation is subject to the following two conditions:

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation

Cet équipement est conforme aux limites d'exposition de rayonnement d'IC RSS-102 déterminées pour un environnement non contrôlé. Cet équipement devrait être installé et actionné avec la distance minimum 20 cm entre le radiateur et votre corps.

Son utilisation est soumise aux deux conditions suivantes:

1. Cet appareil ne doit pas causer d’interférences et
2. il doit accepter toutes interférences reçues, y compris celles susceptibles d’avoir des effets indésirables sur son fonctionnement.

This equipment contains IC ID: **5325A-0941**

Japan Radio Equipment Compliance (MIC)

Contains MIC ID: R 204-310004 (2.4 GHz operation only)

B.4 Licenses

This product contains software under the following licenses:

This page intentionally left blank