WIRELESS LAN

Bintec User's Guide - XGeneration
Version 0.9

Purpose

This document is part of the user's guide to the installation and configuration of gateways running software release or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.funkwerk-ec.com.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, changes and **Release Notes** for gateways can be found at www.funkwerk-ec.com.

As multiprotocol gateways, gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

 and the logo are registered trademarks of .

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

All rights are reserved. No part of this publication may be reproduced or transmitted in any form or by any means – graphic, electronic, or mechanical – including photocopying, recording in any medium, taping, or storage in information retrieval systems, without the prior written permission of . Adaptation and especially translation of the document is inadmissible without the prior consent of .

Guidelines and standards

 gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

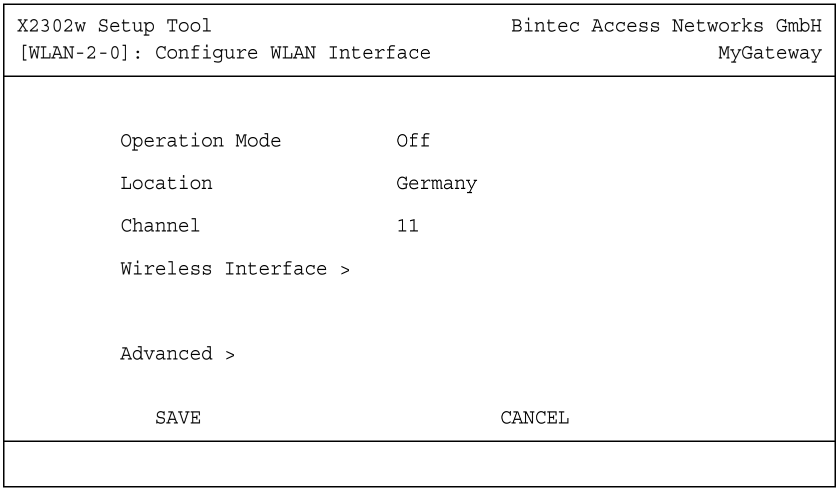
You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com.

How to reach

 Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 Wireless LAN Menu

The fields of the *WIRELESS LAN* menu are described below.



```
X2302w Setup Tool                              Bintec Access Networks GmbH
[WLAN-2-0]: Configure WLAN Interface                             MyGateway


         Operation Mode          Off

         Location                Germany

         Channel                 11

         Wireless Interface >


         Advanced >

            SAVE                          CANCEL
```

The ***WIRELESS LAN*** menu contains the general settings for the configuration of the gateway as an access point (AP).

Wireless LAN (WLAN = Wireless Local Area Network) comprises the setup of a network by means of radio technology.

Network functions

WLAN provides the same required network functions as a cabled network, i.e. access to servers, files, printers and mail system as well as the company Internet access. No cabling is required, so that with a WLAN no edificial constraints are to be considered (i.e. location of device vs. position and number of connections).

Standard: IEEE 802.11

IEEE 802.11b is presently the primarily used standard for radio-based LANs. This method operates at a frequency of 2,4Ghz, which guarantees that buildings are penetrated with the required transmitting power that, however, does not affect health. WLAN transmits indoors and outdoors at a maximum of 100 mW.

Although transmitting only with 11Mb per second, 802.11b WLANs offers all functions of a cabled network. WLAN systems are free of charge and are not to be registered inbetween 5150 MHz - 5350 MHz and 5470 MHz - 5725 MHz.

802.11g is compatible to 802.11b, operating with 2,4 GH and offering a data transfer rate of 54 Mbps.

The ***Wireless LAN*** menu consists of the following fields:

Field	Description
Operation Mode	The operation mode of the gateway. Possible values: ■ *Off* (default value): gateway does not operate as AP ■ *Access Point*: enable gateway operating as access point.
Location	The country setting of the AP. Possible values are all countries preconfigured on the wireless module of the gateway.
Channel	The channel used by the AP. Possible values: *1* ... *13.* Default value is *11*.

