Prepared		JTU	6.6.2002
Checked		JNU	
Approved		TSU	

AILONET 100 EVALUATION USER MANUAL

Change Record

Revision	Date	Page affected	Description of Change
0	19.02.2002	All	Initial issue
1	6.6.2002	All	Support for new user interface

1/24

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

Operation is subject to the following two conditions:

(1)   this device my not cause harmful interference, and

(2)   this device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications made to this equipment not expressly approved by PATRIA AILON may void the FCC authorization to operate this equipment.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Patria Ailon reserves the right to revise this document or withdraw it at any time without prior notice.

FCC Radiation Exposure Statement

The Access Point complies with FCC radiation exposure limits for uncontrolled environment. This equipment must be installed and operated with a minimum distance of 20 cm between radiator and users body. If not expressly approved the transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Contents

1. OVERVIEW

1.1 Features

Processor, Memory and Operating System:

- Processor: Motorola PowerPC, 105 MIPS

- RAM: 32 or 64 MB

- Flash: 8 or 16 MB

- Battery backed real-time clock

- Internal UPS (keeps Ailonet alive for 30 seconds after power break)

- Linux 2.2.14 or 2.4 Operating System

Connectors:

- Ethernet 10BASE-T/100BASE-TX

- RS-232 serial port, 115 kbps max., CTS/RTS handshaking

- PC Card slot with 16-bit PCMCIA bus, Type II

- Bluetooth 1.1 Class 3, 0 dBm

- 12 VDC power input (8-14 VDC acceptable), nominal power dissipation without PCMCIA card 3 W

Services:

- Apache Web Server

- LAN Access profile according to Bluetooth 1.1 specification

- 3rd party application (Plug-in) API

- DHCP (Dynamic Host Control Protocol) Server

- NAT (Network Address Translation)

1.2 Physical Interfaces

1.2.1 Connectors

All wire connectors are located on the bottom of Ailonet.

Ethernet (on the left) supports 10BASE-T and 100BASE-TX connections, so it works with all modern Ethernet switches, hubs, PC Ethernet cards, ADSL and cable modems. When connecting Ailonet directly to a computer, use a special twisted Ethernet cable.

Serial port (in the middle) supports RS-232 standard with CTS/RTS handshake. The maximum speed of the serial port is 115 kbps. Serial port can be used for initial setup or for connecting external peripherals such as X10 controller.

Power input (on the right) accepts 8-14 VDC and supports center negative feed.

PC Card slot can be found from behind of Ailonet. It supports 16-bit PCMCIA PC Cards. Cards must be installed and removed when Ailonet is off. Refer to section "Supported PC Cards" for further information about PC Card compatibility.

1.2.2 Indicators

The left-most led marked with a phone ear piece in this revision of SW indicates a Bluetooth connection.

The led in the middle is power for indication. If the led blinks, Ailonet is either starting up or shutting down.

The right-most led indicates for Ethernet connection. If the led is lit half bright Ethernet link to network is established. If the led blinks, data is been transferred.
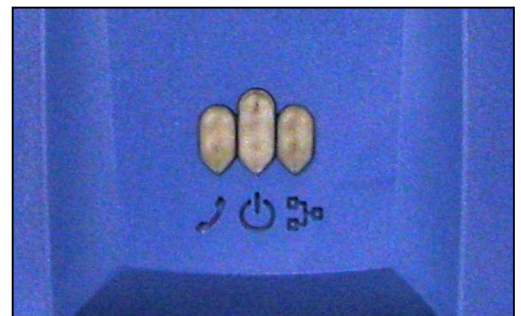
1.2.3   Switches

There are two switches located on the back of Ailonet. The right-most switch is reserved for future use. The left-most switch sets Ailonet into default factory mode in boot phase erasing all user settings, installed plug-ins and any additional information that is not part of Ailonet platform core software.

The switch can be used if the unit gets in a state where it can't be accessed normally. However, **it is not recommended to use the factory settings switch unless the unit is absolutely dead and cannot be accessed in any other method.** In many cases prototype Ailonets contain plug-in like additions tailored for customer use and these settings will be removed in factory settings mode as well.

Figure 1 . Factory settings switch is located on the back of Ailonet.

