

**Benutzerhandbuch**  
**bintec R1200 / R1200w(u) / R3000 / R3000w / R3400 / R3800(wu)**  
**Wireless LAN**

**Ziel und Zweck** Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec-Gateways ab Software-Release 7.4.10. 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](http://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](http://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** Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

**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](http://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](http://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](http://www.bintec.fr)

<b>1</b>	<b>Menü Wireless LAN</b> .....	<b>3</b>
<b>2</b>	<b>Untermenü Wireless Interfaces</b> .....	<b>7</b>
	2.1 Untermenü ACL Filter .....	15
	2.2 Untermenü IP and Bridging .....	16
<b>3</b>	<b>Untermenü WDS Link Configuration</b> .....	<b>19</b>
<b>4</b>	<b>Untermenü Advanced</b> .....	<b>23</b>
	<b>Index: Wireless LAN</b> .....	<b>27</b>



# 1 Menü Wireless LAN

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

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 Interfaces >	
WDS Link Configuration >	
Advanced >	
SAVE	CANCEL

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.



**Hinweis**

Bitte beachten Sie, dass nicht alle bintec-Gateways über Funktechnik verfügen. Ob Ihr Gateway diese Funktion unterstützt, entnehmen Sie bitte dem Datenblatt unter [www.funkwerk-ec.com](http://www.funkwerk-ec.com).

## Netzwerkfunktionen

Ein WLAN ermöglicht genauso wie ein kabelgebundenes Netzwerk alle nötigen Netzwerkfunktionen. Somit steht der Zugriff auf Server, Dateien, Drucker, Mail-system genauso zuverlässig zur Verfügung wie der firmenweite Internetzugang. Da 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 der Position und der Anzahl der Anschlüsse).

**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 Verfahren arbeitet im Funkfrequenzbereich von 2,4 GHz (2400 MHz - 2485 MHz), der gewährleistet, dass Gebäudeteile möglichst gut, bei geringer, gesundheitlich unproblematischer Sendeleistung durchdrungen werden.

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

Mit 802.11a ist im 5 GHz Band (Bereich 5150 MHz bis 5725 MHz) bis 54 Mbit/s nutzbar. Auch dieser Frequenzbereich ist derzeit in Deutschland lizenzfrei nutzbar.

Für Europa bietet 802.11h als Erweiterung zu 802.11a statt 30 mW eine maximale Sendeleistung von 1000 mW (nur Outdoor), unter Einsatz von TPC (TX Power Control, Methode zur Regelung der Sendeleistung bei Funksystemen um Interferenzen zu reduzieren) 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 können Sie festlegen, ob das Gateway als Access Point betrieben werden soll oder nicht ( <i>Off</i> , Standardwert).
Location	Die Ländereinstellung des Access Point. Mögliche Werte sind alle auf dem Wireless-Modul des Gateways vorkonfigurierten Länder. Der Bereich der auswählbaren Kanäle variiert je nach Ländereinstellung. Standardwert ist <i>Germany</i> .

Feld	Bedeutung
Radio band	<p>Frequenzband, in dem der Access Point betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ 2,4 GHz (Standardwert)</li> <li>■ 5 GHz</li> </ul>
Usage area	<p>Nur für <b>RADIO BAND = 5 GHz</b></p> <p>Einsatzort des Access Points.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>anywhere</i> (Standardwert): Der Access Point wird innerhalb oder ausserhalb von Gebäuden betrieben.</li> <li>■ <i>indoor</i>: Der Access Point wird innerhalb von Gebäuden betrieben.</li> <li>■ <i>outdoor</i>: Der Access Point wird außerhalb von Gebäuden betrieben.</li> </ul>
Channel	<p>Der Kanal, der vom Access Point verwendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>auto</i> (Standardwert): der Kanal wird automatisch erkannt; Option für <b>RADIO BAND = 5 GHz</b>.</li> <li>■ 1 ... 13: nur für <b>RADIO BAND = 2,4 GHz</b> (1 ... 11 bei <b>LOCATION = United States</b>)</li> <li>■ 149 ... 165 nur für <b>RADIO BAND = 5 GHz</b> und nur für <b>LOCATION = Austria</b> oder <i>United States</i></li> </ul>

