Supplement

for

XAir's User Guide

Version 2.00

Additional Features in Firmware Version 3.00
and XAir Manager Version 2.06

Version 1.0
June 2002

Changes Overview

This supplement describes the changes between Firmware Version 2.73 and Version 3.0 of XAir Access Points. In addition to the new release following changes took place:

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

The Firmware Release 3.0 mainly focuses on additional and improved security features for the XAir product family.

The new release contains following improvements:

- **WEPplus**
  The key that is input to the WEP64 or 128 RC4 encryption algorithm consists of the secret key configured by the user (or via 802.1x) concatenated with the IV (Initialization Vector). The IV is determined by the transmitting station. By excluding certain IV values that would create so-called "weak keys are avoided. The compliance against IEEE 802.b is still given
- **IEEE 802.1x and EAP**
  The standard IEEE 802.1x defines a radio independent authentication scheme. It works on port level. Due to an authentication server (Radius, Kerberos etc.) the authentication of a user (not a client HW) to the net is performed. This means, that the Access Point has to verify the user first. Access to the net is only possible after verification. Both, client and authentication server have to be able to understand the EAP (Extensive Authentication Protocol). On the client side only Windows XP is supporting EAP. All other operating systems need a so called "supplicant" software.

Further improvements are:

- option for microwave robustness
- selection of RTS/CTS threshold
- selection o load balancing

Table of Contents

8 The BinTec XAir Manager

This chapter describes the extra configuration options provided by the BinTec XAir Manager version 2.06 in addition to the basic configuration (see chapter "Basic Configuration" in "Los Geht's/Getting Started").

It replaces chapter 8 of the XAir Manual version 2.0

Start the BinTec XAir Manager by double clicking the xairm.exe file.

The basic configuration comprises the following settings:

- Enter access point name
- Enter IP address
- Enter net mask
- Enter standard gateway.

You can also make the following configurations with the BinTec XAir Manager:

- Starting a Telnet connection
- Starting a web connection
- Upgrading the firmware
- Rebooting
- Resetting XAir to ex works settings.

Your XAir and the Windows PC you want to use for configuring XAir must be in the same LAN.

Instructions for working with the BinTec XAir Manager:

- The PC must have a working TCP/IP stack with a sensible configuration.
- All settings made over the BinTec XAir Manager can also be made over a router.
- The search function is restricted to the subnetwork of the PC on which the BinTec XAir Manager is located if the router does not forward multicasts.
- With more recent firmware versions, XAir can only be configured via a password. You should change the preset passwords as soon as possible for security reasons. Older firmware versions do not have this feature. You are recommended to update to the current firmware version. You will find the current version of the firmware at www.bintec.net.
- If your PC has several network interfaces, you can configure a certain multicast interface (router or switch) in the BinTec XAir Manager (see chapter 8.1, page 27) over which XAirs are to be searched for.

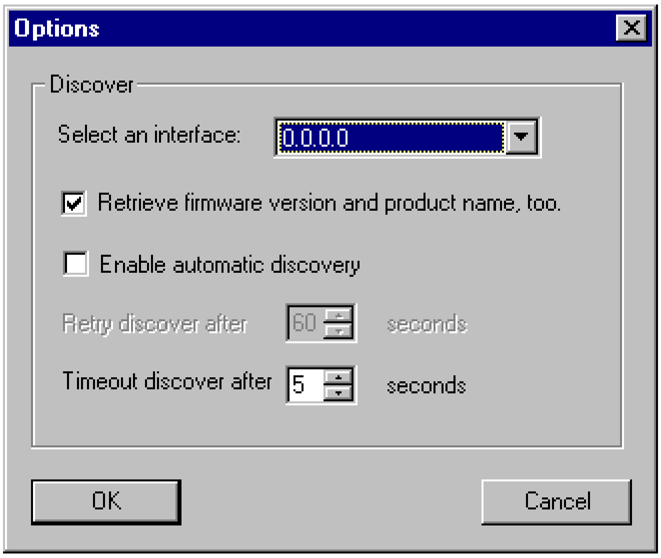
8.1 Defining a Multicast Interface

If the PC on which the BinTec XAir Manager is installed has several network interfaces, one interface can be defined as a multicast interface. This interface is used for searching for XAirs.

Proceed as follows to manually define a multicast interface (router or switch):

➢ Select **Extras ➨ Options.**

The following dialog box opens:



Select an interface: 0.0.0.0

☑ Retrieve firmware version and product name, too.

□ Enable automatic discovery

Retry discover after 60 seconds

Timeout discover after 5 seconds

Figure 8-1: Entering the IP address for the multicast router (switch)

➢ Enter the IP address of the desired multicast interface (router or switch) and press **OK.** Once the multicast interface 0.0.0.0 is defined, a search is made over all network interfaces of the PC.

8.2 The User Interface of the BinTec XAir Manager

The user interface of the BinTec XAir Manager comprises four components, which are described in detail below:

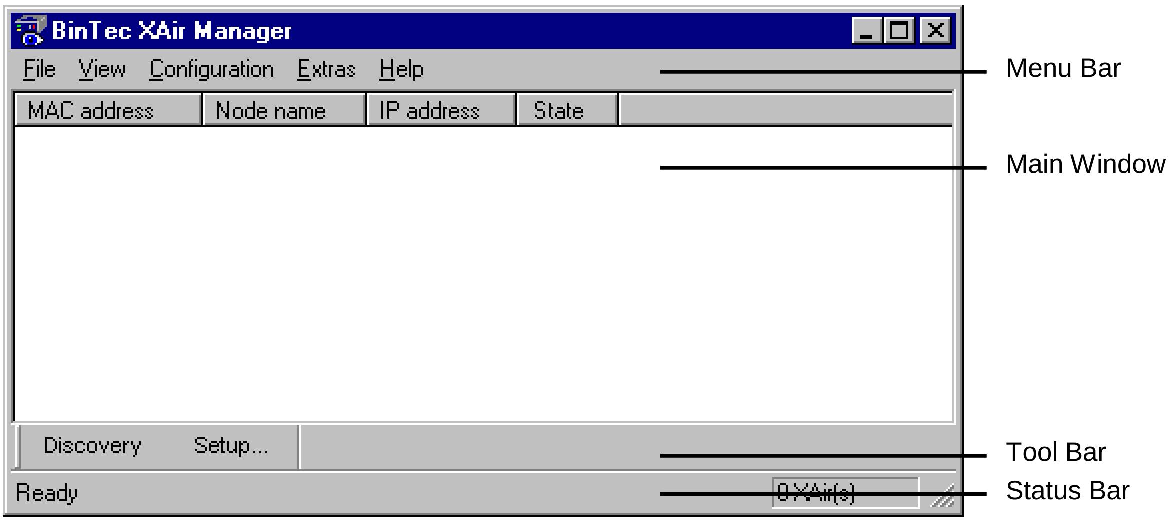


Figure 8-2: User interface of BinTec XAir Manager

8.2.1 The Main Window

The main window is initially blank when starting the BinTec XAir Manager via the BinTec xairm.exe file. The main window consists of tables arranged in columns for **MAC address**, **Node name**, **IP address** and **State**. As soon as XAirs have been searched for and recognized in the network, these columns contain the relevant data for each device.

