ADASA PAD3500
Operations Manual

ADASA Confidential

Disclaimer

The information in the document is believed to be correct at the time of print. The reader remains responsible for the system usage and for ensuring that the overall system satisfies its design objectives taking due account of the information presented herein, the specifications of other associated equipment environment.

ADASA® Inc. has made commercially reasonable efforts to ensure that the information contained in this document is accurate and reliable. However, the information is subject to change without notice. No responsibility is assumed by ADASA Inc. for the use of the information, nor for infringements of patents or other rights of third parties. This document is the property of ADASA Inc.. and does not imply license under patents, copyrights or trade secrets.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by ADASA Inc. could void the user's authority to operate the equipment.

Corporate Headquarters

ADASA Inc. PO Box 2689 Eugene, OR 97402

USA

Telephone:	541-359-1677
Fax:	541-465-2232
Technical Support:	541-359-1677x301 support@adasainc.com
Web Site:	www.adasainc.com

CONTENTS

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

The very essence of RFID technology lies in its ability to be read encoded data electronically WITHOUT optical or human readable markings of any type. In fact, using the Gen2 EPC standard, 3 meters of read range is not untypical for modern RFID tags even on high speed conveyors. This capability gives users newfound supply chain and asset visibility down to the carton or even item level that could not have been imagined just a few years ago.

The ADASA PAD3500 Mobile RFID tag encoder is the first truly portable RFID encoding device that gives its users the freedom to utilize RFID tagging wherever and whenever they choose. This newfound freedom is ushering in new applications for RFID usage that could not be accomplished without the mobile capability of the PAD3500. This manual describes in detail the capabilities and operation of the ADASA PAD3500.

1.2 FEATURES

The following list describes the key features of the ADASA PAD3500.

Gen2 EPC Compatible
Printer Emulation Modes
Rechargeable Li-ion Battery
802.11b wireless LAN (Wi-Fi) standards-based communications
PAD3500 includes various levels of WLAN security
Built-in TCP/IP and UDP features provide flexible LAN connectivity options
Built-in Web server enables drop-in LAN and Internet connectivity
ADASA SmartCartridge™ Technology

1.3 SMARTCARTRIDGE

ADASA's SmartCartridge is a key technology that was invented by ADASA specifically to make the PAD3500 and Mobile RFID in general a practical reality. The SmartCartridge makes reloading the PAD3500 with Gen2 RFID tags convenient, easy and reliable. The SmartCartridge also protects the RFID tags from damage due to excessive handling and during application of the tags.

ADASA is committed to the protection of our environment by recycling your SmartCartridges. Information about SmartCartdrige recycling can be found at www.recyclerfid.org.

1.4 APPLICATIONS

The mobility of PAD3500 allows users to incorporate RFID tagging into their existing business practices utilizing legacy auto ID equipment such as PDT's, Vehicle Mount Terminals and barcode printers. Also since the PAD3500 can emulate legacy output devices such as a barcode printer the PAD3500 integrates easily with RFID tagging software applications, middleware or ERP systems.

The PAD3500 can be wirelessly monitored and controlled by virtually any handheld or mobile device, a host computer in a central location, or over the Internet. This eliminates cabling and allows the PAD3500 to operate completely mobile for RFID tagging applications.

1.5 CONVENTIONS

The following conventions are used in this book:

1.5.1 Terminology

In the following chapters, these terms are used:

"Serial Host" refers to the PAD3500 embedded microcontroller, that communicates with the WLAN module via the module's serial UART interface.

"LAN Host" refers to a LAN-based application such as a Web Browser or TCP client that communicates with the PAD3500 via a wireless network connection.

1.5.2 Notes

A note is information that requires special attention. The following convention is used for notes.

Note: A note contains information that deserves special attention.

1.5.3 Cautions

 A caution contains information that, if not followed, can cause adverse consequences or damage to the product. The following convention is used for cautions.

1.5.4 Courier Typeface

Commands and other input that a user is to provide are indicated with Courier typeface. For example, typing the following command and pressing the Enter key displays the result of a command:

```
wl-scan <cr> SSID: FirstAccessPoint
BSSID: 0006255D537D
signal (dBm): -56
noise (dBm): -92
rate (KB/s): 0x0014
capabilities: 0x0005
channel: 0x0007
```

CHAPTER 2
OPERATIONS OVERVIEW

Starting the PAD

The PAD3500 is started by pressing the On/Off/Next button.

Stopping the PAD

The PAD3500 is put into a sleep mode by pressing the same On/Off/Next button, holding it down for 3 seconds. The LEDs will turn off, indicating that the PAD is asleep.

Encoding a Tag

Once data is downloaded into the PAD3500 for encoding, the user shall initiate tag encoding by hitting the On/Off/Next button as shown above. Tags will continue to encode provided that the operator removes the previous tag and that additional data is

provided for encoding subsequent tags.

Removing a Tag

An encoded tag is removed when an operator places an index finger onto the center of the RFID tag. When the PAD3500 senses the tag being removed, it provides assistance in that process by indexing the tag upward.

The PAD3500 will then wait indefinitely for the tag to be fully removed from the PAD3500 tag encoding zone.

Once fully removed, the next tag will index into position for encoding.

Discarding a Bad Tag

If the PAD3500 detects a bad tag, it will index that tag up and over the top of the peel plate to reject it onto a tag up roll inside of the cartridge.

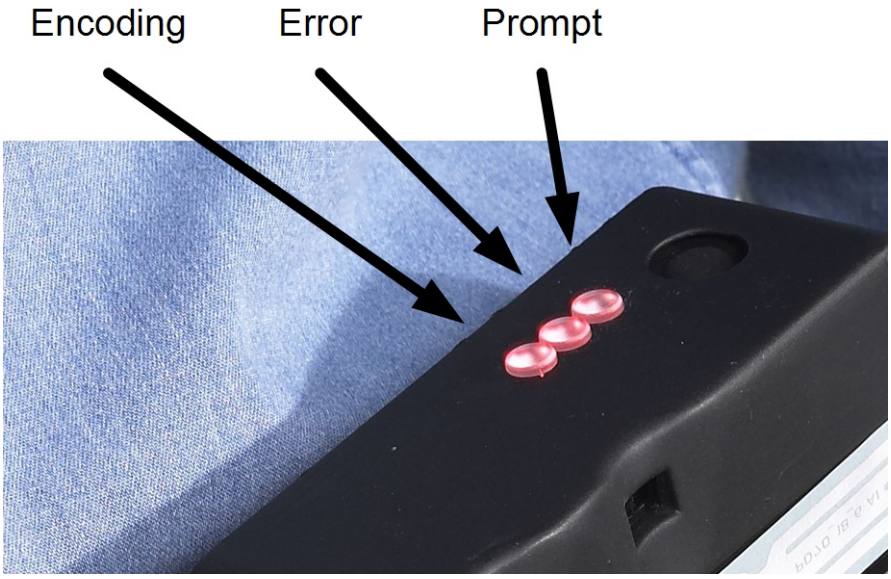
This take-up roll is normally used to collect used release liner, relieving the operator from disposal of this environmental problem. ADASA collects and will reprocess used release liner using best industry practices.

Re-encoding a Tag

If an operator makes a mistake such as damaging an RFID tag after it has been removed, an identical set of information can be encoded into the tag using the “ReDo” button located on the side of the PAD3500.