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

Über das Menü gelangen Sie in folgende Untermenüs:

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



## 2 Untermenü Wireless Interfaces

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

R3000w Setup Tool		Funkwerk Enterprise Communications GmbH		
[WLAN-8-0] [WIRELESS]: Interface List		MyGateway		
Network Name	Status	Security	ACL-Filter	ifc Cl.#
-----				
*Funkwerk-ec	enable	NONE	disable	vss8-0 16
ADD		DELETE		EXIT

Das Untermenü **WIRELESS LAN** → **WIRELESS INTERFACES** enthält eine Liste mit allen konfigurierten Wireless Interfaces und zeigt deren grundlegende Einstellungen 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 weit verbreitete WEP hat sich jedoch als anfällig herausgestellt. Ein höheres Maß an Sicherheit erreicht man durch zusätzlich zu konfigurierende, auf Hardware basierende Verschlüsselung (wie z.B. 3DES oder AES). Dann können auch vertrauliche 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). Außerdem 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 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 der vollständige 802.11i-Standard umgesetzt einschließlich des Verschlüsselungsalgorithmus AES (Advanced Encryption Standard).
- Sicherheitsmaßnahmen** Zur Absicherung der auf dem WLAN übertragenen Daten sollten Sie im Menü **WIRELESS LAN → WIRELESS INTERFACES** gegebenenfalls folgende Konfigurationsschritte vornehmen (Alle WLAN Einstellungen sind analog auf den WLAN-Clients vorzunehmen.):
- Ändern Sie die Default-SSID, **NETWORK NAME = Funkwerk-ec**, Ihres Access Points.

- Setzen Sie **WIRELESS INTERFACES** → **NAME IS VISIBLE** = *no*. Damit werden alle WLAN-Clients ausgeschlossen, die mit dem allgemeinen **NETWORK NAME** (SSID) *Any* einen Verbindungsaufbau versuchen und welche die eingestellten SSIDs nicht 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)*, und tragen Sie den entsprechenden Schlüssel im Access Point unter **KEY 1 - 4** bzw. unter **ENTER PRESHARED KEY** bzw. unter dem RADIUS Server ein.
- Der WEP-Schlüssel sollte regelmässig geändert werden. Wechseln Sie dazu **DEFAULT KEY**. Wählen Sie den längeren 104/128 Bit WEP-Schlüssel.
- Die höchste Sicherheit bietet **SECURITY MODE** = *WPA (802.1x)* mit **WPA/WPA2 MIXED MODE** = *WPA2 only*. Diese Methode beinhaltet eine hardwarebasierte Verschlüsselung und RADIUS-Authentifizierung des Clients. Zusätzlich 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	<p>Hier setzen Sie den Betriebsstatus des Wireless Interfaces.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>enable</i> (Standardwert): Aktiviert das Interface.</li> <li>■ <i>disable</i>: Deaktiviert das Interface.</li> </ul>
Network Name	<p>Hier geben Sie den Namen des Wireless Interfaces (SSID) ein.</p> <p>Geben Sie eine ASCII Zeichenfolge mit max. 32 Zeichen ein.</p>
Name is visible	<p>Hier können Sie die Übertragung von <b>NETWORK NAME</b> (SSID) aktivieren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>yes</i> (Standardwert): <b>NETWORK NAME</b> ist sichtbar für Clients im Sendebereich.</li> <li>■ <i>no</i>: <b>NETWORK NAME</b> ist für die Clients nicht sichtbar.</li> </ul>
Max. Clients	<p>Maximale Anzahl der für dieses Interface erlaubten WLAN-Client-Verbindungen. Insgesamt können 64 Verbindungen auf alle Wireless Interfaces verteilt werden.</p>

