DPAC TECHNOLOGIES®
Products & Services for the Integration Age™

WIRELESS PRODUCTS

Airborne™ Wireless LAN Node Module Data Book

For use with:

WLNB-AN-DP100 Series
WLNB-AN-DP500 Enterprise Series
WLNB-SE-DP100 Series
WLNB-ET-DP100 Series
WLNB-ET-DP500 Enterprise Series
WLNB-SE-DP500 Enterprise Series

Disclaimer
The information in the document is believed to be correct at the time of print. The reader remains responsible for the system design 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 and the test environment.

DPAC Technologies Corp 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 DPAC for the use of the information, nor for infringements of patents or other rights of third parties. This document is the property of DPAC Technologies Corp. and does not imply license under patents, copyrights or trade secrets.

Corporate Headquarters
DPAC Technologies® Corp.
7321 Lincoln Way
Garden Grove, CA 92841
USA

Telephone:	714-898-0007
Toll Free:	800-642-4477
Fax:	714-897-1772
Technical Support:	714-899-7543 / wirelesssupport@dpactech.com
Web Site:	www.dpactech.com

Contents

CHAPTER 1 INTRODUCTION 1

1.1 OVERVIEW 1
1.2 CONFIGURATIONS 1
1.3 FEATURES 2
1.4 APPLICATIONS 2
1.5 USING THIS DOCUMENT 2
1.6 CONVENTIONS 3
1.6.1 Terminology 3
1.6.2 Notes 4
1.6.3 Cautions 4
1.6.4 Courier Typeface 5
1.7 RELATED DOCUMENTATION 5

CHAPTER 2 AIRBORNE WIRELESS LAN NODE MODULE 7

2.1 OVERVIEW 7
2.2 SPECIFICATIONS 8
2.3 BLOCK DIAGRAM 9
2.4 HARDWARE DESCRIPTION 9
2.4.1 Application Processor 9
2.4.2 General Purpose Input/Output 10
2.4.3 Static Random Access Memory 10
2.4.4 Flash Memory 10
2.4.5 IEEE 802.11 Media Access Control 10
2.4.6 IEEE 802.11 Baseband/RF 10
2.4.7 Transmit/Receive Switch 10
2.4.8 A/B Diversity Switch 11
2.4.9 External Antenna Connections 11
2.4.10 Power Supply 11
2.4.11 High Speed UART Configurations 11
2.4.12 SPI Configurations 11
2.5 HOST PIN ASSIGNMENTS AND SIGNAL DESCRIPTIONS 11
2.6 ANTENNA PIN ASSIGNMENTS AND DESCRIPTIONS 15
2.7 RESET 15
2.8 AIRBORNE WLN MODULE OPERATION 17
2.8.1 Power-up 17
2.8.2 Factory Restart 17
2.9 DESIGN GUIDELINES 18
2.9.1 General Design Guidelines 18
2.9.2 SPI Design Guidelines 18
2.9.3 WLN UART Connections 19
2.9.4 WLN SPI Connections 20
2.10 PACKAGE CONFIGURATION 21
2.11 ELECTRICAL CHARACTERISTICS 22
2.11.1 Absolute Maximum Ratings 22
2.11.2 Electrical Characteristics 23
2.11.3 AC Electrical Characteristics – Receiver 24
2.11.4 AC Electrical Characteristics – Transmitter 24
2.11.5 Performance/Range 24

CHAPTER 3 RECOMMENDED LAYOUT PRACTICES 25

3.1 OVERVIEW 25
3.2 MODULE MOUNTING GUIDELINES 25
3.3 CIRCUIT BOARD LAYOUT PRACTICES 25
3.4 EMI / RFI GUIDELINES 26
3.5 ASLIP 27
3.5.1 Protocol 27
3.5.2 Packet Transfer 28
3.5.3 Platform 28
3.6 WPA-LEAP SECURITY 29
3.6.1 Terminology 29
3.6.2 System Requirements 31
3.6.3 Web Interface 31
3.6.5 Example Security Configurations 31
3.6.6 Computer Resource Requirements 32
3.6.7 System Implementation Considerations 32
3.6.8 Migration 33

CHAPTER 4 SERIAL PERIPHERAL INTERFACE (SPI) 35

4.1 OVERVIEW 35
4.2 SPI STANDARD SUPPORT SUMMARY 35
4.3 SPI HARDWARE CONFIGURATION 35
4.4 SPI LOGICAL INTERFACE 36
4.4.1 SPI Read Configuration 36
4.4.2 SPI Write Configuration 37
4.4.3 SPI Write Data 37
4.4.4 SPI Read Data 38

CHAPTER 5 WEB INTERFACE 39

5.1 OVERVIEW 39
5.2 ACCESSING THE WEB INTERFACE 39
5.3 NAVIGATING THROUGH THE WEB INTERFACE 40
5.4 STATUS PAGE 40
5.5 WLN UART MODEL ONLY — SERIAL INTERFACE CONFIGURATION PAGE 42
5.6 WLN SPI MODEL ONLY — SERIAL INTERFACE CONFIGURATION PAGE 45
5.7 GENERAL PURPOSE I/O SETTINGS PAGE 46
5.8 NETWORK SERVICES CONFIGURATION PAGE 47
5.9 WLN UART MODEL ONLY — MISCELLANEOUS OEM SETTINGS PAGE 49
5.10 WLN SPI MODEL ONLY — MISCELLANEOUS OEM SETTINGS PAGE 51
5.11 WIRELESS NETWORK CONFIGURATION PAGE 52
5.12 SECURITY CONFIGURATION PAGE 56
5.13 FIRMWARE UPDATE PAGE 58
5.14 RESET PAGE 60

APPENDIX A POWER CONTROL 63

A.1 OVERVIEW 63
A.2 INTRODUCTION 63
A.3 LOAD HOT SWAPPING 63
A.4 APPLICATION CIRCUIT 65
A.4.1 High-Side Switch 66
A.4.2 Voltage Regulator 66
A.4.3 Bus Switch 66
A.4.4 Circuit Performance 67

A.4.5 Off Current ... 67
A.4.6 Thermal Characteristics ... 68

APPENDIX B RADIO FREQUENCY CHANNELS ... 71

APPENDIX C WLN ETHERNET BRIDGE ... 73

C.1 OVERVIEW ... 73
C.2 ETHERNET BRIDGE MODULE PIN ASSIGNMENTS ... 73
C.3 STATUS PORTS SIGNAL ASSIGNMENT ... 75
C.4 DESIGN GUIDELINES ... 75

APPENDIX D CABLE REPLACEMENT ... 77

D.1 INFRASTRUCTURE NETWORK CONSIDERATIONS ... 79

GLOSSARY ... 81

INDEX ... 85

List Of Figures

Figure 1. Airborne WLN Module Hardware Block Diagram 9
Figure 2. Antenna Connectors 15
Figure 3. Power-up Sequence (Separate /RESET Signal) 16
Figure 4. Power-up Sequence (/RESET Tied to DV_{DD}) 16
Figure 5. DV_{DD} Rise Time Exceeds Tstartup 16
Figure 6. External Reset Circuit 17
Figure 7. Mechanical Dimensions (Airborne WLN Module) 21
Figure 8. Guidelines for Mounting the Airborne WLN Module 26
Figure 9 - WPA-PSK Security Configuration 31
Figure 10 - WPA-LEAP Security Configuration 31
Figure 11. SPI Data Clock Timing 35
Figure 12. Read Configuration Timing Diagram 36
Figure 13. Write Data Timing Diagram 37
Figure 14. Read Data Timing Diagram 38
Figure 15. User Name and Password Screen 39
Figure 16. Status Page 41
Figure 17. WLN UART Model Only — Serial Interface Configuration Page 42
Figure 18. WLN SPI Model Only — Serial Interface Configuration Page 45
Figure 19. General Purpose I/O Settings Page 46
Figure 20. Network Services Configuration Page 47
Figure 21. WLN UART MODEL ONLY — Miscellaneous OEM Settings Page 49
Figure 22. WLN SPI MODEL ONLY — Miscellaneous OEM Settings Page 51
Figure 23. Wireless Network Configuration Page 52
Figure 24. Security Configuration Page 56
Figure 25. Firmware Update Page 58
Figure 26. Warning Message Before Updating the Firmware 59
Figure 27. Firmware Update Success Message 59
Figure 28. Reset Page 60
Figure 29. Warning Message After Clicking the Restart Button 60
Figure 30. Warning Message After Clicking the Defaults Button 61
Figure 31. Inrush Current Characteristics 64
Figure 32. Voltage Droop with Current-Limited Supply 64
Figure 33. Recommended Application Circuit 65
Figure 34. Circuit Soft-start Characteristics 67
Figure 35. Recommended Magnetics Schematic 74

LIST OF TABLES

Table 1. Airborne WLN Module Configurations 1
Table 2. Airborne WLN Module Specifications 8
Table 3. Airborne WLN Module Pin Assignments 12
Table 4. F0, F2, F3, F6 and RF_LED Signal Assignments 14
Table 5. F1, F4, F5, and F7 Signal Assignments 14
Table 6. G0 through G7 Signal Assignments 14
Table 7. E4, E5, E6, E7 Signal Assignments 14
Table 8. Airborne WLN Module Antenna Pin Assignments 15
Table 9. SPI Modes 19
Table 10. Absolute Maximum Ratings 22
Table 11. Electrical Characteristics 23
Table 12. RF Performance Receive Sensitivity 24
Table 13. Performance/Range* 24
Table 14. ASLIP Characters 27
Table 15. SPI Read Configuration Command 36
Table 16. SPI Write Data Command 37
Table 17. SPI Read Data Command 38
Table 18. WLN UART Model Only — Serial Interface Configuration Settings 43
Table 19. General Purpose I/O Settings 46
Table 20. Network Services Configuration Settings 48
Table 21. WLN UART MODEL ONLY — Miscellaneous OEM Settings 50
Table 22. Wireless Network Configuration Settings 53
Table 23. Security Configuration Settings 57
Table 24. Parts List for Recommended Application Circuit 65
Table 25. 802.11b Channel Frequencies 71
Table 26. WLN Module Ethernet-Specific Pin Assignments 74
Table 27. WLN Ethernet Module Status Ports 75
Table 28. Slave Configuration and Set-up 77
Table 29 - Master Configuration and Set-up 78

This page intentionally left blank

1.1 OVERVIEW

The Airborne™ family is a line of highly integrated 802.11 wireless products based on the Airborne Wireless LAN Node Module. The Airborne Wireless LAN Node Module includes a radio, a baseband processor, an application processor, and firmware for a "drop-in" Web-enabled Wi-Fi solution. Since there is no need to develop driver software or to develop the RF and communications expertise in-house, original equipment manufacturers (OEMs) can realize reduced product-development costs and a quick time-to-market. Airborne™ modules provide instant Local Area Network (LAN) and Internet connectivity, and connect through simple standard interfaces to a wide variety of applications.

1.2 CONFIGURATIONS

The Airborne Wireless LAN Node (WLN) Module consists of a fully integrated 802.11 radio and application processor available in four models (see Table 1). This book is designed for the serial versions of the module. Refer to Appendix D for the differences in hardware required for the Ethernet Module.