8.2.2 The Menu Bar

The menu is located at the top edge of the BinTec XAir Manager and contains the menu items **File**, **View**, **Configuration**, **Extras** and **Help** with the respective menu subitems.

8.2.3 The Tool Bar

The tool bar, which is located directly below the main window, provides fast access to the two most important functions of the XAir Manager, **Discovery** and **Setup**. These two functions, which can also be selected via the menu, are explained in more detail below (see chapter 8.3.1, page 30 and chapter 8.3.3, page 33).

Proceed as follows to show or hide the tool bar:

➢ **Select View ➨ Tool Bar**.

8.2.4 The Status Bar

The status bar at the bottom edge of the window shows you the status of the XAir Manager. If the mouse pointer is over a menu item that activates a function (e.g. Discovery), the function of this menu item is also shown in the status bar.

Proceed as follows to show or hide the status bar:

➢ Select **View ➨ Status Bar**.

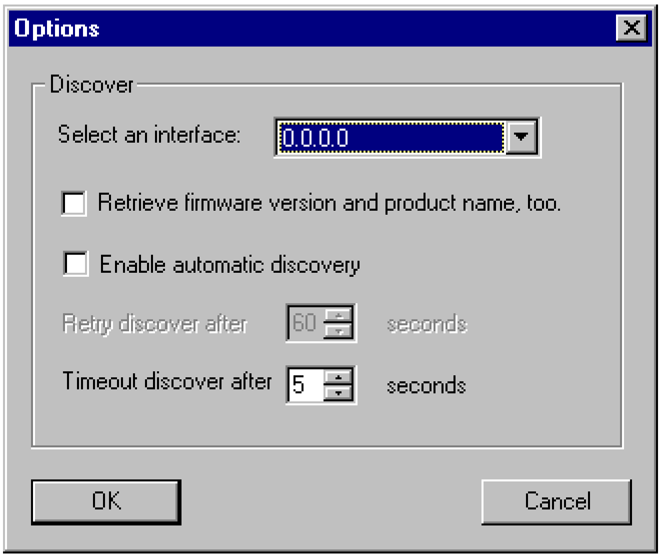
8.3 Functions of BinTec XAir Manager

This chapter describes the following:

- Finding Available XAirs
- Manually Processing Entries
- The Basic Configuration
- Entering the Password
- Starting a Telnet Connection
- Starting a Web Connection
- Upgrading the Firmware
- Resetting XAir to Ex Works Settings
- Rebooting XAir
- Closing the BinTec XAir Manager

8.3.1 Finding Available XAirs

The Discovery function can be activated via the menu item **File ➔ Discovery**



Options

Discover

Select an interface: 0.0.0.0

☐ Retrieve firmware version and product name, too.

☐ Enable automatic discovery

Retry discover after 60 seconds

Timeout discover after 5 seconds

Figure 8-3: Options window

If the corresponding check box is tagged, it is possible to display the product name and version of the access point.

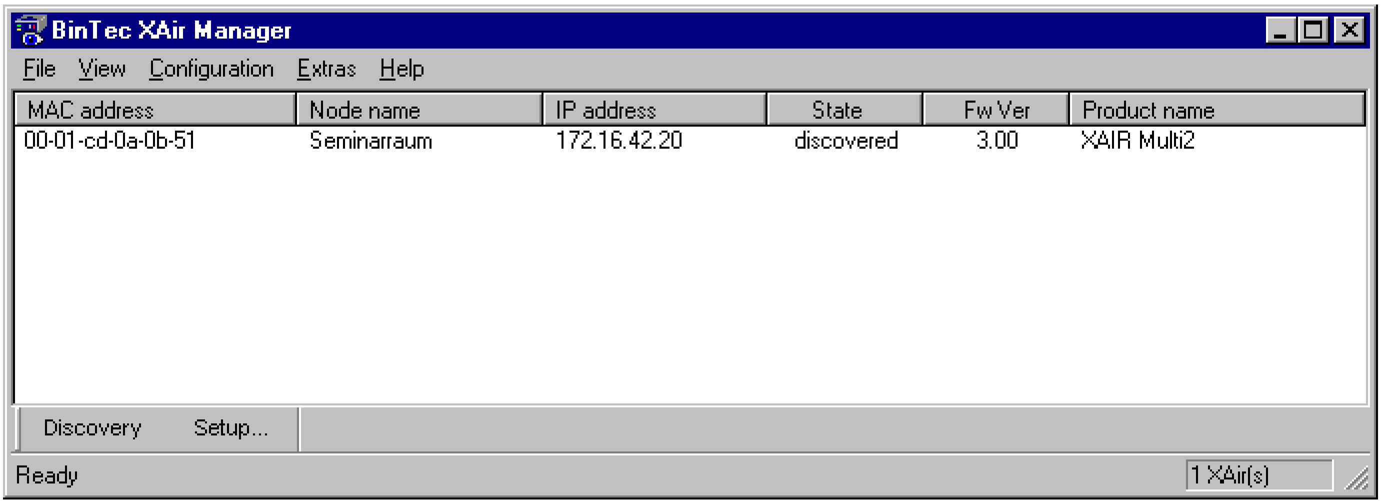
To activate the automatic search function you can tag the check box for this function. In the input box underneath you can enter the duration between 2 search cycles. Values between 10 to 60 seconds are possible.

The time to interrupt the search function can be defined in the next input box. For small WLANs 1 second is sufficient. The maximum time is 10 s.

Confirm your entry by clicking the **OK** button.

The Discovery function can be activated via the menu item **File ➔ Discovery** or directly via the **Discovery** button on the tool bar.

The BinTec XAir Manager then recognizes the XAir Access Points installed in the network automatically and shows them in the main window with the associated network parameters (**MAC address, Node name**, **IP address**), according adjustment also the Firmware version (**Fw Ver**) and **product name**.



MAC address	Node name	IP address	State	Fw Ver	Product name
00-01-cd-0a-0b-51	Seminarraum	172.16.42.20	discovered	3.00	XAIR Multi2

Figure 8-4: XAirs found

The entries in the State column mean:

- discovered = found by BinTec XAir Manager,
- by user = manual entry and
- not found = XAir is not found by a new search.