Feld	Bedeutung
Security Mode	<p>Hier wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Wireless Interfaces.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>NONE</i> (Standardwert): weder Verschlüsselung noch Authentifizierung</li> <li>■ <i>WEP 40/64</i>: WEP 40Bit</li> <li>■ <i>WEP 104/128</i>: WEP 104Bit</li> <li>■ <i>WPA PSK</i>: WPA mit Preshared Key Authentifizierung</li> <li>■ <i>WPA (802.1x)</i>: WPA mit EAP (RADIUS-Authentifizierung)</li> </ul> <p>Für <b>SECURITY MODE = WPA (802.1x)</b> wird folgender Hinweis angezeigt: <i>A Radius Server configuration in RADIUS setup is required.</i></p>
Default Key	<p>Nur für <b>SECURITY MODE = WEP 40/64, WEP 104/128</b></p> <p>Hier wählen Sie einen der in <b>KEY &lt;1 - 4&gt;</b> konfigurierten Schlüssel als Defaultschlüssel aus.</p> <p>Standardwert ist Key 1.</p>

Feld	Bedeutung
Key <1 - 4>	<p>Nur für <b>SECURITY MODE</b> = <i>WEP 40/64</i>, <i>WEP 104/128</i></p> <p>Hier geben Sie den WEP Schlüssel ein. Es gibt zwei Möglichkeiten, einen WEP Schlüssel einzugeben:</p> <ul style="list-style-type: none"> <li>■ Direkte Eingabe in hexadezimaler Form 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: <i>A0B23574C5</i>, WEP104: <i>81DC9BDB52D04DC20036DBD831</i></li> <li>■ Direkte Eingabe von ASCII Zeichen Geben Sie eine Zeichenfolge mit der für den gewählten WEP Modus passenden Zeichenanzahl ein. Nach Bestätigen mit der Eingabetaste werden die ASCII Zeichen in eine hexadezimale Zeichenfolge umgewandelt. Für WEP40 benötigen Sie eine Zeichenfolge mit 5 Zeichen, für WEP104 mit 13 Zeichen. Z.B. <i>hallo</i> for WEP40, <i>funkwerk-wep1</i> for WEP104.</li> </ul>
Enter Preshared Key	<p>Nur für <b>SECURITY MODE</b> = <i>WPA PSK</i></p> <p>Hier geben Sie das WPA Passwort ein. Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.</p>

Feld	Bedeutung
WPA/WPA2 mixed mode	<p>Nur für <b>SECURITY MODE = WPA PSK</b> und <b>WPA (802.1x)</b></p> <p>Hier wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <b>WPA + WPA2</b> (Standardwert für das initial vorhandene Interface)</li> <li>■ <b>WPA only</b> (Standardwert für alle weiteren Interfaces)</li> <li>■ <b>WPA2 only</b></li> </ul>
WPA2 preauthentication	<p>Nur für <b>SECURITY MODE = WPA (802.1x)</b> mit <b>WPA/WPA2 MIXED MODE = WPA + WPA2</b> und <b>WPA2 only</b></p> <p>Mit dieser Option erlauben Sie, dass angemeldete Clients vorab bei anderen Access Points in derselben Funkzelle authentifiziert werden. 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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <b>enabled</b> (Standardwert): der Access Point erlaubt Vorab-Authentisierung von Clients auf anderen Access Points.</li> <li>■ <b>disabled</b>: Anfragen von Clients zur Vorab-Authentisierung werden ignoriert.</li> </ul>

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



## 2.1 Untermenü ACL Filter

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

```

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
  
```

Im Untermenü **WIRELESS LAN → WIRELESS INTERFACES → ACL FILTER** wird eine hardware-spezifische 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 die **ACCEPT** Liste eingetragen werden 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 der 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: <i>enable</i> , <i>disable</i> (Standardwert)
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 <b>ADD</b> , um die eingegebene MAC Adresse der <b>ACCEPT</b> Liste hinzuzufügen. Wenn Sie einen Eintrag der <b>REJECT</b> Liste markieren und die <b>a</b> Taste drücken (Kleinschreibung beachten), wird der entsprechende Eintrag in die <b>ACCEPT</b> Liste verschoben. So müssen Sie die Adressen, die akzeptiert werden sollen, nicht manuell eingeben.

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.