Table 1. Airborne WLN Module Configurations

Configuration	Description	DPAC Model Number
Airborne 802.11b Wireless LAN Node Module – UART Version	Airborne Embedded Wireless Device Server Serial to Wireless LAN Module with UART firmware and UART interface	WLNB-AN-DP101 WLNB-AN-DP501(LEAP enabled)
Airborne 802.11b Wireless LAN Node Module – SPI Version	Airborne Embedded Wireless Device Server Serial to Wireless LAN Module with SPI (Serial Peripheral Interface) firmware and SPI interface	WLNB-AN-DP102
Airborne 802.11b Serial Bridge Module	Airborne Embedded Wireless Device Server Serial to Wireless LAN Module provides RS-422 and RS-485 capability	WLNB-SE-DP101
Airborne 802.11b Ethernet Bridge Module	Airborne Embedded Wireless Bridge, Ethernet to Wireless LAN Module with Ethernet Bridge functionality (No serial interface)	WLNB-ET-DP101 WLNB-ET-DP501 (LEAP Enabled)

1.3 FEATURES

The following list describes the key features of the Airborne WLN Module.

- 802.11b wireless LAN (Wi-Fi) standards-based technology
- Highly integrated module includes radio, baseband and MAC processor, and application processor
- Extended temperature and environmental specifications
- Built-in TCP/IP and UDP features provide flexible LAN connectivity options

- Built-in Web server enables drop-in LAN and Internet connectivity
- Built in WEP,WPA, and WPA security protocols
- Simplified data communication interface speeds development and time-to-market with reduced development costs
- Simplified antenna connections reduce the need for RF communications expertise
- Powerful integrated command interface eliminates the need to develop complicated software drivers
- Configurable serial, digital, analog I/O, I^2C (master), and SPI (slave) ports
- UART, SPI, or Ethernet interface

1.4 APPLICATIONS

The Airborne WLN Module’s small physical footprint makes the Module easy to embed into new or existing designs. The Module is interoperable with industry-standard IEEE 802.11 Access Points that provide a low-cost infrastructure for connection to a LAN and to the Internet.

The built-in TCP/IP stack, Real Time Operating System (RTOS), and application firmware provide embedded devices with instant LAN and Internet connectivity, without requiring special WLN Module programming. Advanced security standards such as WEP, WPA and EAP deliver a low cost secured infrastructure for connection to a LAN and to the Internet. Only a simple configuration procedure is required using either DPAC's built-in Web-page interface or the WLN Module’s powerful Command Line Interface. An integrated Web server makes it easy to monitor and control any device remotely using a standard browser. Additionally, OEMs can create custom Web pages that deliver content from their application.

The Airborne WLN Module has been designed specifically to provide wireless LAN and Internet connectivity in industrial, scientific, medical, transportation, and other OEM applications. It is an excellent solution for remote sensing and data collection. Equipment with an embedded Airborne WLN Module can be monitored and controlled by a handheld device, by a personal computer in a central location, or over the Internet. This eliminates cabling and allows the equipment to be moved. Additionally, e-mail or text messages can be sent, advising appropriate personnel of alarm conditions or equipment status.

1.5 USING THIS DOCUMENT

In addition to this chapter, this book contains the following chapters and appendixes:

- *Chapter 2, Airborne Wireless LAN Node Module* — describes the hardware and software characteristics of the Airborne WLN Module.
- *Chapter 3, Recommended Layout Practices* — provides suggested layout practices for the Airborne WLN Module.
- *Chapter 4, Serial Peripheral Interface (SPI)* — describes the Airborne WLN Module's SPI interface.
- *Chapter 5, Web Interface* — describes how to use the Web-based console to configure, manage, and view the status of the Airborne WLN Module.
- *Appendix A, ASLIP Functionality* — describes the functionality of the ASLIP component.
- *Appendix B, Power Control* — describes a suggested power supply design.
- *Appendix C, Radio Frequency Channels* — lists radio-frequency channels.
- *Appendix D, Ethernet WLN Bridge* — describes how to configure and use the bridge.
- *Glossary* — defines the terms associated with the Airborne WLN Module and wireless networks in general.

For convenience, an Index appears at the end of this book.

1.6 CONVENTIONS

The following conventions are used in this book:

1.6.1 Terminology

In the following chapters, these terms are used:

- "Airborne Wireless LAN Node Module" (abbreviated Airborne WLN Module) is used to identify the Module the first time in a chapter. Thereafter, the term "Module" is used.
- "Serial Host" refers to a device, such as an embedded microcontroller, that communicates with the Airborne WLN 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 Airborne WLN Module via a wireless network connection.

1.6.2 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.

1.6.3 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.

Caution:	A caution contains information that, if not followed, can cause damage to the product or adverse consequences to the user.

