funkwerk
enterprise communications

User's Guide

bintec R3000w / R3400 / R3800

Wireless LAN

Version 0.9

Purpose

This document is part of the user's guide to the installation and configuration of bintec gateways running software release 7.3.1 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, Funkwerk Enterprise Communications GmbH 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 bintec gateways can be found at www.funkwerk-ec.com.

As multiprotocol gateways, bintec 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. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

bintec and the bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

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

Copyright

Guidelines and standards

bintec 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 Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH 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 3

2 Wireless Interface Submenu 7

2.1 ACL Filter Submenu 14

2.2 IP and Bridging Submenu 15

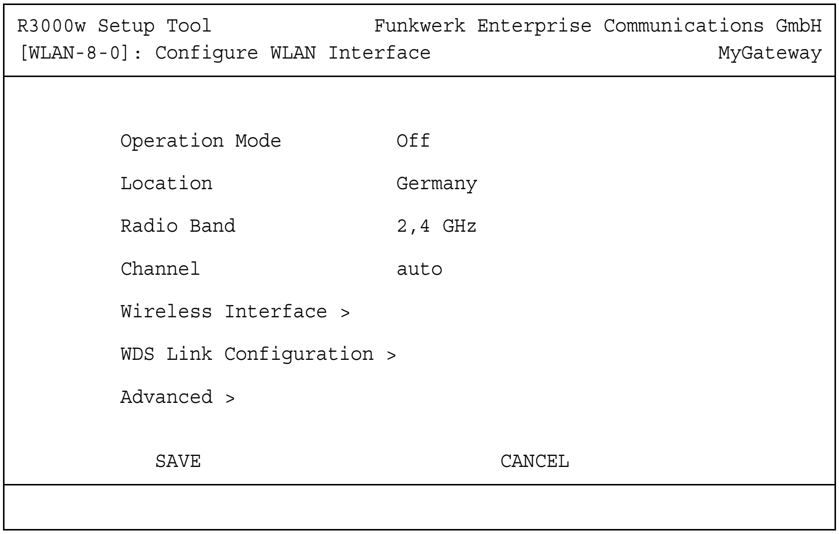
3 WDS Link Configuration Submenu 19

4 Advanced 23

Index: Wireless LAN 27

1 Wireless LAN Menu

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



```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[WLAN-8-0]: Configure WLAN Interface                         MyGateway


         Operation Mode          Off

         Location                Germany

         Radio Band              2,4 GHz

         Channel                 auto

         Wireless Interface >

         WDS Link Configuration >

         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 is independent of position and number of connections).

Standard: IEEE 802.11

802.11 WLANs offer all functions of a cabled network. WLAN transmits indoors and outdoors at a maximum of 100 mW.

IEEE 802.11g is presently the primarily used standard for radio-based LANs and offers a data transfer rate of 54 mbps. This method operates at a frequency of 2,4GHz (2400 MHz - 2485 MHz), which guarantees that buildings are penetrated with the required transmitting power that, however, does not affect health.

802.11b is compatible with 802.11g, operating with 2,4 GHz (2400 MHz - 2485 MHz) and offering a data transfer rate of 11 Mbps. 802.11g and 802.11b WLAN systems are free of charge and are not to be registered.

