# Ergänzung

**zum**

# XAir Handbuch

## Version 2.00

Beschreibung der zusätzlichen Funktionen der Firmware Version 3.00
und des neuen XAir Managers Version 2.06



Version 1.0
Juni 2002

# Übersicht der Änderungen

Diese Ergänzung zum XAir Handbuch erläutert die Änderungen zwischen der Firmware 2.73 und der Firmware 3.00 der XAir Access Points. Im Rahmen dieses neuen Releases wurden ebenfalls folgende weitere Änderungen vorgenommen:

- XAir Manager Release 2.06
- XAir PC-Cards Release 8.10

Das Firmware Release 3.00 beinhaltet vor allem Weiterentwicklungen im Bereich der **Sicherheitseigenschaften** der WLAN Produktfamilie XAir.

Folgende Neuerungen wurden implementiert:

- **WEPplus**
  Bestimmte Werte für die unverschlüsselt über Funk übertragenen Initialisierungsvektoren des WEP-Keys erlauben eine besonders einfache Rekonstruktion der Verschlüsselung. Dies sind die sogenannten „weak keys“. Die Implementierung von WEPplus stellt sicher, dass die schwachen Initialisierungsvektoren nicht verwendet werden. Trotz der Änderung bleibt die Kompatibilität mit der IEEE 802.11b Norm erhalten.
- **IEEE 802.1x und EAP**
  Der Standard 802.1x definiert ein vom Funk unabhängiges Authentifizierungsverfahren auf Port-Ebene. Dabei wird die Authentifizierung eines Users (nicht einer Client-Hardware) für den Zugang zum Netzwerk über die Einbindung eines Authentifizierungsservers (wie RADIUS, Kerberos oder auch propritäre Systeme) realisiert. Für die Verwendung von 802.1x in Wireless LANs bedeutet dies, dass der User eines Funkclients erst dann mit einem Access Point kommunizieren kann und Zugang zum Netzwerk erhält, wenn der Access Point diesen User an einem Authentifizierungsserver im Netzwerk verifiziert hat. Voraussetztung für das Verfahren ist, dass sowohl das Betriebssystem des Clients als auch der Authentifizierungsserver das in 802.1x definierte Protokoll EAP (Extensive Authentication Protocol) unterstützen. Von Seiten des Clients unterstützt derzeit nur das Betriebssystem WinXP dieses Protokoll. Für andere Betriebssysteme gibt es sogenannte „Supplicant“- Software, die EAP ermöglichen.

Weitere Neuerungen sind:

- Einstellbarkeit von Robustheit gegen Mikrowellenöfen
- Empfangsempfindlichkeit der XAir Access Point
- Load Balancing

# Inhaltsverzeichnis

# 8 XAir Manager Version 2.06

In diesem Kapitel werden die zusätzlichen Einstellungsmöglichkeiten des BinTec XAir Managers Version 2.06 beschrieben, die über die Basiskonfiguration hinausgehen (siehe Installationshandbuch im Kapitel Basiskonfiguration im Dokument Los Geht's / Getting Started).

Es ersetzt das Kapitel 8 des XAir Handbuchs Version 2.0

Den BinTec XAir Manager starten Sie mit einem Doppelklick auf die Datei xairm.exe.

Unter der Basiskonfiguration werden folgende Einstellungen zusammengefaßt:

- Name eingeben
- Netzmaske eingeben
- Standard Gateway eingeben

  Weitere Konfigurationen, die über den BinTec XAir Manager vorgenommen werden können, sind:
- Telnet-Verbindung starten
- Web-Verbindung starten
- Firmware-Upgrade durchführen
- Reboot-Vorgang durchführen
- XAir Access Point auf Werkseinstellungen zurücksetzen

Der PC mit einem Windows-Betriebssystem, über den Sie Ihren XAir Access Point konfigurieren möchten, muß sich im gleichen Netzwerk wie der zu konfigurierende XAir Access Point befinden.

**Hinweis zum Arbeiten mit dem BinTec XAir Manager:**

- Der Rechner muß einen funktionierenden und sinnvoll konfigurierten TCP/IP-Stack haben.
- Alle Einstellungen über den XAir Manager sind auch über einen Router hinweg möglich.
- Die Suchfunktion beschränkt sich auf das Subnetz des PCs, auf dem sich der XAir Manager befindet, falls der Router Multicasts nicht weiterleitet.
- Der XAir Access Point kann bei neueren Firmwareversionen nur über ein Paßwort konfiguriert werden. Aus Sicherheitsgründen sollten Sie schnellstmöglich die voreingestellten Paßwörter ändern.
- Falls Ihr Rechner über mehrere Netzwerkschnittstellen verfügt, können Sie eine bestimmte Multicast-Schnittstelle (Router oder Switch) im BinTec XAir Manager einstellen (Siehe Kapitel 1), über die XAirs gesucht werden sollen.

## 8.1 Multicast-Schnittstelle festlegen

Falls der PC auf dem der BinTec XAir Manager installiert ist, mehrere Netzwerkschnittstellen besitzt, kann eine Schnittstelle als Multicast-Schnittstelle festgelegt werden. Über diese Schnittstelle wird nach XAirs gesucht.

Gehen Sie folgendermaßen vor, um eine Multicast-Schnittstelle (Router oder Switch) manuell zu bestimmen:

- Wählen Sie **Extras ➨ Optionen**

Folgendes Dialogfenster öffnet sich:

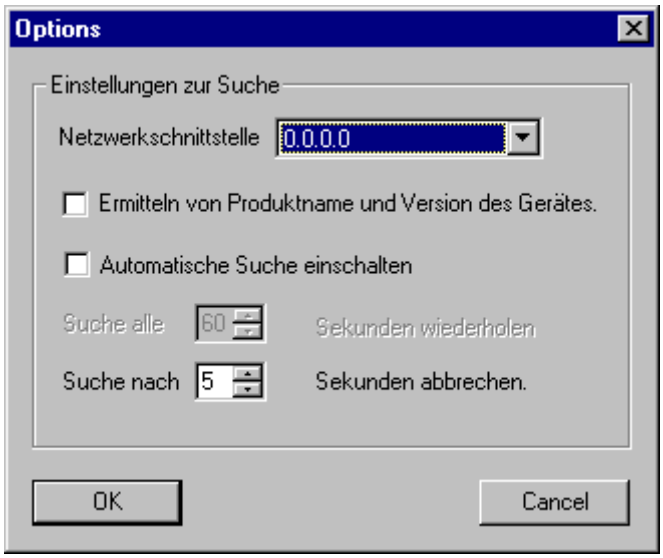


Bild 8-1: Eingabe der IP-Adresse für den Multicast-Router (-Switch)

- Tragen Sie die IP-Adresse der gewünschten Multicast-Schnittstelle (Router oder Switch) ein und bestätigen Sie mit **OK**.
  Ist die Multicast-Schnittstelle 0.0.0.0 definiert, wird über alle Netzwerkschnittstellen des PCs gesucht.

## 8.2 Die Oberfläche des BinTec XAir Managers

Die Oberfläche des BinTec XAir Managers besteht aus vier Komponenten, die im folgenden näher erläutert werden:


Bild 8-2: Die Oberfläche des BinTec XAir Managers

### 8.2.1 Das Hauptfenster

Beim Start des BinTec XAir Managers über die BinTec xairm.exe ist das Hauptfenster zunächst leer. Es ist tabellenförmig angelegt und gliedert sich in die Spalten **MAC-Adresse**, **Name**, **IP-Adresse** und **Zustand**. Je nach Einstellung enthält es auch die **Spalten Fw Ver** und **Produktname**. Sobald XAirs im Netz gesucht und erkannt wurden, finden sich in diesen Spalten die entsprechenden Daten zum jeweiligen Gerät.

### 8.2.2 Die Menüleiste

Das Menü befindet sich am oberen Rand des BinTec XAir Managers und enthält die Menüpunkte **Datei**, **Ansicht**, **Konfiguration**, **Extras** und **Hilfe** mit jeweils bis zu fünf Unterpunkten.

### 8.2.3 Die Werkzeugleiste

Die Werkzeugleiste, welche sich direkt unterhalb des Hauptfensters befindet erlaubt den schnellen Zugriff auf die zwei wichtigsten Funktionen des XAir Managers, **Suchen** und **Einstellen**. Diese beiden Funktionen, die auch über das Menü anwählbar sind, werden im folgenden noch genauer erläutert (Siehe auch Kapitel 8.3.1 und Kapitel 8.3.3).