If for some reason, the current tag is crushed, ruined or lost, the operator needs only to press the ReDo button, and the PAD3500 will re-write the ReDo Tag ID to the current tag, and therefore provide a way to duplicate just one tag, without re-writing the entire set. If the ReDo button is pressed in Index Mode, the ReDo Tag ID will simply over-write the current Tag ID and index it up to be peeled off.

Operator Indicators



Prompt LED

The Prompt LED indicates that the operator should remove a successfully encoded RFID tag from the PAD3500 encoding zone.

Error LED

The Error LED indicates that an operation failed.

Encoding LED

The Encoding LED blinks rapidly when an RFID tag is being encoded.

Charging

If the PAD3500 runs out of battery power, the unit will need to be plugged into the ADASA wall charger and not used again until the battery is fully charged.

Replacing Cartridges

When a tag cartridge is empty, it can be easily replaced with a full cartridge. First the empty cartridge is to be released from the PAD3500 by pressing the Cartridge Release Button. A spring assists the operator in removing the empty cartridge.

A full cartridge is aligned with the bottom guide lip, and is slid laterally toward the Cartridge Release Button. The cartridge will self align and latch into the PAD3500.

Note: Some Beta units require a little extra rap to close the latch. This is due to the tolerance of the plastic fabrication process of the Beta units.

CHAPTER 3
PAD3500 WIRELESS LAN

3.1 OVERVIEW


Note:

3.2 SPECIFICATIONS

Table 1. PAD3500 WLAN Specifications

Specification	Description
Technology	IEEE 802.11b DSSS, Wi-Fi compliant
Frequency	2.400 – 2.4835 GHz (US)
Modulation	DQPSK
Clock Frequencies	4.8 MHz – CPU reference clock 32.768 KHz – real-time clock
Channels	USA/Canada: 11 channels (1 – 11)
Data Rate	2 Mbps (fixed raw wireless rate)
MAC	CSMA/CA with ACK, RTS, CTS
RF Power	+14.7 dBm Approx.30 mW
Sensitivity	-88 dBm
Security	WEP standard encryption, 64 or 128 bits
Antenna	2dBi Omni Half Wave Dipole for 50 ohm SMA connector on PAD3500

3.3 WLAN BLOCK DIAGRAM

Figure 1 shows the block diagram of the PAD3500 WLAN hardware module.

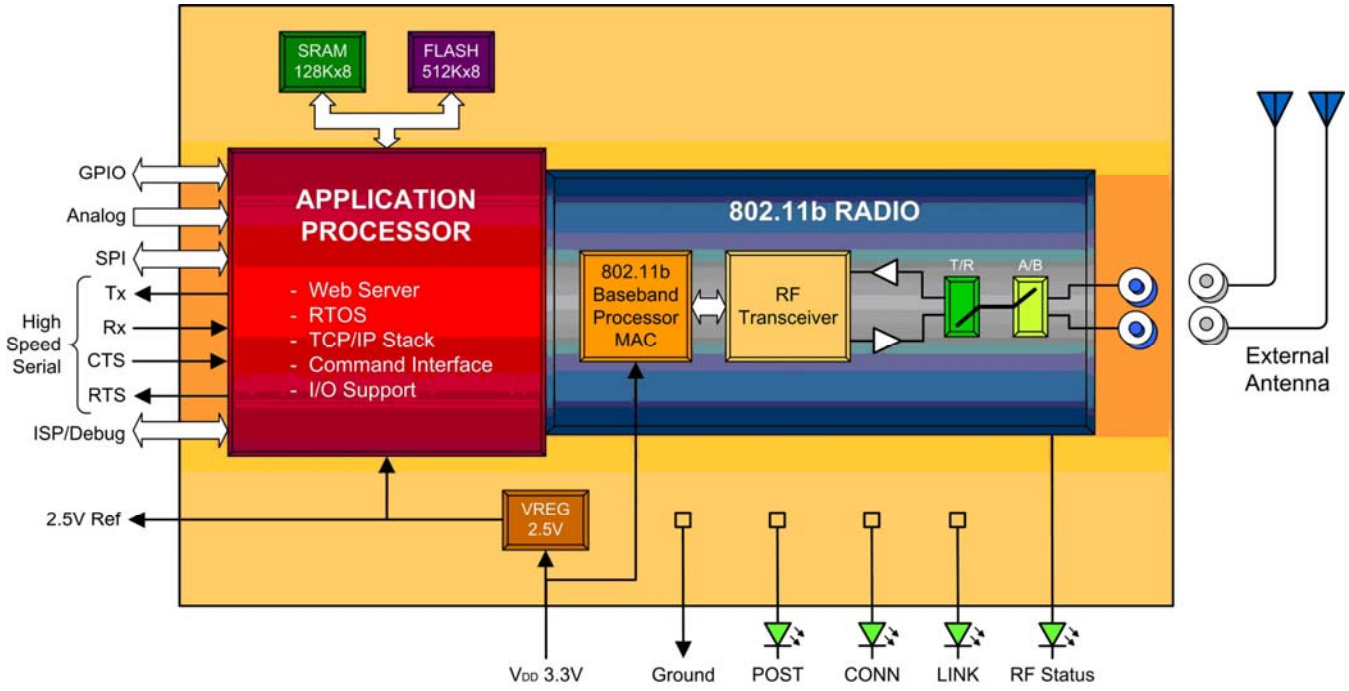


Figure 1. PAD3500 WLAN Hardware Block Diagram

3.4 WLAN HARDWARE DESCRIPTION

3.4.1 Application Processor

The application processor interfaces to the radio module and is the link between the wireless LAN and the embedded Host application. A TCP/IP stack with TCP server, TCP client and Web server capabilities, an RTOS kernel, a radio Link Layer interface, and a Host application layer Command Line Interface all support features required for flexible LAN connectivity.

The application processor contains its own memory, Flash, and RAM, which are used exclusively to support the WLAN functionality.

3.4.3 Static Random Access Memory

The PAD3500 includes up to 128 KB Static Random Access Memory (SRAM) to support WLAN functions and features. SRAM is built-in and is used exclusively by the WLAN application processor.

3.4.4 Flash Memory

The PAD3500 includes up to 512 KB Flash memory to support WLAN functions and features. Flash memory is built-in and used exclusively by the WLAN application processor.

3.4.5 IEEE 802.11 Media Access Control

The IEEE 802.11 Media Access Control (MAC) provides for, and manages, all time-critical wireless media control.

3.4.6 IEEE 802.11 Baseband/RF

The IEEE 802.11 Baseband RF device provides the appropriate baseband signal processing, as well as the appropriate RF modulation for the wireless connection.

CHAPTER 4

WEB INTERFACE

4.1 OVERVIEW

This chapter describes how to use the Web interface to configure, manage, and view the status of PAD3500 WLAN Module. Topics in this chapter include:

4.2 ACCESSING THE WEB INTERFACE

Use your Web Browser to access the Web interface. The PAD3500's built-in security requires you to log in with your user name and password.

Note: The factory default to log into the web interface user name: `pad3500` password: `pad3500`

4.3 NAVIGATING THROUGH THE WEB INTERFACE

The Web interface provides an intuitive point-and-click interface. A menu bar at the top-right area of each page provides links you can click to navigate from one page to another. Some pages have **Save** and **Cancel** buttons. If you change parameters on one of these pages, click **Save** to save your changes or click **Cancel** to discard them.