With 802.11a data transfer rates up to 54 Mbps can be used inbetween 5150 MHz - 5725 MHz. Due to the greater frequency range 19 frequencies are available (in Germany). This frequency range is not to be registered, too. In Europe a transmitting power of 1000 mW is available with 802.11h, but has to be applied with TPC (TX Power Control, methode to control the transmitting power of radio equipment to reduce interferences) and DFS (Dynamic Frequency Selection). TPC and DFS are applied to avoid interferences with satellite communication and radar equipment.

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

Field	Description
Operation Mode	Defines, whether the gateway operates as access point (*Access Point*) or not (*Off*, default value).
Location	The country setting of the AP. Possible values are all countries preconfigured on the wireless module of the gateway. The range of the optional channels differs according to the country setting selected. Default value is *Germany*.
Radio band	Frequency range the access point is to operate in. Possible values: ■ *2,4 GHz* (default value): in ***ADVANCED WIRELESS*** ➜ ***WIRELESS MODE*** you can choose from different WLAN standards. *802.11 mixed* is used per default. ■ *5 GHz*

Field	Description
Usage area	Only for ***RADIO BAND*** = *5 GHz* Installation location of the access point. Possible values: ■ *anywhere* (default value): The access point is to operate indoors and outdoors. ■ *indoor*: The access point is to operate indoors. ■ *outdoor*: The access point is to operate outdoors.
Channel	The channel used by the AP. Possible values: ■ *1 ... 13*: only for ***RADIO BAND*** = *2,4 GHz* ■ *auto* (default value): the channel is detected automatically; single option for ***RADIO BAND*** = *5 GHz.*

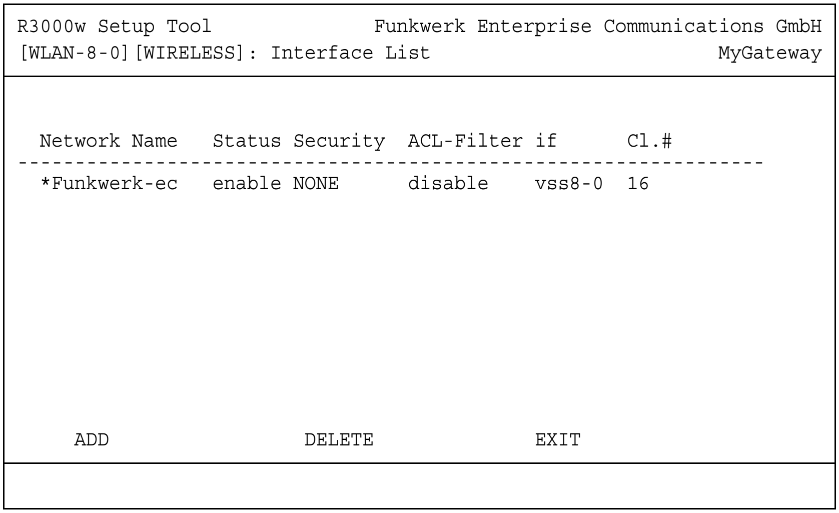
Table 1-1: ***WIRELESS LAN*** menu fields

The menu provides access to the following submenus:

- ***WIRELESS INTERFACE***
- ***WDS LINK CONFIGURATION***
  only for ***RADIO BAND*** = *2,4 GHz*
- ***ADVANCED***

2 Wireless Interface Submenu

The fields of the *Wireless Interace* menu are described below.



```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[WLAN-8-0][WIRELESS]: Interface List                         MyGateway


  Network Name   Status Security  ACL-Filter if      Cl.#
-----------------------------------------------------------------
  *Funkwerk-ec   enable NONE      disable    vss8-0  16