1.6.4 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
```

1.7 RELATED DOCUMENTATION

In addition to this document, other related documents are on the supplied CD. These documents are provided as Portable Document Format (PDF) files. To read them, you need Adobe® Acrobat® Reader® 4.0.5 or higher. For your convenience, Adobe Reader is on the CD. For the latest version of Adobe Acrobat Reader, go to the Adobe Web site: www.adobe.com.

Additional literature about AirborneDirect® products and the Airborne WLN Module that powers them, such as application notes, product briefs, and white papers, can be found on the DPAC Technologies Web site: www.dpactech.com.

DPAC Technologies also offers developer documentation for its AirborneDirect® products. Please contact DPAC Technologies for more information.

These documents are provided as Portable Document Format (PDF) files. To read them, you need Adobe® Acrobat® Reader® 4.0.5 or higher. For your convenience, Adobe Reader is provided on Airborne distribution CDs. For the latest version of Adobe Acrobat Reader, go to the Adobe Web site: www.adobe.com.

Additional literature about AirborneDirect products and the Airborne WLN Module that powers them, such as application notes, product briefs, and white papers, can be found on the DPAC Technologies Web site: www.dpactech.com.

DPAC Technologies also offers developer documentation for its AirborneDirect products. Please contact DPAC Technologies for more information.

This page intentionally left blank

CHAPTER 2
AIRBORNE WIRELESS LAN NODE MODULE

2.1 OVERVIEW

This chapter describes the hardware and software characteristics of the Airborne WLN Module. Topics in this chapter include:

- 2.2 Specifications (page 8)
- 2.3 Block Diagram (page 9)
- 2.4 Hardware Description (page 9)
- 2.5 Host Pin Assignments and Signal Descriptions (page 11)
- 2.6 Antenna Pin Assignments and Descriptions (page 15)
- 2.7 Reset (page 15)
- 2.8 Airborne WLN Module Operation (page 17)
- 2.9 Design Guidelines (page 18)
- 2.10 Package Configuration (page 21)
- 2.11 Electrical Characteristics (page 22)

Note: Unless otherwise noted, the information in this chapter applies to both the UART WLN Module and SPI WLN Module.

2.2 SPECIFICATIONS

Table 2. Airborne WLN Module Specifications

Specification	Description
Technology	IEEE 802.11b DSSS, Wi-Fi compliant
Frequency	2.400 – 2.4835 GHz (US/Can/Japan/Europe) 2.471 – 2.497 GHz (Japan)
Modulation	DBPSK (1 Mbps), DQPSK (2 Mbps), and CCK (5.5 and 11 Mbps)
Clock Frequencies	4.8 MHz – CPU reference clock 32.768 KHz – real-time clock
Channels	USA/Canada: 11 channels (1 – 11) Europe: 13 channels (1 – 13) Japan: 14 channels (1 – 14) France: 4 channels (10 – 13)
Data Rate	11, 5.5, 2, 1 Mbps (raw wireless rate)
MAC	CSMA/CA with ACK, RTS, CTS
RF Power	+15 dBm (typical) Approx.32 mW
Sensitivity	-82 dBm for 11 Mbps -86 dBm for 5.5 Mbps -88 dBm for 2 Mbps -90 dBm for 1 Mbps
Security	WEP, WPA-PSK, and LEAP standard encryption, 64 or 128 bits
Antenna	Two U.FL coaxial connectors, 50Ω, supports receive diversity
Supply	3.3 VDC
Current Consumption	420 mA – transmit mode (typical) 350 mA – receive mode (typical) 250 mA – doze mode (typical – see Note 1 and Note 5 below) 235 mA – snooze mode (typical – see Note 1 and Note 5 below) 50 mA – sleep mode (typical – see Note 5 below)
Power Up Inrush Current	1900 mA (max)
Operating Temperature	Industrial: -40°C – +85°C (see Note 2 below) (Meets IEEE 802.11 industrial temperature range)
Application Processor	16-bit, 120 MIPS @ 120 MHz
Serial Interface	UART: Up to 921 kbps SPI (slave): Can be clocked up to 20 MHz
Data Throughput	UART-to-LAN – up to 800 kbps (max) (see Note 5 below) LAN-to-UART – up to 800 kbps (max) (see Note 3 and Note 5 below)
Memory	Flash: 64 Kbytes onboard, 512 Kbytes expansion (see Note 4 below) SRAM:20 Kbytes onboard, 128 Kbytes expansion
Digital I/O	Up to 8 digital I/O ports and status
Analog Inputs	Up to 8 channels, 10-bit resolution, single ended, 0 – 2.5 V
Connector	36 pin (pn: HRS DF12-36DS-0.5 V) 4-mm height

Note 1: The doze, snooze, and sleep mode current consumption depends on an Access Point's low power support implementation. Some Access Points do not include support for low-power stations.
Note 2: Temperatures above +80°C reduce wireless performance. Module operates from -40°C cold start.
Note 3: Rates are based on operation at maximum wireless data rate, with escape checking set off, serial buffer size set to maximum, minimum wireless interference, and no other LAN traffic.
Note 4: Flash and SRAM are not available to external applications.
Note 5: WLN UART model only.

2.3 BLOCK DIAGRAM

Figure 1 shows the block diagram of the Module hardware.

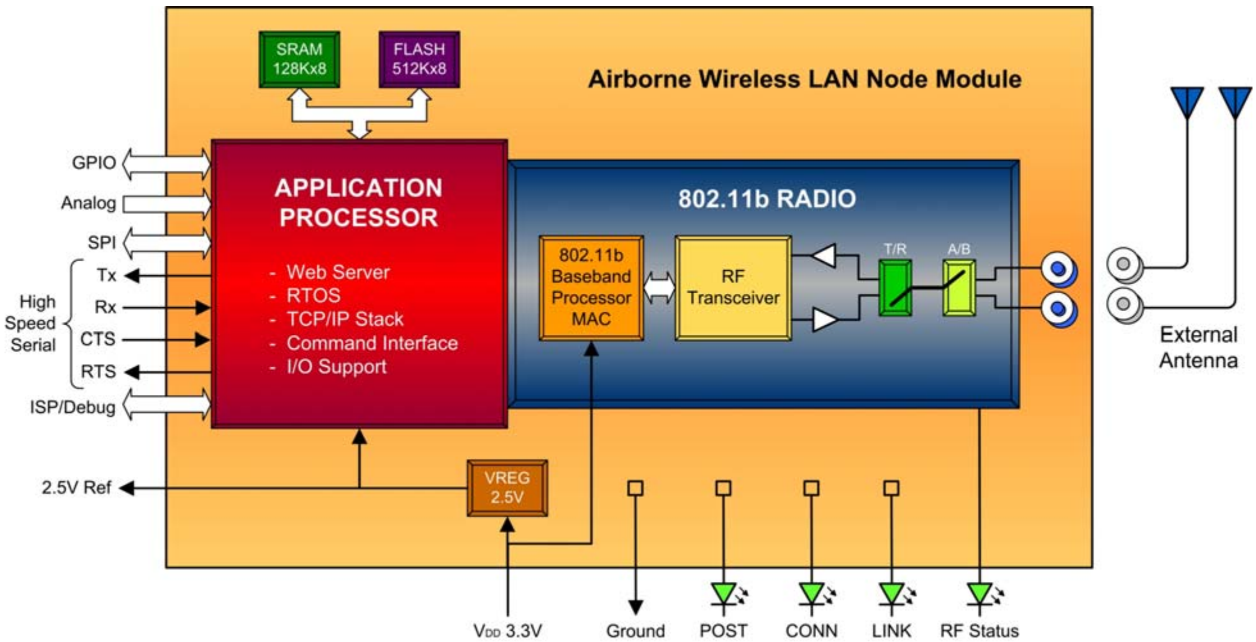


Figure 1. Airborne WLN Module Hardware Block Diagram

Note:

Note: The SPI and UART are not available in the same model.

2.4 HARDWARE DESCRIPTION

The Module contains all of the hardware and firmware components required to implement a full Wireless Fidelity (Wi-Fi)-compatible IEEE 802.11b network interface. It includes two antenna connections, along with all required RF, baseband, and application-processor circuitry. Depending on the configuration of the application firmware, the Module can operate as an embedded communication module under the control of a Host application, or as an application Host. The following sections describe the hardware associated with the Module.

2.4.1 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 Module's application functionality.

2.4.2 General Purpose Input/Output

A set of General Purpose Input/Output (GPIO) ports is provided for control, sensing, and data exchange with the Host system or interface. These ports include digital input/output, analog input, and serial interfaces.

2.4.2.1 Digital Inputs

All digital ports are configurable as digital inputs. The ports use 3.3 V signal levels and are 5.0 V tolerant.

2.4.2.2 Analog Inputs

The analog input ports accept analog signals from 0 - 2.5 V levels and are 3.3 V tolerant. These ports can be alternatively used as digital inputs and can be set for use as digital outputs.

2.4.2.3 Serial Ports

The High Speed serial port can be used as a serial UART or as an SPI Slave. An I^2C Master interface is also available. The serial ports use 3.3 V signal levels and are 5.0 V tolerant.

2.4.3 Static Random Access Memory

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

2.4.4 Flash Memory

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

2.4.5 IEEE 802.11 Media Access Control

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

2.4.6 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.

2.4.7 Transmit/Receive Switch

The Transmit/Receive (T/R) Switch selects the appropriate signal path for the antenna during transmit and receive operations. The IEEE 802.11 MAC controls the T/R Switch automatically.

2.4.8 A/B Diversity Switch

The A/B Diversity Switch controls whether Antenna 1 (J1) or Antenna 2 (J2) is selected. The IEEE 802.11 MAC controls the A/B Diversity Switch automatically when diversity is enabled. Diversity is limited to receive only (no transmit). In a single antenna design, the J1 antenna connection should be used and the A/B Diversity switch will automatically select this antenna. No special configuration changes are necessary.

2.4.9 External Antenna Connections

The Module provides two U.FL-style connectors for connection to external antennas. The two external antenna connectors provide 50 Ω impedance RF signals at 2.4 GHz and offer receive diversity support for OEM system implementations.

2.4.10 Power Supply

The Module requires a single 3.3 V power source (Tolerance: ±5%). The power source must provide sufficient current for peak startup inrush and peak transmit burst in accordance with the Module's specifications (see page 8).