In order to set Ailonet into factory settings mode, the unit must be started with the factory settings switch in down (ON) position. User defined settings done in factory settings mode are store normally, but the switch must be switched in up (OFF) position before the unit is restarted.

1.3 System Setup

1.3.1 First Connection Using Serial Port

By default Ailonet serial port is configured for a PC with direct cable connection. Use supplied serial port cable (RJ45 – D9) to make the physical connection between Ailonet's and PC's serial ports. To configure Windows 98/Me/2000/XP properly for direct cable connection, refer to Windows help (Start->Help) with keyword "Direct Cable Connection".

Make the direct cable connection using the following parameters:

Speed: 38 400 bps
Handshaking: CTS/RTS (or Hardware)
Data bits: 8
Stop bits: 1
Parity: None
Username: dialin
Password: dialin

1.3.2 First Connection Using Bluetooth

The Ailonet Bluetooth network is configured by default to be discovered publicly. Ailonet Bluetooth device name, PIN code (optional) and IP address can be found from CONFIGURATION STATUS LIST – AILONET SAMPLE INFORMATION document delivered with the unit.

To access Ailonet from a Bluetooth enabled PC or PDA, use web browser to connect to

https://192.168.5.1/

(please verify the IP address from CONFIGURATION STATUS LIST – AILONET SAMPLE INFORMATION)

1.3.3 First Connection Using 802.11b

Ailonet can be accessed via 802.11b network, if both PC/PDA and Ailonet are equipped with IEEE-802.11b network PC Cards. See section "Supported PC Cards" for further information.

DHCP configuration, network name, encryption key and possible fixed IP address can be found from CONFIGURATION STATUS LIST – AILONET SAMPLE INFORMATION document delivered with the unit.

NOTICE: If Ailonet is configured to be a DHCP Client for 802.11b, it can not be accessed from 802.11b network – it can only act as a gateway from another interface (Bluetooth, Ethernet, etc.) to 802.11b. This is due to fact that there's no easy way of finding out Ailonet's 802.11b IP address.

To access Ailonet via 802.11b, use web browser to connect to

https://192.168.102.1/

(please verify the IP address from CONFIGURATION STATUS LIST – AILONET SAMPLE INFORMATION)

1.3.4   First Connection Using Ethernet

PC can be connected directly to Ailonet using so called twisted Ethernet cable. PC and Ailonet can also be connected together with a hub using traditional Ethernet cables.

DHCP configuration and possible fixed IP address can be found from CONFIGURATION STATUS LIST – AILONET SAMPLE INFORMATION document delivered with the unit.

NOTICE: If Ailonet is configured to be a DHCP Client for Ethernet, it can not be accessed from Ethernet – it can only act as a gateway from another interface (Bluetooth, 802.11b, etc.) to Ethernet. This is due to fact that there's no easy way of finding out Ailonet's Ethernet IP address.

To access Ailonet via Ethernet, use web browser to connect to

https://192.168.100.1/

(please verify the IP address from CONFIGURATION STATUS LIST – AILONET SAMPLE IN-FORMATION)

1.3.5   After First Connection Is Established

When the first connection is established, your web browser might ask a confirmation for a certifi-cate. You must accept it in order to proceed. After that Ailonet asks for administrator's username and password. These can be found from CONFIGURATION STATUS LIST – AILONET SAMPLE INFORMATION document delivered with the unit. It suggested that the password is changed dur-ing the first connection. For further information, see section 1.3.8, Security.

If there's trouble in connecting Ailonet in the future, original factory settings can be restored using Factory Settings Switch. See section 1.2.3 Switches for further details.

1.3.6   Selecting User Interface Language

User interface language can be changed from the top right corner of the screen by clicking appro-priate flag. Currently English and Finnish are supported.

1.3.7 Selecting Internet Interface

Internet interface means the network Ailonet uses to connect to outside world. Quite often the interface is connected to Internet via Internet Service Provider. From Ailonet's side there can only be one external interface, which is one of the following:

– Ethernet

– 802.11b

Internet interface is selected in Ailonet user interface by browsing to *SETTINGS->Internet Interface*.

Internet interface can not be used for local/personal area network (LAN/PAN) at the same time. For example if Ethernet is selected to be Internet interface, only Bluetooth and 802.11b can be used as local interfaces (for LAN/PAN), if network traffic is intended to be routed through Ailonet.

