Benutzerhandbuch

bintec R3000w / R3400 / R3800

Wireless LAN

Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec-Gateways ab Software-Release 7.3.1. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.funkwerk-ec.com.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für bintec-Gateways finden Sie unter www.funkwerk-ec.com.

Als Multiprotokollgateways bauen bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

bintec und das bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

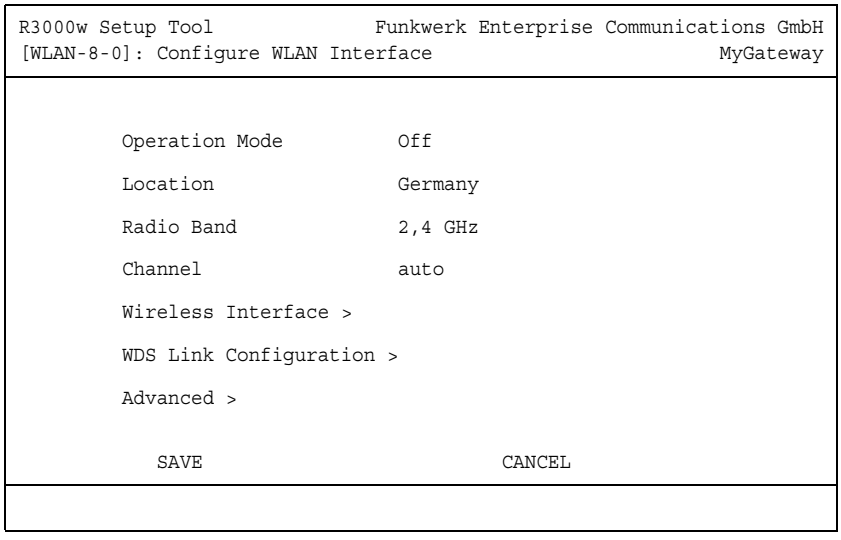
Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Menü Wireless LAN

Im Folgenden werden die Felder des Menüs *WIRELESS LAN* beschrieben.



Das Menü ***WIRELESS LAN*** enthält grundlegende Einstellungen, um Ihr Gateway als ➤➤ **Access Point** (AP) zu betreiben.

Bei Funk-LAN oder Wireless LAN (WLAN = Wireless Local Area Network), handelt es sich um den Aufbau eines Netzwerkes mittels Funktechnik.

Netzwerkfunktionen

Ein WLAN ermöglicht genauso wie ein kabelgebundenes Netzwerk alle nötigen Netzwerkfunktionen. Somit steht der Zugriff auf Server, Dateien, Drucker, Mailsystem genauso zuverlässig zur Verfügung wie der firmenweite Internetzugang. Dadurch dass keine Verkabelung der Geräte nötig ist, hat ein WLAN den großen Vorteil, dass nicht auf bauliche Einschränkungen geachtet werden muß (d.h. der Gerätestandort ist unabhängig von Position und Anzahl von Anschlüssen).

Derzeit gültiger Standard: IEEE 802.11

Bei 802.11-WLANs sind alle Funktionen eines verkabelten Netzwerks möglich. WLAN sendet innerhalb und ausserhalb von Gebäuden mit maximal 100 mW.

IEEE 802.11g ist der derzeit am weitesten verbreitete Standard für Funk-LANs und bietet eine maximale Datenübertragungsrate von 54 Mbit/s. Dieses Verfah-

ren arbeitet im Funkfrequenzbereich von 2,4 GHz, der gewährleistet, dass Gebäudeteile möglichst gut, bei geringer, gesundheitlich unproblematischer Sendeleistung durchdrungen werden.

Ein zu 802.11g kompatibler Standard ist 802.11b, der im 2,4 GHz-Band (2400 MHz - 2485 MHz) arbeitet und eine maximale Datenübertragungsrate von 11 Mbit/s bietet. 802.11b- und 802.11g-WLAN Systeme sind anmelde- und gebührenfrei.

Mit 802.11a sind im Bereich 5150 GHz bis 5725 MHz Bandbreiten bis 54 Mbit/s nutzbar. Mit dem größeren Frequenzbereich stehen 19 nicht überlappende Frequenzen (in Deutschland) zur Verfügung. Auch dieser Frequenzbereich ist in Deutschland lizenzfrei nutzbar. In Europa werden mit 802.11h nicht nur 30 mW sondern 1000 mW Sendeleistung nutzbar, jedoch nur unter Einsatz von TPC (TX Power Control, Methode zur Regelung der Sendeleistung bei Funksystemen zur Reduktion von Interferenzen) und DFS (Dynamic Frequency Selection). TPC und DFS sollen sicherstellen, dass Satellitenverbindungen und Radargeräte nicht gestört werden.