8.3.2 Manually Processing Entries

The **Add**, **Delete** and **Delete All** functions can be selected in the menu **item File ➨ Manual Entry**:

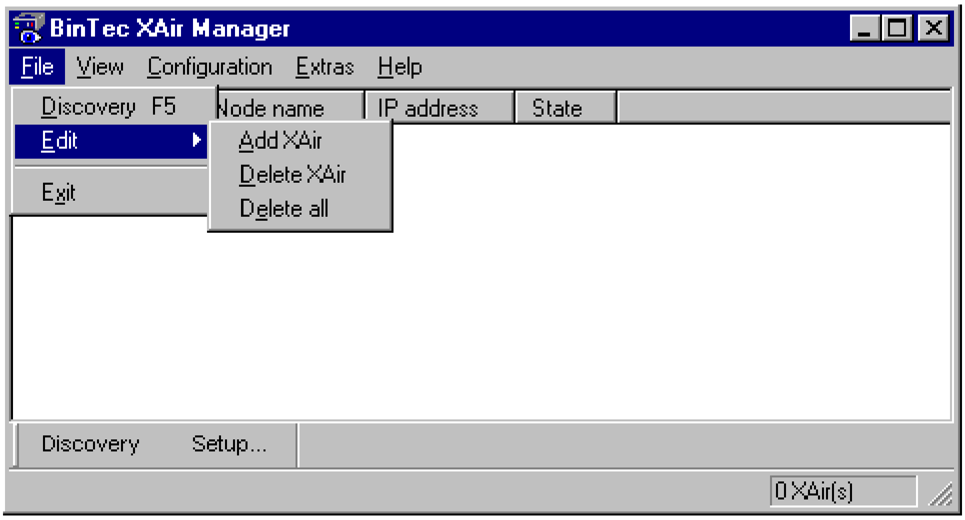


Figure 8-5: Submenu **Edit**

Manually adding an XAir

- ➢ Select **File** ➨ **Edit** ➨ **Add**

A dialog box opens in which you can enter the IP address of the XAir to be added:

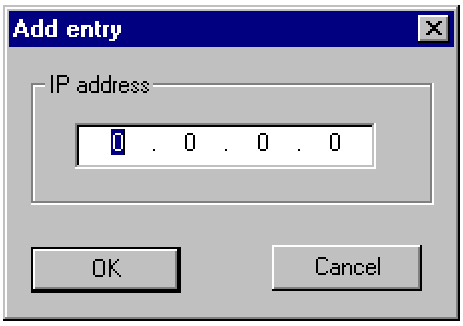


Figure 8-6: Entering the IP address of XAir

- ➢ Confirm your entry by clicking the OK button. The manually entered XAir is searched for and appears in the list in the main window when it is found.

Deleting an XAir manually entered or not found.

Proceed as follows to delete manually added XAirs (**State** by user) and XAirs tagged as not found from the list:

- ➢ Tag the MAC address of the entry to be deleted.
- ➢ Select **File** ➨ **Edit** ➨ **Delete** alternative the "Del" key is also possible.

Entries that have been created automatically with the Discovery function cannot be deleted in this way.

Deleting all XAirs not found

Proceed as follows to simultaneously delete all entries tagged as not found from the list in the main window:

- ➢ Select **File** ➨ **Edit** ➨ **Delete All**.

8.3.3 The Basic Configuration

To configure an XAir, tag the relevant entry in the main window, enter the password (**Configuration** ➨ **Password**) and select either **Configuration** ➨ **Setup** or press the **Setup...** button in the tool bar.

You will find details on carrying out the basic configuration in chapter "The Basic Configuration" in Los Geht's/Getting Started.

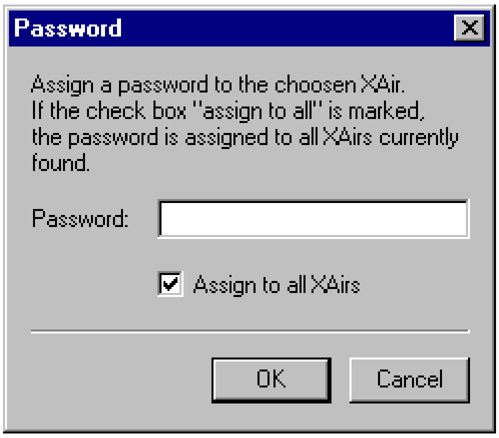
8.3.4 Entering the Password

The password is necessary for using the following settings of the BinTec XAir Manager:

- Firmware Upgrade
- Reboot
- Reset
- Setup.

Proceed as follows to enter the password:

- ➢ Tag the XAir in the list and select **Configuration** ➨ **Password**.



Password

Assign a password to the choosen XAir.
If the check box "assign to all" is marked, the password is assigned to all XAirs currently found.

Password:

☑ Assign to all XAirs

Figure 8-7: Entering the Password

- ➢ Enter the password for the user level "Admin" and press **OK**.
  The ex works password set for the user level "Admin" is admin.
- ➢ If the function field **Assign to all XAirs** is activated, the same password is also used for all other XAirs. If the BinTec XAir Manager is closed, the password must be entered again when the BinTec XAir Manager is restarted.

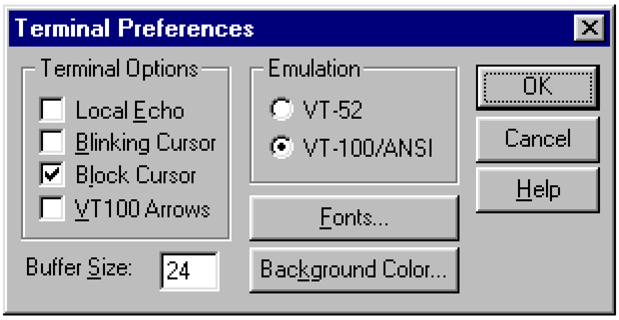
If you have not already done so, you should change the passwords for the three user levels "Admin", "User" and "View" immediately to prevent unauthorized access.
You can change the passwords in the user interface of the XAir in **the Control ➨ Security ➨ UserLevel ➨ Edit** menu (see chapter 7.1, page 18).

8.3.5 Starting a Telnet Connection

Proceed as follows to start a Telnet connection:

- ➢ Tag the XAir you wish to access over Telnet in the main window.
- ➢ Select **Configuration ➨ Advanced ➨ Telnet**.
- ➢ A terminal is now emulated in a new dialog box.
- ➢ Select **Terminal ➨ Settings** in the new dialog box.

The following window opens:



Terminal Preferences

Terminal Options
□ Local Echo
□ Blinking Cursor
☑ Block Cursor
□ VT100 Arrows

Emulation
○ VT-52
● VT-100/ANSI

Buffer Size: 24

Figure 8-8: Terminal Settings window

- ➢ If you wish to use all the functions of the terminal, make sure
  - – the option field VT-100/ANSI is activated in **Emulation** field,
  - – the **Buffer Size** for an optimum display is set to at least 25.

If necessary, you can adapt the interface design of the terminal window to suit your needs via the **Fonts** and **Background Color** buttons.
You can obtain detailed information about the various configuration options via the Help button on the right of the window.

- ➢ Once you have completed all the settings, confirm them with **OK**.

8.3.6 Starting a Web Connection

Proceed as follows to start a web connection:

- ➢ Tag the XAir you wish to access over a web connection (Web user interface) in the main window
- ➢ Select Configuration Web. **Configuration ➨ Advanced ➨ Web**
  XAir's web user interface is started.
- ➢ Click the graphic.
  A dialog appears for entering the user name and password.

Important!
Refer to the description of user names and passwords in XAir's User Guide version, 2.0 chapter 7.1, page 18.

- ➢ Enter **user name** and **password**. The user name here corresponds to the level you wish to access and the password to the corresponding password.
- ➢ Confirm your entries with **OK**.
  The configuration menu of the web user interface opens.

You will find a detailed description of the web user interface and activating the web user interface from a browser in XAir User Guide version 2.0, chapter 10, page 103.