Gehen Sie Folgendermaßen vor, um die Werkzeugleiste ein- bzw. auszublenden:

- Wählen Sie **Ansicht ➡ Tool Bar**

### 8.2.4 Die Statusleiste

Die Statusleiste am unteren Rand des Fensters zeigt Ihnen den Status des XAir Managers an. Wenn sich der Mauszeiger auf einem Menüpunkt befindet, der eine Funktion aufruft (wie z.B. Suchen), wird die Funktion dieses Menüpunktes ebenfalls in der Statusleiste angezeigt.

Gehen Sie folgendermaßen vor, um die Statusleiste ein- bzw. auszublenden:

- Wählen Sie **Ansicht ➡ Status Bar**

## 8.3 Funktionen des BinTec XAir Managers

Dieses Kapitel beschreibt:

- Suche nach verfügbaren XAirs
- Manuelle Bearbeitung der Einträge
- Die Basiskonfiguration
- Paßwort angeben
- Starten einer Telnet-Verbindung
- Starten einer Web-Verbindung
- Durchführen eines Upgrades der Firmware
- XAir auf Werkseinstellungen zurücksetzen
- XAir rebooten
- BinTec XAir Manager beenden

### 8.3.1 Suche nach verfügbaren XAirs

Die Suchoptionen können über den Menüpunkt Extras > Optionen eingestellt werden.

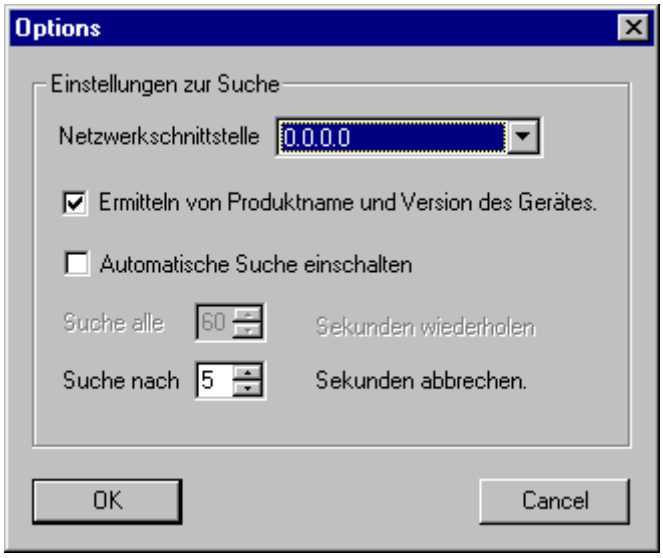


Bild 8-3: Auswahlfenster Optionen

Sie können sich im Hauptfenster die Information über Produktname und Version des Gerätes anzeigen lassen, wenn Sie das entsprechende Kontrollkästchen aktivieren.

Falls Sie die Suchfunktion automatisch wiederholen lassen möchten, aktivieren Sie das entsprechende Kontrollkästchen. In dem Feld darunter können Sie Werte von 10 bis 60 Sekunden eintragen. Nach Ablauf dieser Zeit sucht der XAir Manager automatisch erneut.

Sie können nach einer festgelegten Zeit die Suche abbrechen lassen, z.B. kann man in kleinen Netzen mit wenigen XAirs diese Zeit auf 1 Sekunde reduzieren. Der Maximalwert beträgt 10 Sekunden.

Nachdem Sie alle Einstellungen vorgenommen haben klicken Sie auf **OK** um die Einstellungen zu übernehmen.

Die Funktion **Suchen** kann sowohl über den Menüpunkt **Datei ➔ Suchen** als auch direkt über die Schaltfläche **Suchen** auf der Werkzeugleiste aufgerufen werden.

Der BinTec XAir Manager erkennt daraufhin automatisch im Netz installierte XAirs und zeigt sie im Hauptfenster mit den zugehörigen Netzwerkparametern (**MAC-Adresse**, **Name**, **IP-Adresse**) an. Je nach Einstellung der Optionen werden auch die Firmware-Version (**Fw Ver**) und der **Produktname** angezeigt.


Bild 8-4: Gefundene XAirs

Die Einträge in der Spalte **Zustand** bedeuten:

- gefunden = vom BinTec XAir Manager gefunden,
- vom Benutzer = manueller Eintrag und
- nicht gefunden = XAir wird beim erneuten Suchen nicht gefunden.

### 8.3.2 Manuelle Bearbeitung der Einträge

Unter dem Menüpunkt **Datei ➨ Editieren** stehen die Funktionen **XAir hinzufügen**, **XAir löschen** und **Alle löschen** zur Auswahl:


Bild 8-5: Das Untermenü **Editieren**

**Manuelles Hinzufügen eines XAirs**

- Wählen Sie **Datei ➨ Editieren ➨ XAir hinzufügen**.

Es öffnet sich ein Dialogfenster, in welchem Sie die IP-Adresse des hinzuzufügenden XAir eintragen:

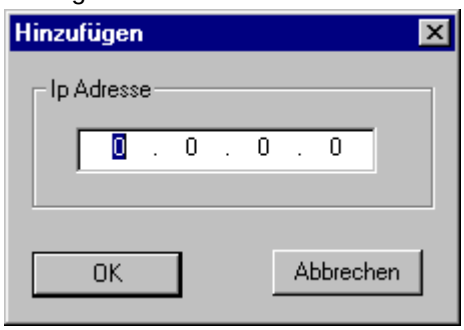


Bild 8-6: IP-Adresse von XAir eintragen

- Bestätigen Sie die Eingabe, indem Sie auf die Schaltfläche **OK** klicken. Der manuell eingetragene XAir wird gesucht und erscheint, wenn er gefunden wurde, in der Liste im Hauptfenster.

**Löschen eines manuell eingetragenen oder nicht gefundenen XAirs**

Manuell hinzugefügte XAirs (**Zustand** vom Benutzer) und XAirs, die als nicht gefunden markiert sind, können Sie folgendermaßen wieder aus der Liste löschen:

- Markieren Sie die MAC-Adresse des zu entfernenden Eintrags.
- Wählen Sie **Datei ➨ Editieren ➨ XAir löschen**, alternativ können Sie auch die "Del" bzw. "Entf" Taste verwenden.

Einträge, die mit der Funktion Suchen automatisch erstellt wurden, können auf diese Weise nicht gelöscht werden.

**Löschen aller nicht gefundenen XAirs**

Um alle Einträge, die als nicht gefunden markiert sind, gleichzeitig aus der Liste im Hauptfenster zu entfernen, gehen Sie folgendermaßen vor:

- Wählen Sie **Datei ➨ Editieren ➨ Alle löschen**.

### 8.3.3 Die Basiskonfiguration

Um einen XAir zu konfigurieren, markieren Sie den entsprechenden Eintrag im Hauptfenster, geben Sie das Paßwort ein (**Konfiguration ➨ Kennwort**) und wählen Sie entweder **Konfiguration ➨ IP-Einstellungen** oder betätigen Sie die Schaltfläche **Einstellen...** in der Werkzeugleiste.

Details zur Durchführung der Basiskonfiguration finden Sie im Kapitel "Die Basiskonfiguration" im Dokument Los Geht's / Getting Started.

### 8.3.4 Paßwort angeben

Das Paßwort wird benötigt, damit die folgenden Einstellungen des BinTec XAir Managers genutzt werden können:

- Firmware Upgrade
- Reboot
- Reset
- Setup

Um das Paßwort anzugeben, gehen Sie wie folgt vor:

- Markieren Sie den XAir in der Liste und wählen Sie **Konfiguration ➨ Kennwort**.

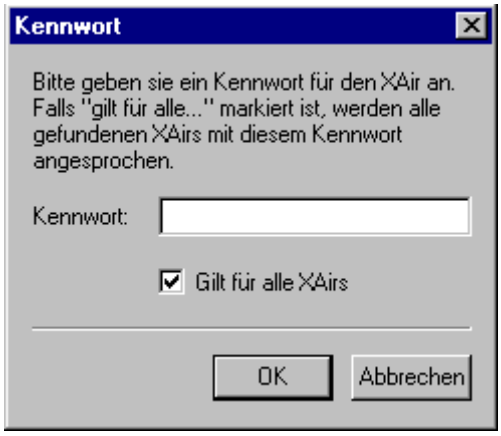


Bild 8-7: Kennworteingabe

- Geben Sie das Paßwort für die Benutzerebene "Admin" ein und bestätigen Sie mit **OK**. Das werkseitig eingestellte Paßwort für die Benutzerebene "Admin" ist admin.
- Ist das Funktionsfeld **Gilt für alle XAir** aktiviert, wird das Paßwort für alle anderen XAirs mit verwendet. Wird der BinTec XAir Manager beendet, muß nach einem Neustart des BinTec XAir Managers das Paßwort erneut eingegeben werden.