Das Menü ***WIRELESS LAN*** besteht aus folgenden Feldern:

Feld	Bedeutung
Operation Mode	Hier wird festgelegt, ob das Gateway als Access Point (*Access Point*) betrieben wird oder nicht (*Off*, Defaultwert).
Location	Die Ländereinstellung des AP. Mögliche Werte sind alle auf dem Wireless-Modul des Gateways vorkonfigurierten Länder. Der Bereich der auswählbaren Kanäle variiert je nach Ländereinstellung. Defaultwert ist *Germany*.

Feld	Bedeutung
Radio band	Frequenzbereich, in dem der Access Point betrieben werden soll. Mögliche Werte: ■ *2,4 GHz* (Defaultwert): in ***ADVANCED WIRELESS*** ➜ ***WIRELESS MODE*** stehen hierfür verschiedene WLAN Standards zur Auswahl. Standardmässig wird *802.11 mixed* angewendet. ■ *5 GHz*
Usage area	Nur für ***RADIO BAND*** = *5 GHz* Einsatzbereich des Access Points. Mögliche Werte: ■ *anywhere* (Defaultwert): Der Access Point wird innerhalb oder ausserhalb von Gebäuden betrieben. ■ *indoor*: Der Access Point wird innerhalb von Gebäuden betrieben. ■ *outdoor*: Der Access Point wird ausserhalb von Gebäuden betrieben.
Channel	Der Kanal, der vom AP verwendet wird. Mögliche Werte: ■ *1 ... 13:* nur für ***RADIO BAND*** = *2,4 GHz* ■ *auto* (Defaultwert): der Kanal wird automatisch erkannt; einzige Option für ***RADIO BAND*** = *5 GHz*.

Tabelle 1-1: Felder im Menüs ***WIRELESS LAN***

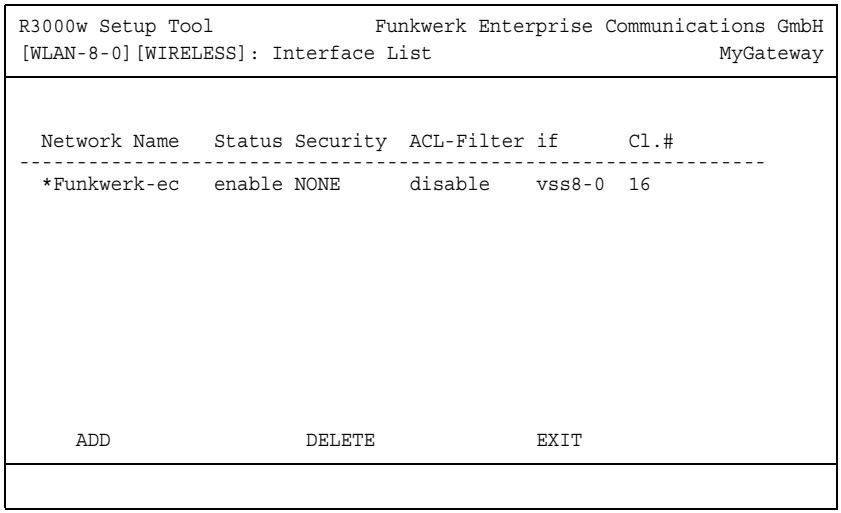
Über das Menü gelangen Sie in folgende Untermenüs:

- ***WIRELESS INTERFACE***

- ***WDS LINK CONFIGURATION***
  nur für ***RADIO BAND*** = *2,4 GHz*
- ***ADVANCED***

2 Untermenü Wireless Interface

Im Folgenden werden die Felder des Menüs *WIRELESS INTERACE* beschrieben.



Das Untermenü ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACE*** enthält eine Liste mit allen konfigurierten Wireless Interfaces und zeigt deren grundlegende Einstellungen des Wireless Interfaces wie Netzwerkname, Status, Sicherheitsmodus etc. Ein '*' vor den Netzwerknamen (***NETWORK NAME***, ➤➤ **SSID**) weist darauf hin, dass der Netzwerkname bei ➤➤ **Active Probing** propagiert wird.