8.3.7 Upgrading the Firmware

You will find the current firmware for XAir in the download section for XAir on BinTec's website at www.bintec.net. The current version of the BinTec XAir Manager can also be found here.

Always use the latest version of the BinTec XAir Manager for upgrading the XAir firmware and observe the instructions in the relevant release notes.

Note that after upgrading the firmware, you may have to reset your XAir to the ex works settings. This means that you lose your current configuration and have to configure the device again after the upgrade.

The monitor, firmware and boot loader are always upgraded at the same time when you upgrade the firmware for XAir. The upgrade files have the file extension ".afw".

Caution!

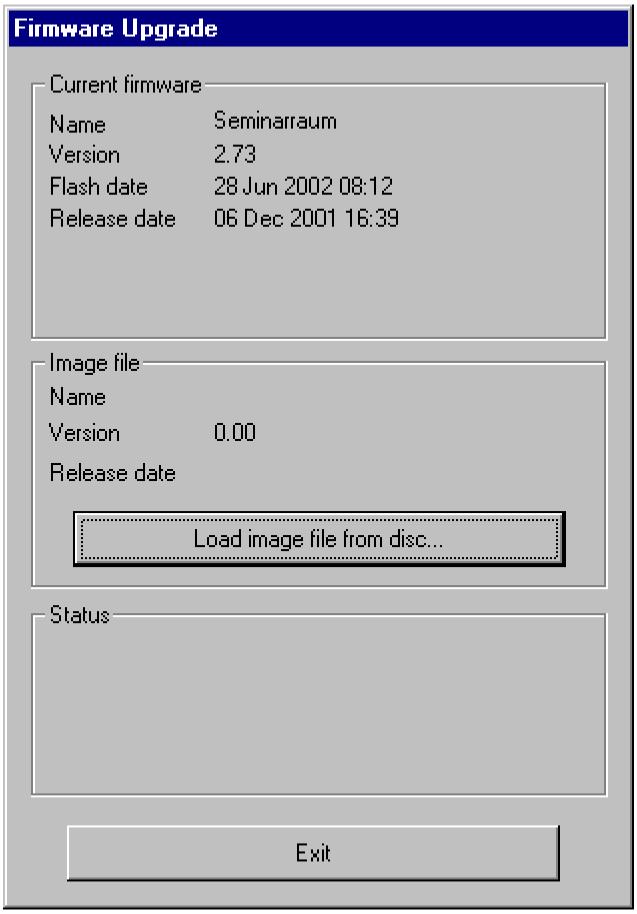
When carrying out the upgrade on your XAir, you must not switch XAir off. The data connection must not be interrupted, as otherwise the XAir software is destroyed and you must return the device to the manufacturer.

- ➢ Never switch off XAir during the upgrade or interrupt the data connection.

Proceed as follows to upgrade the firmware:

- ➢ Before starting the upgrade, make sure that the new version of the firmware (file with extension *.afw) is available on the hard disk of your PC or another storage medium.
- ➢ Tag the XAir you want to upgrade in the main window of the BinTec XAir Manager.
- ➢ If not already done, enter the user name and password for the user level "Admin" under **Configuration ➨ Password**. This must be done before an upgrade is possible.
- ➢ Select **Configuration ➨ Load firmware ...**

The following window opens:



Firmware Upgrade

Current firmware

Name Seminarraum
Version 2.73
Flash date 28 Jun 2002 08:12
Release date 06 Dec 2001 16:39

Image file

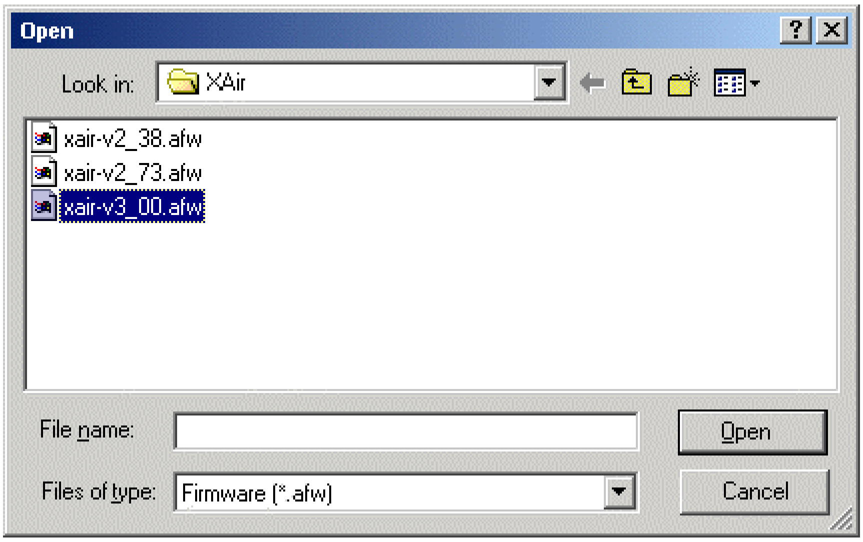
Name
Version 0.00
Release date

Status

Figure 8-9: Firmware Upgrade window

- ➢ Press the **Load image file from disc...** button.

The following window opens:



Open

Look in: XAir

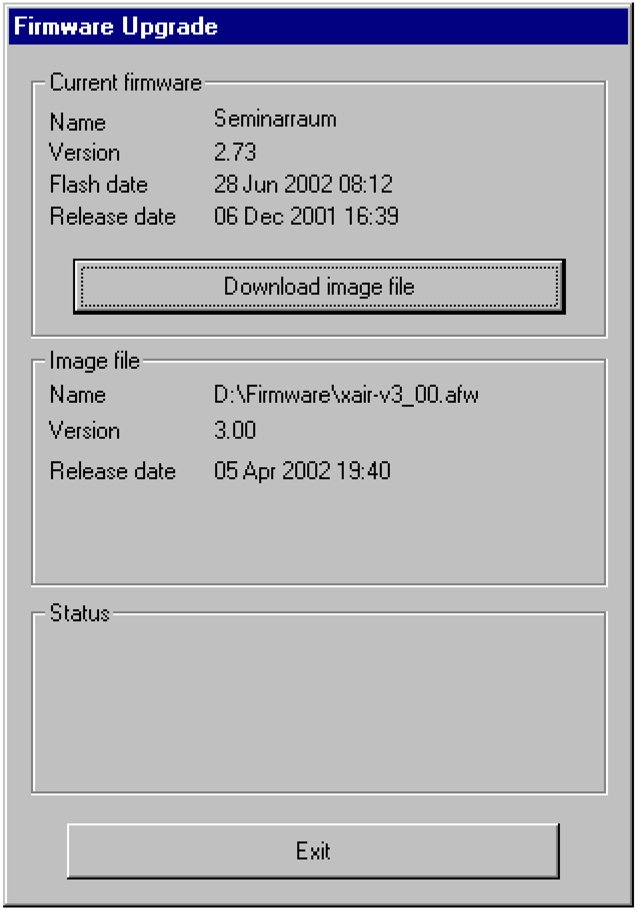
xair-v2_38.afw
xair-v2_73.afw
xair-v3_00.afw

File name:
Files of type: Firmware (*.afw)

Figure 8-10: Selecting the firmware upgrade file

- ➢ Select the file containing the new firmware.
  This is the file **xair-v2_73.afw** in our example.
- ➢ Click the **Open** button.