The Module includes an on-board regulator that derives 2.5 V for the Analog Converter. The 2.5 V is provided as a reference source for analog input signals.

Caution: The 2.5 V source is for reference only and must not be used to power devices.

2.4.11 High Speed UART Configurations

- Baud rate parameters: 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 57600, 115200, 230400, 460800, 921000 bps
- Flow control parameters:
  - Hardware handshake: supports CTS and RTS
  - Software handshake: supports XON and XOFF
  - No flow control

2.4.12 SPI Configurations

There are no user-configurable parameters.

2.5 HOST PIN ASSIGNMENTS AND SIGNAL DESCRIPTIONS

The interconnect between the Module and the Host system is a 4 mm high, 36-pin, Hirose DF12-36DS-0.5 V(80) connector.

The part number for the 4-mm high mating connector to be mounted on the PCB is the Hirose DF12-36DP-0.5 V(80). Table 3 lists the Module's Host pin assignments.

Table 3. Airborne WLN Module Pin Assignments

Pin	Signal	Sink	Source	Description
1	GND			Ground
2	TSI			ISP Serial Data In (see Note 1)
3	DV_{DD}			Power, +3.3 V
4	DV_{DD}			Power, +3.3 V
5	V2.5			2.5 V Reference output (for reference only)
6	RFU			Reserved (see Note 1)
7	/RESET			Reset – active low. A transition to high releases the reset condition (see "Reset" on page 15). There is a weak pull-up on this pin, but floating this pin does not guarantee a logic high.
8	/TSS			ISP Slave Select (active low) (see Note 1)
9	G6	4 mA	4 mA	Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}).
10	TSO			ISP Serial Data Out (see Note 1)
11	G3	4 mA	4 mA	Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}). Port can be used at bootup to reset the Module to factory defaults – see Section 2.8.2, Factory Restart on page 17 for more information.
12	F5	8 mA	8 mA	Used as high-speed UART or high-speed SPI Slave (see Table 5). Signal is TTL-compatible and 5 V tolerant.
13	G5	4 mA	4 mA	Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}).
14	G4	4 mA	4 mA	Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}).
15	V_{SS}			Ground
16	V_{SS}			Ground
17	G2	4 mA	4 mA	Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}).
18	F4	8 mA	8 mA	Used as high-speed UART or high-speed SPI Slave (see Table 5). Signal is TTL-compatible and 5 V tolerant.
19	G1	4 mA	4 mA	Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}).
20	TSCK			ISP Serial Clock (see Note 1)
21	G7	4 mA	4 mA	Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}).
22	G0	4 mA	4 mA	UART: Used as analog input or digital output (see Table 6). Provides 3.3 V CMOS-compatible digital output (V_{OL}≤0.4, 2.4 V≤ V_{OH}). SPI: Used as system interrupt (see Table 5). Signal is 3.3 V TTL-compatible and 5 V tolerant.

Table 3. Airborne WLN Module Pin Assignments

Pin	Signal	Sink	Source	Description
23	F6	8 mA	8 mA	Used for digital I/O and Status (see Table 4). Pre-configured as a digital output in firmware and represents the CONNECT status.
24	F7	8 mA	8 mA	Used as high-speed UART or high-speed SPI Slave (see Table 5). Signal is 3.3 V TTL-compatible and 5 V tolerant.
25	F0	8 mA	8 mA	Used for digital I/O and status (see Table 4). Pre-configured as a digital output in firmware and represents the POST status.
26	F3	8 mA	8 mA	Used for digital I/O and status (see Table 4). Pre-configured as a digital output in firmware and represents the WLAN CFG status.
27	F2	24 mA	24 mA	Used for digital I/O and status (see Table 4). Pre-configured as a digital output in firmware and represents the RF LINK status.
28	F1	24 mA	24 mA	Used as high-speed UART or high-speed SPI Slave (see Table 5). Signal is TTL-compatible and 5 V tolerant.
29	E6	24 mA	24 mA	General Purpose Digital I/O, 5 V tolerant.
30	E5	24 mA	24 mA	General Purpose Digital I/O, 5 V tolerant
31	E7	8 mA	8 mA	General Purpose Digital I/O, 5 V tolerant. Optional I^2C SDA (Data) input/output (see Table 7).
32	E4	8 mA	8 mA	General Purpose Digital I/O, 5 V tolerant. Optional I^2C SCL (Clock) output (see Table 7).
33	DV_{DD}			Power, +3.3 V
34	DV_{DD}			Power, +3.3 V
35	/RF_LED	2 mA		RF Status output, active low, represents RADIO ACTIVITY (see Table 4)
36	V_{SS}			Ground

Note 1: The ISP pins should be left as no connects and are tied high internally. ISP pins are reserved for factory loading firmware.

ISP = in-system programming port
V_{OL} = low-output voltage
V_{OH} = high-output voltage

Table 4. F0, F2, F3, F6 and RF_LED Signal Assignments

Port	Direction	
	Status*	Status Description
F0	POST	Indicates that the Module has passed its Power On Self Test (POST).
F2	RF LINK	Indicates that the Module has associated with an Access Point or peer.
F3	WLAN CFG LINK	Indicates that the Module has a Dynamic Host Configuration Protocol (DHCP) or static IP configuration.
F6	CONNECT	Indicates that the Module has made an IP connection with a device on the LAN.
/RF_LED	RADIO ACTIVITY	Blinks when radio is on and scanning for an Access Point. Solid ON when radio is on and associated.

* Status I/O is pre-assigned and controlled by the Airborne firmware.

Table 5. F1, F4, F5, and F7 Signal Assignments

Port	High Speed UART		High Speed SPI Slave	
	Signal*	Direction	Signal*	Direction
F4	HS.RTS	Out	HS.SCLK	In
F5	HS.CTS	In	HS.SS	Out
F7	HS.RXD	In	HS.SDI	In
F1	HS.TXD	Out	HS.SDO	Out
G0	(see Table 6)	(see Table 6)	HS.INT	Out

* I/O is pre-assigned and controlled by the Airborne firmware.

Table 6. G0 through G7 Signal Assignments

Port	Direction	
	Digital	Analog
G0	Out	In
G1	Out	In
G2	Out	In
G3	Out	In
G4	Out	In
G5	Out	In
G6	Out	In
G7	Out	In

Table 7. E4, E5, E6, E7 Signal Assignments

		I^2C Master	
Port	Digital	Signal	Direction
E4	Digital In/Out	SCL - Clock	Out
E5	Digital In/Out	—	—
E6	Digital In/Out	—	—
E7	Digital In/Out	SDA – Bidirectional Data	In/Out

2.6 ANTENNA PIN ASSIGNMENTS AND DESCRIPTIONS

Figure 2 shows the Module antenna connectors and Table 8 describes their pin assignments.

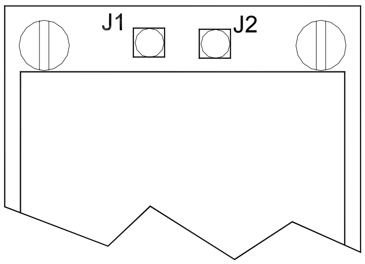


Figure 2. Antenna Connectors

Table 8. Airborne WLN Module Antenna Pin Assignments

Pin	Description
J1 (left connector)	Antenna 1
J2 (right connector)	Antenna 2

2.7 RESET

The Module incorporates a Power-On Reset (POR) detector that generates an internal reset as DV_{dd} rises during power-up. An internal startup timer together with a reset latch control the reset timeout delay. On power-up, the reset latch is cleared (CPU held in reset), and the startup timer starts counting when it detects a valid logic high signal on the /RESET pin (pin 7). When the startup timer reaches the end of the timeout period, the reset latch is cleared, releasing the CPU from reset.

Note: CPU operation does not start until the CPU is released from reset and valid core clocks are received past the system clock suspend circuit. The Module's POR is set to 1 millisecond.

Figure 3 shows a power-up sequence in which /RESET is not tied to the DV_{dd} pin, and the DV_{dd} signal is allowed to rise and stabilize before the /RESET pin is brought high. WUDX specifies the length of time from the rising edge of /RESET until the device leaves reset. For the Module, this length of time is set to 1 millisecond. In this case, the CPU receives a reliable reset.

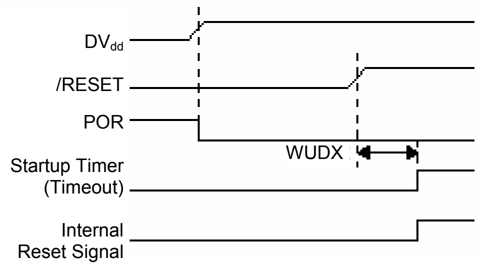


Figure 3. Power-up Sequence (Separate /RESET Signal)

Figure 4 shows the on-chip POR sequence in which the /RESET and DV_{DD} pins are tied together. The DV_{DD} signal is stable before the startup timer expires. In this case, the CPU receives a reliable reset.

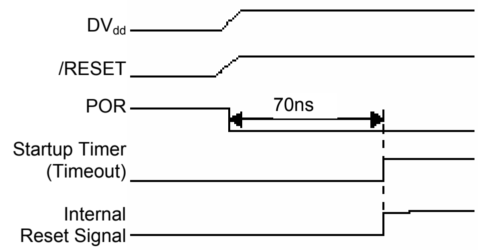


Figure 4. Power-up Sequence (/RESET Tied to DV_{DD})

Figure 5 shows a situation where DV_{DD} rises too slowly. In this scenario, the startup timer times-out before DV_{DD} reaches a valid operating voltage level (DV_{DD} min). As a result, the CPU comes out of reset and starts operating with the supply voltage below the level required for reliable performance. In this situation, an external RC circuit is recommended for driving /RESET. The RC delay should exceed five times the time period required for DV_{DD} to reach a valid operating voltage.