Jedes Wireless Interface (mit dem Präfix ➤➤ **vss**) erhält eigene IP-Einstellungen und kann alle Möglichkeiten eines Standardinterfaces wie QoS, Stateful Inspection, Accounting, Access Listen, NAT etc. nutzen. Dadurch bieten sich für das Wireless Interface breitgefächerte Anwendungsmöglichkeiten.

Das bintec WLAN Gateway kann nicht nur im Bridging Modus betrieben werden, sondern ist auch komplett in die Routingumgebung integriert.

Absicherung von Funknetzwerken

Sicherheit Da im WLAN Daten über das Übertragungsmedium Luft gesendet werden, können diese theoretisch von jedem Angreifer, der über die entsprechenden Mittel

verfügt, abgefangen und gelesen werden. Daher muss der Absicherung der Funkverbindung besondere Beachtung geschenkt werden.

WEP 802.11 definiert den Sicherheitsstandard WEP (Wired Equivalent Privacy = Verschlüsselung der Daten mit 40/64 bit (***Security Mode*** = *WEP 40/64*) bzw. 104/128 bit (***Security Mode*** = *WEP 104/128*)). Das verbreitet genutzte WEP hat sich jedoch als anfällig herausgestellt. Ein höheres Maß an Sicherheit erreicht man jedoch nur durch zusätzlich zu konfigurierende, auf Hardware basierende Verschlüsselung (wie z.B. 3DES oder AES). Hierdurch können auch die sensibelsten Daten ohne Angst vor Datendiebstahl über die Funkstrecke übertragen werden.

IEEE 802.11i Der Standard IEEE 802.11i für Wireless Systeme beinhaltet Sicherheitsspezifikationen für Funknetze, besonders im Hinblick auf Verschlüsselung. Er ersetzt das unsichere Verschlüsselungsverfahren WEP (Wired Equivalent Privacy) durch WPA (Wi-Fi Protected Access). Zudem beschreibt er die Verwendung von Advanced Encryption Standard (AES) zur Verschlüsselung von Daten.

WPA WPA (Wi-Fi Protected Access) bietet zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Nutzern PSK (Pre-Shared-Keys) oder Extensible Authentication Protocol (EAP) über 802.1x (z. B. RADIUS) an.

Die Authentifizierung über EAP wird meist in grossen Wireless LAN Installationen genutzt, da hierfür eine Authentifizierungsinstanz in Form eines Servers (z.B. ein RADIUS-Server) benötigt wird. In kleineren Netzwerken, wie sie im SoHo (Small Office, Home Office) Bereich häufig auftreten, werden meist PSK (Pre-Shared-Keys) genutzt. Der PSK muss somit allen Teilnehmern des Wireless LAN bekannt sein, da mit seiner Hilfe der Sitzungsschlüssel generiert wird.

WPA2 Die Erweiterung von WPA ist WPA2. In WPA2 wurde nicht nur der vollständige 802.11i-Standard umgesetzt, sondern es nutzt auch einen anderen Verschlüsselungsalgorithmus AES (Advanced Encryption Standard).

Sicherheitsmaßnahmen Zur Absicherung der auf dem WLAN übertragenen Daten sollten Sie im Menü ***Wireless LAN*** ➜ ***Wireless Interface*** gegebenenfalls folgende Konfigurationsschritte vornehmen:

- Ändern Sie die Default-SSID, ***Network Name*** = *Funkwerk-ec*, Ihres Access Points.

- Setzen Sie ***WIRELESS INTERFACE*** ➜ ***NAME IS VISIBLE*** = *no*. Damit werden alle WLAN-Clients ausgeschlossen, die mit dem allgemeinen ***NETWORK NAME*** (SSID) *Any* einen Verbindungsaufbau versuchen und die nicht die eingestellten SSIDs kennen.
- Nutzen Sie die zur Verfügung stehenden Verschlüsselungsmethoden. Wählen Sie dazu ***SECURITY MODE*** = *WEP 40/64*, *WEP 104/128*, *WPA PSK* oder *WPA 802.1x* mit TKIP (WPA) oder AES (WPA2) oder beidem, und tragen Sie den entsprechenden Schlüssel im Access Point unter ***KEY 1 - 4*** oder ***ENTER PRESHARED KEY*** und in den WLAN-Clients ein.
- Der WEP-Schlüssel sollte regelmässig geändert werden. Wechseln Sie dazu ***DEFAULT KEY***. Wählen Sie den längeren 104/128 Bit WEP-Schlüssel.
- Für die Übertragung von extrem sicherheitsrelevante Informationen, sollte ***SECURITY MODE*** = *WPA 802.1x* mit ***WPA/WPA2 MIXED MODE*** = *WPA2 only* konfiguriert werden. Diese Methode beinhaltet eine hardwarebasierte Verschlüsselung und RADIUS-Authentifizierung des Clients. In Sonderfällen ist auch eine Kombination mit IPSec möglich.
- Beschränken Sie den Zugriff auf das WLAN auf zugelassene Clients. Tragen Sie die MAC-Adressen der Funknetzwerkkarten dieser Clients in die ***MAC FILTER*** ➜ ***ACCEPT*** Liste ein. Schließen Sie alle anderen Clients von der Kommunikation mit dem Access Point aus, indem Sie die MAC-Adresse dieser Karten in die ***REJECT*** Liste eintragen (siehe “Untermenü ACL Filter” auf Seite 15).+