Soweit noch nicht geschehen, sollten Sie umgehend die Paßwörter der drei Benutzerebenen "Admin", "User" und "View" ändern, um unbefugten Zugriff zu verhindern.
Die Paßwörter können Sie in der Benutzeroberfläche des XAirs im **Menü Control ➨ Security ➨ UserLevel ➨ Edit** ändern (siehe XAir Benutzerhandbuch Version 2.0, Kapitel 7.1, Seite 20).

### 8.3.5 Starten einer Telnet-Verbindung

Gehen Sie folgendermaßen vor, um eine Telnet-Verbindung zu starten:

- Markieren Sie den XAir im Hauptfenster, auf den Sie über Telnet zugreifen wollen.
- Wählen Sie **Konfiguration ➨ Erweitert ➨ Telnet**.
- In einem neuen Dialogfenster wird nun ein Terminal emuliert.
- Wählen Sie im neuen Dialogfenster **Terminal ➨ Einstellungen**.

Folgendes Fenster öffnet sich:

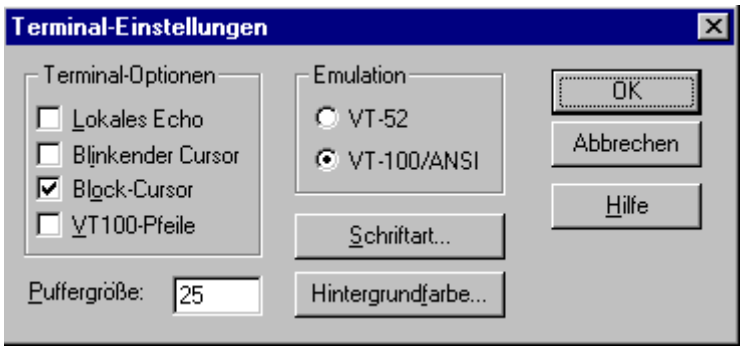


Bild 8-8: Das Fenster Terminal-Einstellungen

- Um die volle Funktionsfähigkeit des Terminals zu nutzen, achten Sie darauf, daß
  - im Bereich **Emulation** das Optionsfeld VT-100/ANSI aktiviert ist,
  - die **Puffergröße** für eine optimale Darstellung auf mindestens 25 eingestellt ist.

Über die Schaltflächen **Schriftart** und **Hintergrundfarbe** können Sie gegebenenfalls die Oberflächengestaltung des Terminal-Fensters Ihren Wünschen anpassen.
Detaillierte Informationen zu den verschiedenen Einstellungsmöglichkeiten erhalten Sie über die Schaltfläche Hilfe im rechten Fensterbereich.

- Haben Sie alle Einstellungen abgeschlossen, bestätigen Sie mit **OK**.

### 8.3.6 Starten einer Web-Verbindung

Gehen Sie folgendermaßen vor, um eine Web-Verbindung zu starten:

- Markieren Sie den XAir im Hauptfenster, auf den Sie über eine Web-Verbindung (Web-Benutzeroberfläche) zugreifen wollen.
- Wählen Sie **Konfiguration ➨ Erweitert ➨ Web**.
  Die Web-Benutzeroberfläche des XAir wird gestartet.
- Klicken Sie auf die Grafik.
  Es erscheint ein Dialog zur Eingabe von Benutzername und Paßwort.

Zu Benutzernamen und Paßwörtern beachten Sie bitte unbedingt die Beschreibung in Benutzerhandbuch XAir Version 2.0, Kapitel 7.1, Seite 20.

- Geben Sie **Benutzername** und **Kennwort** ein. Der Benutzername entspricht dabei der Benutzerebene, auf die Sie zugreifen wollen, und das Paßwort dem entsprechenden Paßwort.
- Bestätigen Sie die Eingaben mit **OK**.
  Das Konfigurationsmenü der Web-Benutzeroberfläche öffnet sich.

Eine ausführliche Beschreibung der Web-Benutzeroberfläche und den Aufruf der Web-Benutzeroberfläche von einem Browser aus finden Sie in Benutzerhandbuch XAir Version 2.0, Kapitel 10, Seite 113.

### 8.3.7 Durchführen eines Upgrades der Firmware

Die aktuelle Firmware für XAir finden Sie im Download-Bereich für XAir auf BinTecs Website unter www.bintec.de. Dort finden Sie auch die aktuelle Version des BinTec XAir Managers.
Benutzen Sie zum Upgrade der Firmware von XAir immer die aktuellste Version des BinTec XAir Managers und beachten Sie die Hinweise in den entsprechenden Release Notes.

Beachten Sie, daß ein Upgrade der Firmware zur Folge haben kann, daß Ihr XAir nach dem Upgrade auf die Werkseinstellungen zurückgesetzt werden muß. Das bedeutet, daß die aktuelle Konfiguration verloren geht und das Gerät nach dem Upgrade neu konfiguriert werden muß.

Beim Upgrade der Firmware für XAir wird immer gleichzeitig ein Update von Monitor, Firmware und Bootloader durchgeführt. Die Upgrade-Dateien besitzen die Dateiendung ".afw".

**Achtung!**
Während des Upgrades von XAir darf XAir nicht ausgeschaltet werden. Die Datenverbindung darf nicht unterbrochen werden. Die Software von XAir wird sonst zerstört und Sie müssen das Gerät zum Hersteller einschicken.

- Schalten Sie XAir während des Upgrades nicht aus und unterbrechen Sie nicht die Datenverbindung.

Gehen Sie folgendermaßen vor, um ein Upgrade der Firmware vorzunehmen:

- Stellen Sie vor Beginn des Upgrades sicher, daß die neue Version der Firmware (Datei mit Endung *.afw) auf der Festplatte Ihres PC oder einem anderen Speichermedium vorliegt.

- Markieren Sie im Hauptfenster des BinTec XAir Managers den XAir, für den Sie ein Upgrade durchführen wollen.
- Geben Sie unter **Konfiguration ➨ Kennwort** Benutzernamen und Paßwort für die Benutzerebene "Admin" ein, wenn dies noch nicht erfolgt ist. Nur dann ist ein Upgrade möglich.
- Wählen Sie **Konfiguration ➨ Firmware laden...**.

Folgendes Fenster öffnet sich:

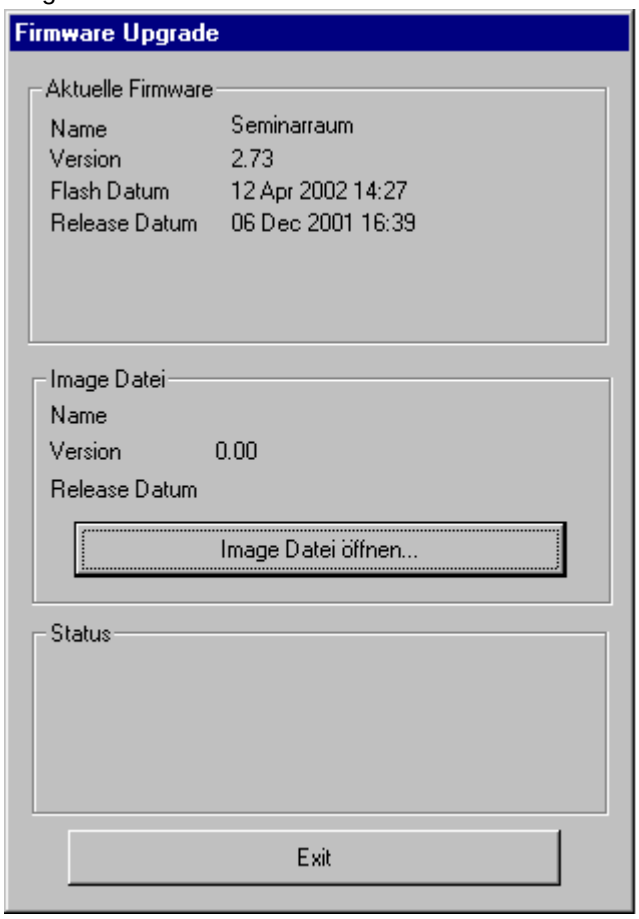


Bild 8-9: Das Fenster Firmware Upgrade

- Betätigen Sie die Schaltfläche **Image Datei öffnen...** .