1.3.8 Security

All the wireless interfaces are unprotected in factory settings in order to ease the initial setup. First thing for administrator is to make sure the wireless connections are safe and unauthorized parties can not use them.

Administrator and Dial-in Passwords:

Administrator's username (*admin*) and password are common for all interfaces. For dial-in connection through a modem, PPP authentication username (*dialin*) and password are separate from administrator's password. Change both of these passwords by browsing to *SETTINGS->Password*.

Protecting Bluetooth Connections:

Bluetooth security features can be configured at *SETTINGS->Bluetooth Security*. There are three different security features available: Encryption, PIN code and Mode. PIN code usage is defined by the authentication selection on the top of screen:

– No authentication means that connection without prior pairing is allowed

– Authentication means that PIN code is requested and pairing required

– Authentication & Encryption means that PIN code is requested, pairing required and the data transfers are encrypted if one of the connecting parties request it

PIN code is set by entering the code into "New PIN" and "Re-enter PIN" fields. Old PIN code must be entered into "Old PIN" field. Refer to CONFIGURATION STATUS LIST – AILONET SAMPLE INFORMATION for correct PIN number. Maximum length for PIN code is 16 characters and it can contain numbers and letters.

Mode controls how Ailonet advertises itself in Bluetooth network. Non Discoverable/Non Connectable means that Ailonet do not respond to Bluetooth inquiries and do not allow incoming connections. Connectable means that Ailonet allows incoming Bluetooth connections with earlier paired devices, but does not respond to inquiries. Discoverable/Connectable means that it responds to inquiries and allows incoming connections.

Protecting 802.11b Connections:

The actions protecting 802.11b connections must first be done in Ailonet and after that in terminal (PC, PDA). Browse to *SETTINGS->802.11b Settings* and enter your private network name into *Network name* field. After that enter a 5 character encryption key into *Encryption key* field. Accept the changes after which your browser gives a notification about disconnection. This is due to 802.11b network changes you just made. Now make the same changes into your terminal's 802.11b settings. By doing that your 802.11b connections are protected in the future.

1.4   Supported PC Cards

Modems:

- – Nokia CardPhone GSM modem
- – Nokia CardPhone2 GSM modem
- – Nearly all PSTN modems with AT command interface

802.11b Cards:

- – Orinoco 802.11b Silver
- – Orionoco 802.11b Gold

2. ADMINISTRATION

2.1 Shutdown And Restart

While it is possible to turn Ailonet safely off by disconnecting the power cord, it is recommended that you always use "*Shutdown*" button on the user interface to increase the life span of internal UPS.

2.1.1 Shutdown

Shutdown step-by-step
1. In Ailonet's user interface, browse to *POWER* menu
2. Press *Shutdown* hyperlink on the menu
3. Confirm the shutdown by clicking *Yes*

2.1.2 Restart

Restart step-by-step
1. In Ailonet's user interface, browse to *POWER* menu
2. Press *Restart* hyperlink on the menu
3. Confirm your choice by clicking *Yes*

2.2   Plug-ins

Plug-ins are small applications that are available for Ailonet users. Using plug-ins, you can auto-mate for example device functions in Bluetooth network or be able to control devices remotely with a mobile phone or PDA. Installed plug-ins are located in "PLUGINS" menu in Ailonet user interface.

2.2.1   Installing a Plug-in

When installing a Plug-in package, it must be on stored on hard drive of the computer you're using for browsing Ailonet's user interface.

Installing a plugin step-by-step
1.   Download or copy a Plug-in package to computer hard disk
2.   In Ailonet's user interface, browse to *PLUGINS->Install*
3.   Press "Browse…" button and select the Plug-in package from the computer hard disk
4.   Press *"Send"* button
5.   Reboot after successful transfer

Installed plug-in will become available in Ailonet user interface in the "PLUGINS" menu.

2.2.2   Removing a Plugin

Installed plug-ins can be removed as well. Need for this might be a new version of the plug-in or simply Ailonet's memory is getting full and the plug-in is obsolete.

Removing a plugin step-by-step
1.   In Ailonet's user interface, browse to *PLUGINS->Remove*
2.   Select the plug-in from the list
3.   Double-check that the plugin you have chosen is the one you need to remove
4.   Press *"Remove Plugin"* button

2.3   Settings

Settings define how Ailonet uses its interfaces. In addition time and date, several security aspects and network settings are configured here.