Changes made to the parameters on all pages in the Web interface will not take effect until you restart the Module.

4.4 STATUS PAGE

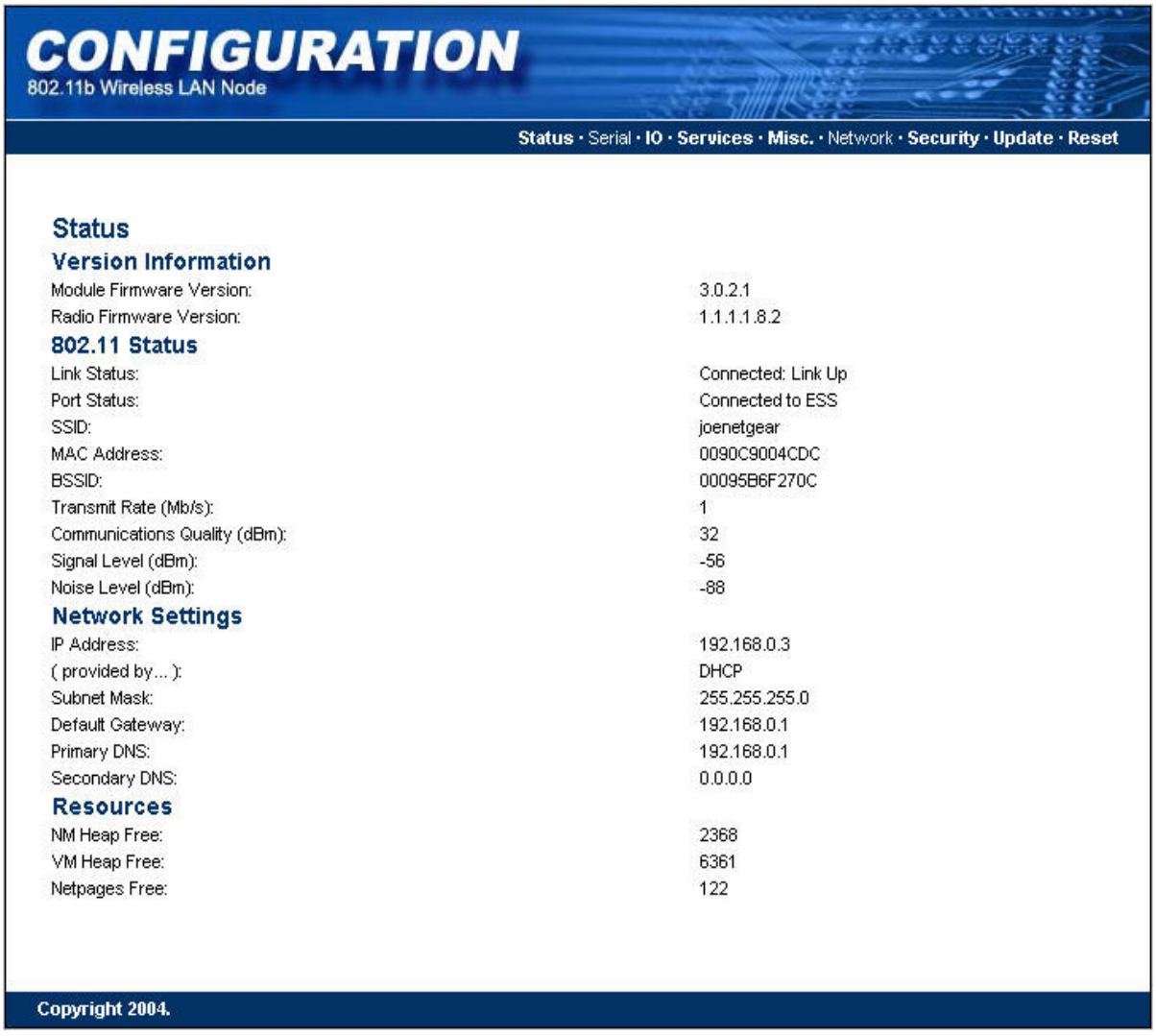
The Status page is the first page that appears when you log into the Web interface. It also appears when you click the **Status** link in the menu bar. This read-only page shows the PAD3500's version number, 802.11 status, network settings, and resources.

Parameters to note in this screen are:

MAC address is MAC address of the PAD3500.

BSSID is the MAC address of the associated Access Point (AP).

Communications Quality, **Signal Level**, and **Noise Level** are in dBm (see Table 29 on page 80 for a description of status results)



4.5 SERIAL INTERFACE CONFIGURATION PAGE

Clicking the **Serial** link in the menu bar displays the Serial Interface Configuration page. This page lets you change the PAD3500's serial port and network connection settings.