     ADD                 DELETE              EXIT

```

The ***Wireless LAN*** ➜ ***Wireless Interface*** submenu displays a list with already configured wireless interfaces and contains essential settings such as network name, status, security mode etc. The '*' in front of the ***Network Name*** (➤➤ **SSID**) means that the network name is visible on ➤➤ **active probing**.

Each wireless interface (with prefix ➤➤ **vss**) has its own IP settings and can use all standard interface specific features such as QoS, Stateful Inspection, Accounting, Access Lists, NAT 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.

WPA WPA (Wi-Fi Protected Access) offers increased protection by means of dynamic keys, which are based on the Temporal Key Integrity Protocol (TKIP), and offers PSK (Pre-Shared-Keys) or Extensible Authentication Protocol (EAP) via 802.1x (e.g. via RADIUS) for the authentication of users.

The authentication via EAP is normally used in vast Wireless LAN installations, because it requires an authentication server (e.g. a RADIUS server). In smaller networks, mostly for SoHo (Small Office, Home Office), PSK (Pre-Shared-Keys) are normally used. All participants of the Wireless LAN must thus know the PSK, as the session key is generated by means of it.

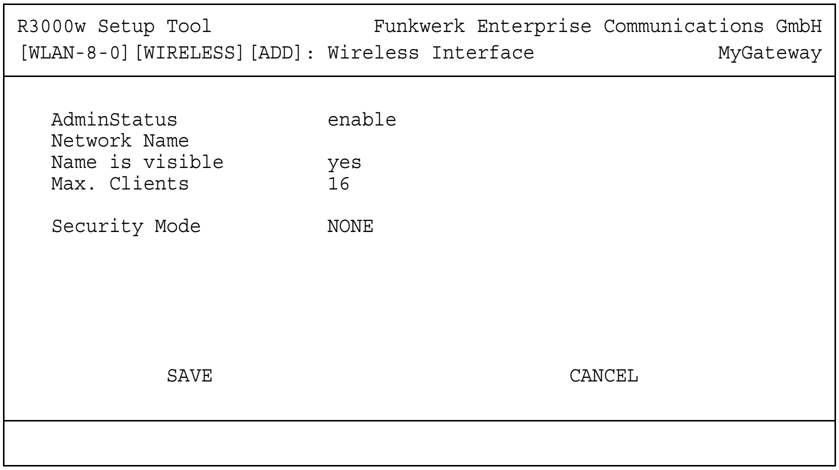
WPA2 WPA2 is the successor of WPA. It implements the full 802.11i-standard and uses the encryption algorithm AES (Advanced Encryption Standard).

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.
- Set ***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*, *WPA PSK* or *WPA 802.1x* with TKIP (WPA) or AES (WPA2) or both, and entering the respective key for the access point into ***Key 1 - 4*** resp. ***Enter Preshared Key*** and for the WLAN clients.

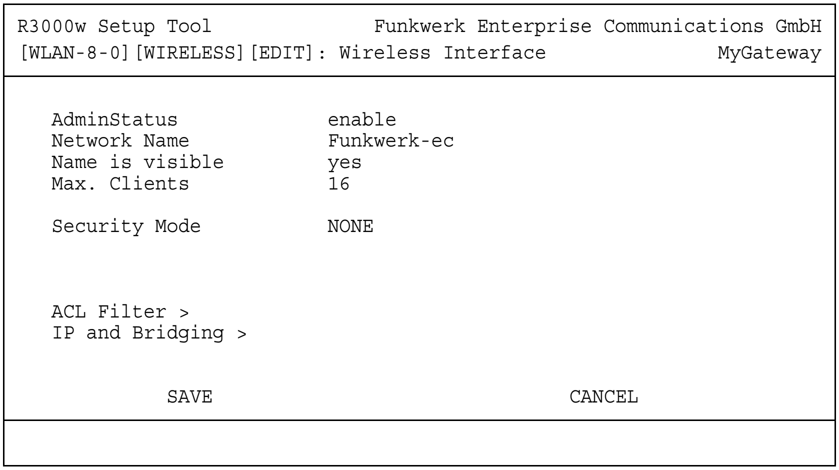
- The WEP key should regularly be changed by modifying the ***Default Key***. Chose the longer WEP key with 104/128 bits.
- To transfer highly sensitive data it is recommended to select ***Security Mode*** = *WPA 802.1x* with ***WPA/WPA2 mixed mode*** = *WPA2 only*. These methods comprise hardware based 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. All other clients are rejected and listed under ***REJECT***.

The generation of new wireless interfaces is carried out in ***Wireless LAN*** ➜ ***Wireless Interfaces*** ➜ **ADD**:



```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[WLAN-8-0][WIRELESS][ADD]: Wireless Interface                MyGateway

   AdminStatus              enable
   Network Name
   Name is visible          yes
   Max. Clients             16

   Security Mode            NONE




             SAVE                               CANCEL
```

The adjustment of already configured wireless interfaces is carried out in ***Wireless LAN*** ➜ ***Wireless Interfaces*** ➜ **EDIT**:



```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[WLAN-8-0][WIRELESS][EDIT]: Wireless Interface                MyGateway