By browsing into SETTINGS menu, Ailonet shows general information about the unit and a visual presentation about current network configuration.

2.3.1   Time and Date

Installed plugins can use time and date. Ailonet contains a battery backed real-time clock, which maintains the clock even if the unit not powered.

Changing time and date step-by-step
1.   In Ailonet's user interface, browse to *SETTINGS->Time and date*
2.   Enter time into fields in hours:minutes:seconds format
3.   Enter date into fields in day:month:year (4 digits) format
4.   Press *Confirm* button

2.3.2   System Update

Ailonet system software can be updated with System Update function.

Installing system update package step-by-step
1.   Download or copy a system update package to computer hard disk
2.   In Ailonet's user interface, browse to *PLUGINS->System update*
3.   Press "Browse…" button and select the system update package from the computer hard disk
4.   Press *"Send"* button
5.   Reboot after successful transfer

2.3.3   Internet Interface

Internet interface defines interface which Ailonet uses to connect to ISP. Very often Internet connection is brought via cable or DSL modem using Ethernet connection to Ailonet. However, Internet interface connection can also be 802.11b. For further information about selecting external interface, see section 1.3.7, Selecting Internet Interface.

Changing external interface (WAN) step-by-step
1. In Ailonet's user interface, browse to *SETTINGS->Internet Interface*
2. Select appropriate interface from *External interface* list
3. Press *Confirm* button

2.3.4   Bluetooth

Ailonet supports at the moment the routing of traffic coming through Bluetooth to other interfaces or networks of Ailonet. Ailonet can therefore function as an access point for other Bluetooth devices to the external network. With the Bluetooth settings, the discoverability of Ailonet on the device inquiries of other devices and the settings of bonds and connections can be influenced.

The controlling of discoverability and connections is simple. The user can choose whether Ailonet can be discovered with Bluetooth device inquiries and whether Bluetooth connections are allowed. Pairing always requires a PIN code. You can ask for authentication for connections, in which case Ailonet requires pairing when establishing a connection. The connection initiator is asked to enter PIN code, and if the code is correct, he is allowed to establish a connection.

From the Bluetooth settings front page you can see, to which devices Ailonet is paired and to which it has a connection. The pairings made on the page *Device discovery* appear updated on the front page. The device name, Bluetooth address and device class can be seen on this list. The device class indicates the type of Bluetooth device.

2.3.4.1 Settings

The Ailonet name which can be discovered as the device name in the network is defined on the page *Bluetooth: Settings*.

2.3.4.2 Security

On the page *SETTINGS->Network: Bluetooth: Security* the security of Ailonet Bluetooth connetions can be defined. The page contains the choices on PIN code inquiry, Ailonet discoverability and on accepting the connections to be taken to Ailonet. The Change PIN code function can be found on the same page. The PIN code inquiry can be switched off by choosing *no authentication*, in which case a connection can be established without a PIN code inquiry. If the option *Authentication* is chosen, no connection can be established without bonding. If *Authentication & Encryption* is chosen, encryption is used in the connection, if possible.

Changing PIN code:

The PIN code can be easily changed by entering the old code in the field *Change PIN code: PIN Code*. The new PIN code is first entered in the field *New PIN* and again in *Re-enter PIN*.

Security:
This choice defines, whether Ailonet can receive a Bluetooth connection or whether any device can bond to Ailonet. If *Not discoverable* is chosen, Ailonet cannot be found in device inquiries and it doesn't allow connections or bonding. If the option *Connectable* is chosen, Ailonet cannot be found in device inquiries and Ailonet cannot be bonded to, but devices previously bonded to Ailonet can connect to Ailonet. If *Discoverabe/Connectable* is chosen, a Bluetooth device can bond to or establish a connection to Ailonet and can be found on device inquiries.

2.3.4.3 Device Discovery

Ailonet can be bonded to another Bluetooth device, but Ailonet cannot establish Bluetooth connections. The bonding is done by going to the subpage *Device discovery* and by choosing *Inquiry*. The found devices appear on the page. The device information contains the *name*, *address* and *class* of the device, the *Services* link and the *Bond* link. If you choose *Services*, you can see the services offered by the Bluetooth device. By choosing *Bond* you can bond the device to Ailonet. When Ailonet bonds to a Bluetooth device, after the connection has been established, the device appears on the list of bonded devices which can be seen on the Bluetooth front page and on the subpage *Device discovery*.