The path for the firmware is now updated automatically in the control window for the **Image file**. The BinTec XAir Manager also checks if an upgrade is possible and meaningful:



Current firmware

Name: Seminarraum
Version: 2.73
Flash date: 28 Jun 2002 08:12
Release date: 06 Dec 2001 16:39

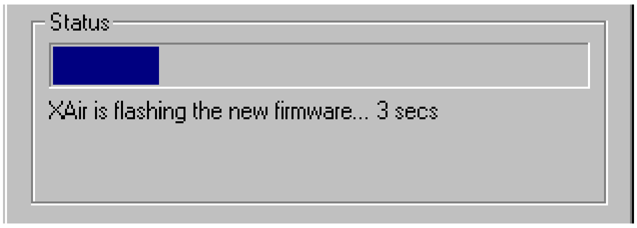
Image file

Name: D:\Firmware\xair-v3_00.afw
Version: 3.00
Release date: 05 Apr 2002 19:40

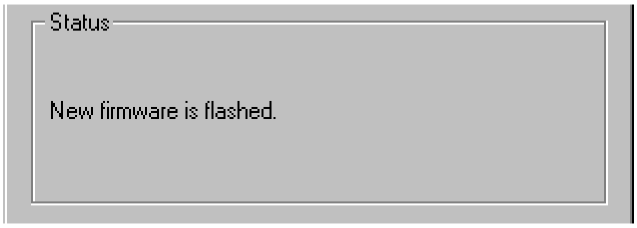
Figure 8-11: Firmware Upgrade window with selected firmware

- Click the **Download image file button**.
  The firmware upgrade is carried out.

The Status field shows a progress bar and the current process:



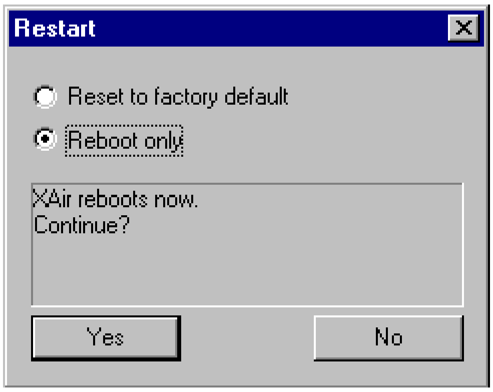
XAir is flashing the new firmware... 3 secs



New firmware is flashed.

Figure 8-12: Status window for upgrade process

The following dialog box appears on successful completion of the firmware upgrade:



Restart

○ Reset to factory default

● Reboot only

XAir reboots now.
Continue?

Figure 8-13: Reboot confirmation

The BinTec XAir Manager always suggests the necessary option in this dialog box: **The Reboot only** option field if the XAir is only to be rebooted or the **Reset to factory default option** field to reboot XAir and to reset it to the ex works settings at the same time.

If the BinTec XAir Manager has tagged **the Reset to factory default** option field here, you should not change the setting to **Reboot only**, as your configuration then no longer works. In this case, it is necessary to reconfigure the XAir after upgrading the firmware.

If the BinTec XAir Manager suggests the **Reboot only** option field here, you can also select the **Reset to factory default** if required.

- Confirm with **Yes** to restart XAir or to reset XAir to the ex works settings at the same time.

If the **Reboot only** option field is tagged, a reboot is also carried out by clicking the **No** button.

The reboot of XAir is not shown on the screen of your PC, but you can use the LEDs on XAir to check radio activity, radio status and Ethernet activity (see XAir's User Guide version 2.0, chapter 12.3, page 161).

- Finally check the operation of your XAir, for example, by searching for XAirs installed in the network using the BinTec XAir Manager.

8.3.8 Resetting XAir to Ex Works Settings

Proceed as follows to discard the configuration already made and reset XAir to the ex works settings:

➢ Select **Configuration** ➨ **Reset to factory default**.
XAir is reset to the ex works settings and a reboot is carried out automatically.

The following settings are not reset as part of resetting to the ex works settings:

- IP address
- Subnet mask
- Gateway
- Access point name
- Passwords.

8.3.9 Rebooting XAir

Proceed as follows to reboot the XAir:

➢ Select **Configuration** ➨ **Reboot**.
XAir is rebooted.

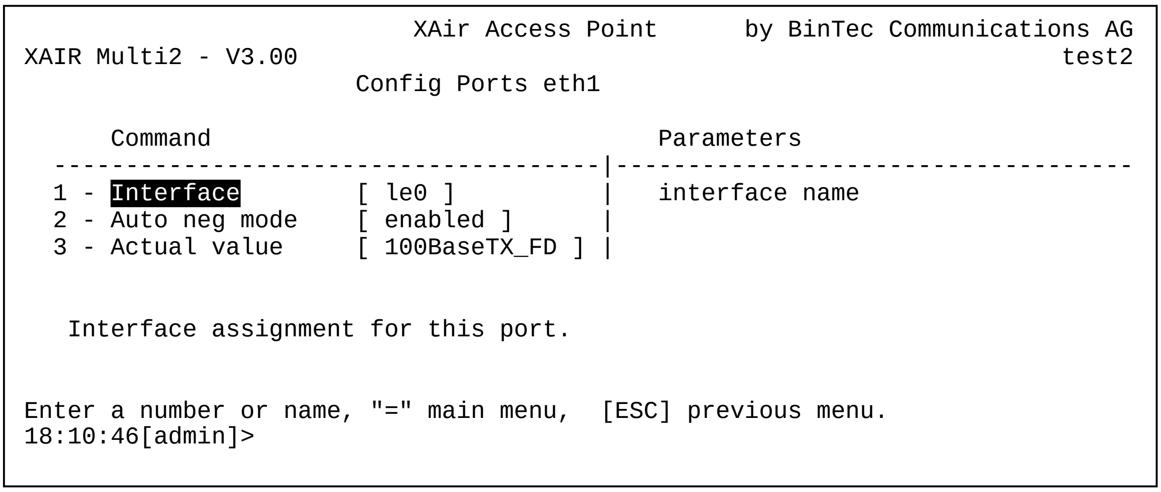
8.3.10 Closing the BinTec XAir Manager

Proceed as follows to close the BinTec XAir Manager:

➢ Select **File** ➨ **Exit**.
The program is closed.