Folgendes Fenster öffnet sich:

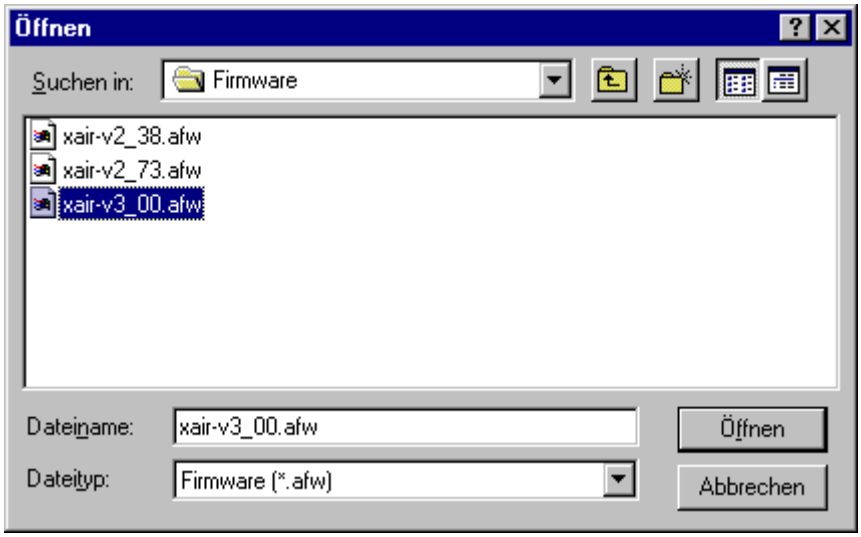


Bild 8-10: Die Firmware-Upgrade-Datei wählen

- Wählen Sie die Datei aus, welche die neue Firmware enthält.
  Dies ist in unserem Beispiel die Datei **xair-v3_00.afw**.
- Klicken Sie auf die Schaltfläche **Öffnen**.

Im Kontrollfenster wird nun im Bereich **Image Datei** automatisch der Pfad für die Firmware aktualisiert. Der BinTec XAir Manager prüft außerdem, ob ein Upgrade möglich und sinnvoll ist:

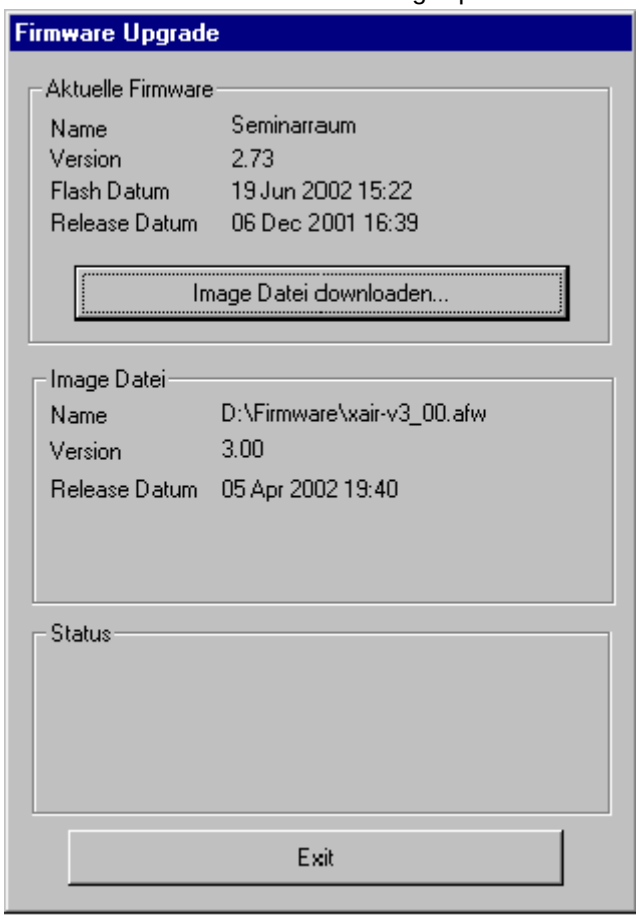


Bild 8-11: Das Fenster Firmware Upgrade mit gewählter Firmware

- Klicken Sie die Schaltfläche **Image Datei downloaden...** .
  Das Upgrade der Firmware wird durchgeführt.

Im Bereich **Status** werden ein Fortschrittsbalken und der aktuelle Vorgang angezeigt:

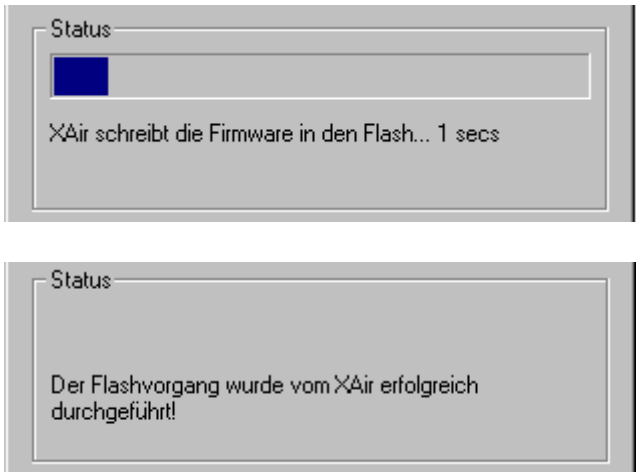


Bild 8-12: Statusfenster des Upgrade-Vorgangs

Nach erfolgreicher Beendigung des Upgrades der Firmware erscheint folgendes Dialogfenster:

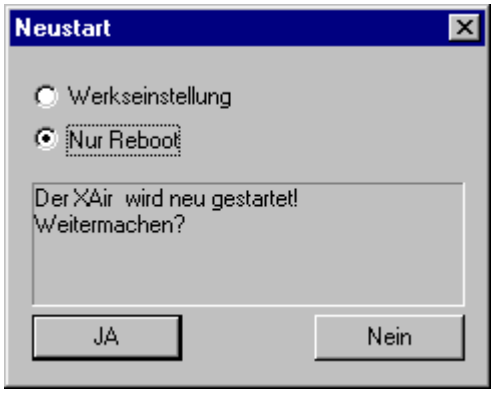


Bild 8-13: Bestätigung Neustart

In diesem Dialogfeld schlägt der BinTec XAir Manager immer bereits die notwendige Option vor: Das Optionsfeld **Nur Reboot**, um den XAir nur neu zu starten oder das Optionsfeld **Werkseinstellung**, um XAir neu zu starten und ihn gleichzeitig auf die Werkseinstellungen zurückzusetzen.

Wenn der BinTec XAir Manager hier das Optionsfeld **Werkseinstellung** markiert hat, sollten Sie die Einstellung nicht auf **Nur Reboot** ändern, da Ihre Konfiguration dann nicht mehr funktionsfähig ist. In diesem Fall ist es notwendig, nach dem Upgrade der Firmware den XAir neu zu konfigurieren.

Schlägt der BinTec XAir Manager hier das Optionsfeld **Nur Reboot** vor, können Sie bei Bedarf auch das Optionsfeld **Werkseinstellung** wählen.

- Bestätigen Sie mit **JA**, um XAir neu zu starten bzw. um XAir neu zu starten und in gleichzeitig auf die Werkseinstellungen zurückzusetzen.

Ist das Optionsfeld **Nur Reboot** markiert, wird auch bei Klicken der Schaltfläche **Nein** ein Reboot durchgeführt.

Der Reboot des XAir (ca. 20 Sekunden) wird Ihnen nicht auf dem Bildschirm Ihres Computers angezeigt. Sie können jedoch anhand der LEDs des XAir die Funkaktivität, den Funkstatus und die Ethernetaktivität überprüfen (siehe XAir Handbuch Version 2.0, Kapitel 12.3, Seite 173).

- Kontrollieren Sie abschließend die Funktionsfähigkeit des XAir, indem Sie über den BinTec XAir Manager z. B. nach im Netz installierten XAirs suchen.

### 8.3.8 XAir auf Werkseinstellungen zurücksetzen

Gehen Sie folgendermaßen vor, um die bereits durchgeführte Konfiguration zu verwerfen und XAir auf die Werkseinstellungen zurückzusetzen:

- Wählen Sie **Konfiguration ➨ Werkseinstellung**.
  XAir wird auf die Werkseinstellungen zurückgesetzt. Dabei wird automatisch ein Neustart durchgeführt.