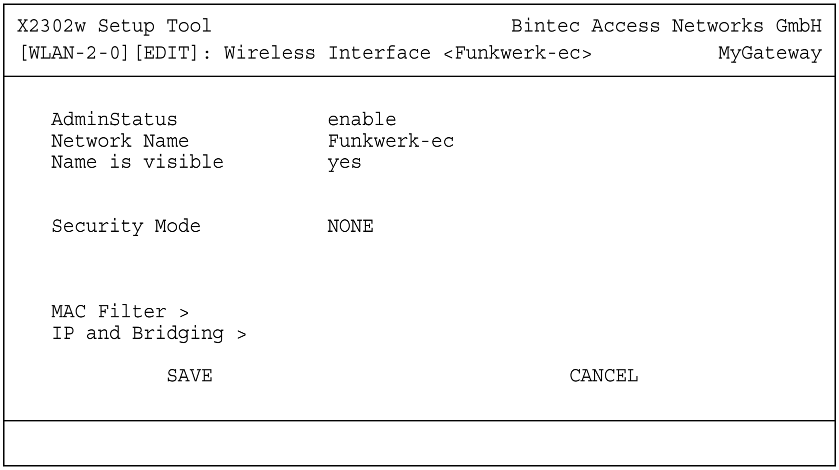
Table 1-1: ***Wireless LAN*** menu fields

The menu provides access to the following submenus:

- ***Wireless Interface***
- ***Advanced***

2 Wireless Interface Submenu

The fields of the *WIRELESS INTERACE* menu are described below.



```
X2302w Setup Tool                                Bintec Access Networks GmbH
[WLAN-2-0][EDIT]: Wireless Interface <Funkwerk-ec>                MyGateway


   AdminStatus              enable
   Network Name             Funkwerk-ec
   Name is visible          yes


   Security Mode            NONE



   MAC Filter >
   IP and Bridging >

            SAVE                                  CANCEL
```

The ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACE*** submenu contains essential settings such as network name, status etc.

The wireless interface (with prefix *vss*) has its own IP settings and can use all standard interface specific features such as QoS, Stateful Inspection, Accounting etc. This opens a wide range of applications for the WLAN interface.

The Bintec WLAN gateway not only offers bridging for wireless connections, but is also fully integrated into the routing environment.

Securing your WLAN

Security As WLAN uses the air as transmission medium, the transferred data can theoretically be intercepted and read by anyone with the respective means. Thus, safeguarding the radio link is to be paid special attention.

WEP 802.11 defines the security standard WEP (Wired Equivalent Privacy = data encryption with 40/64 bit (***SECURITY MODE*** = *WEP 40/64*) resp. 104/128 bit (***SECURITY MODE*** = *WEP 104/128*)). The commonly used WEP, however, turned out to be vulnerable. For increased security you have to configure hardware-based encryption (as e.g. 3DES or AES) additionally. Thus even sensitive data can be transferred via the WLAN.

IEEE 802.11i The IEEE 802.11i standard for wireless systems comprises security specifications for radio networks especially concerning encryption. The relatively unsecure WEP (Wired Equivalent Privacy) is replaced by WPA (Wi-Fi Protected Access). In addition, the Advanced Encryption Standard (AES) is defined for data encryption. This complies with the Federal Information Standards (FIPS).

WPA WPA provides enhanced encryption by using the so-called "Temporal Key Integrity Protocol" (TKIP). Furthermore, preshared keys are applied as well as the RADIUS-based 802.1X, where clients must authenticate distinctly. In addition, WPA requires authentication by means of IEEE 802.1x and EAP (Extensible Authentication Protocol), which refer to a RADIUS server that administrates the authentication of clients.

Security options To safeguard the data transferred via WLAN you should if applicable configure the options of the ***WIRELESS LAN* ➜ *WIRELESS INTERFACE*** menu:

- Change the default SSID, ***NETWORK NAME*** = *Funkwerk-ec*, of your access point.
- Configure ***WIRELESS INTERFACE* ➜ *NAME IS VISIBLE*** = *no*. Thus all WLAN clients are refused who try to connect with the common ***NETWORK NAME*** (SSID) *Any* and do not know the specified SSIDs.
- Use one of the provided encryption methods by selecting ***SECURITY MODE*** = *WEP 40/64*, *WEP 104/128* or *WPA PSK (TKIP)*, and entering the respective key for the access point into ***KEY 1 - 4*** resp. ***PRESHARED KEY*** and for the WLAN clients.
- The WEP key should regularly be changed by modifying the ***DEFAULT KEY***.
- To transfer highly sensitive data it is recommended to select ***SECURITY MODE*** = *WPA (TKIP + 802.1x)*. These methods comprise hardware based encrytion and RADIUS authentication of the client. In special cases even a combined operation with IPSec is possible.
- Limit the access to the WLAN for allowed clients by entering the MAC adresses of the WLAN cards of these clients into the ***MAC FILTER* ➜ *ACCEPT*** list. Refuse all other clients from access by entering their WLAN