By clicking *SETTINGS->Bluetooth* gives a brief overview of current connections and bonded devices. Ailonet's own Bluetooth information including device name and Bluetooth address is also shown.

Modifying Bluetooth settings step-by-step

1. Choose Ailonet name. From the subpage *Settings*, the Ailonet name which can be discovered in the network to other devices, can be changed.

2. Confirm the changes by clicking *Confirm*.

3. Go to subpage *Security*.

4. Choose authentication, if you wan to prevent contacting Ailonet without a code.

5. Change PIN-code.

6. Choose *not discoverable*, *connectable*, *connectable/discoverable*.

7. Confirm changes by clicking *Confirm* Continue, if you want to bond Ailonet to another Bluetooth device.

8. Go to subpage *Device discovery*.

9. Choose the device to be bonded. If the device is not on the list, make a new inquiry by clicking the link *Inquiry*. If the device can still not be found, its discovery has been denied or the device power is off.

10. Choose the *Bond* link to bond the device and enter the required PIN code. The device appears on the bonded devices list on the Bluetooth front page.

MANUAL

AILONET 100

AILONET USER MANUAL

21846

6.6.2002

Done

2.3.5   802.11b

802.11b settings how define how radio card installed in PC Card slot works. 802.11b settings contain network name, network mode, handshaking and encryption key. In addition administrator must define DHCP functionality, IP address, gateway and DNS name servers. Notice, that these settings affect only to 802.11b interface.

In 802.11b networks *Network name* differs separate radio networks from each other. If there are several 802.11b networks in the same area, users can choose the right one with the network name. *Mode* is currently only *AdHoc*. Enabling *CTS/RTS* flow control may help in a situation, where in rapid data transfers a lot of data packets are lost. Using *Encryption key* improves security of wireless data transfers, because all the data is encrypted before wireless transmission. Notice, that in some 802.11b PC Cards the length of the encryption key is limited. Refer card's user manual before using encryption.

If 802.11b is selected to be external interface (see section 2.3.3, Internet Interface for further information), the settings are defined by the network service provider. If the connection is with fixed IP address, *DHCP mode* must be selected to be *None* and administrator must fill the fields below with network service provider defined settings. If the connection supports dynamic IP address, *DHCP mode* must be selected to be *Client*. In this case there is no need for further Ethernet settings modifications, because all the settings are modified automatically by Ailonet.

If 802.11b is used for LAN, it pays off to select DHCP mode to be *Server*. That way all the devices connected to 802.11b network can get their IP addresses and other network settings from Ailonet and administration of the wireless LAN becomes easier. In this case *IP address* field is filled with for example *192.168.0.1*, *Netmask* with *255.255.255.0* and *Gateway* and *DNS* fields are left blank.

Modifying 802.11b settings step-by-step

1. In Ailonet's user interface, browse to *SETTINGS->802.11b Addresses*
2. Select *DHCP Mode* (If *Client*, go to step 8)
3. Enter Ailonet's *IP address* in Ethernet network
4. Enter *Netmask*
5. Enter *Gateway* IP address
6. Enter *Primary DNS* IP address
7. Enter *Secondary DNS* IP address
8. Press *Confirm* button
9. In Ailonet's user interface, browse to *SETTINGS->802.11b Settings*
10. Enter 802.11b network name without spaces
11. Selected *Mode* (only AdHoc supported at the moment)
12. Select *RTS/CTS* flow control *on/off*
13. Enter *Encryption key* or leave the field blank (no encryption)
14. Press *Confirm* button

2.3.6   Ethernet Settings

Ethernet settings define DHCP functionality, IP address, gateway and DNS name servers. Notice, that these settings affect only to Ethernet interface.

If Ethernet is selected to be external interface (see section 2.3.3, Internet Interface for further information), the settings are defined by the network service provider. If the connection is with fixed IP address, *DHCP mode* must be selected to be *None* and administrator must fill the fields below with network service provider defined settings. If the connection supports dynamic IP address, *DHCP mode* must be selected to be *Client*. In this case there is no need for further Ethernet settings modifications, because all the settings are modified automatically by Ailonet.