Die folgenden Einstellungen werden bei einem Zurücksetzen auf die Werkseinstellungen nicht zurückgesetzt:

- IP-Adresse
- Subnet Mask
- Gateway
- Access-Point-Name
- Paßwörter

### 8.3.9 XAir rebooten

Gehen Sie folgendermaßen vor, um einen Neustart des XAirs zu veranlassen:

- Wählen Sie **Konfiguration ➨ Reboot** aus.
  XAir wird neu gestartet.

### 8.3.10 BinTec XAir Manager beenden

Gehen Sie folgendermaßen vor, um den BinTec XAir Manager zu schließen:

- Wählen Sie **Datei ➨ Beenden**.
  Das Programm wird geschlossen.

## 9.4.2 Das Config-Untermenü PORTS

Dieses Kapitel ersetzt das Kapitel 9.4.2 im XAir Handbuch Version 2.0.
Im Menü **Config ➨ Ports** können Sie die einzelnen aktiven Ports konfigurieren. Die Ethernetschnittstelle erreicht man unter **Config ➨ Ports ➨ Port <Ethernet-Port>.**

```
                          XAir Access Point      by BinTec Communications AG
XAIR Multi2 - V3.00                                                   test2
                       Config Ports eth1

     Command                                  Parameters
  ------------------------------------|-----------------------------------
  1 - Interface          [ le0 ]          |   interface name
  2 - Auto neg mode      [ enabled ]      |
  3 - Actual value       [ 100BaseTX_FD ] |


   Interface assignment for this port.


Enter a number or name, "=" main menu,  [ESC] previous menu.
18:10:46[admin]>
```

Bild 9-14:Das Menü **Config ➨ Ports ➨ Port <Ethernet-Port>**

In der folgenden Tabelle werden die im Menü verwendeten Begriffe und Optionen erläutert:

| Option | Bedeutung |
|---|---|
| **Interface** | Über diese Option kann eine Schnittstelle zugewiesen werden. |
| **Auto neg mode** | Mit dieser Funktion läßt sich der Auto-Negotiation Mode ein- bzw. ausschalten (*enabled/disabled*). Standardmäßig ist der Modus eingeschaltet. Falls Sie z. B. die Geschwindigkeit und den Operation Mode des Ports manuell einstellen möchten, müssen Sie den **Auto neg mode** hier auf *disabled* setzen. |
| **CurrentValue** | Hier werden Ihnen die aktuelle Geschwindigkeit sowie der Duplex-Modus des Ports angezeigt. Der angegebene Wert kann nur dann verändert werden, wenn Sie den Auto-Negotiation Mode ausgeschaltet haben. |

Tabelle 9-9: Die Felder von **Config ➨ Ports ➨ Port <Ethernet-Port>**

### Config ➨ Ports ➨ <Funk-Port>

```
                          XAir Access Point      by BinTec Communications AG
XAIR Multi2 - V3.00                                                   test2
                       Config Ports wl1_ap

     Command                                  Parameters
  ------------------------------------|-----------------------------------
  1 - Interface          [ le0 ]          |   interface name
  2 - OperatingMode      [ AP ]           |
  3 - Actual value       [ bintec ]       |
  4 - Basic              [ -> ]           |
  5 - WEP                [ -> ]           |
  6 - Extended           [ -> ]           |

   Interface assignment for this port.


Enter a number or name, "=" main menu,  [ESC] previous menu.
18:12:25[admin]>
```

Bild 9-15:Das Menü **Config ➨ Ports ➨ <Funk-Port>**

Sicherheitsfunktionen:

Im Untermenü **Basic** finden Sie den Parameter **BcstSSID**, der, wenn er ausgeschaltet ist, verhindert, daß sich Clients, die den Network Name von XAir nicht kennen, an XAir anmelden können. Das Ausschalten von **BcstSSID** (*disabled*) bewirkt, daß der Network Name von XAir nicht mehr gebroadcastet wird und sich dadurch auch Clients mit dem Network-Name-Eintrag *ANY*, nicht mehr an XAir anmelden können. Siehe auch Kapitel 7.3, Seite 25.

Zur Verschlüsselung steht Ihnen die Wireless Equivalent Privacy (WEP) im Untermenü **WEP** zur Verfügung.

Weiterhin bietet die BinTec Communications AG die IPSec-Verschlüsselung als Sicherheitsfunktion an. Informationen dazu finden Sie im Produktbereich für IPSec auf BinTecs Website unter www.bintec.de.

Die folgende Tabelle erläutert die im Menü verwendeten Optionen:

| Option | Bedeutung |
|---|---|
| **Interface** | Über diese Option kann durch den Administrator eine Schnittstelle zugewiesen werden. Auf den Benutzerebenen "User" und "View" ist dieser Menüpunkt lediglich eine statische Anzeige. |
| **OperatingMode** | Unter diesem Menüpunkt können Sie auf der Benutzerebene "Admin" den gewünschten Operation Mode des Ports aus einer Liste auswählen oder manuell in den Prompt eingeben. Auf den Benutzerebenen "User" und "View" ist der Operation Mode unveränderlich. Mögliche Werte:<br>• **AP**<br>Modus, um den Port als Access Point zu betreiben, so daß sich Clients an diesem Port anmelden können.<br>• **Bridge**<br>Modus für eine Bridge. Siehe "**Config ➨ Ports ➨ Port_wlx_br**", XAir Benutzerhandbuch Version 2.0, Seite 134.<br>• **D-Bridge**<br>Modus für eine Double Bridge. Siehe **"Config ➨ Ports ➨ Port_wlx_br**", XAir Benutzerhandbuch Version 2.0, Seite 134. |
| **Network name** | Diese Option, die eine Festlegung des Netzwerknamens erlaubt, wird nur auf der Benutzerebene "Admin" angezeigt. |
| **Basic** | • **DS channel**<br>Hier können Sie als "Admin" oder "User" die Frequenz des Funkkanals einstellen.<br>• **Bcst SSID**<br>Das Ausschalten dieser Option verhindert das Anmelden der Funk-Clients, die den NetworkName des XAirs nicht kennen.<br>Dieser Eintrag existiert nur auf der Benutzerebene "Admin".<br>Das Ausschalten von **Bcst SSID** bedeutet zusätzliche Sicherheit für XAir. BinTec empfiehlt, den **Network name** auf XAir zu konfigurieren und **Bcst SSID** auszuschalten. So wird der **Network name** nicht mehr durch XAir gebroadcastet.<br>• **Repeating**<br>Ermöglicht die direkte Kommunikation zwischen Funk-Clients, die am selben XAir angemeldet sind. Ist **Repeating** ausgeschaltet, können die Funk-Clients, die an diesem XAir angemeldet sind, keine Daten untereinander austauschen.<br>Die Einstellung **Repeating** kann als "Admin" verändert, auf der Ebene "User" lediglich betrachtet werden und ist auf der Ebenen "View" nicht vorhanden.<br>• **Mcast rate**<br>Dient zum Einstellen der Übertragungsrate für Multicast-Frames. Dieser Unterpunkt wird bei entsprechender Konfiguration auf allen Benutzerebenen angezeigt, kann aber ausschließlich auf den Ebenen "User" und "Admin" modifiziert werden. |