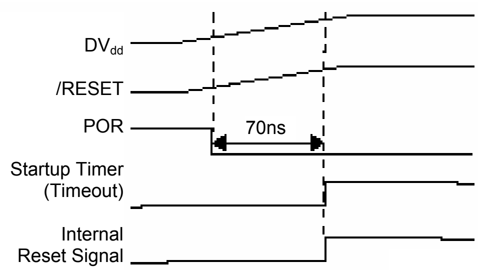


Figure 5. DV_{DD} Rise Time Exceeds Tstartup

Figure 6 shows the recommended external reset circuit. The external reset circuit is required only if the DV_{DD} rise time has the possibility of being too slow (refer to Table 11 on page 23).

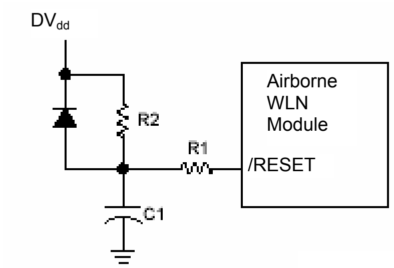


Figure 6. External Reset Circuit

In Figure 6:

- The diode D discharges the capacitor when DV_{DD} is powered down.
- R1 = 100 Ω to 1K Ω limits any current flowing into /RESET from external capacitor C1. This protects the /RESET pin from breakdown due to Electrostatic Discharge (ESD) or Electrical Overstress (EOS).
- R2 < 40K Ω is recommended to ensure that voltage drop across R2 leaves the /RESET pin above a V_{IHGP} level.

Choose C1 to have R2 ∞ C1 exceed five times the time period required for DV_{DD} to reach a valid operating voltage. V_{DD} must start rising from V_{ss} to ensure proper Power-On-Reset when relying on the internal Power-On-Reset circuitry. If power supply takes more than 50 ms to rise from 0 to 2.5 V, use RCs on /RESET pin (see Figure 6).

2.8 AIRBORNE WLN MODULE OPERATION

2.8.1 Power-up

When the Module powers-up, it performs a Power On Self Test (POST). The POST procedure checks that RAM, Flash memory, real-time clock, and radio are operating as expected. If the Module passes the POST, the POST line is set high (POST). Any failures cause the Module to reset.

2.8.2 Factory Restart

The Module provides a factory-restart function that returns the Module to its original factory default settings. There are three ways to activate this feature:

- Use the **Reset** page in the Web interface (see page 60).
- Use the CLI command `reset` (see CLI Reference Guide)
- Hold Port G3 low during Module startup.

To ensure proper operation, a resistor (4.7 K Ω to 47 K Ω) should be used to pull up Port G3 to +2.5 V (use the Module's 2.5 V reference). This signal can be pulled low using either a push-button switch to GND or an open-drain output signal from the Host. For proper factory-reset operation, Port G3 must be held low for 100 ms before /RESET goes high and kept low until 750 ms after /RESET goes high.

Caution: Port G3 must be tied high to no more than 2.5 V. Higher voltages may cause latch-up or damage to the application processor.

2.9 DESIGN GUIDELINES

2.9.1 General Design Guidelines

The Module is designed to be implemented into a variety of applications. Any design must meet the following guidelines:

- Provide 3.3 V to all DV_{dd} power pins.
- Provide ground connections to all V_{ss} pins.
- Tie port G3 to the Module's 2.5 V V_{ref} through a 10 KΩ resistor to prevent the Module from resetting itself to factory defaults at startup.
- Tie all unused I/O to ground via 10 KΩ resistors. If the state of the I/O can be controlled, set all unused I/O as outputs.
- Do not exceed 2.5 V on any port G pins configured as analog inputs.
- Provide a connection to a suitable antenna.
- TSI, TSS, TSO, TSCK, and RFU should be left as No Connects (they are pulled up internally).
- Carefully follow the Hirose DF12 connector placement, mounting, and precautions for use to avoid shorts due to an incorrect soldering profile.

2.9.2 SPI Design Guidelines

The Module with the SPI interface is designed to be implemented into a variety of applications. Any design must meet the following guidelines:

- Data transfer from master to slave is carried out across the MOSI (Master-Out/Slave-In) line.
- Data transfer from slave to master is carried out across the MISO (Master-In/Slave-Out) line.
- All data transfers are synchronized by the Master's serial clock (SCK). One bit of data is transferred every clock pulse, and one octet can be exchanged in eight (8) clock cycles.
- Communication is enabled when the /SS (Slave Select) line is pulled low.
- An Interrupt Master (INT) line is used by the Slave to signal the Master that data is available.

- This protocol is completely octet (8 bits) aligned. Octets used for commands and returned status are in Intel ("little-endian") format.
- A frame is defined as those octets that are bounded by the Slave Select assertion (from the time /SS goes low, until it returns high). SPI requires that commands be framed, so a frame can be of varying sizes, especially for the read and write command sequences. This puts a timing strain on the system to quickly deal with the data. With the SCK running at 2MHz, the system has 4 microseconds to deal with an octet transferred (read or write) between the driver and the buffer.
- If a frame is prematurely terminated (before the octet count is completed), the driver must ensure that the data is properly accounted for and the pointers managed with the actual number of octets transferred, not the number of initially defined.
- The Configuration Status must be available to be shifted out of the MISO port at the beginning of each command, requiring its update immediately at the end of a frame to be prepared for the next frame.
- A pre-defined data frame has to be agreed upon by both the master and slave for the exchange of data. The data frame is described by two parameters, the clock polarity and the clock phase. These parameters have four possible states that correspond to four SPI Modes.

Table 9. SPI Modes

SPI Mode	Clock Polarity (CPOL)	Clock Phase (CPHA)	Clock (SCK) Idle Low: Output on rising, sample on falling High: Output on falling, sample on rising	Output Sample Edge	Input Sample Edge
0	0	0	Low	Falling	Rising
*1	0	1	Low	Rising	Falling
2	1	0	High	Rising	Falling
3	1	1	High	Falling	Rising

- ***The WLN SPI Slave shall run in Mode 1 ***only***.
- The Slave's MOSI needs to be setup by the Master on the first-edge (rising if Idle = Low, falling if Idle = High) following the assertion of /SS. Therefore, the Slave will sample its MOSI on the second-edge (transition).
- The bit ordering of data coming into the SPI Slave is MSB-first for both transmit and receive.

2.9.3 WLN UART Connections

For embedded applications that will communicate with the serial UART interface, the following guidelines are also recommended:

- Connect HS.TXD (port F1) to the receive line of the embedded processor UART.
- Connect HS.RXD (port F7) to the transmit line of the embedded processor UART.

- Connect HS.RTS (port F4) and HS.CTS (port F5) if hardware handshaking is desired.
- Connect the CONNECT status line (port F6) to a digital input on the embedded processor. This line indicates whether a TCP connection is active.
- Connection to the other status lines — POST, RF LINK, WLAN CFG LINK — is optional.
- If HS.RTS and HS.CTS (Ports F4 and F5) are not used, tie them to ground via 10 kΩ resistors.

2.9.4 WLN SPI Connections

- Connect the application's MOSI line to port F7 of the WLN to transfer data from the Master.
- Connect the application's MISO line to port F1 of the WLN to receive data from the Slave.
- Connect the application's SCK line to port F4 of the WLN to send the Master's serial clock.
- Connect the application's /SS line to port F5 of the WLN to select the WLN Module.
- Connection the application's INT line to port G0 of the WLN to receive interrupts from the Slave. This indicates that data is available on the WLN.

Caution: If the Module is connected to a circuit that is powered on while the Module is powered off, the design should ensure that no logic highs are present on the connections while the Module is powered off. Otherwise, the Module can be damaged beyond repair. If the state of the connections cannot be controlled, insert a tri-state buffer between the Module and its Host. For additional information, see Appendix B, Power Control.

Caution: The 3.3 V power supply should be a low-noise design, with less than 150 mV ripple at the maximum average transmit current. The power supply should also be designed to provide sufficient power to handle the Module's power-up inrush current. For additional information, see Appendix B, Power Control.