Die Erstellung von Wireless Interfaces erfolgt im Menü ***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
```

Die Anpassung von bereits konfigurierten Wireless Interfaces erfolgt im Menü ***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
```

Das Menü besteht aus folgenden Feldern:

Feld	Bedeutung
AdminStatus	Setzen des Betriebsstatus des Wireless Interfaces. Mögliche Werte: ■ *enable* (Defaultwert): Aktiviert das Interface. ■ *disable*: Deaktiviert das Interface.
Network Name	Name des Wireless Interfaces (SSID). Geben Sie eine ASCII Zeichenfolge mit max. 32 Zeichen ein.
Name is visible	Aktiviert die Übertragung von ***Network Name*** (SSID). Mögliche Werte: ■ *yes* (Defaultwert): ***Network Name*** ist sichtbar für Clients im Sendebereich. ■ *no*: ***Network Name*** ist für die Clients nicht sichtbar.
Max. Clients	Maximale Anzahl der erlaubten Client-Verbindungen, die für dieses Interface festgelegt werden. Maximal können 64 Verbindungen auf alle Wireless Interfaces verteilt werden.

Feld	Bedeutung
Security Mode	Der Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Wireless Interfaces. Mögliche Werte: ■ *NONE* (Defaultwert): weder Verschlüsselung noch Authentifizierung ■ *WEP 40/64*: WEP 40Bit ■ *WEP 104/128*: WEP 104Bit ■ *WPA PSK*: WPA mit Preshared Key Authentifizierung ■ *WPA 802.1x*: WPA mit EAP (RADIUS-Authentifizierung) Für ***SECURITY MODE*** = *WPA 802.1x* wird folgender Hinweis angezeigt: *A Radius Server configuration in RADIUS setup is required.*
Default Key	Nur für ***SECURITY MODE*** = *WEP 40/64, WEP 104/128* Hier wählen Sie einen der in ***KEY <1 - 4>*** konfigurierten Schlüssel als Defaultschlüssel aus. Defaultwert ist *Key 1*.

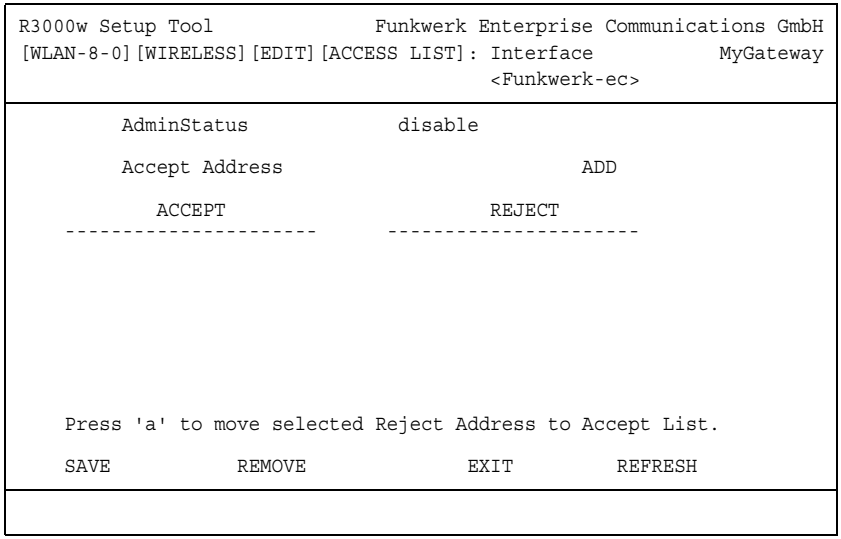
Feld	Bedeutung
Key <1 - 4>	Nur für ***Security Mode*** = *WEP 40/64, WEP 104/128* Hier geben Sie den WEP Schlüssel ein. Es gibt zwei Möglichkeiten, einen WEP Schlüssel einzugeben: ■ Direkte Eingabe in hexadezimaler Form Beginnt die Eingabe mit *0x*, wird der Generator deaktiviert. Geben Sie eine hexadezimale Zeichenfolge mit exakt der für den gewählten WEP Modus passenden Zeichenanzahl ein. 10 Zeichen für WEP40 oder 26 Zeichen für WEP104. Z.B. WEP40: *0xA0B23574C5*, WEP104: *0x81DC9BDB52D04DC20036DBD831* ■ Direkte Eingabe von ASCII Zeichen Wird ein Schlüssel beginnend mit " eingegeben, wird der Generator deaktiviert. Geben Sie eine Zeichenfolge mit der für den gewählten WEP Modus passenden Zeichenanzahl ein. Die Zeichenfolge endet mit ". Für WEP40 benötigen Sie eine Zeichenfolge mit 5 Zeichen, für WEP104 mit 13 Zeichen. Z.B. "*hallo*" for WEP40, "*funkwerk-wep1*" for WEP104.
Enter Preshared Key	Nur für ***Security Mode*** = *WPA PSK* Hier geben Sie das WPA Passwort ein. Geben Sie eine ASCII Zeichenfolge mit 8 - 64 Zeichen ein.