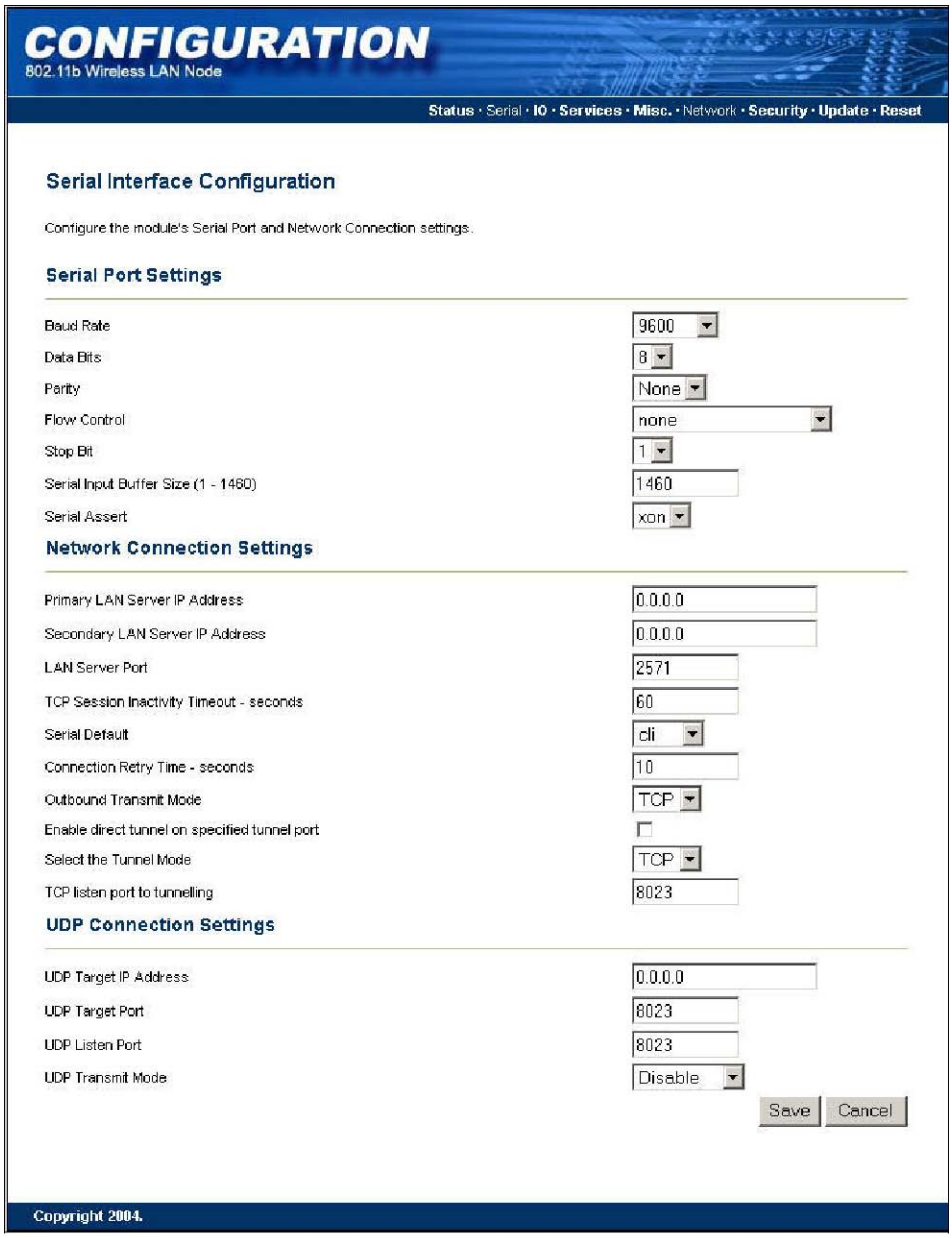


Figure 15. WLN UART Model Only — Serial Interface Configuration Page

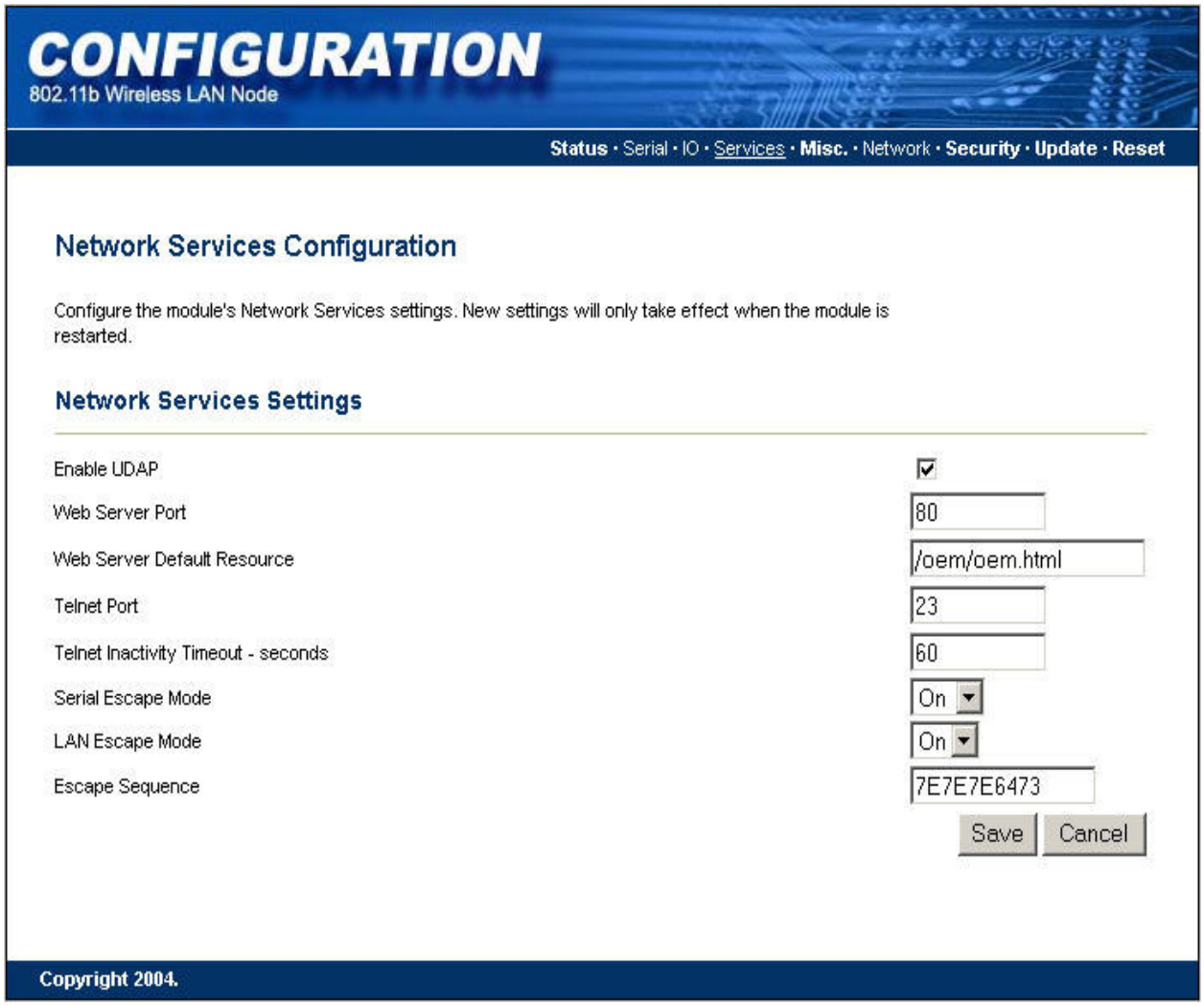
Table 2. Serial Interface Configuration Settings

Parameter	Description
Serial Port Settings	
Baud Rate	300 – 460800 bps Default is 9600. See "High Speed UART Configurations" on page 11.
Data Bits	• 7 • 8 (default)
Parity	• None (default) • Even • Odd
Flow Control	• none (default) • Hardware (RTS/CTS) • Software (XON/XOFF)
Stop Bit	Sets the stop bits to one (1) or two (2). Default is 1.
Serial Input Buffer Size (1 - 1460)	1 -1460 bytes Default is 1460.
Serial Assert	Allows the serial software flow control to be asserted or deasserted via CLI over TCP. The value committed is also applied to the system at startup. • xoff • xon (default)
Network Connection Settings	
Primary LAN Server IP Address	Specifies the IP Address of the primary LAN device to which the PAD3500 will connect to in pass-through mode; four octets separated by a period. Default is 0.0.0.0.
Secondary LAN Server IP Address	Specifies the IP Address of the secondary LAN device to which the PAD3500 will connect to in pass-through mode; four octets separated by a period. Default is 0.0.0.0.
LAN Server Port	Specifies the port number of the LAN Host to which the PAD3500 will connect to in pass-through mode. Default is 2571.
TCP Session Inactivity Timeout - seconds	Specifies the number of seconds of inactivity after which the TCP session with the LAN Host ends. A setting of 0 disables TCP timeout. Default is 60.
Serial Default	Specifies the startup mode that the PAD3500 enters as seen by the attached Serial Host device: • listen = PAD3500 "listens" for connections from LAN-based devices and applications. • pass = PAD3500 tries to connect to the LAN server at the IP address and port defined above, and enters pass-through mode. • cli = PAD3500 accepts CLI commands from the Serial Host (default).
Connection Retry Time - seconds	Specifies the number of seconds the PAD3500 waits before trying to reconnect with the LAN Host following a session inactivity timeout or a failed connection in pass-through mode. Default is 10.