   AdminStatus             enable
   Network Name            Funkwerk-ec
   Name is visible         yes
   Max. Clients            16

   Security Mode           NONE



   ACL Filter >
   IP and Bridging >


             SAVE                               CANCEL
```

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

Field	Description
AdminStatus	Defines the 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 for the clients.

Field	Description
Max. Clients	Maximum number of client connections allowed defined for this interface. Maximum 64 connections can be distributed to all wireless interfaces.
Security Mode	The security mode (encryption and authentication) of the wireless interface. Possible values: ■ *NONE* (default value): no encryption or authentication ■ *WEP 40/64*: WEP 40Bit ■ *WEP 104/128*: WEP 104Bit ■ *WPA PSK*: WPA with Preshared Key authentication ■ *WPA 802.1x*: WPA with EAP (RADIUS-authentication) If ***SECURITY MODE*** is set to *WPA 802.1x* the following note is displayed: *A Radius Server configuration in RADIUS setup is required.*
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. Default value is *Key 1*.

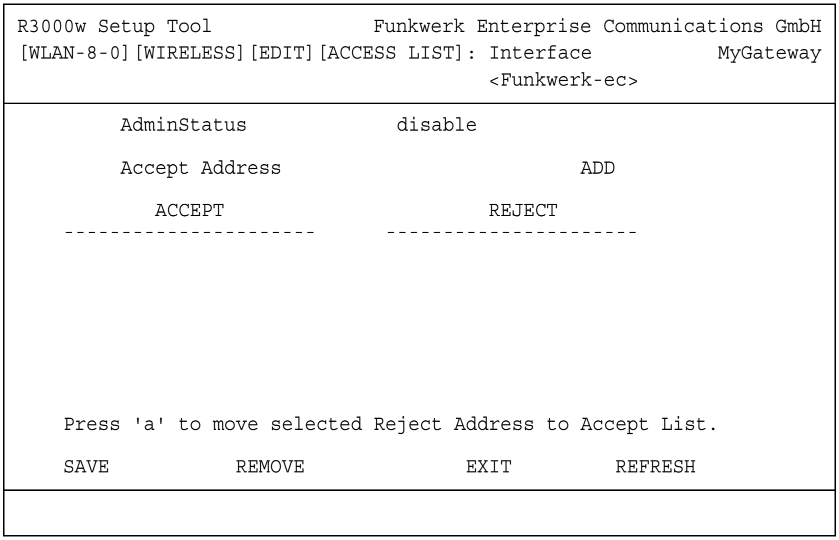
Field	Description
Key <1 - 4>	Only for **SECURITY MODE** = *WEP 40/64, WEP 104/128* Here you enter the WEP key. WEP keys can be entered in two different ways: ■ Direct Digit Input in hexadecimal format Starting the key with *0x*, disables the generator. Enter the key with the exact count of hexadecimal digits 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
Enter Preshared Key	Only for ***SECURITY MODE*** = *WPA PSK* Here you enter the WPA passphrase. Enter an ASCII String of 8 - 64 characters.
WPA/WPA2 mixed mode	Only for ***SECURITY MODE*** = *WPA PSK* and *WPA 802.1x* Here you select whether to apply WPA (with TKIP encryption) or WPA2 (with AES encryption) or both. Possible values: ■ *WPA + WPA2* (default value) ■ *WPA only* ■ *WPA2 only*
WPA2 preauthentication	Only for ***SECURITY MODE*** = *WPA 802.1x* with ***WPA/WPA2 MIXED MODE*** = *WPA + WPA2* and *WPA2 only* With this option registered clients can pre authenticate at other access points in the same radio cell. Thus these clients can change faster to the other access point ("roaming"), as the RADIUS authentication can be omitted during registration. The preauthentication is only possible with the client being registered at the access point with WPA2. Possible values: ■ *enabled*: The Access Point allows preauthentication of clients at other access points. ■ *disabled* (default value): Preauthentication requests of clients are ignored.

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

2.1 ACL Filter Submenu

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



```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[WLAN-8-0][WIRELESS][EDIT][ACCESS LIST]: Interface           MyGateway
                                         <Funkwerk-ec>

         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*** ➜ ***MAC FILTER*** submenu, hardware specific acces control is configured. Thus it is possible to allow only specific clients to access the access point. This filter is checked before any other security mechanism is activated. The entered addresses are MAC based.