card MAC addresses into the ***REJECT*** list (see “MAC Filter Submenu” on page 9).

The ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACE*** menu consists of the following fields:

Field	Description
AdminStatus	Administrative status of the wireless interface. Possible values: ■ *enable* (default value): enable the interface ■ *disable*: disable the interface
Network Name	Name of the wireless interface (SSID). Enter an ASCII string of max. 32 characters.
Name is visible	Enable broadcasting of the network name (SSID) of the wireless interface. Possible values: ■ *yes* (default value): network name is visible for clients within reach ■ *no*: network name is hidden
Security Mode	The security mode of the wireless interface. Possible values: ■ *NONE* (default value): no security mode ■ *WEP 40/64*: WEP 40Bit ■ *WEP 104/128*: WEP 104Bit ■ *WPA PSK (TKIP)*: WPA Preshared Key ■ *WPA (TKIP + 802.1x)*: 802.11i/TKIP If ***SECURITY MODE*** is set to *WPA (TKIP + 802.1x)*, the following note is displayed: *A Radius Server configuration in RADIUS setup is required.*

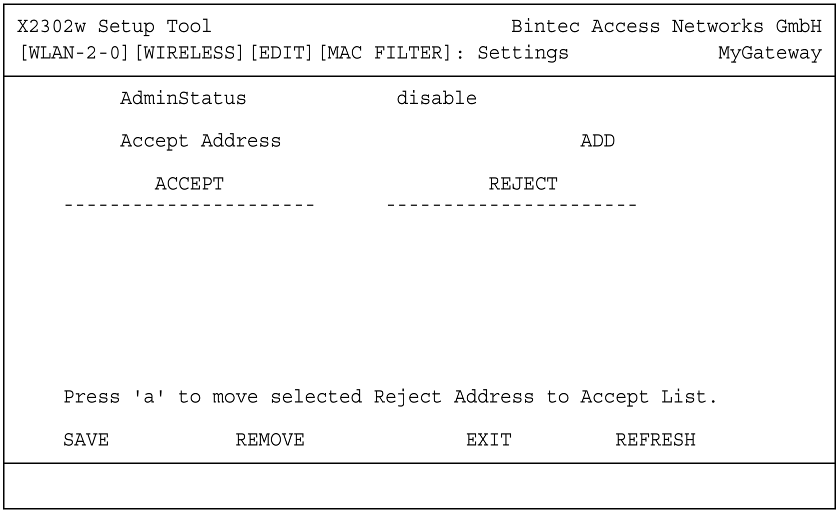
Field	Description
Default Key	Only for ***Security Mode*** = *WEP 40/64, WEP 104/128* Here you select one of the configured keys in ***Key <1 - 4>*** to be the one used as default.
Key <1 - 4>	Only for ***Security Mode*** = *WEP 40/64, WEP 104/128* Here you enter the WEP key. WEP keys can be entered in three different ways: ■ Automatic key generation (recommenced): Entering any phrase not starting with *0x* or " generates a MD5 based WEP phrase with the exact count of digits for the current WEP mode. ■ Direct Hex Digit Input Starting the key with *0x*, disables the generator. Enter the key with the exact count of hexdigits for the selected WEP mode. 10 digits for WEP40 or 26 digits for WEP104. e.g. WEP40: *0xA0B23574C5* , WEP104: *0x81DC9BDB52D04DC20036DBD831* ■ Direct ASCII based input Starting the key with ", disables the generator. Enter a string with the exact count of characters for the selected WEP mode. The phrase ends with ". For WEP40 the phrase must have 5 characters, for WEP104 13 characters. e.g. "*hallo*" for WEP40 "*funkwerk-wep1*" for WEP104.