Feld	Bedeutung
WPA/WPA2 mixed mode	Nur für ***SECURITY MODE*** = *WPA PSK* und *WPA 802.1x* Hier wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA2 (mit AES-Verschlüsselung) oder beides anwenden wollen. Mögliche Werte: ■ *WPA + WPA2* (Defaultwert) ■ *WPA only* ■ *WPA2 only*
WPA2 preauthentication	Nur für ***SECURITY MODE*** = *WPA 802.1x* mit ***WPA/WPA2 MIXED MODE*** = *WPA + WPA2* und *WPA2 only* Mit dieser Option erlauben Sie, daß sich angemeldete Clients vorab bei anderen Access Points in derselben Funkzelle authentifizieren. Dies ermöglicht einen deutlich schnelleren Wechsel des Clients zum nächsten Access Point ("Roaming"), da bei der Anmeldung die RADIUS-Authentisierung übersprungen werden kann. Die Vorab-Authentisierung ist nur möglich, wenn der Client mit WPA2 am Access Point angemeldet ist. Mögliche Werte: ■ *enabled*: der Access Point erlaubt Vorab-Authentisierung von Clients auf anderen Access Points. ■ *disabled* (Defaultwert): Anfragen von Clients zur Vorab-Authentisierung werden ignoriert.

Tabelle 2-1: Felder im Menü ***WIRELESS INTERFACES***

2.1 Untermenü ACL Filter

Im Folgenden werden die Felder des Menüs *ACL FILTER* beschrieben.



Im Untermenü ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ ***ACL FILTER*** wird eine hardwarespezifische Zugangskontrolle konfiguriert. Dadurch ist es möglich, nur bestimmten Clients den Zugang zum Access Point zu gewähren. Dieses Filter wird aktiv, bevor andere Sicherheitsmechanismen greifen. Die eingegebenen Adressen sind MAC-basiert.

MAC Adresslisten

Die ***ACCEPT*** Liste enthält alle MAC Adressen, die für das Wireless Interface zugelassen werden sollen.

Die ***REJECT*** Liste zeigt alle abgewiesenen Adressen an.

Defaultverhalten: Wenn ***ADMINSTATUS*** = *disabled* gesetzt ist, werden alle Clients zugelassen. Sobald ***ADMINSTATUS*** = *enabled* gesetzt wird und kein Eintrag in der ***ACCEPT*** Liste vorhanden ist, werden alle Clients geblockt. Nur diejenigen Clients werden dann angenommen, die entweder manuell in ***ACCEPT*** Liste eingetragen oder von der ***REJECT*** in die ***ACCEPT*** Liste verschoben werden.

Zusätzliche Schaltflächen

Die Schaltfläche **REFRESH** aktualisiert die ***REJECT*** Liste, so dass Sie jederzeit den aktuellen Status über die abgewiesenen Adressen abrufen können.

Mit der Schaltfläche **REMOVE** können markierte Adressen von der ***ACCEPT*** Liste gelöscht werden. Bei Entfernen einer Adresse von der ***ACCEPT*** Liste wird eine aktive Verbindung sofort getrennt.