MAC Address Lists

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

The ***REJECT*** list displays all rejected addresses.

Default behaviour: If ***ADMINSTATUS*** = *disabled*, all clients are accepted. As soon as ***ADMINSTATUS*** = *enabled* is set and no MAC address is listed in the ***ACCEPT*** list, all clients are blocked. Only those clients whos MAC addresses are then entered manually into the ***ACCEPT*** list or are moved from the ***REJECT*** to the ***ACCEPT*** list are accepted.

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.

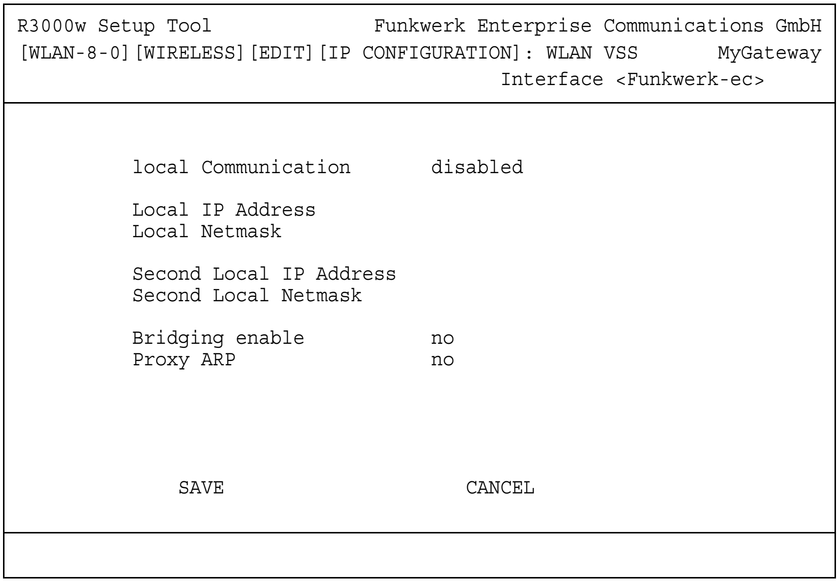
The menu consists of the following fields:

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: ***ACL FILTER*** menu fields

2.2 IP and Bridging Submenu

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



```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[WLAN-8-0][WIRELESS][EDIT][IP CONFIGURATION]: WLAN VSS       MyGateway
                                           Interface <Funkwerk-ec>


          local Communication       disabled

          Local IP Address
          Local Netmask

          Second Local IP Address
          Second Local Netmask

          Bridging enable           no
          Proxy ARP                 no




              SAVE                     CANCEL
```

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

The menu consists of the following fields:

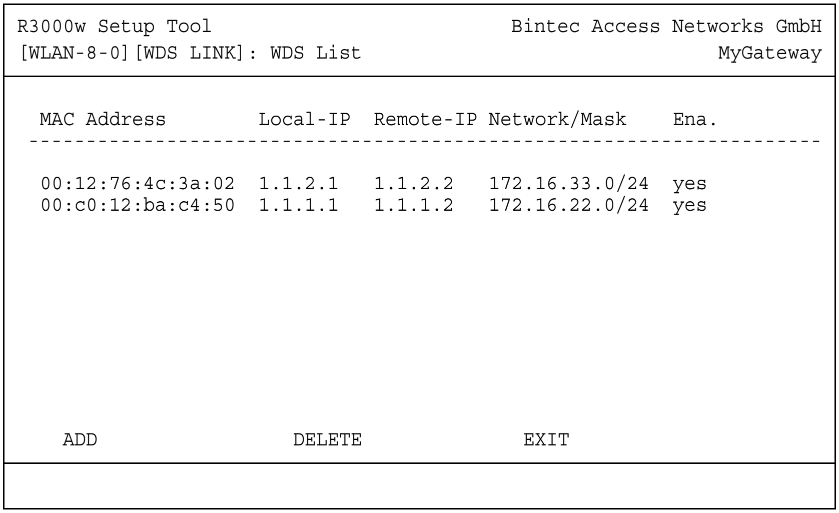
Field	Description
local communication	Allows the communication between the clients, authenticated at this SSID, to e.g. access common shares. Possible values: *enabled*, *disabled* (default value)
Local IP Address	Here you assign an IP address to the wireless interface.
Local Netmask	Netmask for ***Local IP Number***.
Second Local IP Address	Here you assign a second IP address to the wireless interface.
Second Local Netmask	Netmask for ***Second Local IP Number***.