2.10 PACKAGE CONFIGURATION

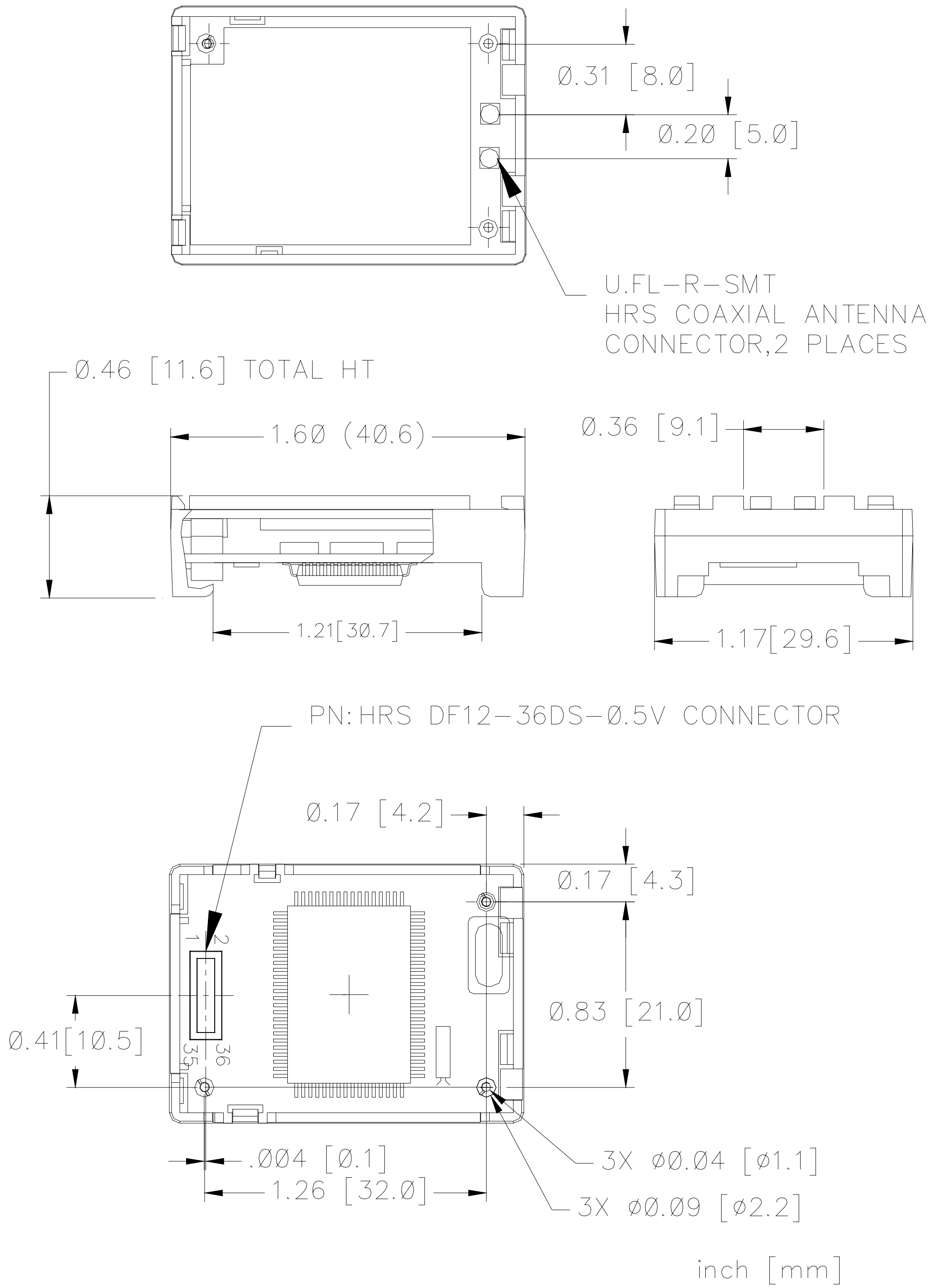


Figure 7. Mechanical Dimensions (Airborne WLN Module)

2.11 ELECTRICAL CHARACTERISTICS

2.11.1 Absolute Maximum Ratings

Table 10 shows the absolute maximum ratings for supply voltage and voltages on the Module's digital and analog pins. Exceeding these values will permanently damage the Module.

Table 10. Absolute Maximum Ratings

Parameter	Min	Max	Unit
Peak instantaneous operating current		480	mA
Startup inrush current		1900	mA
Voltage at GPIO pins	-0.3	5.7	V
Voltage at Analog pins	-0.3	3.5	V
Voltage at V_{DD} pin	0	7	V
Operating temperature	-40	+85	°C
Storage temperature	-40	+100	°C

2.11.2 Electrical Characteristics

Table 11. Electrical Characteristics

Symbol	Parameter	Min	Typ	Max	Unit
V_{DD}	Supply Voltage (3.3 V ±5%)	3.135	3.3	3.465	V
I_{DDTX}	Transmit Mode Current		400	480	mA
I_{DDRX}	Receive Mode Current		300	380	mA
$I_{DDSNOOZE}$	Snooze Mode Current (WLN UART only)		275	300	mA
$I_{IDDDOZE}$	Doze Mode Current (WLN UART only)		235	280	mA
$I_{DDSLEEP}$	Sleep Mode Current (WLN UART only)		50	80	mA
V_{IHGP}	GPIO Input High voltage	1.8		5.5	V
V_{ILGP}	GPIO Input Low voltage			1.0	V
V_{OHGP}	GPIO Output High voltage	2.4		V_{DD}	V
V_{OLGP}	GPIO Output Low voltage			0.4	V
I_{OHGP}	GPIO Output High Current Port E5 and Port E6 only			24 60	mA
I_{OLGP}	GPIO Output Low Current Port E5 and Port E6 only			16 40	mA
V_{IHAn}	Analog Input High voltage	1.8		$V_{2.5}$	V
V_{ILAN}	Analog Input Low voltage			1.0	V
V_{OHAn}	Analog Output High voltage	2.4		$V_{2.5}$	V
V_{OLAn}	Analog Output Low voltage			0.4	V
I_{OHAn}	Analog Output High Current			6	mA
I_{OLAn}	Analog Output Low Current			6	mA
$V_{2.5}$	Internal 2.5 V monitor and Reference	2.37	2.5	2.75	V
$I_{V2.5}$	Reference 2.5 V output current			25	mA
SV_{DD}	DV_{DD} slew rate to ensure Power-On Reset	0.05			V/ms

2.11.3 AC Electrical Characteristics – Receiver

Table 12. RF Performance Receive Sensitivity

Data Rate	Sensitivity
11.0 Mb/s	-82 dBm
5.5 Mb/s	-86 dBm
2.0 Mb/s	-88 dBm
1.0 Mb/s	-90 dBm

2.11.4 AC Electrical Characteristics – Transmitter

Transmit power is managed by the Module automatically. The maximum transmit output power is typically +15 dBm.

2.11.5 Performance/Range

Table 13 shows the typical data rates, performance, and range the Module can provide with an omnidirectional antenna.

Table 13. Performance/Range*

Wireless Data Rate	Indoor Distance	Outdoor Distance (Max)
11.0 Mb/s	30 – 100 m	300 m
5.5 Mb/s	32 – 107 m	330 m
2.0 Mb/s	35 – 115 m	375 m
1.0 Mb/s	40 – 130 m	400 m

* Ranges are based on signal-to-noise ratio and performance estimates.

Note:

- Wireless Data Rate is the raw rate provided over the wireless link and does not represent the throughput data rate of the Module.
- Indoor Distance is “Office Environment.”
- Outdoor Distance is “Open Field.”

CHAPTER 3
RECOMMENDED LAYOUT PRACTICES

3.1 OVERVIEW

This chapter contains recommended layout practices. Topics covered in this chapter include:

- 3.2 Module Mounting Guidelines (below)
- 3.3 Circuit Board Layout Practices (below)
- 3.4 EMI/RFI Guidelines (page 26)

3.2 MODULE MOUNTING GUIDELINES

Special care must be observed when placing the Airborne WLN Module. In particular:

- The antenna must not be mounted below any other printed circuit boards, components, or metallic housing.
- The proximity of the antenna to large metallic objects can affect the Module's range and performance.
- Packaging and enclosure designers must carefully review the placement of the Module in the enclosure and the placement of the antenna to minimize interference or blocking sources.
- The mounting screw for the module is a Pan Head Torx Screw for Plastic Zinc-Plated Steel, 0-42 Thread, 3/8" Length.
- For mechanical clearance, performance, and emissions reasons, there should be no components placed on the main printed circuit board facing the Module. This region should be clear of components, as indicated by the clear area in Figure 8 on the next page.

3.3 CIRCUIT BOARD LAYOUT PRACTICES

When considering capacitance, calculations must take into account all device loads and capacitance due to printed circuit board traces. Capacitance due to the traces depends on a number of factors, including the trace width, dielectric material from which the circuit board is made, and proximity to ground and power planes.

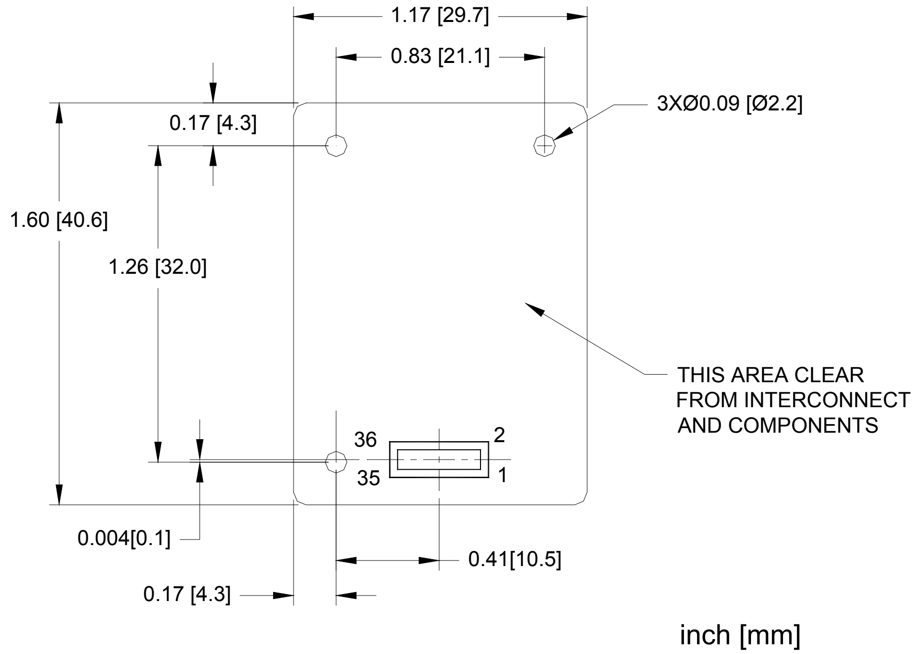


Figure 8. Guidelines for Mounting the Airborne WLN Module

3.4 EMI / RFI GUIDELINES

To minimize electromagnetic interference (EMI) and radio-frequency interference (RFI), pay strict attention to power and signal routing near the Module. As much as possible, the keep-clear area below the Module should be a solid copper ground plane. It is anticipated that the Module will be mounted on a board with a committed ground plane. Ensure that the interconnect has a designed impedance of 50-75 Ohms.

To keep signal impedance as low as possible, connect the ground plane to internal ground planes by several vias. Ground signals to the Module connector should connect directly to the ground plane below the Module. Individual ground connections to the Module should have a solid ground connection, preferably directly to the ground plane on the same surface side where the Module resides. Do not connect ground pins directly to an inside layer ground plane using vias.

Keep interconnects from the Module connector as short as possible on the mounting layer. All inboard signals must immediately transition to a different routing layer using a via as close to the connector as possible. Outboard signals (odd pin numbers) should also be kept to a minimum length.

3.5 ASLIP

ASLIP (Airborne Serial Line IP) is a simple packet framing protocol: ASLIP defines a sequence of characters that frame IP packets on a serial line, and nothing more. It provides no addressing, packet type identification, error detection/correction or compression mechanisms. Because the protocol does so little, though, it is usually very easy to implement. ASLIP functionality is enabled via the command line interface.

3.5.1 Protocol

The proposed ASLIP protocol defines four special characters:

Table 14. ASLIP Characters

Character	Definition
START	0xC1 (decimal 193)
END	0xC0 (decimal 192)
ESC	0xDB (decimal 219)

- Each data packet sent will begin with the START character.
- Each data packet sent will end with the END character.
- The ESC character is inserted by the transmitter to indicate that the following byte is a literal data byte. The receiver removes the ESC character and passes the following byte as data without interpretation.
- If the data packet contains a character the same as the END character a two-byte sequence of ESC and END is sent instead.
- If the data packet contains a character the same as the START character a two-byte sequence of ESC and START is sent instead.
- If the data packet contains a character the same as the ESC character a two-byte sequence of ESC and ESC is sent instead.
- ASLIP is applicable only in data pass-through mode.
- If the data packet contains a START character between a START and END sequence, it will be treated as an END START sequence i.e. all data preceding the START will be sent as a data packet and a new data packet will be started.

3.5.2 Packet Transfer

Each datagram received across the serial line will be sent as a separate IP packet from the wireless interface.
Each IP packet received on the wireless interface will be identified as a separate datagram, using the above protocol across the serial interface.

3.5.3 Platform

The above protocol will be implemented on the Airborne WLN UART v4 WPA only firmware platform.
It will be designed to be portable to the Airborne WLN UART 802.11g product.

3.6 WPA-LEAP SECURITY