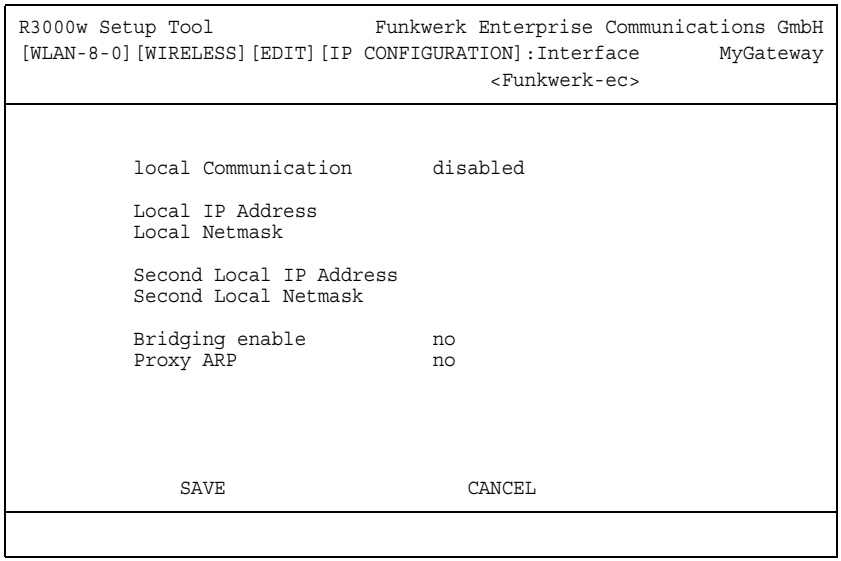
Das Menü besteht aus folgenden Feldern:

Feld	Bedeutung
AdminStatus	Aktiviert bzw. deaktiviert das Filter für das ausgewählte Interface. Mögliche Werte: *enable*, *disable* (Defaultwert)
Accept Address	Geben Sie die MAC Adresse ein, die zugelassen werden soll. Mögliche Werte: MAC Adressen mit 12 Zeichen. Die Adresse wird ohne ":" eingegeben. Wählen Sie **ADD**, um die eingegebene MAC Adresse der ***ACCEPT*** Liste hinzuzufügen. Wenn Sie einen Eintrag der ***REJECT*** Liste markieren und die **a** Taste drücken (Kleinschreibung beachten), wird der entsprechende Eintrag in die ***ACCEPT*** Liste verschoben. So müssen die zu akzeptierenden Adressen nicht manuell eingegeben werden.

Tabelle 2-2: Felder im Menü ***ACL FILTER***

2.2 Untermenü IP and Bridging

Im Folgenden werden die Felder des Menüs *IP AND BRIDGING* beschrieben.



Im Menü ***Wireless LAN*** ➜ ***Wireless Interfaces*** ➜ ***ADD/EDIT*** ➜ ***IP and Bridging*** konfigurieren Sie interface-spezifische IP Einstellungen und aktivieren gegebenenfalls den Bridging-Modus.

Das Menü besteht aus folgenden Feldern:

Feld	Bedeutung
local communication	Erlaubt die Kommunikation zwischen den Clients, die an dieser SSID authentifiziert sind, um z.B. auf Freigaben gemeinsam zuzugreifen. Mögliche Werte: *enabled*, *disabled* (Default-wert)
Local IP Address	Hier weisen Sie dem Wireless Interface eine IP-Adresse zu.
Local Netmask	Netzmaske zu ***Local IP Address***.
Second Local IP Address	Hier weisen Sie dem Wireless Interface eine zweite IP-Adresse zu.
Second Local Netmask	Netzmaske zu ***Second Local IP Address*** .

Feld	Bedeutung
Bridging enable	Definiert die Betriebsart des Wireless Interfaces. Mögliche Werte: ■ *no* (Defaultwert): Routing ist auf dem Wireless Interface aktiviert. ■ *yes*: Bridging ist auf dem Wireless Interface aktiviert.
Proxy ARP	Ermöglicht dem Gateway, ARP-Requests aus dem eigenen LAN stellvertretend für definierte WAN Partner zu beantworten. Mögliche Werte: *on*, *off* (Defaultwert).