| | |
|---|---|
| **WEP** | WEP (Wireless Equivalent Privacy) dient zur Konfiguration der Verschlüsselung des Funkverkehrs. Diese Parameter existieren ausschließlich auf der Ebene "Admin" und können nur dort konfiguriert werden. BinTec empfiehlt, sofern Sie kein VPN einsetzen, die Funktion WEP zu verwenden.<br>• **Status**<br>Aktiviert (enabled) oder deaktiviert (disabled) die Verschlüsselung.<br>• **Key number**<br>Bestimmt den Schlüssel (1-4), mit dem die Daten beim Versenden verschlüsselt werden.<br>• **Key 1-4**<br>Hier werden die Schlüssel eingetragen, die XAir kennen soll. XAir kann ein Funk-Frame entschlüsseln, das mit einem ihm bekannten Schlüssel verschlüsselt wurde.<br>Wichtig ist, daß immer der Schlüssel des entsprechenden Eintrags zur Entschlüsselung herangezogen wird. Das bedeutet, wenn der Client mit Schlüssel 3 verschlüsselt, muß bei XAir in Schlüssel 3 derselbe Wert eingetragen sein wie beim Client. Das gilt natürlich in beiden Richtungen.<br>Der verwendete Schlüssel ist abhängig von der Länge des von Ihnen eingegebenen Keys (entspricht den Bits). Es gibt zwei Kartentypen, die bis zu 128 Bit bzw. nur bis zu 40 Bit unterstützen: Wird ein Schlüssel mit 40 Bit Breite eingegeben, wird mit 64 Bit verschlüsselt (Schlüssel + 24 Bit).<br>Wird ein Key mit 104 Bit eingegeben, wird mit 128 Bit chiffriert.<br>Die Eingabe der Schlüssel kann in ASCII **(**a-z, A-Z, 0-9) oder in hexadezimaler Schreibweise erfolgen (0x gefolgt von der entsprechenden Anzahl Hexzahlen).<br>Beispiele:<br>• **64-Bit-Verschlüsselung**<br>"ABCDE" (ASCII) = "0x4142434445" (Hexadezimal)<br>• **128-Bit-Verschlüsselung**<br>"1234567890123" (ASCII) = "0x31323334353637383930313233" (Hexadezimal)<br>Gesetzte Schlüssel werden durch das Zeichen "*" dargestellt. |
| **Extended** | Spezifische Einstellungen:<br>• **MW robustness**<br>Dient der Übertragungssicherheit bei stark gestörten Umgebungen durch Mikrowellenöfen. Frames werden fragmentiert versendet um die Wahrscheinlichkeit einer Störung zu verringern. Diese Einstellung wird an alle assoziierten Clients übertragen, falls "**medium distr. enabled**" ist. Voraussetzung ist, dass die Clients diese Funktion unterstützen.<br>• **RTS threshold**<br>Hier kann der Schwellenwert in Bytes (1..2346) angegeben werden, ab wann der RTS/CTS Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden. Der Mechanismus kann auch immer ein bzw. ausgeschaltet werden.<br>• **AP distance**<br>Mit dieser Funktion wird das Roamingverhalten des Clients verändert. Je kleiner die Funkzelle eingestellt wird, um so eher roamen die Clients zum nächsten XAir. Voraussetzung ist, das "**Medium distr. enabled**" ist und die Clients diese Funktion unterstützen.<br>• **Load balanc.**<br>Aktivieren Sie "Load balanc.", wenn die Clients ihre XAirs dynamisch je nach Lastverteilung auswählen sollen. Der XAir sendet in diesem Fall die entsprechenden Informationen in den Probe Response und Beacon Frames. |

| | |
|---|---|
| **Extended** (Fortsetzung) | • **Medium distr.** Aktivieren Sie diese Funktion, wenn Clients die oben definierten Parameter ("**MW Robustness**", "**RTS threshold**", "**AP distance**", "**Load balanc**.") übertragen bekommen sollen. Wenn die Clients diese Funktion unterstützen werden deren lokalen Einstellungen von denen des XAirs überschrieben.<br>• **Encapsulation** Auf diese Funktion kann nur bei entsprechender Konfiguration auf der Ebene "Admin" zugegriffen werden. Dieser Menüpunkt besitzt zahlreiche Untermenüs, die im folgenden detailliert erläutert werden. |

Tabelle 9-10: Die Felder von **Config ➨ Ports ➨ <Funk-Port>**

## Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation

Über einen Funk-Port werden nur LLC-Frames gesendet. Alle anderen Frames müssen mit einem LLC-Header versehen werden. Der Menüpunkt **Encapsulation** ermöglicht die Konfiguration dieses Vorganges und die Art und Weise, wie die Encapsulation beim Empfang rückgängig gemacht wird.

Die Funktion **Encapsulation** sollte nur von erfahrenen Administratoren verwendet werden.

Im Menü **Encapsulation** haben Sie zunächst die Wahl zwischen den Optionen **Mode** und **Customize**.

- Unter **Mode Default** können Sie alle bisher vorgenommenen Einstellungen bezüglich der Frame-Aufbereitung rückgängig machen und die Ausgangswerte wieder herstellen.
- Unter **Customized** können Sie genau festlegen, wie mit eingehenden und ausgehenden Datenpaketen verfahren werden soll:
  - Ausgehende Pakete können Sie in **Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customized ➨ Transmit** bearbeiten.
  - Die Konfiguration für eingehende Pakete legen Sie in **Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customized ➨ Receive** fest.

## Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customized ➨ Transmit

In der folgenden Tabelle werden die im Menü verwendeten Optionen und die daraus resultierenden Einstellungsmöglichkeiten erläutert:

| Option | Bedeutung |
|---|---|
| **Encapsulation** | Wählen Sie unter dieser Option die Default Encapsulation aus, d. h. stellen Sie die Norm ein, die standardmäßig als Grundlage zur Übertragung von Frames ohne **LLC**-Header dienen soll. Vorgegeben sind die beiden Standards **RFC_1042** und **IEEE_802.1H**, welche Sie entweder aus der Liste auswählen oder direkt in den Prompt eingeben können. |
| **Exceptions** | Hier legen Sie fest, für welche Protokolle die **Default Encapsulation** nicht gelten soll.<br>Mit der Option **Show** können Sie sich alle bisher ausgeschlossenen Protokolle anzeigen lassen, wobei der Wert in eckigen Klammern die Anzahl dieser Protokolle angibt.<br>Wählen Sie **Add**, um der Ausschlußliste weitere Protokolle hinzuzufügen (max. 10). Diese können entweder in der vorgegebenen Liste selektiert oder in den Prompt eingegeben werden.<br>Dementsprechend können Sie unter **Remove** Protokolle von der Ausschlußliste entfernen, d. h., für diese Protokolle gilt ab diesem Punkt wieder die **Default Encapsulation**. |

Tabelle 9-11: Die Felder von **Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customize ➨ Transmit**

## Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customize ➨ Receive

Unter diesem Menüpunkt wählen Sie zunächst die Norm, für welche Sie die beim Empfang eines Datenpaketes auszuführende Aktion definieren möchten. Standardmäßig sind hier die Spezifikationen RFC_1042 und IEEE_802.1H vorgegeben.

Die Untermenüs der Optionen in Tabelle 9-11sind identisch aufgebaut und werden in der folgenden Tabelle zusammengefaßt erläutert:

| Option | Bedeutung |
|---|---|
| **DefaultAction** | Hier können Sie festlegen, ob bei ankommenden Datenpaketen standardmäßig der LLC-Header entfernt werden soll. Wählen Sie **remove**, um den Header entfernen zu lassen, bzw. **unchanged**, um das Datenpaket unverändert zu lassen. |
| **Exceptions** | Hier legen Sie fest, für welche Protokolle die **Default Action** nicht gelten soll.<br>Mit der Option **Show** können Sie sich alle bisher ausgeschlossenen Protokolle anzeigen lassen, wobei der Wert in eckigen Klammern die Anzahl dieser Protokolle angibt.<br>Wählen Sie **Add**, um der Ausschlußliste weitere Protokolle hinzuzufügen (max. 10). Diese können entweder in der vorgegebenen Liste selektiert oder in den Prompt eingegeben werden.<br>Dementsprechend können Sie unter **Remove** Protokolle von der Ausschlußliste entfernen, d. h., für diese Protokolle gilt ab diesem Punkt wieder die **Default Action**. |

Tabelle 9-12: Die Felder von **Config ➨ Ports ➨<Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customize ➨ Receive**

## Config ➨ Ports ➨ <Bridge-Port>

Beschreibungen der Menüs für den Bridge-Port finden Sie in XAir Handbuch Version 2.0, Kapitel 11.3.1, Seite 130 und in Kapitel 11.4.2, Seite 161.

## 9.5.3 Das Control-Untermenü SECURITY

Unter diesem Menü können Sie sich die verschiedenen Benutzerebenen anzeigen lassen, deren Paßwörter ändern und die Zugriffsrechte konfigurieren.

```
                          XAir Access Point      by BinTec Communications AG
XAIR Multi2 - V3.00                                                   test2
                       Control Security

     Menu                                    Submenu
  ---------------------------------------|-----------------------------------
  1 - User info    [ -> ]                |   Show                 [3]
  2 - Authenticate [ -> ]                |   Edit


     Configuration User Group Menu.


Enter a number or name, "=" main menu,  [ESC] previous menu.
18:13:11[admin]>
```

Bild 9-29:Das Menü **Control ➨ Security**

### Control ➨ Security ➨ User info

Über dieses Menü können Sie sich die verschiedenen Benutzerebenen anzeigen lassen.
Sie können auch die Paßwörter der einzelnen Benutzerebenen ändern, wenn Ihnen das Paßwort der Benutzerebene "Admin" bekannt ist.