The WPA and LEAP software modules provide advanced security configuration and communication services required by today's enterprise-class deployments.

Please refer to IEEE standard 802.1X 2001 (section 4) and IEEE standard 802.11i 2004 (section 4) for additional information.

3.6.1 Terminology

- "4-Way Handshake" refers to a connection method where each side of the connection acts independently (four packets are exchanged between the supplicant and the authenticator) and is required to successfully complete the WPA authentication process.

- "Authentication Server" refers to an entity providing authentication service to the authenticator. It may be co-located with an authenticator (e.g., as in a Cisco 1200 Access Point), but is usually an external server (e.g., RADIUS).

- "Authenticator" refers to the entity that requires the entity on the other end of the link to be authenticated.

- "EAP" refers to Extensible Authentication Protocol, a general protocol supporting multiple authentication methods used between the client and the authenticator. The 802.1X standard specifies encapsulation methods for transmitting EAP messages so they can be carried over different media.

- "EAPOL" refers to EAP over LAN, an 802.1X delivery mechanism used in authentication. EAPOL encapsulates EAP messages between the supplicant and the authenticator.

- "ESS". Each set of wireless devices communicating directly with each other is called a basic service set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). A Service Set Identifier (SSID) is the 1-32 byte alphanumeric name given to each ESS.

- "IEEE 802.1X" refers to the IEEE standard for port-based network control. 802.1X provides multiple methods to authenticate devices attached to a LAN port and functions with both wired and wireless LAN media. 802.1X is based on the Extensible Authentication Protocol (EAP), and features dynamic distribution and management of session keys. A RADIUS server is required for this security standard.

- "IEEE 802.11i" refers to the IEEE security standard officially ratified in June 2004 as part of the 802.11 family. 802.11i was tested and certified for interoperability by the Wi-Fi Alliance. In addition to improved encryption, this standard contains the 802.1X standard, improving key management and user authentication.

- "LEAP" refers to the Lightweight Extensible Authentication Protocol developed by Cisco. LEAP provides username/password-based authentication between a wireless client and a RADIUS server. It is one of several protocols used with the IEEE 802.1X standard for LAN port access control.

- "PSK" refers to Pre-Shared Key and is used in authentication. This is a shared key between the station and the AP and is entered as a passphrase.

- "RADIUS" refers to Remote Authentication Dial In User Service. A backend server that performs authentication using Extensible Authentication Protocol (EAP). This server is required by the IEEE 802.1X security standard.

- "Supplicant" refers to the entity being authenticated by the authenticator and desiring access to the services of the authenticator.

- "TKIP" refers to Temporal Key Integrity Protocol and is used in encryption. TKIP is an IEEE 802.11i standard and an enhancement to WEP security.

- "WLN", "WLN Module", or "Module" refers to the Airborne Wireless LAN Node Module.

- "WPA" refers to Wi-Fi Protected Access. It addresses all known Wired Equivalent Privacy (WEP) vulnerabilities. WPA uses RC4 for encryption and TKIP for key management. It includes a message integrity mechanism commonly called Michael or MIC.

- "WPA-LEAP" refers to "Wi-Fi Protected Access - Light Extensible Authentication Protocol", an implementation based on the IEEE 802.11i 2004 and IEEE 802.1X 2001 standards, which includes the LEAP protocol for initial key assignment.

- "WPA-PSK" refers to "Wi-Fi Protected Access - Pre-Shared Key", an implementation based on the IEEE 802.11i 2004 and IEEE 802.1X 2001 standards, where the PSK is stored on the client.

3.6.2 System Requirements

Both WPA and LEAP require radio firmware version 1.1.1.111.8.4 or later. The AP requires WPA support. LEAP must be supported in the AP or a separate authentication server.

3.6.3 Web Interface

The LEAP enabled firmware does not support a web interface.

Note: In this release, the blank character (space) may not be included in a passphrase, LEAP user name, or LEAP password.

3.6.5 Example Security Configurations

	If Configuring With CLI		If Configuring With the Web Interface
1	`wl-security wpa-psk<CR>`	`OK<CR><LF>`	Select wpa-psk as the "Security" option on the Network Services Configuration page, and then click SAVE.
2	`pw-wpa-psk <passphrase><CR>`	`OK<CR><LF>`	
3	`commit<CR>`	`OK<CR><LF>`	Enter your WPA passphrase on the Security Configuration page, and then click SAVE.
4	`restart<CR>`		Click RESTART on the Reset page, and then click OK (to reboot the Airborne device).
5	Module Restarts		

Figure 9 - WPA-PSK Security Configuration

	If Configuring With CLI		If Configuring With the Web Interface
1	`wl-security wpa-leap<CR>`	`OK<CR><LF>`	Not applicable.
2	`user-leap <username><CR>`	`OK<CR><LF>`	
3	`pw-leap <password><CR>`	`OK<CR><LF>`	
4	`commit<CR>`	`OK<CR><LF>`	
5	`restart<CR>`		
6	Module Restarts		

Figure 10 - WPA-LEAP Security Configuration

3.6.6 Computer Resource Requirements

WPA-PSK
In order to function properly, an Access Point that supports WPA-PSK must be available. The WPA-PSK passphrase installed on the Access Point must match the passphrase configured on the WLN.

LEAP
In order to function properly, a RADIUS server configured for LEAP containing usernames/passwords, and an Access Point that supports LEAP, must be available. The RADIUS server username and password must match the `user-leap` and `pw-leap` command values configured on the WLN.

3.6.7 System Implementation Considerations

The WLN must be in infrastructure mode for WPA-PSK or LEAP to operate properly. A WLN configured for WPA-PSK requires a connection to an AP with WPA-PSK enabled. A WLN configured for LEAP requires a connection to an AP with LEAP enabled and connected to a RADIUS server to provide authentication.

Until the WLN is authenticated by either the WPA-PSK enabled AP or the RADIUS server, no IP network communication can proceed.

Symptoms of an unauthenticated client include:

- A WLN with `serial-default` set to “PASS” will not connect to the network client.
- A WLN configured for DHCP will not obtain host configuration from the DHCP server; therefore, the IP address will remain `0.0.0.0`.
- The Link LED turns on when 802.11 association completes. However, if the 802.1X authentication fails, the WLN becomes disassociated by the AP and the Link LED turns off. In effect, the Link LED will blink slowly as the process repeats.
- The WLN will not respond to discovery requests.

Once the WLN is authenticated, additional impacts include:

- **Roaming**
  A WLN configured for WPA-PSK can only roam to APs that have WPA-PSK enabled in the same ESS.

  A WLN configured for LEAP can only roam to APs that support LEAP, roaming, and are connected to the same RADIUS server.

- **Data Throughput and Latency**
  Round trip latency may increase and overall throughput may decrease, due to the additional steps to encrypt or decrypt data.

- **Re-Keying**
  The session key may expire and the authentication process will be executed again causing streaming data to stop until a new key is authorized.

3.6.8 Migration

DPAC is currently supporting the WPA upgrade for existing Modules through customer-loaded firmware. Please contact DPAC Wireless Support for more details.

CHAPTER 4
SERIAL PERIPHERAL INTERFACE (SPI)

4.1 OVERVIEW

This chapter defines the DPAC Technologies Airborne SPI Module interface. The Host SPI interface is based on the Motorola SPI industry standard, which does not provide anything beyond a physical protocol.