9.4.2 Config Submenu Ports

This chapter replaces chapter 9.4.2 XAir's User Guide, version 2.0.
You can configure the individual active ports in the **Config ➨ Ports** menu:
Ethernet could be found under **Config ➨ Ports ➨ Port <EthernetPort>**



```
                           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]>
```

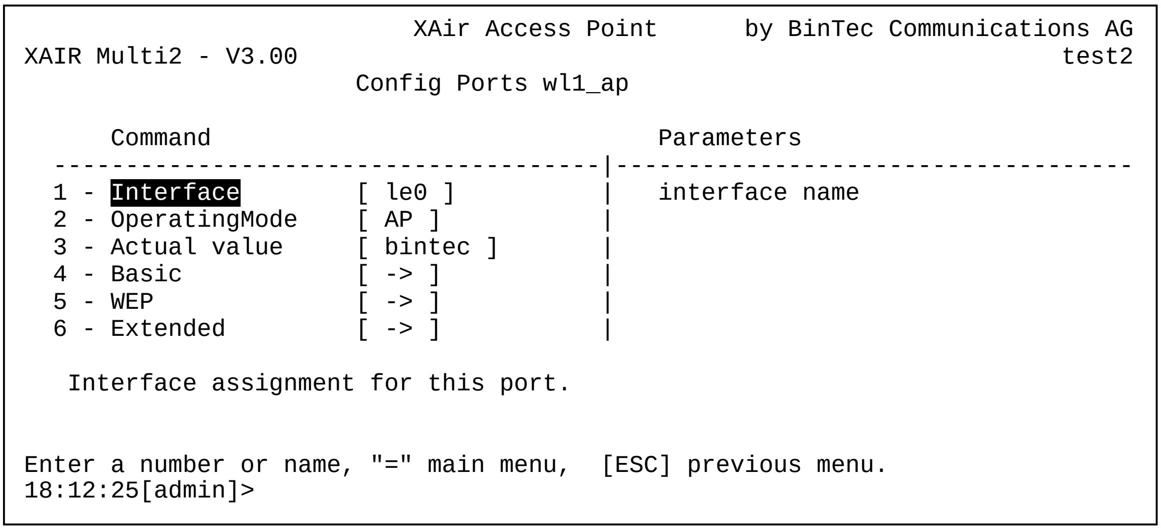
Figure 9-14: **Config ➨ Ports ➨ Port <Ethernet-Port>**

The terms and options used are explained in the following table:

Option	Meaning
Interface	For assigning an interface.
Auto neg mode	This function is for switching the Auto Negotiation Mode on and off (enabled/disabled). This mode is normally enabled. If you would like to set the speed and operation mode of the port manually, you must set the **Auto neg mode** here to disabled.
CurrentValue	Shows the current speed and duplex mode of the port. The indicated value can only be changed if you have disabled the Auto Negotiation Mode.