Field	Description
Preshared Key	Only for ***SECURITY MODE*** = *WPA PSK (TKIP)* Here you enter the WPA passphrase. Enter an ASCII String of 8 - 32 characters.

Table 2-1: ***WIRELESS INTERFACES*** menu fields

2.1 MAC Filter Submenu

The fields of the *MAC FILTER* submenu are described below.



```
X2302w Setup Tool                                 Bintec Access Networks GmbH
[WLAN-2-0][WIRELESS][EDIT][MAC FILTER]: Settings                    MyGateway

         AdminStatus             disable

         Accept Address                          ADD

            ACCEPT                      REJECT
     ----------------------      ----------------------








     Press 'a' to move selected Reject Address to Accept List.

     SAVE           REMOVE              EXIT         REFRESH
```

In the ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ ***ADD/EDIT*** ➜ ***MAC FILTER*** submenu, hardware specific acces control is configured. Thus it is possible to allow only specific clients to access the AP. This filter is checked before any other security mechanism is activated. The entered addresses are MAC based and are configured separately for each wireless interface.

MAC Address Lists

The ***ACCEPT*** list displays all MAC addresses to be accepted for the current wireless interface.

The ***REJECT*** list displays all rejected addresses or adresses assigned to another interface but not accepted by this interface.

Additional buttons The **REFRESH** button reloads the ***REJECT*** list, so that at any time the current status of rejects can be listed.

With the **REMOVE** button selected addresses can be deleted from the ***ACCEPT*** list. Removing an address from the ***ACCEPT*** list immediately disconnects an established link.

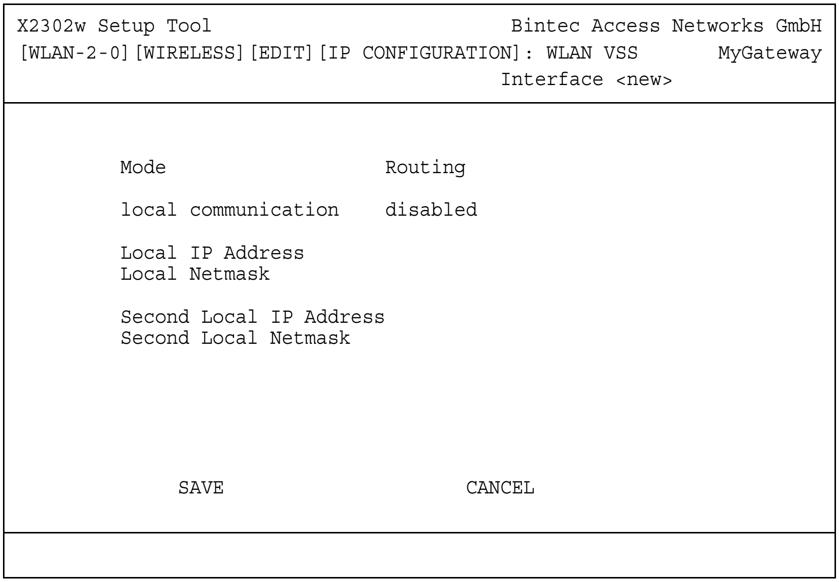
The menu consists of the following fields:

Field	Description
AdminStatus	Enable or disable the filter for this wireless interface. Possible values: *enable*, *disable* (default value)
Accept Address	Enter a MAC address to be accepted. Possible values: 12 digit MAC addresses; the addresses are entered without any ":". Press **ADD** to add the entered MAC address to the ***ACCEPT*** list. If you highlight an entry from the ***REJECT*** list and press **a** (must be lowercase) on your keyboard, the respective entry is moved to the ***ACCEPT*** list. Thus you do not have to manually enter acceptable addresses.

Table 2-2: ***MAC FILTER*** menu fields

2.2 IP and Bridging Submenu

The fields of the *IP AND BRIDGING* submenu are described below.



```
X2302w Setup Tool                              Bintec Access Networks GmbH
[WLAN-2-0][WIRELESS][EDIT][IP CONFIGURATION]: WLAN VSS        MyGateway
                                              Interface <new>


         Mode                       Routing

         local communication        disabled

         Local IP Address
         Local Netmask

         Second Local IP Address
         Second Local Netmask




              SAVE                        CANCEL
```

In the ***Wireless LAN*** ➜ ***Wireless Interfaces*** ➜ ***ADD/EDIT*** ➜ ***IP and Bridging*** submenu you enter the interface specific IP configuration.