Tabelle 2-3: Felder im Menü ***IP AND BRIDGING***

3 Untermenü WDS Link Configuration

Im Folgenden werden die Felder des Menüs *WDS LINK CONFIGURATION* beschrieben. (Die Abbildung enthält Beispielwerte.)

```
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
```

Das Menü ***WIRELESS LAN → WDS LINK CONFIGURATION*** enthält eine Liste aller konfigurierten WDS (Wireless Distribution System) Links.

Das Menü wird nur für ***RADIO BAND*** = *2,4 GHz* angezeigt.

WDS Links sind statische Links zwischen Access Points (AP), welche im allgemeinen dazu genutzt werden, Clients mit Netzen zu verbinden, die für diese nicht direkt erreichbar sind, z.B. wegen zu grosser Entfernung. Der AP sendet dabei Daten des einen Client zu einem weiteren AP, der dann die Daten an den anderen Client weiterleitet.

Achtung!

Beachten Sie, dass die Daten zwischen den APs über den WDS Link unverschlüsselt übertragen werden. Daher wird dringend empfohlen, IPSec anzuwenden, um die Daten auf WDS Links abzusichern.

WDS Links werden als Interfaces mit dem Präfix *wds* konfiguriert. Sie verhalten sich wie VSS Interfaces, und unterscheiden sich von diesen nur durch vordefiniertes Routing. Ein WDS Link wird als Transfernetzwerk definiert: es handelt sich um eine Punkt-zu-Punkt-Verbindung oder eine Punkt-zu-Mehrpunkt-Verbindung zwischen zwei Gateways, die in verschiedene Netzwerke eingebunden sind.

Die angezeigte Liste enthält folgende Informationen

Spalte	Inhalt
MAC Address	Die MAC Adresse des Ziel-WDS-Links. (= ***Remote WDS MAC Address*** in ***WDS Link Configuration*** ➜ ***ADD/EDIT***)
Local IP	Die IP-Adresse des lokalen WDS-Interfaces. (= ***Local IP-Address*** in ***WDS Link Configuration*** ➜ ***ADD/EDIT***)
Remote IP	Die IP-Adresse des Ziel-WDS-Interfaces. (= ***Partner IP-Address*** in ***WDS Link Configuration*** ➜ ***ADD/EDIT***)
Network/Mask	Das Ziel-Netzwerk, das mittels dieses WDS-Links an den Ziel-AP per Ethernet oder Wireless LAN angeschlossen ist. (= ***Remote Network*** & ***Remote Netmask*** ➜ ***ADD/EDIT***)
Ena.	Der WDS-Link ist aktiviert (*yes*) bzw. deaktiviert (*no*). (= ***AdminStatus*** in ***WDS Link Configuration*** ➜ ***ADD/EDIT***)

Tabelle 3-1: WDS Liste

Die Konfiguration der WDS Links erfolgt im Untermenü ***Wireless LAN*** ➜ ***WDS Link Configuration*** ➜ ***ADD/EDIT***.

```
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
```

Das Menü besteht aus folgenden Feldern:

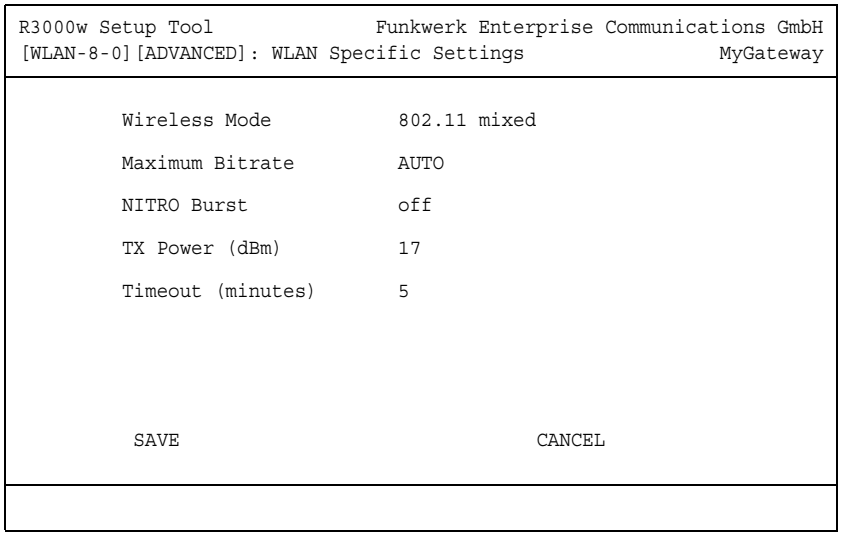
Feld	Bedeutung
AdminStatus	Status des WDS-Links. Mögliche Werte: *enable* (Defaultwert), *disable*
Mode	Auswahl des Modus, in dem der WDS Link betrieben wird. Mögliche Werte: ■ *transient routing* (Defaultwert): IP Routing zu einem Ziel-Host oder -Netzwerk unter Berücksichtigung eines vorhandenen Transitnetzwerks. ■ *bridging*: Bridging Modus aktiviert. ■ *routing*: IP Routing zu einem Ziel-Host oder -Netzwerk ohne Berücksichtigung eines vorhandenen Transitnetzwerks.

