WIRELESS LAN

Bintec Benutzerhandbuch - XGeneration
Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von -Gateways ab Software-Release . 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. 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 -Gateways finden Sie unter www.funkwerk-ec.com.

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

Marken

und das -Logo sind eingetragene Warenzeichen der .

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

Copyright

Richtlinien und Normen

-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 erreichen

Südwestpark 94
D-90449 Nürnberg
Deutschland

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

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.

```
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
```

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 die Herstellung 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 (Gerätestandort vs. Position und Anzahl von Anschlüssen) geachtet werden muß.

Derzeit gültiger Standard: IEEE 802.11

IEEE 802.11b ist der derzeit am weitesten verbreitete Standard für Funk-LANs. Dieses Verfahren arbeitet im Funkfrequenzbereich von 2,4Ghz, der gewährleistet, dass Gebäudeteile möglichst gut, bei geringer, gesundheitlich unproblematischer Sendeleistung durchdrungen werden. WLAN sendet innerhalb und ausserhalb von Gebäuden mit maximal 100 mW.

Trotz der geringen Übertragungskapazität von 11Mb pro Sekunde sind bei 802.11b WLANs alle Funktionen eines verkabelten Netzwerks möglich. WLAN Systeme sind auf Frequenzen in den Bereichen 5150 MHz - 5350 MHz und 5470 MHz - 5725 MHz anmelde- und gebührenfrei.

Ein zu 802.11b kompatibeler Standard ist 802.11g, der im 2,4 GH-Band arbeitet und eine maximale Datenübertragungsrate von 54 Mbit/s bietet.

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

Feld	Bedeutung
Operation Mode	Der Betriebsmodus des Gateways. Mögliche Werte: ■ *Off* (Defaultwert): Das Gateway wird nicht als AP betrieben. ■ *Access Point*: Das Gateway wird als Access Point betrieben.
Location	Die Ländereinstellung des AP. Mögliche Werte sind alle auf dem Wirelessmodul des Gateways vorkonfigurierten Länder.
Channel	Der Kanal, der vom AP verwendet wird. Mögliche Werte: *1* ... *13.* Defaultwert ist *11*.

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

Über das Menü gelangen Sie in folgende Untermenüs:

- ***WIRELESS INTERFACE***
- ***ADVANCED***

2 Untermenü Wireless Interface

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

```
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
```

Das Untermenü ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACE*** enthält grundlegende Einstellungen des Wireless Interfaces wie Netzwerkname, Status etc.

Das Wireless Interface (mit dem Präfix *vss*) erhält eigene IP-Einstellungen und kann alle Möglichkeiten eines Standardinterfaces wie QoS, Stateful Inspection, Accounting 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. Damit genügt er den Vorschriften des Federal Information Standards (FIPS).

WPA WPA sieht eine bessere Verschlüsselung vor, da es das sogenannte "Temporal Key Integrity Protocol" (TKIP) verwendet. Ferner werden Pre-shared Keys verwendet sowie das RADIUS-basierende 802.1X, mit dem man Benutzer eindeutig identifizieren kann. Außerdem sieht WPA eine Authentifizierung mittels IEEE 802.1x und EAP (Extensible Authentication Protocol) vor, die auf einen vorhandenen RADIUS-Server für die Nutzerverwaltung zurückgreifen.

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.
- Konfigurieren Sie in ***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* oder *WPA PSK (TKIP)*, und tragen Sie den entsprechenden Schlüssel im Access Point unter ***KEY 1 - 4*** oder ***PRESHARED KEY*** und in den WLAN-Clients ein.
- Der WEP-Schlüssel sollte regelmässig geändert werden. Wechseln Sie dazu ***DEFAULT KEY***.

- Für die Übertragung von extrem sicherheitsrelevante Informationen, sollte ***SECURITY MODE*** = *WPA (TKIP + 802.1x)* 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 MAC Filter" auf Seite 10).

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

Feld	Bedeutung
AdminStatus	Administrativer Status 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 nicht sichtbar.

Feld	Bedeutung
Security Mode	Der Sicherheitsmodus des Wireless Interfaces. Mögliche Werte: ■ *NONE* (Defaultwert): kein Sicherheitsmodus ■ *WEP 40/64*: WEP 40Bit ■ *WEP 104/128*: WEP 104Bit ■ *WPA PSK (TKIP)*: WPA Preshared Key ■ *WPA (TKIP + 802.1x)*: 802.11i/TKIP Für ***SECURITY MODE*** = *WPA (TKIP + 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 Default aus.

Feld	Bedeutung
Key <1 - 4>	Nur für ***SECURITY MODE*** = *WEP 40/64, WEP 104/128* Hier geben Sie den WEP Schlüssel ein. Es gibt drei Möglichkeiten, einen WEP Schlüssel einzugeben: ■ Automatische Schlüsselgenerierung (empfohlen): Wenn eine beliebige Zeichenfolge, die nicht mit *0x* oder " anfängt, eingegeben wird, wird ein MD5 basierter WEP Schlüssel mit exakt der für den gewählten WEP Modus passenden Zeichenanzahl generiert. ■ Direkte Eingabe in Hex Beginnt die Eingabe mit *0x*, wird der Generator deaktiviert. Geben Sie eine 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.