The menu consists of the following fields:

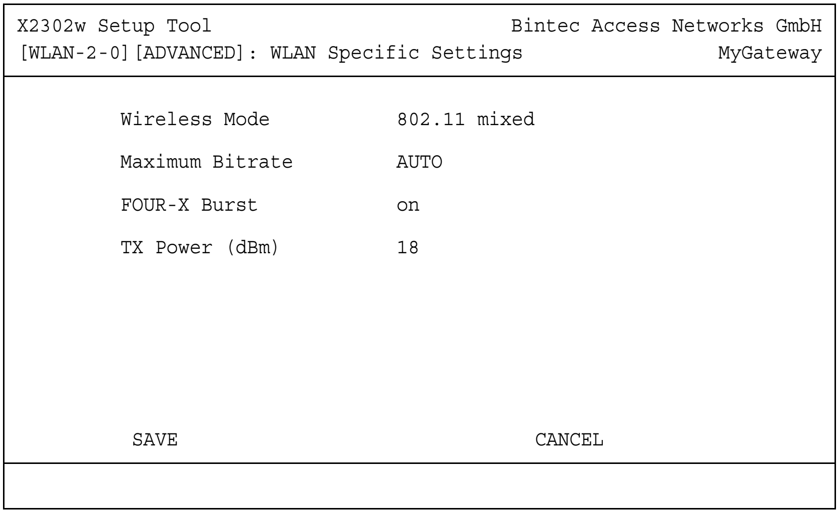
Field	Description
Mode	Defines the mode of the wireless interface. Possible values: ■ *Routing* (default value): Routing is enabled on the wireless interface. ■ *Bridging*: Bridging is enabled on the wireless interface.
local communication	Allows the communication between the clients, authenticated at this SSID, to e.g. access common shares. Possible values: *enabled*, *disabled* (default value)

Field	Description
Local IP Address	Only for ***Working Mode*** = *Routing* Here you assign an IP address to the wireless interface.
Local Netmask	Only for ***Working Mode*** = *Routing* Netmask for ***local IP Number***.
Second Local IP Address	Only for ***Working Mode*** = *Routing* Here you assign a second IP address to the wireless interface.
Second Local Netmask	Only for ***Working Mode*** = *Routing* Netmask for ***Second Local IP Number***.

Table 2-3: ***IP and Bridging*** menu fields

3 Advanced

The fields of the *ADVANCED* menu are described below.



```
X2302w Setup Tool                                 Bintec Access Networks GmbH
[WLAN-2-0][ADVANCED]: WLAN Specific Settings                        MyGateway

         Wireless Mode            802.11 mixed

         Maximum Bitrate          AUTO

         FOUR-X Burst             on

         TX Power (dBm)           18



          SAVE                               CANCEL
```

In the ***WIRELESS LAN*** ➜ ***ADVANCED*** menu WLAN specific settings can be modified. Changes, however, are not necessary in general.

The menu consists of the following fields:

Field	Description
Wireless Mode	Operating mode of the AP. Possible values: - *802.11g*: 54Mbit Clients only - *802.11b*: 11Mbit Mode - *802.11 mixed* (default value): 11Mbit and 54Mbit mixed mode - *802.11 mixed short:* 11Mbit and 54Mbit mixed mode with short preamble - *802.11 mixed long*: 11Mbit and 54Mbit mixed mode with long preamble. This mode is used for Centrino Clients if there are connecting problems.
Maximum Bitrate	The maximum Bitrate from/to a client. Possible values: - *AUTO* (default value) - *1* up to *54 Mbit*
FOUR-X Burst	This feature increases the maximum burst time for the transmission to a connected station, thus increasing the throughout in slower WLANs. If problems arise with older WLAN hardware, set to *off*. Possible values: *off*, *on* (default)
TX Power (dBm)	TX output from the AP in dB. Possible values: *6, 9, 12, 15, 18* dB Default value is *18*.

Table 3-1: ***ADVANCED*** menu fields

Index: Wireless LAN