### Control ➨ Security ➨ User info ➨ Show

Zeigt die Bezeichnungen der verschiedenen Benutzerebenen an. Das sind admin, user und view.
Die Paßwörter der Benutzerebenen werden nicht angezeigt.

### Control ➨ Security ➨ User info ➨ Edit

Unter diesem Menüpunkt haben Sie die Möglichkeit, als "Admin" oder als "User" die Paßwörter aller drei Benutzerebenen zu ändern. Auf der Ebene "View" existiert dieser Menüpunkt nicht.

Als Voraussetzung zur Änderung der Paßwörter müssen Sie das Paßwort der Benutzerebene "Admin" kennen.

Gehen Sie folgendermaßen vor, um ein Paßwort zu ändern:

- Wählen Sie **Control ➨ Security ➨ User info ➨ Edit**.
- Markieren Sie im Untermenü auf der rechten Tabellenseite die Benutzerebene, für die Sie das Paßwort ändern wollen: view, user oder admin. Bestätigen Sie mit der **Eingabetaste**.
- Geben Sie das "Admin"-Paßwort am Prompt ein und bestätigen Sie mit der **Eingabetaste**.
- Geben Sie nun zweimal hintereinander das neue Paßwort für die vorher markierte Benutzerebene ein und bestätigen Sie jeweils mit der **Eingabetaste**.

Ab der nächsten Telnet-Verbindung können Sie sich mit dem neuen Paßwort für die entsprechende Benutzerebene anmelden.

Achtung!
Die Paßwörter werden beim ResetToFD nicht auf die Werkseinstellungen zurückgesetzt. Vergessen Sie das "Admin"-Paßwort, müssen Sie XAir einschicken.

- Merken Sie sich das "Admin"-Paßwort.

## Control ➨ Security ➨ Authenticate

Über dieses Menü konfigurieren Sie die lokale Access Control List und den Zugriff auf einen externen Access Control Server. Weiterhin werden hier die Einstellungen zur IEEE802.1x vorgenommen. Wenn Sie diese Funktionen aktivieren, können Sie den Zugriff auf das Datennetz über XAir einschränken, da nur die Clients über XAir auf Ihr LAN zugreifen können, deren MAC-Adresse in die lokale bzw. Remote Access Control List eingetragen ist. Zusätzlich können Sie eine Authentisierung der User mittels Passwort und Username an einem Authentisierungsserver vornehmen.

Die Access Control List (ACL) und die Authentisierung mittels eines eigenen Servers sind zusätzliche Möglichkeiten, Ihr WLAN besser zu schützen. Sie erreichen dadurch eine höhere Zugangssicherheit.
Mit dem optional erhältlichen BinTec **ACL-Manager** können u. a. das WLAN einfach verwaltet werden und nicht erlaubte Zugriffsversuche protokolliert werden.

Wenn Sie sich für **ACL local** entscheiden, wird die Liste der MAC-Adressen im XAir gehalten. Sie müssen dann in jedem XAir eine eigene Liste pflegen.
Wenn Sie **ACL remote** verwenden wollen, müssen Sie einen **ACL-Manager** von der BinTec Communications AG erwerben. Dieser verwaltet dann die Liste zentral für alle Funkzellen und alle Funknetzwerke.

Das Menü **Control ➨ Security ➨ Authenticate**:

```
                          XAir Access Point      by BinTec Communications AG
XAIR Multi2 - V3.00                                                    test2
                      Control Security Authenticate

     Menu                                    Submenu
  ---------------------------------------|-----------------------------------
  1 - wl1_ap       [ -> ]                |   ACL local            [disabled]
  2 - ACL local    [ -> ]                |   ACL remote           [disabled]
  3 - ACL remote   [ -> ]                |   IEEE802.1x           [disabled]
  4 - EAP          [ -> ]                |
  5 - Auth. Cache  [3]                   |


     Wireless authentication operating modes


Enter a number or name, "=" main menu,  [ESC] previous menu.
18:13:11[admin]>
```

Bild 9-30:Das Menü **Control ➨ Security ➨ Authenticate**

In der folgenden Tabelle werden die Parameter näher beschrieben:

| Option | Bedeutung |
|---|---|
| **wl1_ap** | Hiermit konfigurieren Sie die Zugriffskontrolle des entsprechenden Funk-Ports.<br>• **ACL local**<br>Hier können Sie die Verwendung einer lokalen Access Control List aktivieren "**enable**" oder deaktivieren "**disable**".<br>• **ACL remote**<br>Hier können Sie die Verwendung eines externen ACL-Servers aktivieren "**enable**" oder deaktivieren "**disable**".<br>• **IEEE802.1x**<br>Hier können Sie die Verwendung eines externen Authentisierungs-Servers aktivieren "**enable**" oder deaktivieren "**disable**". |
| **ACL local** | Dient zum Konfigurieren einer lokalen Access Control List.<br>• **Show**<br>Zeigt Ihnen die lokale Access Control List an. |

| | |
|---|---|
| **ACL local** (Fortsetzung**)** | • **Add**<br>Fügt einen neuen Eintrag in der Access Control List hinzu.<br>◊ **client MAC addr**<br>Angabe der MAC-Adresse des Clients, der in die Access Control List aufgenommen werden soll.<br>◊ **port**<br>Wählen Sie auf welchen wireless Port von XAir der Client Zugriff hat:<br>- **all ports,** auf alle wireless Ports von XAir;<br>- **<Funk-Port>,** der entsprechende wireless Port.<br>• **Remove**<br>Entfernt einen Eintrag aus der Access Control List.<br>• **client MAC addr**<br>Angabe der MAC-Adresse des Clients, der aus der Access Control List entfernt werden soll. |
| **ACL remote** | Dient zum Konfigurieren der Kommunikation mit einem externen ACL-Server.<br>• **IP address**<br>Dient zur Angabe der IP-Adresse des ACL-Servers.<br>• **Port number**<br>Dient zur Angabe des IP-Ports, über den der ACL-Server erreichbar ist.<br>• **Comm. state**<br>Gibt den Status der Verbindung zum ACL-Server an.<br>◊ **disconnected -** Verbindung besteht nicht.<br>◊ **connected -** Verbindung besteht.<br>• **Def. access**<br>Gibt den Access Code an, der verwendet wird, wenn der ACL-Server nicht erreichbar ist.<br>◊ **denied -** Zugriff wird verweigert.<br>◊ **granted -** Zugriff wird gewährt.<br>• **Sync period**<br>Geben Sie das Zeitintervall (in Minuten) an, nach dem der ACL Cache aktualisiert werden soll. Diese Zeit läuft für jeden Client getrennt. |
| **EAP** | • **Prim. Server**<br>Gibt die Nummer des primären Authentisierungs-Servers an. Falls mehrere Server eingetragen sind kann der primäre Server aus einer Liste ausgewählt werden.<br>• **Server Config**<br>◊ **Edit server**<br>Hier können Sie die Einstellungen zu den Authentisierungs-Servern ändern. Es gibt folgende Möglichkeiten:<br>- **Select Server -** Wählt den zu editierenden Server aus einer Liste aus.<br>- **IP address -** IP Adresse des Servers<br>- **Port number -** Portnummer auf der die Kommunikation mit dem Server stattfinden soll. Default ist 1812.<br>- **Shared secret -** der Schlüssel, mit dem die Datenpakete zwischen XAir und Server verschlüsselt werden. Tragen Sie hier den gleichen Schlüssel wie im Server ein.<br>- **Remove server -** Löscht den gerade ausgewählten Servereintrag.<br>◊ **Add Server**<br>Erstellt einen Servereintrag. |