Field	Description
Bridging enable	Defines the operatin mode of the wireless interface. Possible values: ■ *no* (default value): Routing is enabled on the wireless interface. ■ *yes*: Bridging is enabled on the wireless interface.
Proxy ARP	Enables the gateway to answer ARP requests from its own LAN acting for a defined WAN partner. Possible values: *on*, *off* (default value).

Table 2-3: ***IP AND BRIDGING*** menu fields

3 WDS Link Configuration Submenu

The fields of the *WDS LINK CONFIGURATION* menu are described below. (The screenshot shows example values.)



```
R3000w Setup Tool                            Bintec Access Networks GmbH
[WLAN-8-0][WDS LINK]: WDS List                                 MyGateway

  MAC Address        Local-IP  Remote-IP Network/Mask    Ena.
 --------------------------------------------------------------------

  00:12:76:4c:3a:02  1.1.2.1   1.1.2.2   172.16.33.0/24  yes
  00:c0:12:ba:c4:50  1.1.1.1   1.1.1.2   172.16.22.0/24  yes










    ADD                 DELETE              EXIT
```

The ***WIRELESS LAN*** ➜ ***WDS LINK CONFIGURATION*** menu shows a list of all configured WDS (Wireless Distribution System) Links.

The menu is only displayed for ***RADIO BAND*** = *2,4 GHz*.

WDS links are static links between access points (AP). These links are used in general to connect clients to networks which cannot be reached directly, e.g. because of long distances. The AP sends data from one client to another AP that transfers the data then to the other client.

Attention!

Note that traffic sent between access points in an WDS link is transferred unencrypted. We strongly recommend the use of IPSec to secure traffic in WDS links.

WDS links are configured as interfaces with the prefix *wds*. They operate in the same way as the VSS interfaces, differing, however, by predefined routing. A

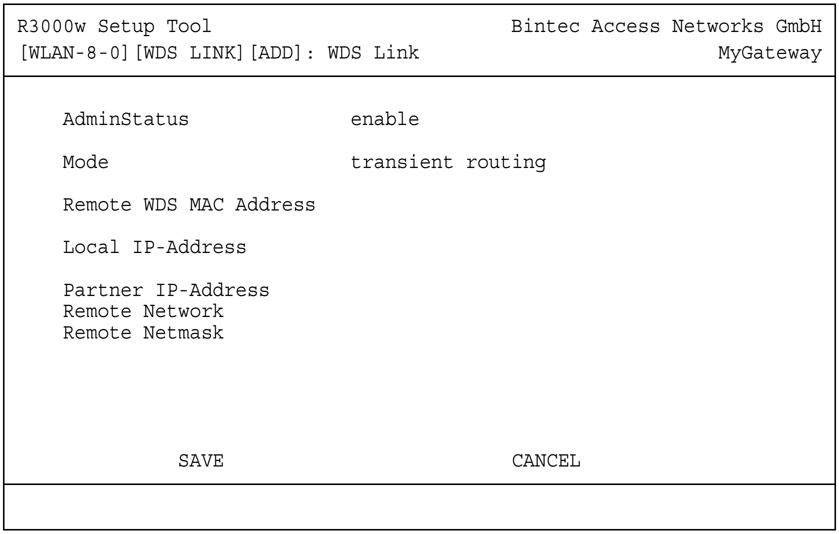
WDS link is configured as transfer network: it is a point-to-point or a point-to-multipoint connection between two gateways serving different networks.