Outbound Transmit Mode	Specifies TCP, UDP, or both, as the protocol to use for outbound data. • TCP = Data is passed to the network using TCP packets (default). • UDP = Data is passed to the network using UDP packets. • BOTH = Data is passed to the network using both TCP and UDP packets.
Enable direct tunnel on specified tunnel port	When checked, enables tunnel port TCP/UDP connections. When unchecked, disables tunnel port TCP/UDP connections. Default is unchecked.
Select the Tunnel Mode	Specifies UDP or TCP as the tunnel mode. Default is TCP.
TCP listen port to tunneling	Specifies the TCP port that the device should listen on for inbound connections. Default is 8023.
UDP Connection Settings	
UDP Target IP Address	Specifies the UDP IP address to use when the serial Host wishes to send UDP data packets to a remote UDP listener/server. Default is: 0.0.0.0.
UDP Target Port	Specifies the UDP port number to use when the serial Host wishes to send UDP unicast data packets to a remote listener/server. Default is: 8023 (decimal).
UDP Listen Port	Defines the UDP port the Tunnel server will listen on for inbound UDP data. Unicast and broadcast packets will be received and transferred to the serial interface. Only when the PAD3500 is in pass mode will UDP payload be conveyed to the serial interface. Default is 8023 (decimal).
UDP Transmit Mode	Sets the mode for outbound UDP transmissions. Disable – disables outbound UDP packet transmission Unicast – enables UDP unicast only Broadcast – enables UDP broadcast only Both – enables UDP broadcast and unicast – a broadcast and a unicast packet is transmitted. If wl-xmit-type is set to both, three packets will be transmitted: TCP, UDP unicast, and a UDP broadcast. Default is Disable.

4.6 NETWORK SERVICES CONFIGURATION PAGE

Clicking the **Services** link in the menu bar displays the Network Services Configuration page. This page lets you configure the PAD3500's network service settings.



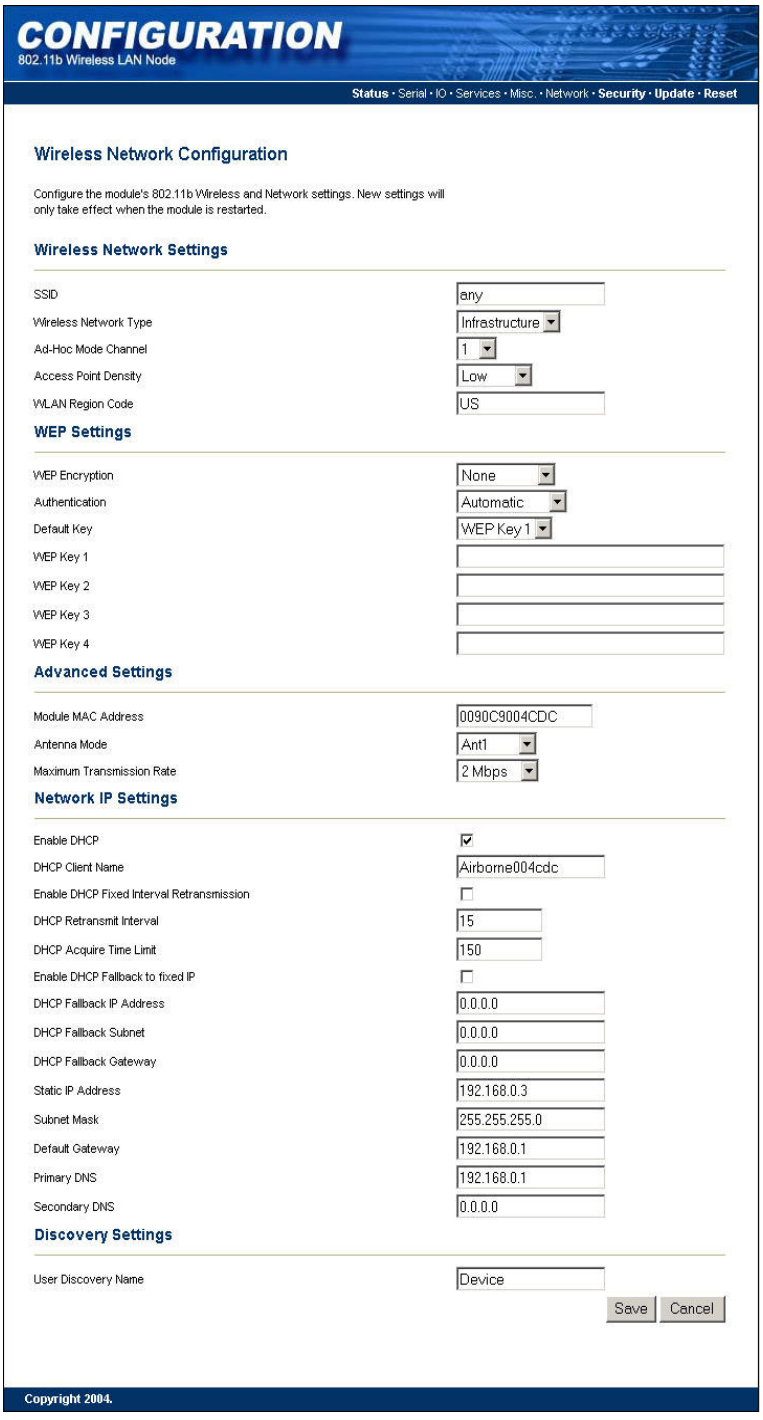
Network Services Configuration Settings

Parameter	Description
Enable UDAP	When checked, enables Universal Data Appliance Protocol (UDAP). This allows the PAD3500 to be discovered from a LAN-based device that supports the UDAP protocol. Default is checked.
Web Server Port	Specifies the port number of the Web server. Default is 80.
Web Server Default Resource	Specifies the default HTML page where users go when they log on. This can be customized to be an OEM's HTML page. Default is /oem/oem.html.
Telnet Port	Specifies the port number of the Telnet server. Default is 23.

Telnet Inactivity Timeout - seconds	Specifies the number of seconds of inactivity that must occur for the Telnet session to timeout. Setting the timeout to 0 disables it. Default is 60.
Serial Escape Mode	Determines whether the PAD3500 recognizes or ignores the escape sequence in the data stream. • On = PAD3500 always looks for the escape sequence in the data stream and reacts to it. • Off = PAD3500 ignores the escape sequence, allowing the sequence to be embedded in the data stream without concern about having the PAD3500 react to it. **Note: When parsing is disabled, the Host will never be able to escape to the CLI mode.**
LAN Escape Mode	Enables or disables the PAD3500's ability to escape from data pass mode to CLI mode. When enabled, escape occurs upon receipt of the escape string or the break character from the wireless LAN interface. • On = enables LAN escape string checking. (default) • Off = disables LAN escape checking.
Escape Sequence	Defines the characters used as the escape sequence. Default is 7E7E7E6473, which corresponds to the characters ~~~ds.

4.7 WIRELESS NETWORK CONFIGURATION PAGE

Clicking the **Network** link in the menu bar displays the Wireless Network Configuration page. This page lets you change the PAD3500's wireless network, WEP security, advanced, network IP, and discovery settings.