| | |
|---|---|
| **EAP**<br>(Fortsetzung) | • **Comm. state**<br>Gibt den Status der Verbindung zum Server an.<br>◊ **disconnect**<br>Verbindung besteht nicht<br>◊ **connected**<br>Verbindung besteht<br>• **Def. Access**<br>Gibt das Verhalten des XAir an, wenn der primäre Server nicht erreichbar ist.<br>◊ **denied -** Zugriff wird verweigert<br>◊ **granted -** Zugriff wird gewährt<br>• **Timeout**<br>Der globale Timeout, nach dem der Authentisierungsvorgang abgebrochen wird.<br>• **Advanced**<br>Hier können erweiterte Einstellungen vorgenommen werden.<br>◊ **Supp. Timeout**<br>Timeout-Zeit für Anfragen des Clients an den Access Point (in Sekunden).<br>◊ **Max. requests**<br>Maximale Anzahl der Anfragen von Usern, nach der die Authetisierung abgebrochen wird.<br>◊ **Quiet period**<br>Wartezeit nach einem Authentisierungsabbruch.<br>◊ **Reauth switch**<br>Dient zum ein- oder ausschalten der automatischen Wiederanmeldung von Clients<br>- **enabled -** Der User wird automatisch nach der vorgegebenen Zeit erneut authentisiert.<br>- **disabled -** Der User wird nicht automatisch erneut authentisiert.<br>◊ **Reauth period**<br>Die Zeit, nach der ein User erneut automatisch authentisiert wird (in Sekunden).<br>◊ **Max. reauth.**<br>Die maximale Anzahl der automatischen Reauthentisierungs-versuche. |
| **Auth. cache** | Die Zahl in den eckigen Klammern gibt die aktuelle Anzahl der internen und externen Einträge in der Authentisierungsliste an. Diese Liste enthält sowohl die Einträge von ACL als auch die von EAP.<br>Mit der Eingabetaste können Sie sich die Liste anzeigen lassen. Sie erhalten Auskunft zu der Client MAC-Adresse, dem Port, an dem der Client angemeldet ist, ob der Zugriff erlaubt oder verweigert wurde (Error, InProgress, Granted, Denied) und die Quelle der Authentisierung (ACL local, ACL remote oder EAP).<br>Bei Auth. cache wird zusätzlich der Zustand, in dem sich die Anfrage befindet (Request, Reply, Sync, Disconn) und die Zeit bis zur nächsten Timeout angezeigt. |

Tabelle 9-25: Die Parameter von **Control ➨ Security ➨ Authenticate**

# Anhang: Änderungen der Bezeichnung einzelner Menü-Punkte

## Status

### Firmware Version 2.73

- Status
  - Summary
  - Ports
    - <Ethernet-Port>
      - MAC
      - MAXSpeed
      - Statistics
    - <Funk-Port>
      - MAC
      - MaxSpeed
      - Statistics
      - CardFirmware
      - NodeTable (nicht im BR-Modus)
  - ARPCache
  - BufferUtil
  - Software

### Firmware Version 3.00

- Status
  - Summary
  - Ports
    - <Ethernet>
      - MAC
      - Max speed
      - Statistcs
    - <Funk-Port>
      - MAC
      - Max speed
      - Statistics
      - Card firmware
      - Node table (nicht im BR-Modus)
  - ARP cache
  - Buffer util.
  - Software

## Config

### Firmware Version 2.73

- Config
  - System
    - NodeName
  - Ports
    - Ports <Ethernet-Port>
      - Interface
      - AutoNegMode
      - CurrentValue
    - Ports <AP-Funk-Port>
      - Interface
      - OperatingMode
      - NetworkName
      - Basic
        - DSChannel
        - BcstSSID
        - Repeating
        - McastRate
      - WEP
        - Status
        - TxKeyNumber
        - Key 1-4
      - Extended
        - -
        - -
        - -
        - -
        - -
      - Encapsulation
        - Mode
        - Default
          - Modification
            - Transmit
              - Def.Encaps.
              - Exeptions
            - Receive
              - DefaultAction
              - Exceptions
    - Ports <BR und BRx - Funk-Port>
      - Interface
      - OperatingMode
      - BridgePort

### Firmware Version 3.00

- Config
  - Status
    - Node name
  - Ports
    - Ports <Etherner-Port>
      - Interface
      - Auto neg mode
      - Actual value
    - Ports <AP-Funk-Port>
      - Interface
      - OperatingMode
      - Network name
      - Basic
        - DS channel
        - Bcst SSID
        - Repeating
        - Mcast rate
      - WEP
        - Status
        - Key number
        - Key 1-4
      - Extended
        - MW robustness
        - RTS threshold
        - AP distance
        - Load balanc.
        - Medium distr.
        - Encapsulation
          - Mode
          - Default
            - Customize
              - Transmit
                - Encapsulation
                - Exeptions
              - Receive
                - Def. Action
                - Exeptions
    - Ports <BR und BRx - Funk-Port>
      - Interface
      - OperatingMode
      - Bridge port

| | |
|---|---|
| BridgePort | Bridge link |
| DstMac | Remote MAC |
| DSChannel | DS channel |
| TxSpeedMode | Speed mode |
| CurTxSpeed | Actual speed |
| WEP | WEP |
| Status | Status |
| TxKeyNumber | Key number |
| Key 1-4 | Key 1-4 |
| Extended | Extended |
| - | MW robustness |
| - | RTS threshold |
| - | AP distance |
| - | Load balanc. |
| - | Medium distr. |
| Encapsulation | Encapsulation |
| Mode | Mode |
| Default | Default |
| Modification | Customize |
| Transmit | Transmit |
| Def.Encaps. | Encapsulation |
| Exeptions | Exeptions |
| Receive | Receive |
| DefaultAction | Def. Action |
| Exceptions | Exeptions |
| RemoteConfig | Remote bridge |
| RemoteMac | Remote MAC |
| RemoteConfig | Remote config |
| RemoteBridge | Remote bridge |
| Settings | Settings |
| TXSpeedMode | Speed mode |
| DSChannel | DS channel |
| WEP_Status | WEP_Status |
| WEP_TxKeyNo | WEP_TxKeyNo |
| WEP_Key1-4 | WEP_Key1-4 |
| Connection | Connection |
| LinkTest | Link test |
| LinkPartner | LinkPartner |
| LinkTest | Link test |
| StartTest | StartTest |
| Interfaces | Interfaces |
| IP_Address | IP address |
| Subnet_Mask | Subnet mask |
| GateWay | Gateway |
| DHCP_StartUp | DHCP startup |
| DHCP_Fallback | DHCP fallback |
| DHCP_Options | DHCP options |
| Lease | Lease |
| none | none |
| in use | used |
| trying | in process |
| failure | failure |
| RequestedIP | Requested IP |
| ClientID | Client ID |
| Server | Server |
| VendorID | Vendor ID |
| Duration | Duration |
| Filtering | Filtering |
| ARPProcessing | ARP process. |
| Protocol | Protocol |
| DefaultMode | Default mode |
| Show | Show |
| Add | Add |
| Remove | Remove |
| MAC_Multicast | MAC filter |
| DefaultRule | Default rule |
| ShowAll | Show all |
| AddFrom | Add from |
| Remove | Remove |
| Edit | Edit |
| SortShow | Sort show |
| IPRoutes | IP_routes |
| Show | Show |
| Add | Add |
| Remove | Remove |

## Control

| Firmware Version 2.73 | Firmware Version 3.00 |
|---|---|
| Control | Control |
| DHCP_Client | DHCP client |
| Leases | Leases |
| Retransm. | Retransm. Time |
| Retries | Retries |
| SNMP | SNMP |
| Status | Status |
| Port_SNMP | SNMP port |
| SysObjectID | SysObject ID |
| Contact | Contact |
| Location | Location |
| Read_Access | Read access |
| Write_Access | Write access |
| Send_Trap | Send trap |
| Manager | Manager |
| Show | Show |
| Add | Add |
| Remove | Remove |
| Edit | Edit |
| ManageName | Manager name |
| IP_Address | IÜ address |
| Mask | Mask |
| Read_Access | Read access |
| Write_Access | Write access |
| Send_Trap | Send trap |
| Port_Trap | Port trap |
| Timeout | Timeout |
| Retries | Retries |
| Security | Security |
| UserInfo | User info |
| Show | Show |
| Edit | Edit |
| ACL | Authenticate |
| <Funk-Port> | <Funk-Port> |
| AclLocal | ACL local |
| AclRemote | ACL remote |
| - | IEEE802.1x |
| AclLocal | ACL local |
| Show | Show |
| Add | Add |
| Remove | Remove |
| AclRemote | ACL remote |
| IPAddress | IP address |
| PortNumber | Port number |
| CommState | Comm. State |
| DefaultAccess | Def. Access |
| SyncPeriod | Sync period |
| - | EAP |
| - | Prim. server |
| - | Server config |
| - | Comm. state |
| - | Def. access |
| - | Timeout |
| - | Advanced |
| AclCache | Auth. cache |
| ViewLogs | View logs |
| SystemReset | System reset |
| ResetToFD | Reset to FD |

## Refresh, Help und Exit

| Firmware Version 2.73 | Firmware Version 3.00 |
|---|---|
| Refresh | Refresh |
| Help | Help |
| Exit | Exit |