Feld	Bedeutung
Preshared Key	Nur für ***SECURITY MODE*** = *WPA PSK (TKIP)* Hier geben Sie das WPA Passwort ein. Geben Sie eine ASCII Zeichenfolge mit 8 - 32 Zeichen ein.

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

2.1 Untermenü MAC Filter

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

```
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
```

Im Untermenü ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ ***ADD/EDIT*** ➜ ***MAC FILTER*** wird eine hardwarespezifische Zugangskontrolle konfiguriert. Dadurch ist es möglich, nur bestimmten Clients den Zugang zum AP zu gewähren. Dieses Filter wird aktiv, bevor andere Sicherheitsmechanismen greifen. Die eingegebenen Adressen sind MAC-basiert und werden für jedes Wireless Interface einzeln konfiguriert.

MAC Adresslisten

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

Die ***REJECT*** Liste enthält alle abgewiesenen Adressen und Adressen, die einem anderen Interface zugewiesen sind, aber von dem ausgewählten Interface nicht zugelassen 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 ***MAC FILTER***

2.2 Untermenü IP and Bridging

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

```
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
```

Im Menü ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ ***ADD/EDIT*** ➜ ***IP AND BRIDGING*** konfigurieren Sie interfacespezifische IP Einstellungen.

Das Menü besteht aus folgenden Feldern:

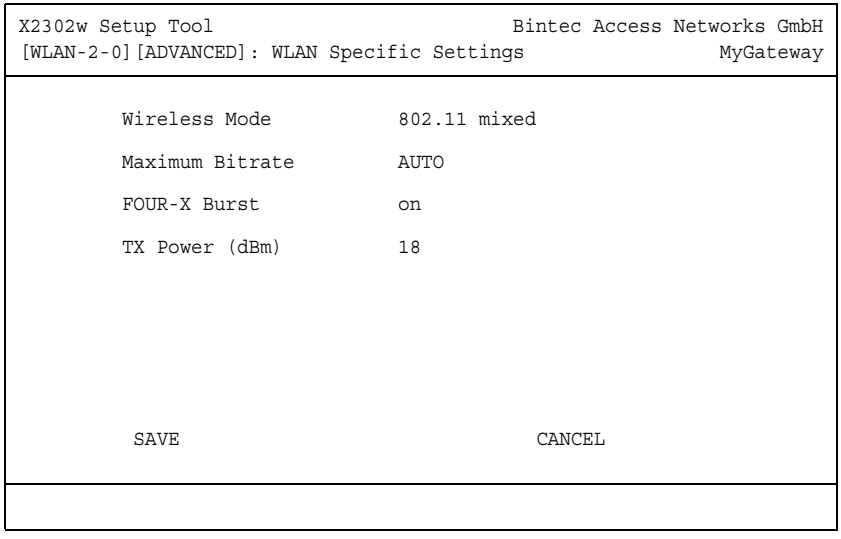
Feld	Bedeutung
Mode	Definiert den Modus des Wireless Interfaces. Mögliche Werte: ■ *Routing* (Defaultwert): Routing ist auf dem Wireless Interface aktiviert. ■ *Bridging*: Bridging ist auf dem Wireless Interface aktiviert.

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	Nur für ***WORKING MODE*** = *Routing* Hier weisen Sie dem Wireless Interface eine IP-Adresse zu.
Local Netmask	Nur für ***WORKING MODE*** = *Routing* Netzmaske zu ***LOCAL IP ADDRESS***.
Second Local IP Address	Nur für ***WORKING MODE*** = *Routing* Hier weisen Sie dem Wireless Interface eine zweite IP-Adresse zu.
Second Local Netmask	Nur für ***WORKING MODE*** = *Routing* Netzmaske zu ***SECOND LOCAL IP ADDRESS*** .

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

3 Untermenü Advanced

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



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

Das Menü besteht aus folgenden Feldern:

Feld	Bedeutung
Wireless Mode	Betriebsmodus des AP. Mögliche Werte: ■ *802.11g*: nur 54Mbit Clients ■ *802.11b*: 11Mbit Modus ■ *802.11 mixed* (Defaultwert): 11Mbit und 54Mbit mixed Modus ■ *802.11mixed short:* 11Mbit und 54Mbit mixed Modus mit kurzer Präambel. ■ *802.11mixed long*: 11Mbit und 54Mbit mixed Modus mit langer Präambel. Dieser Modus wird für Centrino Clients benötigt, falls Verbindungsprobleme aufgetreten sind.
Maximum Bitrate	Die maximale Bitrate vom/zum Client. Mögliche Werte: ■ *AUTO* (Defaultwert) ■ *1 ... 54 Mbit*
FOUR-X Burst	Dieses Leistungsmerkmal erhöht die maximale Burst Time für die Übertragung zu einem verbundenen Client, und erhöht somit den Datendurchsatz in langsameren WLANs. Falls Probleme mit älterer WLAN Hardware auftreten, sollte dieses Feld auf *off* gesetzt werden. Mögliche Werte: *off*, *on* (Defaultwert)

Feld	Bedeutung
TX Power (dBm)	Sendeleistung des AP in dB. Mögliche Werte: *6, 9, 12, 15, 18* dB Defaultwert ist *18*.

Tabelle 3-1: Felder im Menü ***ADVANCED***

3 Untermenü Advanced

Index: Wireless LAN

W Wireless Mode 16