The list contains the following descriptions

Column	Content
MAC Address	MAC address of the destination WDS link. (= ***REMOTE WDS MAC ADDRESS*** in ***WDS LINK CONFIGURATION*** ➜ ***ADD/EDIT***)
Local IP	The IP address of the local WDS interface. (= ***LOCAL IP-ADDRESS*** in ***WDS LINK CONFIGURATION*** ➜ ***ADD/EDIT***)
Remote IP	The IP address of the destination WDS interface. (= ***PARTNER IP-ADDRESS*** in ***WDS LINK CONFIGURATION*** ➜ ***ADD/EDIT***)
Network/Mask	The destination network which is connected via this WDS link to the destination AP via Ethernet or Wireless LAN. (= ***REMOTE NETWORK*** & ***REMOTE NETMASK*** ➜ ***ADD/EDIT***)
Ena.	The link is enabled (*yes*) or not (*no*). (= ***ADMINSTATUS*** in ***WDS LINK CONFIGURATION*** ➜ ***ADD/EDIT***)

Table 3-1: WDS List

The configuration of the WDS links is carried out in the ***WIRELESS LAN*** ➜ ***WDS LINK CONFIGURATION*** ➜ ***ADD/EDIT*** submenu.



```
R3000w Setup Tool                             Bintec Access Networks GmbH
[WLAN-8-0][WDS LINK][ADD]: WDS Link                             MyGateway

    AdminStatus                 enable

    Mode                        transient routing

    Remote WDS MAC Address

    Local IP-Address

    Partner IP-Address
    Remote Network
    Remote Netmask




              SAVE                            CANCEL
```

The menu consists of the following fields:

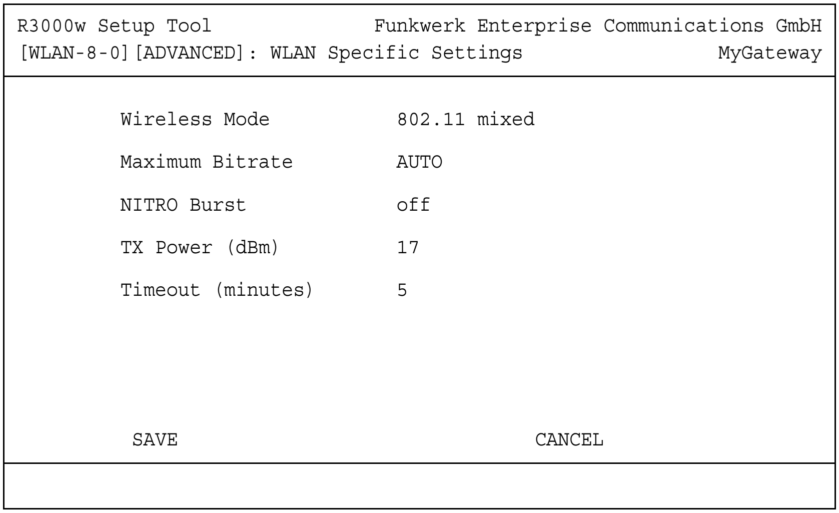
Field	Description
AdminStatus	Status of the WDS link. Possible values: *enable* (default value), *disable*
Mode	Selection of mode the WDS link is to operate in. Possible values: ■ *transient routing* (default value): IP Routing to a destination host or network including any transit network available. ■ *bridging*: Bridging mode activated. ■ *routing*: IP Routing to a destination host or network not including any transit network available.
Remote WDS MAC Address	MAC address of the destination WDS link.

Field	Description
Local IP-Address	Only for ***MODE*** = *routing* or *transient routing* IP address of the local WDS interface.
Local Netmask	Only for ***MODE*** = *routing* Netmask for ***IP-ADDRESS***
Partner IP-Address	Only for ***MODE*** = *transient routing* IP address of the destination WDS interface.
Remote Network	Only for ***MODE*** = *transient routing* The destination network which is connected via this WDS link to the destination AP via Ethernet or Wireless LAN.
Remote Netmask	Only for ***MODE*** = *transient routing* Netmask for ***REMOTE NETWORK***.