Feld	Bedeutung
Remote WDS MAC Address	MAC Adresse des Ziel-WDS-Links.
Local IP-Address	Nur für ***MODE*** = *routing* oder *transient routing* IP-Adresse des lokalen WDS-Interfaces.
Local Netmask	Nur für ***MODE*** = *routing* Netzmaske zu ***IP-ADDRESS***
Partner IP-Address	Nur für ***MODE*** = *transient routing* IP-Adresse des Ziel-WDS-Interfaces.
Remote Network	Nur für ***MODE*** = *transient routing* Das Ziel-Netzwerk, das mittels dieses WDS-Links an den Ziel-AP per Ethernet oder Wireless LAN angeschlossen ist.
Remote Netmask	Nur für ***MODE*** = *transient routing* Netzmaske zu ***REMOTE NETWORK***.

Tabelle 3-2: Felder im Menü ***WDS LINK CONFIGURATION*** ➜ ***ADD/EDIT***

4 Untermenü Advanced

Im Folgenden werden die Felder des Menüs *ADVANCED* beschrieben.



Im Menü ***WIRELESS LAN ➜ ADVANCED*** finden Sie WLAN-spezifische Einstellungen. Änderungen sind jedoch nur in seltenen Fällen nötig.

Das Menü besteht aus folgenden Feldern:

Feld	Bedeutung
Wireless Mode	Nur für ***Wireless LAN*** ➜ ***Radio Band*** = *2,4 GHz* Betriebsmodus des AP. Mögliche Werte: ■ *802.11g*: nur 54Mbit Clients ■ *802.11b*: nur 11Mbit Modus ■ *802.11 mixed* (Defaultwert) / *802.11mixed short*: 11Mbit und 54Mbit mixed Modus ■ *802.11mixed long*: 11Mbit und 54Mbit mixed Modus mit langer Präambel. Dieser Modus ist für Clients notwendig, die nur 1 und 2 Mbit/s unterstützen. Er wird auch für Centrino Clients benötigt, falls Verbindungsprobleme aufgetreten sind.
Maximum Bitrate	Die maximale Bitrate vom/zum Client. Mögliche Werte: ■ *AUTO* (Defaultwert) ■ Auswahl eines vorgegebenen Wertes im Bereich *1 ... 54 Mbit*

Feld	Bedeutung
NITRO Burst	Dieses Leistungsmerkmal erhöht die maximale Burst Time für die Übertragung zu einem verbundenen Client, und erhöht somit den Datendurchsatz in langsameren WLANs. Dabei werden mehrere Funkdatenpakete direkt hintereinander ("Burst") gesendet. Das notwendige CTS-Paket für die Verwaltung fällt dabei nur einmal an. Die Auswahl einer Option, legen Sie die maximale Zeit fest, die ein solcher Paket-Burst dauern darf. Mögliche Werte: ■ *Off* (Defaultwert): 0 (= kein Burst) ■ *Compatible*: Burst Time = 0.65ms ■ *Ideal*: Burst Time = 1.3ms ■ *Maximum*: Burst Time = 5ms Die NITRO Burst-Funktionalität ist konform zu den 802.11 Standards, d.h. der NITRO Burst Mode kann mit jedem 11g-fähigen Client eine Verbesserung bringen. Falls Probleme mit älterer WLAN Hardware auftreten, sollte dieses Feld auf *off* gesetzt werden.
TX Power (dBm)	Sendeleistung des AP in dBm. Mögliche Werte: *1* bis *17*. Defaultwert ist *17*.

Feld	Bedeutung
Timeout (minutes)	Broken Link Detection: Hier konfigurieren Sie die Zeit in Minuten, nach der der Client automatisch getrennt wird, wenn kein Signal mehr empfangen wird. Mögliche Werte: *1..240* Defaultwert ist *5*.

Tabelle 4-1: Felder im Menü ***ADVANCED***

Index: Wireless LAN