Wireless Network Configuration Settings

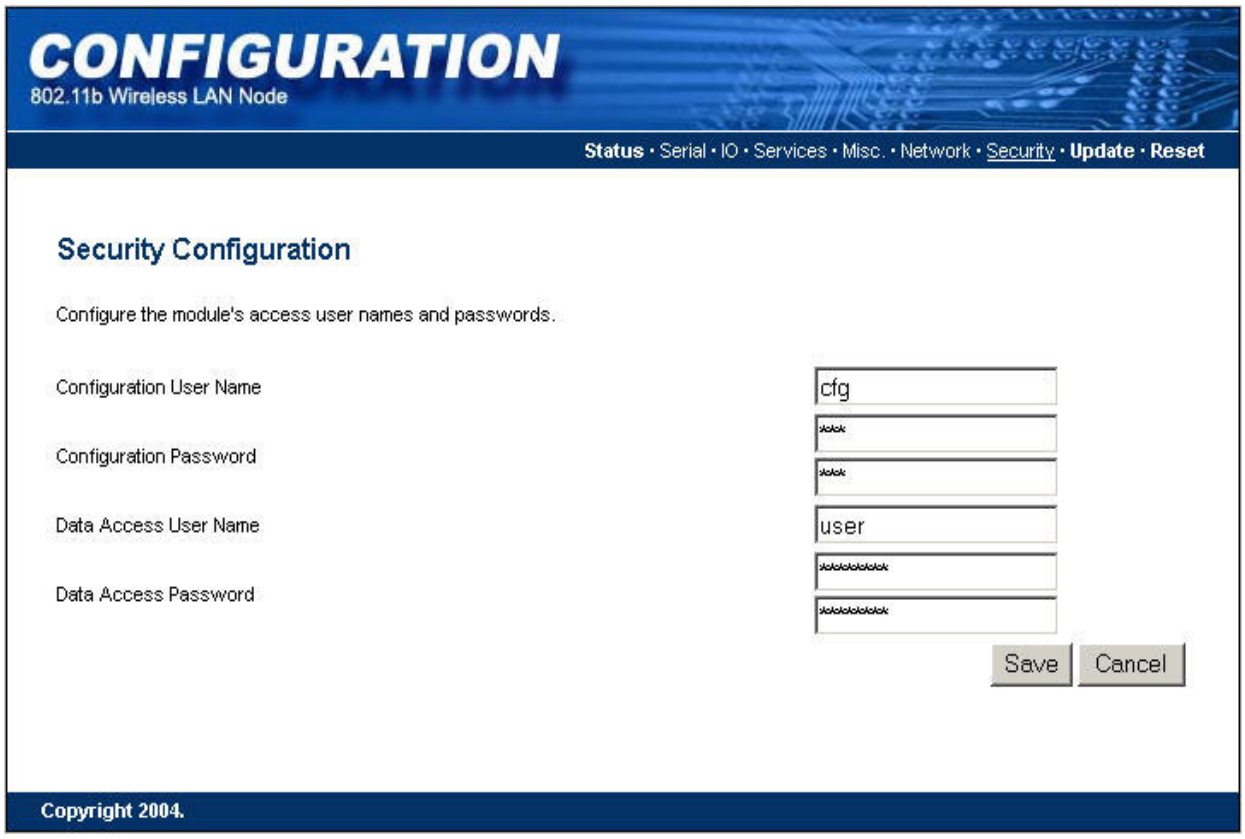
Parameter	Description
Wireless Network Settings	
SSID	Service Set Identifier that identifies the PAD3500 to connect to an AP. To make this connection, the PAD3500 and AP must have the same SSID. The SSID cannot contain spaces. Default setting is any.
Wireless Network Type	Specifies the type of network in which the PAD3500 will be used: • Infrastructure = connects to WLAN using an AP. (default) • Ad Hoc = used to connect two peer-to-peer devices.
Ad Hoc Mode Channel	When Wireless Network Type is Ad Hoc, selects the channel used for communication. The two peer-to-peer devices must use the same channel. Range is 1 to 14 channels. Default channel is 1.
Access Point Density	Specifies a rate that, if not sustainable with the current association, causes the PAD3500 to look for an AP with which it can maintain the specified rate. A high setting causes the PAD3500 to more readily switch to another AP. • Low -2 Mbps cannot be sustained. (default) • Medium - 5.5 Mbps cannot be sustained. • High -11 Mbps cannot be sustained. Only the "Low "setting is supported.
WLAN Region Code	**PAD3500 Operation Region** Specifies the wireless channels allowed. This setting only applies when the PAD3500 is operating in Ad Hoc mode. The AP controls the channel used during Infrastructure mode. For a list of region country codes, see Table 28 on page 79. Default is US.
WEP Settings	
WEP Encryption	Enables or disables WEP security: • None (default) • 64 = 64-bit key length • 128 = 128-bit key length
Authentication	Enables or disables WEP authentication: • Automatic = automatically detects the authentication. (default) • Open System = communicates the key across the network. • Shared Key = allows communication only with devices with identical WEP settings.
Default Key	Selects the default WEP Key from 1 – 4 if Shared Key or Both is selected for Authentication. Default is WEP Key 1.

Parameter	Description
WEP Key 1 through 4	Specify up to four WEP key values: • If WEP Encryption = 64, enter 10 hexadecimal digits for each key. • If WEP Encryption = 128, enter 26 hexadecimal digits for each key.
Advanced Settings	
PAD3500 MAC Address	Specifies the PAD3500's MAC address. Default is factory set. Changing this value may cause unexpected results.
Antenna Mode	Selects the PAD3500's antenna mode: • Ant1 = uses antenna 1. (default) • Diversity = uses antenna 1 and antenna 2. Supports receive diversity only.
Maximum Transmission Rate	Specifies the PAD3500's maximum wireless transmission rate. Default and the only supported rate is 2 Mbps.
Network IP Settings	
Enable DHCP	When checked, enables the Dynamic Host Configuration Protocol (DHCP). For this parameter to work, the AP or network must support DHCP.
DHCP Client Name	Specifies the PAD3500's DHCP client name.
Enable DHCP Fixed Interval Retransmission	Sets the DHCP retransmission mode to either Exponential (0) or Fixed interval (1). Default is 0.
DHCP Retransmit Interval	Sets the DHCP retransmission interval to use when wl-dhcp-mode is set to fixed. This is an integer with a range of 1-64. Default is 15.
DHCP Acquire Time Limit	Sets the number of seconds the DHCP should attempt to acquire an IP address before using the fallback IP address, if wl-dhcp-fb is on. An integer with a range of 1-255. Default is 150.
Enable DHCP Fallback to fixed IP	Sets the DHCP fallback method off (0) or on (1). -If wl-dhcp-fb is on, after the number of seconds of wl-dhcp-acqlimit has been reached, the firmware uses the IP address specified in the wl-dhcp-fbip. -If wl-dhcp-fb is off, the firmware will not use the fallback method. Default is 0.
DHCP Fallback IP Address	Sets the fallback IP address. Default is 0.0.0.0.
DHCP Fallback Subnet	Sets the fallback subnet mask. Default is 0.0.0.0.
DHCP Fallback Gateway	Sets the fallback gateway address. Default is 0.0.0.0.
Static IP Address	Specifies the PAD3500's static IP address; up to four octets separated by a period. If Enable DHCP is checked, this parameter is ignored. Default is 0.0.0.0.
Subnet Mask	Specifies the PAD3500's subnet mask; up to four octets separated by a period. Default is 255.255.255.0

Parameter	Description
Default Gateway	Specifies the PAD3500's LAN IP address; up to four octets separated by a period. Default is 192.168.0.1.
Primary DNS	Sets the primary DNS server address for DNS lookups. If DHCP is enabled, the IP address provided by the DHCP server is used. Default is 0.0.0.0.
Secondary DNS	Sets the secondary DNS server address for DNS lookups when the primary DNS server is unavailable. Default is 0.0.0.0.
Discovery Settings	
User Discovery Name	Identifies the PAD3500 if Enable UDAP is checked in the Network Services Configuration page (see page 39). Default is Device.