If Ethernet is used for LAN, it pays off to select DHCP mode to be *Server*. That way all the devices connected to Ethernet can get their IP addresses and other Ethernet settings from Ailonet and administration of the LAN becomes easier. In this case *IP address* field is filled with for example *192.168.0.1*, *Netmask* with *255.255.255.0* and *Gateway* and *DNS* fields are left blank.

Modifying Ethernet settings step-by-step

1.   In Ailonet's user interface, browse to *SETTINGS->Ethernet*

2.   Select *DHCP mode* (If *Client*, go to step 8)

3.   Enter Ailonet's *IP address* in Ethernet network

4.   Enter *Netmask*

5.   Enter *Gateway* IP address

6.   Enter *Primary DNS* IP address

7.   Enter *Secondary DNS* IP address

8.   Press *Confirm* button

2.3.7   Serial Port Settings

Serial port settings define how Ailonet uses its integrated serial port. Modifiable settings are speed, flow control, initialization string and if Ailonet answers to incoming calls.

In addition, serial port settings define if a local computer is connected to Ailonet via serial port (*direct cable connection*) or is there a modem connected (*modem*). If a direct cable connection is preferred in connecting a computer to Ailonet, *Allow incoming connections* must be enabled. When using Microsoft Windows operating system in the computer, *Microsoft Windows modem emulation* selection must also be enabled. In this case administrator must create a new direct cable connection profile in Windows, where connecting interface is the COM port connected to Ailonet.

It is recommended to enable Hardware *Flow control* to ensure trouble-free communication. With initialization strings special features of modems can be enabled and disabled (packing, speed adjust, etc.) Refer to modem user manual for further information. If *Enable incoming connections* is enabled, Ailonet will answer to incoming calls. *Number of rings before answering* defines the number of rings before Ailonet answers to an incoming call and tries to form a PPP connection. The username for connecting party is *dialin* and password is set at *SETTINGS->Password.*

Modifying serial port settings step-by-step
1.   In Ailonet's user interface, browse to *SETTINGS->Serial port*
2.   Select serial port *Function*
3.   Select serial port *Speed*
4.   Select *Flow control*
5.   Enter *Drop idle line* time in minutes
6.   Enter *Init string*
7.   Select, if incoming connections are allowed
8.   Select if *Microsoft Windows modem emulation* is used with direct cable connection
9.   Enter the *Number of rings before answering*
10. Press *Confirm* button

2.3.8   PC Card Modem Settings

The PC Card modem settings control the bonded PCMCIA modem card. The Ailonet PC Card modem interface supports dial-in, but it is not possible to make an outside call with Ailonet. After establishing a connection, however, it is possible to define the connection so that Ailonet uses the modem as a connection to an external network or other server. In this situation, Ailonet functions as a normal Client.

When using a modem, it is recommendable to check all settings. If you have problems in establishing a connection, you should try another flow control, data transfer speed or number of rings before answering. It is, however, not recommendable to change the initialization string, if you are not completely certain of what you are doing.

Modifying PC Card Modem settings step-by-step
1.   In Ailonet's user interface, browse to *SETTINGS->PC-Card Modem*
2.   Choose modem *Speed* (bps) which defines the bit speed to be used.
3.   Choose *flow control*. The chosen flow control defines the protocol to be used in flow control. It is recommendable to use Hardware flow control.
5.   Enter the initialization string of your choice. The initialization string defines which settings are set for the modem. Commands for setting different settings can be found in the modem manual.
6.   Choose whether incoming connections are allowed. The command *Allow incoming connections* defines, whether the modem answers calls.
7.   Choose the number of rings before answering. The number at *Number of rings before answering* defines, how many times the modem allows the line to ring before answering.
8.   Confirm the changes by clicking the *Confirm*-button.

Patria **Ailon** **MANUAL**

AILONET 100

AILONET USER MANUAL

21846

6.6.2002

Done

2.3.9 Password

Password screen allows change of administrator's password and dial-in password.

Changing administrator's password step-by-step
1. In Ailonet's user interface, browse to *SETTINGS->Password*
2. Enter administrator's old password
3. Enter administrator's new password twice
4. Press *Confirm* button

Changing dial-in password step-by-step
1. In Ailonet's user interface, browse to *SETTINGS->Password*
2. Enter old password of dial-in
3. Enter new password of dial-in twice
4. Press *Confirm* button

2.3.10 Firewall

The user defines with the firewall, what traffic is allowed from Ethernet, 802.11b or other network to Ailonet.