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

Im Menü **WIRELESS LAN → WIRELESS INTERFACES → 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: <ul style="list-style-type: none"> <li>■ <i>enabled</i></li> <li>■ <i>disabled</i> (Standardwert)</li> </ul>
Local IP Address	Hier weisen Sie dem Wireless Interface eine IP-Adresse zu.
Local Netmask	Netzmaske zu <b>LOCAL IP ADDRESS</b> .
Second Local IP Address	Hier weisen Sie dem Wireless Interface eine zweite IP-Adresse zu.

Feld	Bedeutung
Second Local Netmask	Netzmaske zu <b>SECOND LOCAL IP ADDRESS</b> .
Bridging enable	<p>Ermöglicht die Aktivierung der Bridging-Funktion auf dem Wireless Interface.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>no</i> (Standardwert): Bridging ist auf dem Wireless Interface nicht aktiviert.</li> <li>■ <i>yes</i>: Bridging ist auf dem Wireless Interface aktiviert.</li> </ul>
Proxy ARP	<p>Ermöglicht dem Gateway, ARP-Requests aus dem eigenen LAN stellvertretend für WLAN Clients zu beantworten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>no</i> (Standardwert)</li> <li>■ <i>yes</i>.</li> </ul>

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		Funkwerk Enterprise Communications 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.



**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 WDS-Interfaces der Gegenstelle. (= <b>REMOTE WDS MAC ADDRESS</b> in <b>WDS LINK CONFIGURATION → ADD/EDIT</b> )
Local-IP	Die IP-Adresse des eigenen WDS-Interfaces. (= <b>LOCAL IP-ADDRESS</b> in <b>WDS LINK CONFIGURATION → ADD/EDIT</b> )
Remote-IP	Die IP-Adresse des WDS-Interfaces der Gegenstelle. (= <b>PARTNER IP-ADDRESS</b> in <b>WDS LINK CONFIGURATION → ADD/EDIT</b> )
Network/Mask	IP-Adresse und Maske des Netzwerks, welches über den WDS-Link erreicht werden soll. (= <b>REMOTE NETWORK</b> und <b>REMOTE NETMASK</b> in <b>WDS LINK CONFIGURATION → ADD/EDIT</b> )
Ena.	Der WDS-Link ist aktiviert ( <i>yes</i> ) bzw. deaktiviert ( <i>no</i> ). (= <b>ADMINSTATUS</b> in <b>WDS LINK CONFIGURATION → ADD/EDIT</b> )

Tabelle 3-1: WDS Liste

Die Konfiguration der WDS Links erfolgt im Untermenü **WIRELESS LAN → WDS LINK CONFIGURATION → ADD/EDIT**.

R3000w Setup Tool		Funkwerk Enterprise Communications 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: <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>enable</i> (Standardwert)</li> <li><input type="checkbox"/> <i>disable</i></li> </ul>
Mode	Bestimmt den Modus, in dem der WDS Link betrieben wird. Mögliche Werte: <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>transient routing</i> (Standardwert): IP Routing zu einem Ziel-Host oder -Netzwerk mittels eines Transitnetzwerks.</li> <li><input type="checkbox"/> <i>bridging</i>: Bridging Modus aktiviert.</li> <li><input type="checkbox"/> <i>routing</i>: IP Routing zu einem Ziel-Host oder -Netzwerk ohne Transitnetzwerk.</li> </ul>

Feld	Bedeutung
Remote WDS MAC Address	MAC Adresse des WDS-Interfaces der Gegenstelle.
Local IP-Address	Nur für <b>MODE = routing</b> oder <b>transient routing</b> IP-Adresse des eigenen WDS-Interfaces.
Local Netmask	Nur für <b>MODE = routing</b> Netzmaske zu <b>LOCAL IP-ADDRESS</b>
Partner IP-Address	Nur für <b>MODE = transient routing</b> IP-Adresse des WDS-Interfaces der Gegenstelle.
Remote Network	Nur für <b>MODE = transient routing</b> IP-Adresse und Maske des Netzwerks, welches über den WDS-Link erreicht werden soll.
Remote Netmask	Nur für <b>MODE = transient routing</b> Netzmaske zu <b>REMOTE NETWORK</b> .