Table 9-9: Fields of **Config ➨ Ports ➨ Port <EthernetPort>**

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]>
```

Figure 9-15: **Config ➨ Ports ➨ <Funk-Port>** menu

Security Functions

The submenu **Basic** contains the parameter **BcstSSID**. If this parameter is disabled, clients who do not know the network name of XAir cannot log in to XAir. If **BcstSSID** is disabled, the network name of XAir is no longer broadcast, which means that clients with the network name entry ANY can no longer log in to XAir either. See chapter 7.3, page 22.

Wireless Equivalent Privacy (**WEP**) in the **WEP** submenu is available for encryption.

BinTec Communications AG still offers IPSec encryption as a security function. You can find information about this in the IPSec product section on BinTec's web site at www.bintec.net.

The options used in the menu are explained in the following table:

Option	Meaning
Interface	Enables the administrator to assign an interface. This menu item is only a static display at the user levels "User" and "View".
OperatingMode	You can use this menu item at user level "Admin" to select the desired port operation mode from a list or enter it manually in the prompt. The operation mode cannot be changed at user levels "User" and "View". Possible values: • **AP** Mode for operating the port as access point so that clients can log in to this port. • **Bridge** Mode for a bridge. See "**Config ➨ Ports ➨ Port_wlx_br**", XAir's User Guide version 2.0, page 122. • **D-Bridge** Mode for a double bridge. See "**Config ➨ Ports ➨ Port_wlx_br**", XAir's User guide version 2.0, page 122.
Network name	This option is for defining the network name and is only displayed at the user level "Admin".
Basic	• **DS channel** Here you can set the frequency of the DS channel at the user level "Admin" or "User". • **Bcst SSID** Disabling this option prevents radio clients logging in if they do not know XAir's network name. This entry exists only at the user level "Admin". Disabling BcstSSID means extra security for XAir. BinTec recommends that you configure the NetworkName on XAir and disable BcstSSID. This means the NetworkName is no longer broadcast by XAir. • **Repeating** Enables direct communication between radio clients logged in to the same XAir. If Repeating is disabled, the radio clients logged in to this XAir cannot exchange data with each other. The setting Repeating can be changed at the "Admin" user level, only viewed at the "User" level and is not available at the "View" level. • **Mcast rate** For setting the transmission rate for multicast frames. This subitem is shown at all user levels with the corresponding configuration, but can only be changed at the "User" and "Admin" levels.
WEP	WEP (Wireless Equivalent Privacy) is used for configuration of radio traffic encryption. These parameters exist only at the "Admin" level and can only be configured at this level. If you do not use VPN, BinTec recommends that you use the WEP function. • **State** Activates (enabled) or deactivates (disabled) the encryption.

WEP (continued)	• **Key number** Defines the key (1-4) for encrypting the data for transmission. • **Key 1-4** For entering the key that XAir is to know. XAir can decrypt a radio frame that has been encrypted with a key that it knows. It is important that the key of the corresponding entry is always used for decryption. This means that if the client encrypts with key 3, the same value must be entered in key 3 at XAir as at the client. This obviously applies in both directions. The key used depends on the length of the key you have entered (corresponds to bits). There are two types of cards, which support up to 128 bits or only up to 40 bits: If you enter a key with a length of 40 bits, 64-bit encryption is used (key + 24 bits). If you enter a key with 104 bits, 128-bit encryption is used. The key can be entered in ASCII (a-z, A-Z, 0-9) or hexadecimal form (0x followed by the relevant number of hex numbers). Examples: • **64-bit encryption** "ABCDE" (ASCII) = "0x4142434445" (hexadecimal) • **128-bit encryption** "1234567890123" (ASCII) = "0x31323334353637383930313233" (hexadecimal) Set keys are shown by the character "*".
Extended	Specific settings: • **MW robustness** is used for the transmission reliability in heavily disturbed environments by microwaves. In order to keep frames short (in time) to get them transmitted, XAir will fragment long frames. This setting is transmitted to all associated clients if **'medium distr. enabled**' is enabled. The client has to support this function. • **RTS threshold** is the threshold level in bytes (1..2346) for the CTS/RTS mechanism. This is useful if several clients are connected to one XAir, which are not in the radio range of each other. • **AP distance** this function changes the client's roaming behaviour. The smaller the radio cell the sooner the clients will roam to the next XAir. To see the feature, 'Medium distr.enabled' has to be set and the client has to support this function. • **Load balanc.** This feature attempts to balance the load over the available overlapping cells. XAir transmits the information in the Probe Response and Beacon Frames. • **Medium distr.** This function has to be switched on if the parameters ("**MW Robustness**", "**RTS threshold**", "**AP distance**", "**Load balanc**.") should be transmitted to the clients. If the clients support it, their values get overruled by the XAir. • **Encapsulation** Access to this function is only possible with appropriate configuration at the "Admin" level. This menu item has many submenus, which are explained in detail below.

Table 9-10: Fields of **Config ➨ Ports ➨ <RadioPort>**

Config ➨ Ports ➨ <RadioPort> ➨ Extended ➨ Encapsulation

Only LLC frames are sent over a wireless port. All other frames must be provided with an LLC header. The menu item Encapsulation is used to configure this operation and to determine how the encapsulation is to be reversed on receipt.

The Encapsulation function should only be used by experienced administrators.

The **Encapsulation** menu offers you the following options:

- The **Mode Default** option enables you to cancel all the previous settings concerning frame processing and restore the initial values.
- The **Customized** option enables you to define exactly how incoming and outgoing data packets are to be handled:
  - You can process outgoing packets in **Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customized ➨ Transmit**.
  - You can define the configuration for incoming packets in **Config ➨ Ports ➨ <Funk-Port> ➨ Extended ➨ Encapsulation ➨ Customized ➨ Receive**.

Config ➨ Ports ➨ <RadioPort> ➨ Extended ➨ Encapsulation ➨ Customized ➨ Transmit

The options used in the menu and the resulting possible settings are explained in the following table:

Option	Meaning
Encapsulation	Select **Default Encapsulation** with this option, i.e. set the default that is to be used as the basis for transmission of frames without LLC headers. The defaults are the two standards RFC_1042 and IEEE_802.1H, which you can either select from the list or enter directly in the prompt.
Exceptions	Here you can define any protocols to which **Default Encapsulation** is not to apply. The **Show** option enables you to display all the protocols excepted until now and the value in square brackets indicates the number of these protocols. Select **Add** to add more protocols to the exceptions list (max. 10). These can either be selected in the predefined list or entered in the prompt. You can also delete protocols from the exceptions list with **Remove**, i.e. **Default Encapsulation** now applies to these protocols again.

Table 9-11: Fields of **Config ➨ Ports ➨ <RadioPort> ➨ Extended ➨ Encapsulation ➨ Customize ➨ Transmit**

Config ➨ Ports ➨ <RadioPort> ➨ Extended ➨ Encapsulation ➨ Customize ➨ Receive

In this menu item, first select the standard for which you would like to define the action to be taken on receipt of a data packet. The RFC_1042 and IEEE_802.1H specifications are predefined here as defaults.

The submenus of the options in Table 9-11, page 66 have an identical structure and are explained together in the following table:

Option	Meaning
DefaultAction	Here you can define whether the LLC header is to be removed as standard from incoming data packets. Select **remove** to remove the header or unchanged to leave the data packet **unchanged**.
Exceptions	Here you can define any protocols to which **Default Action** is not to apply. The **Show** option enables you to display all the protocols excepted until now and the value in square brackets indicates the number of these protocols. Select **Add** to add more protocols to the list of exceptions (max. 10).

Exceptions (continued)	These can either be selected in the predefined list or entered in the prompt. You can also delete protocols from the exceptions list with **Remove**, i.e. **Default Action** now applies to these protocols again.

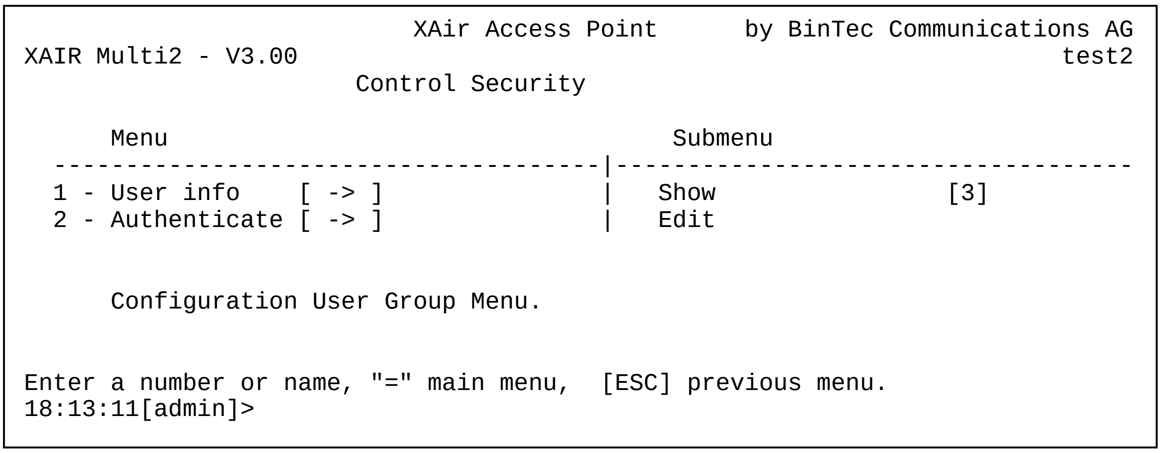
Table 9-12: Fields of **Config ➨ Ports ➨<RadioPort> ➨ Extended ➨ Encapsulation ➨ Customize ➨ Receive**

Config ➨ Ports ➨ <BridgePort>

You will find descriptions of the menus for the bridge port in XAir's User Guide version 2.0, chapter 11.3.1, page 119 and chapter 11.4.2, page 149.

9.5.3 Control Submenu Security

In this menu you can show the various user levels, change their passwords and edit the Access Control List (ACL).