4.8 SECURITY CONFIGURATION PAGE

Clicking the **Security** link in the menu bar displays the Security Configuration page. This page lets you change the user name and password required to access the Web interface.



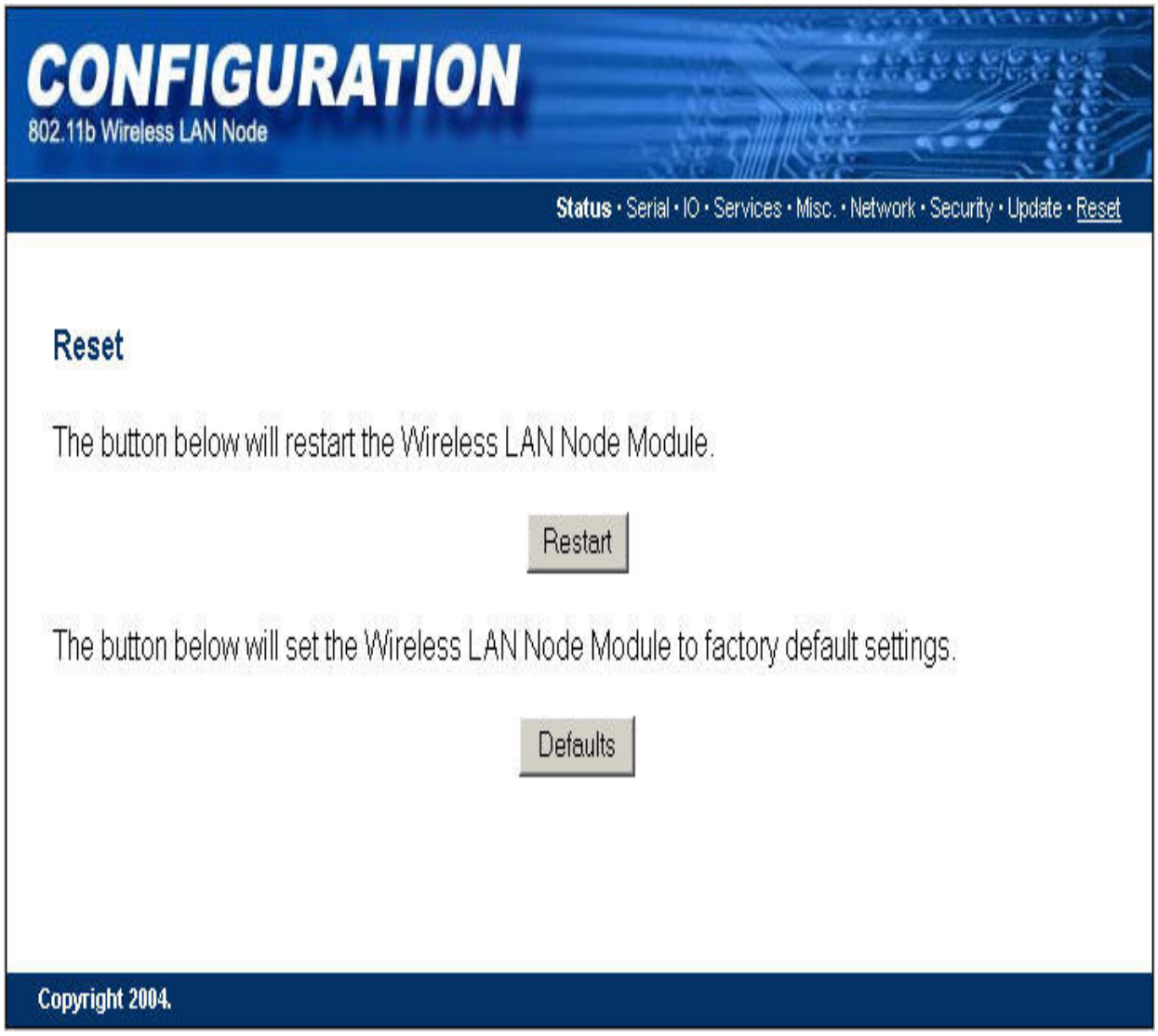
Security Configuration Settings

Parameter	Description
Configuration User Name	Specifies the user name required to log into the Web interface, from 1 to 31 alphanumeric characters. User name is case-sensitive. Default is cfg. If you change it, you are prompted for the user name and password at the next transaction (for example, when you move to another page or refresh the current page).
Configuration Password	Two fields where you type and then retype the configuration password required to access the Web interface, from 1 to 31 alphanumeric characters. Password is case-sensitive. For security, each password character appears as an asterisk. Default is cfg. If you change it, you are prompted for the user name and password at the next transaction (for example, when you move to another page or refresh the current page).
Data Access User Name	Specifies the name required to pass data through the PAD3500. The configuration user name can be 1 to 31 alphanumeric characters and is case-sensitive. Default is user.
Data Access Password	Two fields where you type and then retype the password required to pass data through the PAD3500, from 1 to 31 alphanumeric characters. Password is case-sensitive. For security, each password character appears as an asterisk. Default is password.

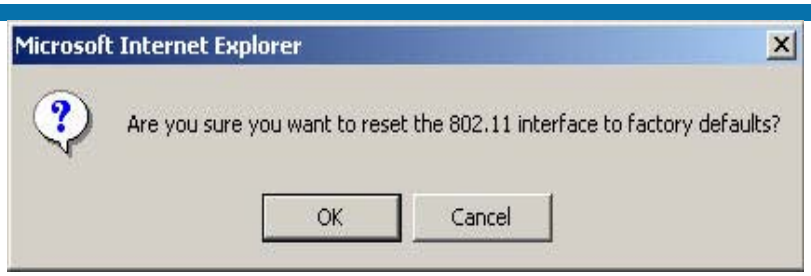
4.9 RESET PAGE

Clicking the **Reset** link in the menu bar displays the Reset page (see Figure 26). This page provides a **Restart** button that lets you restart the PAD3500. It also provides a **Defaults** button that discards your custom settings and returns the PAD3500 to its factory-default settings.

- If you click the **Restart** button, the screen in Figure 27 appears. Click **OK** to restart the Bridge or **Cancel** to not restart it.
- If you click the **Defaults** button, the screen in Figure 28 (on page 53) appears. Click **OK** to reset the Bridge to its factory-default settings or **Cancel** to not reset it.


CONFIGURATION
802.11b Wireless LAN Node
Status • Serial • IO • Services • Misc. • Network • Security • Update • Reset
Reset
The button below will restart the Wireless LAN Node Module.
Restart
The button below will set the Wireless LAN Node Module to factory default settings.
Defaults
Copyright 2004.