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



## 4 Untermenü Advanced

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

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

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

Das Menü besteht aus folgenden Feldern:

Feld	Bedeutung
Wireless Mode	<p>Nur für <b>WIRELESS LAN → RADIO BAND = 2,4 GHz</b></p> <p>Betriebsmodus des Access Point.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>802.11 mixed</i> (Standardwert): für 11 Mbit und 54 Mbit Clients (bei Normalbetrieb)</li> <li>■ <i>802.11 mixed long</i>: Clients mit langer Präambel für 11 Mbit und 54 Mbit. Dieser Modus ist für Clients notwendig, die nur 1 Mbit/s und 2 Mbit/s unterstützen. Er wird auch für Centrino Clients benötigt, falls Verbindungsprobleme auftreten.</li> <li>■ <i>802.11 mixed short</i>: für 11 Mbit und 54 Mbit Clients</li> <li>■ <i>802.11b</i>: nur für 11 Mbit Clients (oder bei Verbindungsproblemen)</li> <li>■ <i>802.11g</i>: nur für 54 Mbit Clients</li> </ul>
Maximum Bitrate	<p>Die maximale Bitrate vom/zum Client.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>AUTO</i> (Standardwert)</li> <li>■ Auswahl eines vorgegebenen Wertes im Bereich 1 ... 54 Mbit</li> </ul>

Feld	Bedeutung
NITRO Burst	<p>Dieses Leistungsmerkmal erhöht die maximale Burst Time für die Übertragung zu einem verbundenen Client, und vergrößert somit den Datendurchsatz in langsameren WLANs.</p> <p>Dabei werden mehrere Funkdatenpakete direkt hintereinander ("Burst") gesendet. Das notwendige CTS-Paket für die Verwaltung fällt dabei nur einmal an. Durch die Auswahl einer Option legen Sie die maximale Zeit fest, die ein solcher Paket-Burst dauern darf.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ <i>Off</i> (Standardwert): 0 (= kein Burst)</li> <li>■ <i>Compatible</i>: Burst Time = 0.65ms</li> <li>■ <i>Ideal</i>: Burst Time = 1.3ms</li> <li>■ <i>Maximum</i>: Burst Time = 5ms</li> </ul> <p>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.</p> <p>Falls Probleme mit älterer WLAN Hardware auftreten, sollte dieses Feld auf <i>off</i> gesetzt werden.</p>
TX Power (dBm)	<p>Sendeleistung des Access Point in dBm.</p> <p>Mögliche Werte: 1 bis 17.</p> <p>Standardwert ist 17.</p>

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

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

# Index: Wireless LAN

<b>Numerics</b>	802.11 b/g mixed	24
<b>A</b>	Accept Address	16
	Access Point	4
	ACL Filter	15
	Active Probing	7
	AdminStatus	11, 16, 21
<b>B</b>	Bridging enable	18
<b>C</b>	Channel	5
<b>D</b>	Default Key	12
<b>E</b>	Ena.	20
	Enter Preshared Key	13
<b>K</b>	Key	13
<b>L</b>	local communication	17
	Local IP	20
	Local IP-Address	22
	local IP-Number	17
	Local Netmask	22
	local Netmask	17
	Location	4
<b>M</b>	MAC Address	20
	Max. Clients	11
	Maximum Bitrate	24
	Mode	21
<b>N</b>	Name is visible	11

	Network Name	11
	Network/Mask	20
	NITRO Burst	25
<b>O</b>	Operation Mode	4
<b>P</b>	Partner IP-Address	22
	Proxy ARP	18
<b>R</b>	Radio band	5
	Remote IP	20
	Remote Netmask	22
	Remote Network	22
	Remote WDS MAC Address	22
<b>S</b>	Second Local IP-Number	17
	Second Local Netmask	18
	Security Mode	12
	SSID	8, 11
<b>T</b>	Timeout (minutes)	26
	TX Power (dBm)	25
<b>U</b>	Usage area	5
<b>V</b>	vss	7
<b>W</b>	wds	20
	WEP	8
	Wireless Mode	24
	WPA	8
	WPA/WPA2 mixed mode	14
	WPA2 preauthentication	14