```
                           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]>
```

Figure 9-29: **Control ➨ Security** menu

Control ➨ Security ➨ User info

You can use this menu to show the various user levels.

You can also change the passwords for the individual user levels if you know the password for the user level "Admin".

Control ➨ Security ➨ User info ➨ Show

Shows the designations of the various user levels. These are admin, user and view.

The passwords for the user levels are not shown.

Control ➨ Security ➨ User info ➨ Edit

This menu item offers you the possibility of changing the passwords of all three user levels at the "Admin" or "User" level. This menu item does not exist at the "View" level.

You must know the password for the user level "Admin" before you can change the passwords.

Proceed as follows to change a password:

- Select **Control ➨ Security ➨ User info ➨ Edit**.
- Tag the user level for which you want to change the password in the submenu on the right side of the table: view, user or admin. Press **Enter**.
- Enter the "Admin" password in the prompt and press **Enter**.
- Now enter the new password for the previously tagged user level twice in succession and press **Enter** each time.

You can log in with the new password for the relevant user level when you set up the next Telnet connection.

Caution!

The passwords are not reset to the ex works settings by ResetToFD. If you forget the "Admin" password, you must send in your XAir.

- Remember the "Admin" password.

Control ➨ Security ➨ Authenticate

This menu is used to configure the local Access Control List and the access to an external Access Control Server. Further more, you can enter the settings for IEEE802. If you activate this function, you can restrict access to the data network over XAir, as clients can only access your LAN over XAir if their MAC address is entered in the local resp. remote Access Control List. Additionally, an authentication with a password and user name is possible at an authentication server.

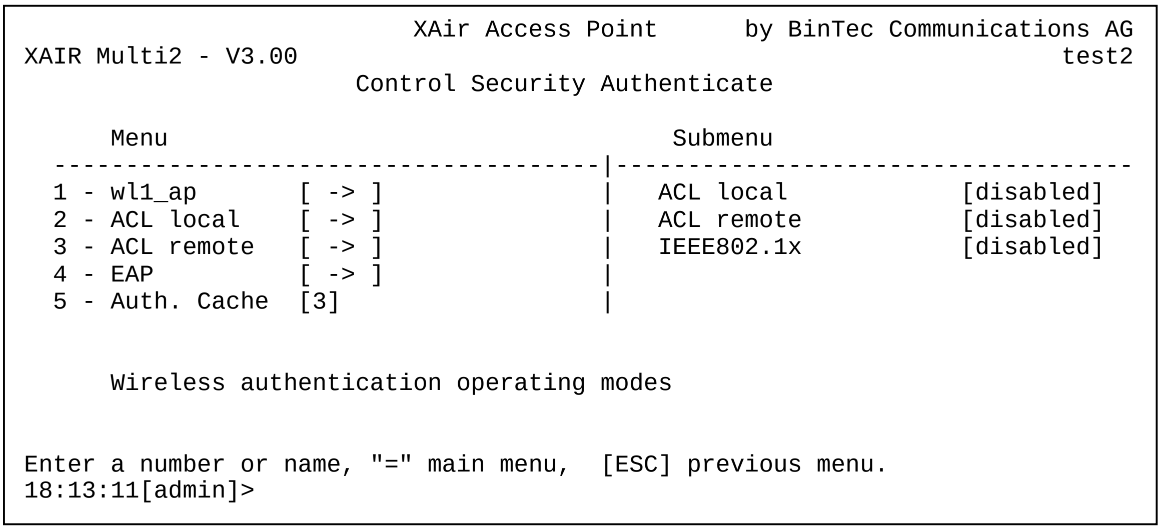
The Access Control List (ACL) is an additional facility that enhances protection of your WLAN and increases access security.

With the optional BinTec **ACL Manager**, your WLAN can be simply administrated and unauthorized access attempts are logged.

If you decide on **ACL local**, the list of the MAC addresses is kept in XAir. You must then maintain a separate list in each XAir.

If you want to use **ACL remote**, you must buy an **ACL Manager** from BinTec Communications AG. This administrates the list centrally for all radio cells and all radio networks.

Control ➨ Security ➨ Authenticate menu:



```
                           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]>
```

Figure 9-30: **Control ➨ Security ➨ Authenticate** menu

The parameters are described in detail in the following table:

Option	Meaning
wl1_ap	For configuring the access control of the relevant wireless port. • **ACL local** Here you can activate (**enable**) or deactivate (**disable**) the use of a local Access Control List. • **AclRemote** Here you can activate (**enable**) or deactivate (**disable**) the use of an external ACL server. • **IEEE802.1x** Here you can activate (**enable**) or deactivate (**disable**) the use of an external authentication server.
ACL local	Used for configuring a local Access Control List. • **Show** Shows the local Access Control List. • **Add** Adds a new entry to the Access Control List. ◊ **client MAC addr** For entering the MAC address of the client to be added to the Access Control List.

ACL local (continued)	◊ **port** Select the wireless port of XAir to which the client has access: - **all ports,** to all wireless ports of XAir; - **<wireless port>,** the corresponding wireless port. • **Remove** Removes an entry from the Access Control List. • **client MAC addr** For entering the MAC address of the client to be removed from the Access Control List.
ACL remote	Used for configuring communication with an external ACL server. • **IP address** Used for entering the IP address of the ACL server. • **Port number** Used for entering the IP port via which the ACL server is reachable. • **Comm. state** Shows the status of the connection to the ACL server. ◊ **disconnected -** no connection established. ◊ **connected -** connection established • **Def. access** Indicates the access code used if the ACL server is not reachable. ◊ **denied -** Access is denied. ◊ **granted -** Access is granted. • **Sync period** Enter the time interval (in minutes) after which the ACL cache is to be updated. This time runs separately for each client.
EAP	• **Prim. Server** indicates the number of the primary authentication server. If several servers are available it is possible to choose one from a list. • **Server Config** ◊ **Edit server** there are following settings for the authentication server possible - **Select Server -** selects the server to edit from a list. - **IP address -** server IP address - **Port number -** port number for the communication with the server. Default is 1812. - **Shared secret** - the key which is used for the encryption between XAir and server. - **Remove server -** deletes the chosen server from the list. ◊ **Add Server** appends a new entry in the server list. • **Comm. state** shows the connection status to the server. ◊ **Disconnect** connection is not established. ◊ **Connected** connection is established. • **Def. Access** defines the behaviour of XAir when the primary server is not available. ◊ **denied** - access denied ◊ **granted -** access allowed • **Timeout** defines the global timeout for the interruption of the authentication.

EAP (continued)	• **Advanced** menu for enhanced settings. ◊ **Supp. Timeout** Timeout for the request of clients to XAir (in seconds). ◊ **Max. requests** maximal number of allowed user requests. ◊ **Quiet period** Waiting period after a authentication abort. ◊ **Reauth switch** Activates or deactivates the automatic re-registration of clients. - **enabled -** a client re-registration occurs after the defined time. - **disabled -** no automatic client re-registration. ◊ **Reauth period** time period for an automatic client re-registration (in seconds). ◊ **Max. reauth.** maximal number of automatic re-authentication attempts.
Auth. cache	The number in the square brackets indicates the current number of internal and external entries in the Access Control List. This list contains both ACL entries and EAP entries. You can show the list by pressing Enter. The list gives you information about the client's MAC address, the port to which the client is logged in, whether the access was granted or denied (Error, InProgress, Granted, Denied) and whether the client is included in the ACL local, ACL remote or EAL list. For Auth. cache, the status of the request (Request, Reply, Sync, Disconn) and the time to the next update are also shown.

Table 9-25: **Control ➨ Security ➨ Authenticate** parameters

Attachement: Changes in the Menu Names and Structure

Status

Firmware Version 2.73	Firmware Version 3.00
Status	Status
Summary	Summary
Ports	Ports
<Ethernet-Port>	<Ethernet>
MAC	MAC
MAXSpeed	Max speed
Statistics	Statistcs
<Funk-Port>	<Funk-Port>
MAC	MAC
MaxSpeed	Max speed
Statistics	Statistics
CardFirmware	Card firmware
NodeTable (nicht im BR-Modus)	Node table (nicht im BR-Modus)
ARPCache	ARP cache
BufferUtil	Buffer util.
Software	Software

Config

Firmware Version 2.73	Firmware Version 3.00
Config	Config
System	Status
NodeName	Node name
Ports	Ports
Ports <Ethernet-Port>	Ports <Etherner-Port>
Interface	Interface
AutoNegMode	Auto neg mode
CurrentValue	Actual value
Ports <AP-Funk-Port>	Ports <AP-Funk-Port>
Interface	Interface
OperatingMode	OperatingMode
NetworkName	Network name
Basic	Basic
DSChannel	DS channel
BcstSSID	Bcst SSID
Repeating	Repeating
McastRate	Mcast rate
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
Ports <BR und BRx - Funk-Port>	Ports <BR und BRx - Funk-Port>
Interface	Interface
OperatingMode	OperatingMode
BridgePort	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