Microsoft Internet Explorer
Are you sure you want to reboot the 802.11 interface? Rebooting will disconnect any currently active sessions.
OK
Cancel


Microsoft Internet Explorer
Are you sure you want to reset the 802.11 interface to factory defaults?
OK
Cancel

APPENDIX A
RADIO FREQUENCY CHANNELS

IEEE 802.11 wireless nodes, like the PAD3500, use radio-frequency signals in the Industrial, Scientific, and Medical (ISM) band between 2.4 GHz and 2.5 GHz to communicate with each other.

Due to the spread-spectrum effect of the signals, a node sending signals on a particular channel uses the frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate WLANs in the same general vicinity that use neighboring channels (channel 1 and channel 2, for instance) can interfere with each other. Applying two channels that allow the maximum channel separation decreases the amount of channel cross-talk and provides performance gains over networks with minimal channel separation.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). Neighboring channels are 5 MHz apart. To minimize adjacent channel interference, you can apply a maximum of three different channels within your WLAN. There are 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap. The following chart lists the 802.11 radio-frequency channels that are used.

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz
14	2484 MHz	2471.5 MHz – 2496.5 MHz

APPENDIX B

GLOSSARY

This appendix provides a glossary of wireless terminology.

802.11	Wireless standards developed by the IEEE that specify an "over-the-air" interface for wireless Local Area Networks. 802.11 is composed of several standards operating in different radio frequencies.
802.11a	802.11a is an IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.725 GHz to 5.850 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4-GHz frequency because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.
802.11b	802.11b is the international standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps.
802.11g	802.11g is similar to 802.11b, but this forthcoming standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology to boost overall bandwidth.
Access Point	An interface between a wireless network and a wired network. Access Points can combine with a distribution system (such as Ethernet) to create multiple radio cells (BSSs) that enable roaming throughout a facility.
Ad hoc mode	A wireless network composed of only stations and no Access Point.
Association service	An IEEE 802.11 service that enables the mapping of a wireless station to the distribution system via an Access Point.
Asynchronous transmission	A type of synchronization where there is no defined time relationship between the transmission of frames.
Authentication	The process a station uses to announce its identity to another station. IEEE 802.11 specifies two forms of authentication: open system and shared key.
Bandwidth	The amount of transmission capacity available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect devices to a network.
Basic Service Set (BSS)	A set of 802.11-compliant stations that operate as a connected wireless network.
Bits per second (bps)	A measurement of data transmission speed over communication lines based on the number of bits that can be sent or received per second.
BSSID	Basic Service Set Identifier. A 48-bit identifier used by all stations in a BSS in frame headers (usually the MAC address).
Clear channel assessment	A function that determines the state of the wireless medium in an IEEE 802.11 network.

Client	Any computer connected to a network that requests services (files, print capability) from another member of the network.

Command Line Interface (CLI)	A method of interacting with the Airborne WLN PAD3500 by sending it typed commands.
DHCP	Short for Dynamic Host Configuration Protocol, DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. DHCP also supports a mix of static and dynamic IP addresses.
Direct Sequence Spread Spectrum (DSSS)	Combines a data signal at the sending station with a higher data rate bit sequence, which many refer to as a "chip sequence" (also known as "processing gain"). A high processing gain increases the signal's resistance to interference. The minimum processing gain that the FCC allows is 10. Most products operate under 20.
Disassociation service	An IEEE 802.11 term that defines the process a station or Access Point uses to notify that it is terminating an existing association.
Distribution service	An IEEE 802.11 station uses the distribution service to send MAC frames across a distribution system.
GPIO	General Purpose Input/Output refers to the digital I/O lines.
Host application	The environment within which the PAD3500 is embedded. It typically includes a processor, which forms part of an OEM's product and application.
Hot spot	Same as an Access Point, usually found in public areas such as coffee shops and airports.
IEEE	Institute of Electrical and Electronic Engineers, an international organization that develops standards for electrical technologies. The organization uses a series of numbers, like the Dewey Decimal system in libraries, to differentiate between the various technology families.
Independent Basic Service Set Network (IBSS Network)	An IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations. This type of network is often referred to as an Ad Hoc network because it can be constructed quickly without too much planning.
Infrastructure mode	A client setting providing connectivity to an Access Point. As compared to Ad Hoc mode, where PCs communicate directly with each other, clients set in Infrastructure mode all pass data through a central Access Point. The Access Point not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad Hoc and Access Point.
LAN application	A software application that runs on a computer that is attached to a LAN, Intranet, or the Internet, and uses various protocols to communicate with the PAD3500.
Local Area Network	A system of connecting PCs and other devices within the same physical proximity for sharing resources such as Internet connections, printers, files, and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.
Media Access Control (MAC) Layer	One of two sub-layers that make up the Data Link Layer of the OSI reference model. The MAC layer is responsible for moving data packets to and from one network node to another across a shared channel.
MPDU	MAC Protocol Data Unit, the unit of data exchanged between two peer MAC entities using the services of the physical layer (PHY).

MSDU	MAC Service Data Unit, information that is delivered as a unit between MAC service Access Points (SAPs).
Peer-to-peer network	A wireless or wired computer network that has no server, central hub, or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an Access Point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.
RS-232	An EIA standard that specifies up to 20 Kbps, 50 foot serial transmission between computers and peripheral devices.
RTOS	An operating system implementing components and services that explicitly offer deterministic responses, and therefore allow the creation of real-time systems. An RTOS is characterized by the richness of the services it provides, the performance characteristics of those services, and the degree that those performance characteristics can be controlled by the application engineer (to satisfy the requirements of the application).
Service Set Identifier (SSID)	An identifier attached to packets sent over the wireless LAN that functions as a "password" for joining a particular radio network (BSS). All radios and Access Points within the same BSS must use the same SSID or their packets will be ignored.
SPI	Short for Serial Peripheral Interface, a full-duplex serial interface for connecting external devices using four wires. SPI devices communicate using a master/slave relationship over two data lines and two control lines.
Telnet	A virtual terminal protocol used (e.g., with the Internet) to enable users to log into a remote Host.
Transceiver	A device for transmitting and receiving packets between the computer and the medium.
Transmission Control Protocol (TCP)	A commonly used protocol for establishing and maintaining communications between applications on different computers. TCP provides full-duplex, acknowledged, and flow-controlled service to upper-layer protocols and applications.
UDP	Short for User Datagram Protocol, UDP is a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages or sending streaming data (e.g., video) over a network.
Wide Area Network (WAN)	A communication system of connecting PCs (and other computing devices) across a large local, regional, national, or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered wireless LANs.
Wi-Fi	Wi-Fi is a name for 802.11 wireless network technology.
Wi-Fi Alliance	A non-profit international association formed in 1999 to certify interoperability of wireless LAN products based on the IEEE 802.11 specification.
Wired Equivalent Privacy (WEP)	A security protocol for wireless LANs defined in the IEEE 802.11 standard. WEP is designed to provide the same level of security as a wired LAN.

WLAN	Also referred to as a wireless LAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes and provide network connectivity.

WLN	Short for Wireless LAN Node, this is the Airborne PAD3500 that provides 802.11 LAN connectivity.
WLN SPI	This is the model of the Airborne PAD3500 that uses an SPI to interface to a Host device.
WLN UART	This is the model of the Airborne PAD3500 that uses a serial UART to interface to a Host device.

PO Box 2689
Eugene, Oregon 97402
Tel: 541.359.1677
www.adasainc.com