Table 3-2: ***WDS LINK CONFIGURATION*** ➜ ***ADD/EDIT*** menu fields

4 Advanced

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



```
R3000w Setup Tool             Funkwerk Enterprise Communications GmbH
[WLAN-8-0][ADVANCED]: WLAN Specific Settings                MyGateway

         Wireless Mode           802.11 mixed

         Maximum Bitrate         AUTO

         NITRO Burst             off

         TX Power (dBm)          17

         Timeout (minutes)       5




          SAVE                                 CANCEL
```

In the ***WIRELESS LAN*** ➜ ***ADVANCED*** menu you will find WLAN specific settings. Changes, however, are not necessary in general.

The menu consists of the following fields:

Field	Description
Wireless Mode	Only for ***WIRELESS LAN*** **➜** ***RADIO BAND*** = *2,4 GHz* Operating mode of the AP. Possible values: ■ *802.11g*: 54Mbit Clients only ■ *802.11b*: 11Mbit Mode only ■ *802.11 mixed* (default value) / *802.11 mixed short*: 11Mbit and 54Mbit mixed mode ■ *802.11 mixed long*: 11Mbit and 54Mbit mixed mode with long preamble. This mode is required for clients that only support 1 and 2 mbps. It is also used for Centrino Clients if there are connecting problems.
Maximum Bitrate	The maximum Bitrate from/to a client. Possible values: ■ *AUTO* (default value) ■ Chose a predefined value in the range of *1* up to *54 Mbit*

Field	Description
NITRO Burst	This feature increases the maximum burst time for the transmission to a connected station, thus increasing the throughout in slower WLANs. Several WLAN data packets are sent consecutively ("Burst"). The necessary CTS packet for administration is only required once. Choosing an option defines the maximum time this packet burst is to last. Possible values: ■ *Off* (default value): 0 (= no Burst) ■ *Compatible*: Burst Time = 0.65ms ■ *Ideal*: Burst Time = 1.3ms ■ *Maximum*: Burst Time = 5ms NITRO Burst conforms with the 802.11 standards, i.e. the with NITRO Burst mode data traffic enhancements can be reached with each 11g-compatible client. If problems arise with older WLAN hardware, set to *off*.
TX Power (dBm)	TX output from the AP in dBm. Possible values: *1* to *18.* Default value is *17*.
Timeout (minutes)	Broken link detection: Here you can set the time after which a client is automatically disconnected if no signal has been received. Possible values: *1..240* Minutes Default value is *5*.

Table 4-1: ***ADVANCED*** menu fields

Index: Wireless LAN

Numerics

802.11 b/g mixed 24

A

Accept Address 15
Access Point 4
ACL Filter 14
Active Probing 7
AdminStatus 10, 15, 21

B

Bridging enable 17

C

Channel 5

D

Default Key 11

E

Ena. 20
Enter Preshared Key 13

K

Key 12

L

local communication 16
Local IP 20
Local IP-Address 22
local IP-Number 16
Local Netmask 22
local Netmask 16
Location 4

M

MAC Address 20
Max. Clients 11
Maximum Bitrate 24
Mode 21

N

Name is visible 10

Network Name	10
Network/Mask	20
NITRO Burst	25

O

Operation Mode	4

P

Partner IP-Address	22
Proxy ARP	17

R

Radio band	4
Remote IP	20
Remote Netmask	22
Remote Network	22
Remote WDS MAC Address	21

S

Second Local IP-Number	16
Second Local Netmask	16
Security Mode	11
SSID	10

T

Timeout (minutes)	25
TX Power (dBm)	25

U

Usage area	5

V

vss	7

W

wds	19
WEP	8
Wireless Mode	24
WPA	8
WPA/WPA2 mixed mode	13
WPA2 preauthentication	13