The traffic running out of Ailonet does not go through the firewall!

In addition, common settings for other network interfaces are found under the option *Others*. There are three profiles for each interface, the settings of which can be changed. The profiles are *All Denied*, *WWW Accepted* and *Common Services*. With an external interface, any profile can be chosen, with other interfaces the option *All Denied* doesn't show up on screen. The external interface can be seen on the firewall settings front page in boldface.

The profile names are:

- *All Denied*

- *WWW Accepted*

- *Common Services*

The *All Denied* option inhibits with its basic setting all traffic through the interface to Ailonet.

WWW Accepted allows only http, https, ftp and ftp-data traffic.

The *Common Services* option allows the use of all protocols' ports supported by Ailonet.

DO NOT CHANGE THE PROFILE UNLESS YOU KNOW EXACTLY WHAT YOU ARE DOING!

2.3.10.1 Interfaces

The profiles of different interfaces can be changed through the *Interfaces* page. All traffic can only be inhibited from an external interface or by modifying the profile of internal interfaces. The profiles for different interfaces are chosen from pull-down menus and brought to use by clicking the *Modify* button. If the *Reset* button is clicked, the firewall settings of different Ailonet interfaces return to the settings that were valid before changes were made to the page. If the option *Off* is chosen, all traffic to Ailonet is allowed.

2.3.10.2 Advanced

The modification of profiles is done from the *Advanced* subpage. On this page, you choose the interface and the profile connected to it, that you want to modify. By clicking *Modify* you get to the page where you can modify the profile.

On the Modify page, you can see a list of previously defined ports and protocols, to which you can directly define their status.

If the option *Off* is chosen, the port in question is not open, in which case the traffic coming through it will be denied.

With the option *On* you can either choose *All*, in which case all traffic through the port is allowed or the *Listed*, in which case a connection can be established from the IP-addresses in the box on the right. The IP-address has the form 192.148.166.221. Instead of an IP-address, a subnetwork can

be defined which is written in the form 192.148.166.0/24. IP-addresses are separated with line spacing.

Example:
The IP-address and the mask have the form 192.168.44.128/24. Thus, the first 24 bits of the address are compared. The firewall gets the packets 192.168.44.3 and 192.168.23.128. The first three segments of the first address **192.168.44**.3 are the same as those of the entered IP-address, and so it gets through, and the segments of the second address **192.168.23**.128 are different, so it doesn't get through.

By clicking *Save* you can save the changes you have made and by clicking *Reset* you can return to the settings which were valid when you entered the page. If you click Cancel, you return to the view where you choose the profile to be modified.

Ports can be added to the list one by one by entering the port number to the lowest field, *Port*, and by choosing a protocol for the port. You can either define one port or a port area that the setting involves. A port area is defined with a colon **[:]**, the left side of which is the start port and the right side the end port. For example the port sequence 21-45 is marked as 21:45. The setting involves all ports between these numbers. If there is no number on the left side, the list starts from the zero (0) port. If there is no number on the right side, the end port number is 65535. The port has three protocol alternatives: *TCP, ICMP, UDP and ALL*. *ALL* means all three. The settings of the new port become valid after clicking the *Save* button, after which a new empty space appears for the definition of the next port. You can add the new ports of your choice to the firewall by repeating the modifications and savings. If you want to remove added ports, choose *Remove* on the left side of the port settings and click *Save*.

2.3.10.3 Factory settings

You can return all profiles to their factory settings from the window *Factory settings*.

Modifying firewall settings step-by-step
1.   In Ailonet's user interface, browse to *SETTINGS->Firewall Interfaces*
2.   Choose Ethernet profile.
3.   Choose WLAN profile.
4.   Choose profiles for other interfaces.
5.   Click *Modify*, and the chosen profiles activate.
6.   Go to the view *SETTINGS->Firewall Advanced* (if you don't want to modify profiles, go on to 11).
7.   Choose interface to be modified.
8.   Choose profile to be modified.
9.   Start modifying by clicking *Modify*.
10.   Choose settings for different ports or add ports.
11.   Click *Save*. The firewall settings have been changed.