4.2 SPI STANDARD SUPPORT SUMMARY

The SPI Module (WLN) supports Serial Peripheral Interface (SPI) data communications. SPI is an industry standard, synchronous, serial link. The SPI interface is for devices that operate at the higher data rates (see the Motorola standard for the full requirements).

The WLN operates as an SPI Slave device.

4.3 SPI HARDWARE CONFIGURATION

The Slave's MOSI needs to be setup by the Master on the first-edge (rising if Idle = Low, falling if Idle = High) following the assertion of /SS. Therefore, the Slave will sample its MOSI on the second-edge (transition).

The bit ordering of data coming into the SPI Slave is MSB-first for both transmit and receive.

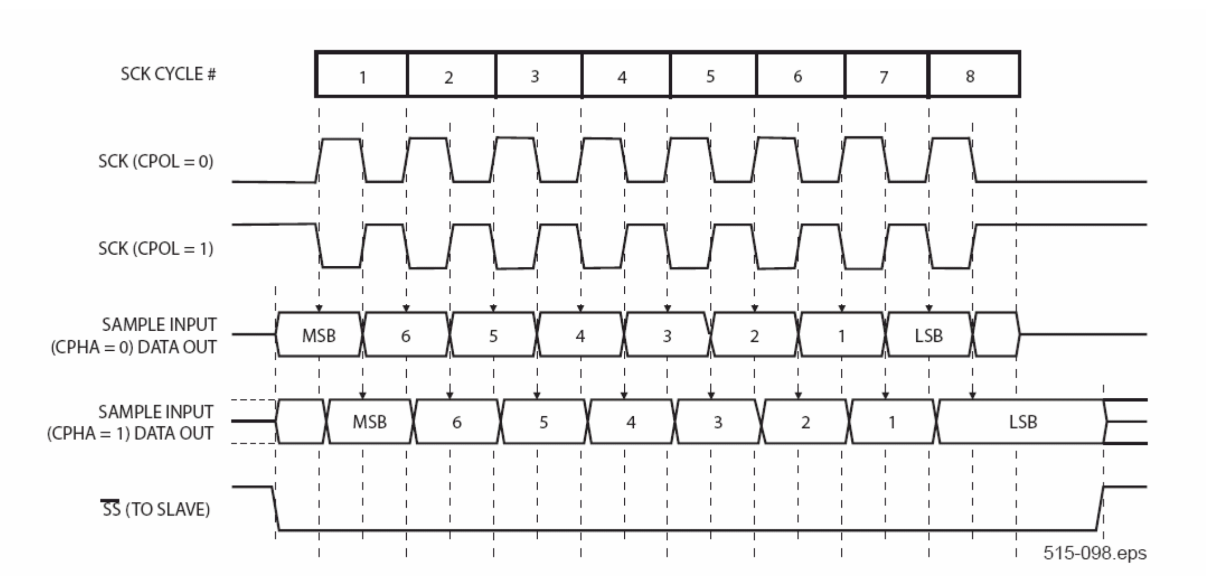


Figure 11. SPI Data Clock Timing

(Note additional information in section “2.9.2 SPI Design Guidelines” on page 18.)

4.4 SPI LOGICAL INTERFACE

4.4.1 SPI Read Configuration

The SPI Slave Status may be obtained by sending the Read Configuration command.

Read Configuration

Table 15. SPI Read Configuration Command

Command	Length	Value (0x40)
RCONF	1 Octet	Bit 7 = 0 Bit 6 = 1 Bits 5:0 = 0 (reserved, must be set to 0)

Response

The returned status is strictly informative and the Host should not assume that the Slave takes any particular action as the result of a status value sent. The following status values are currently defined – other values may be added in the future:

Bit 7	Slave Transmit Buffer:	1 – Data Available;	0 – Buffer Empty
Bit 6	Slave Receive Buffer:	1 – Ready for Data;	0 – Buffer Full
Bit 5	Slave Receive Interrupt Mask:	1 – Interrupt Enabled;	0 – Interrupt Disabled
Bit 4	Slave Transmit Interrupt Mask:	1 – Interrupt Enabled;	0 – Interrupt Disabled
Bits 3:0	Reserved for Future Use		

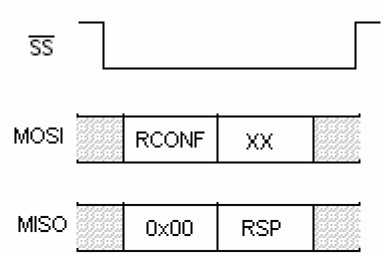


Figure 12. Read Configuration Timing Diagram

4.4.2 SPI Write Configuration

This is an obsolete command and is no longer available.

4.4.3 SPI Write Data

The SPI Master may write data to the Slave with the Write Data command.

Write Data Command

Table 16. SPI Write Data Command

Command	Length	Value (0x80)
WDATA	1 Octet	Bit 7 = 1 Bit 6 = 0 Bits 5:0 = 0 (reserved, must set to 0)

Response

Length (2 Octets) – This tells the Master the maximum number of octets that may be transmitted to the Slave.

After the Response has been received by the Master, the Master should then begin data transmission to the Slave.

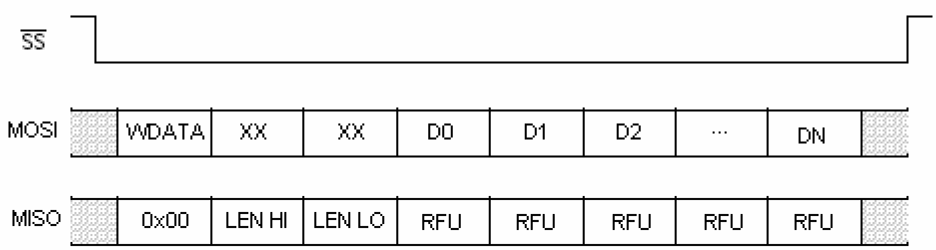


Figure 13. Write Data Timing Diagram

Note:

- RFU means "Reserved for Future Use" – any value may be returned.
- The data sent by the Master to the Slave is only processed by the Slave after /SS is de-asserted.

4.4.4 SPI Read Data

The SPI Master may read data when available by sending the Read Data command.

Read Data Command

Table 17. SPI Read Data Command

Command	Length	Value (0x00)
RDATA	1 Octet	Bit 7 = 0 Bit 6 = 0 Bits 5:0 = 0 (reserved, must set to 0)

Response

Length (2 Octets) – This tells the Master the number of octets that are waiting to be transmitted to the Master.

Data (N Octets, N being the Length) – The data will be sent to the Master immediately after the Length is sent.

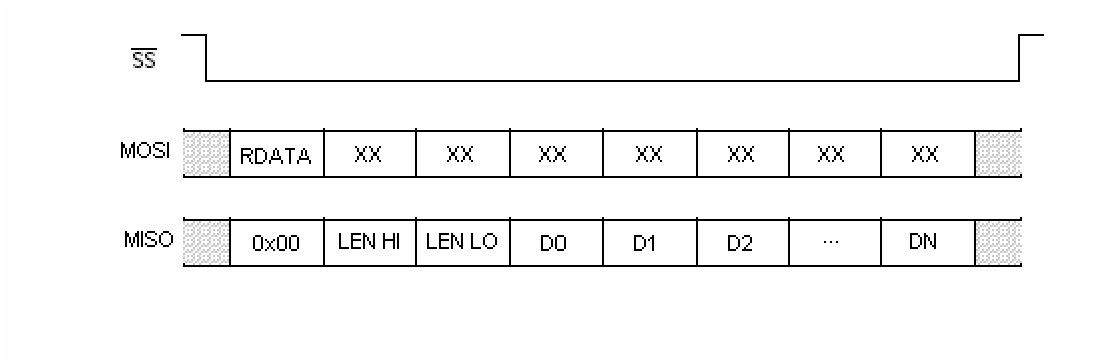


Figure 14. Read Data Timing Diagram

Note:

- Data is transferred as long as /SS is asserted. Flow control for transmissions from the Slave to the Master may be implemented by having the Master assert and de-assert the /SS line. If /SS is de-asserted, the transmission from the Slave will be halted, and the next RDATA command will cause the Slave to continue transmitting data starting at the byte after the byte on which the previous transmission was halted

CHAPTER 5
WEB INTERFACE

5.1 OVERVIEW

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

- 5.2 Accessing the Web Interface (below)
- 5.3 Navigating through the Web Interface (page 40)
- 5.4 Status Page (page 40)
- 5.5 WLN UART MODEL ONLY — Serial Interface Configuration Page (page 42)
- 5.6 WLN SPI MODEL ONLY — Serial Interface Configuration Page (page 45)
- 5.7 General Purpose I/O Settings Page (page 46)
- 5.8 Network Services Configuration Page (page 47)
- 5.9 WLN UART MODEL ONLY — Miscellaneous OEM Settings Page (page 49)
- 5.10 WLN SPI MODEL ONLY — Miscellaneous OEM Settings Page (page 51)
- 5.11 Wireless Network Configuration Page (page 52)
- 5.12 Security Configuration Page (page 56)
- 5.13 Firmware Update Page (page 58)
- 5.14 Reset Page (page 60)

5.2 ACCESSING THE WEB INTERFACE

Use your Web Browser to access the Web interface. The Module's built-in security requires you to log in with your user name and password (see Figure 15).

Figure 15. User Name and Password Screen

Note: The factory-default OEM user name is **oem** and the factory-default OEM password is **oem**. After you log in to the Web interface, we recommend that you use the Security Configuration page to change the default OEM user name and password (see page 49).

5.3 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.

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

5.4 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 Module's version number, 802.11 status, network settings, and resources.

Parameters to note in this screen are:

- **MAC address** is MAC address of the Module.
- **BSSID** is the MAC address of the associated Access Point (AP).
- **Communications Quality**, **Signal Level**, and **Noise Level** are in dBm.

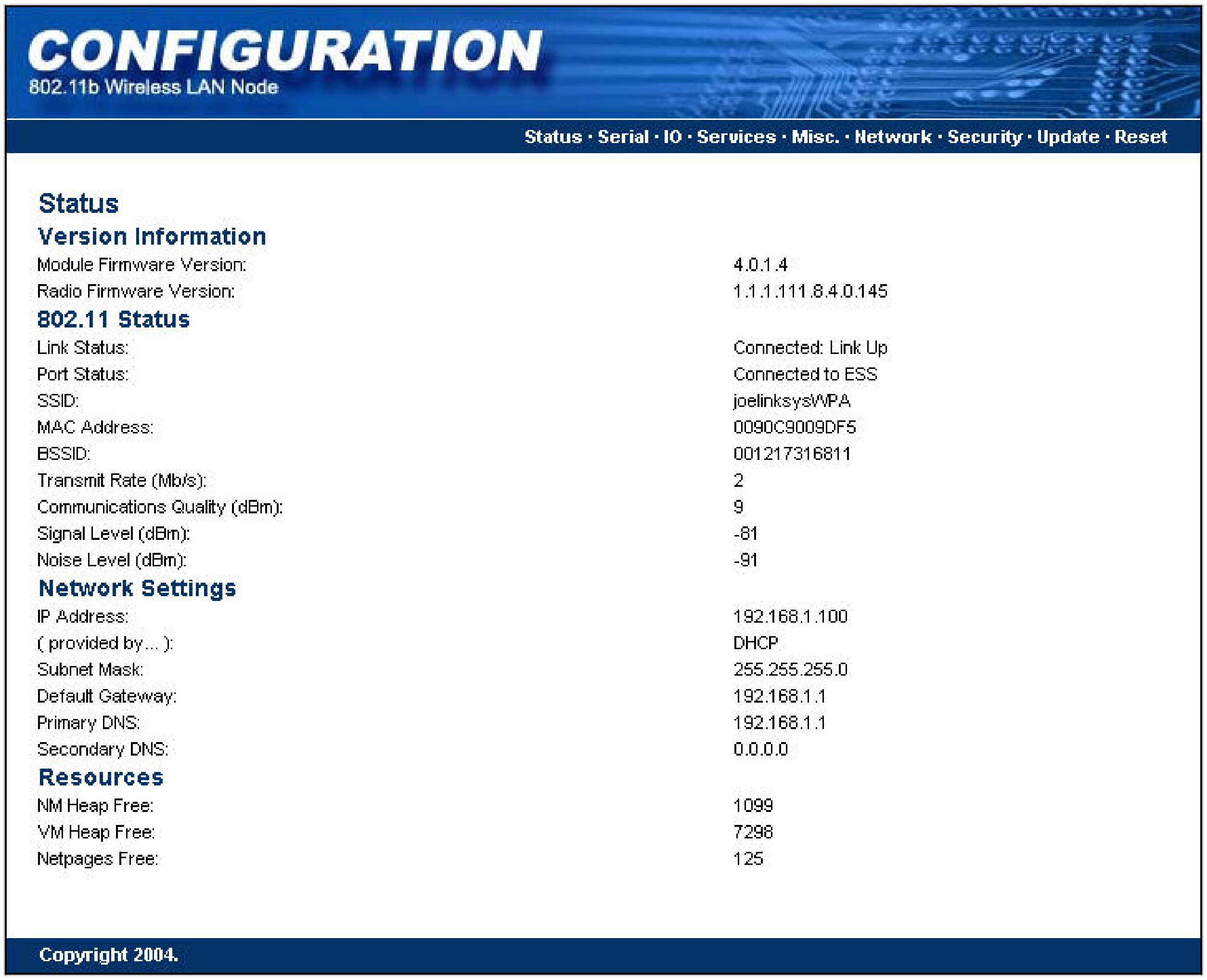


Figure 16. Status Page

5.5 WLN UART MODEL ONLY — SERIAL INTERFACE CONFIGURATION PAGE

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

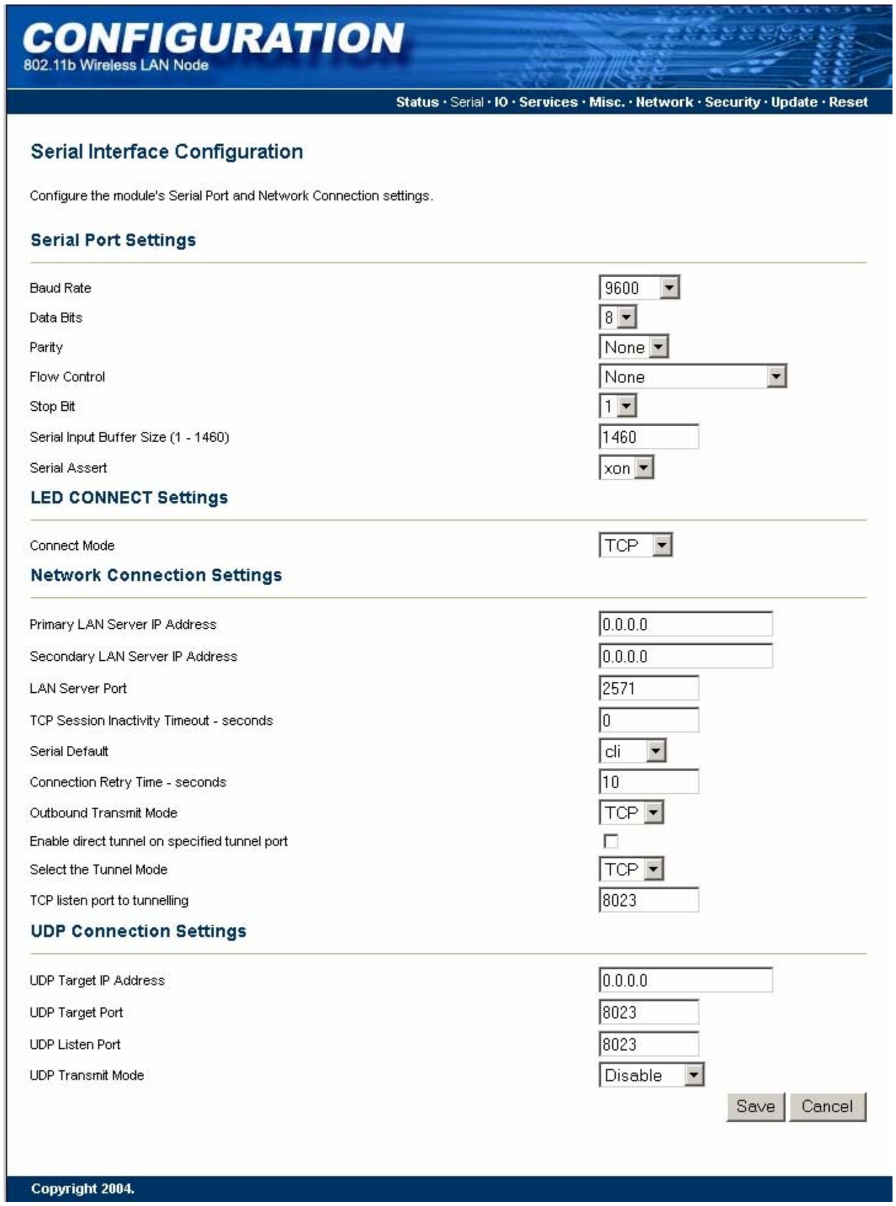


Figure 17. WLN UART Model Only — Serial Interface Configuration Page

Table 18. WLN UART Model Only — Serial Interface Configuration Settings

Parameter	Description
Serial Port Settings	
Baud Rate	`300 – 921000` 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 Module 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 Module 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 Module 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 Module enters as seen by the attached Serial Host device: • `listen` = Module "listens" for connections from LAN-based devices and applications. • `pass` = Module tries to connect to the LAN server at the IP address and port defined above, and enters pass-through mode. • `cli` = Module accepts CLI commands from the Serial Host (*default*).

Connection Retry Time - seconds	Specifies the number of seconds the Module 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 module 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`.

5.6 WLN SPI MODEL ONLY — SERIAL INTERFACE CONFIGURATION PAGE

The WLN SPI Serial Interface Configuration page is very similar to the WLN UART Serial Interface Configuration page and differs only in the following area:

- **Serial Port Settings**: area does not exist (*not applicable*—see Table 18 on page 43)

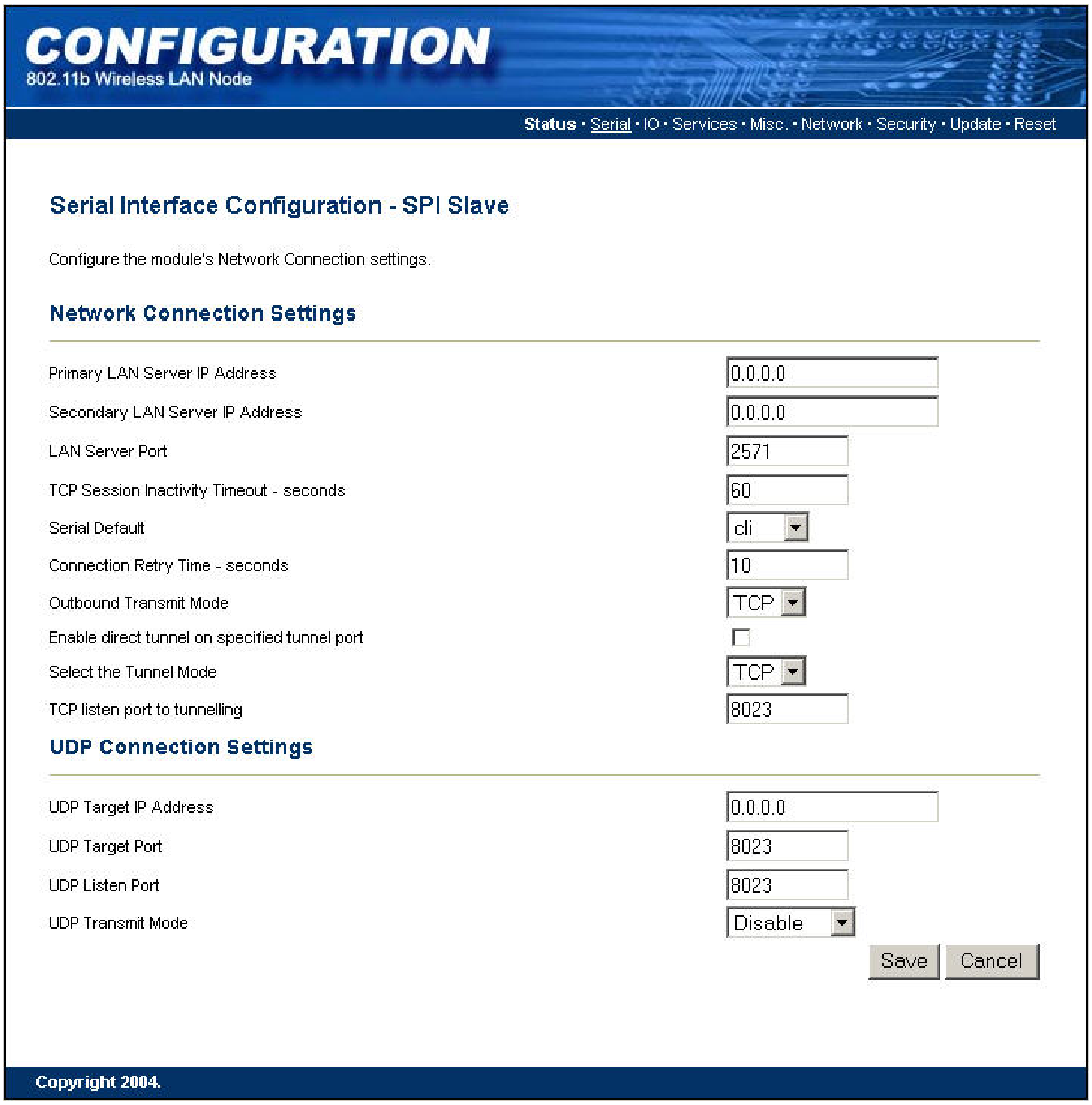


Figure 18. WLN SPI Model Only — Serial Interface Configuration Page

5.7 GENERAL PURPOSE I/O SETTINGS PAGE

Clicking the **IO** link in the menu bar displays the General Purpose I/O Settings page. This page lets you configure the data direction of ports E and G on the Module by entering hexadecimal values. Each hexadecimal value represents an 8-bit register, with each bit representing a data direction: 0 = output and 1 = input. The default value for all ports is FF hexadecimal. This page also lets you enable or disable I^{2}C support.

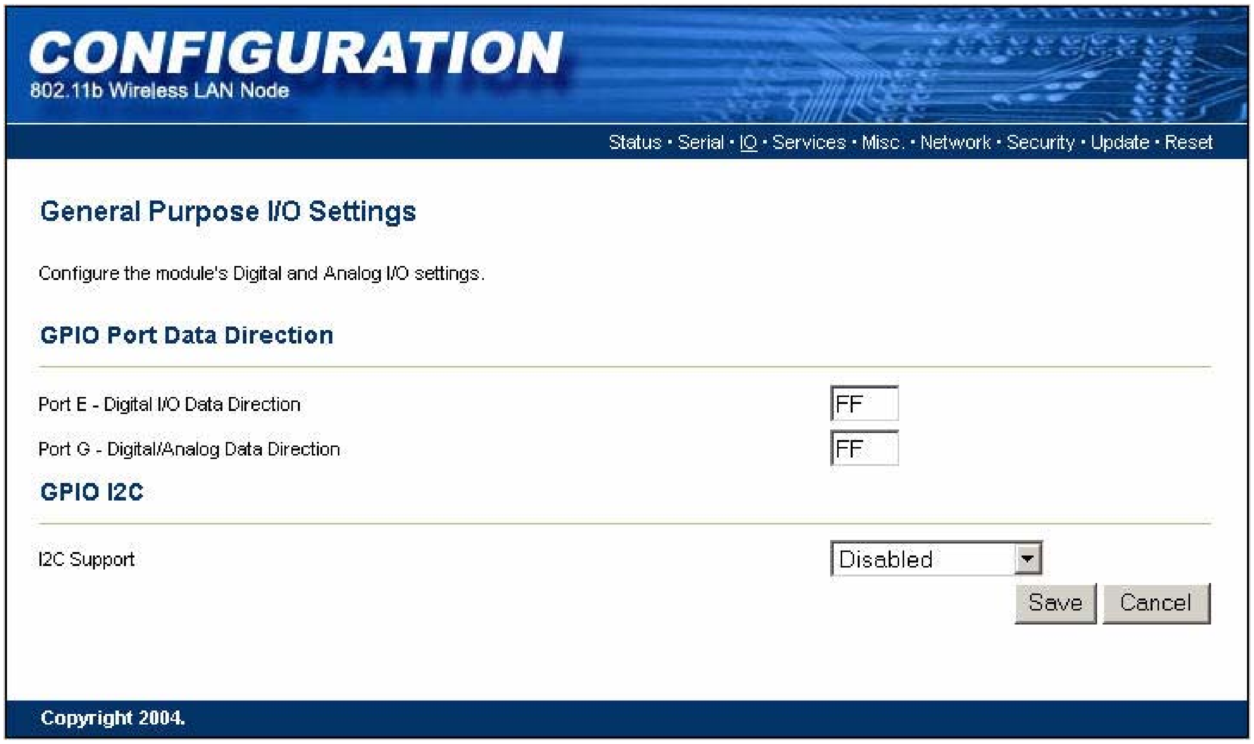


Figure 19. General Purpose I/O Settings Page

Table 19. General Purpose I/O Settings

Parameter	Description
GPIO Port Data Direction	
Port E – Digital I/O Data Direction	Indicates the data direction (input or output) for port E. Default is `FF` hex (ports E0 – E7 are input).
Port G – Digital/Analog Data Direction	Indicates the data direction (digital or analog) for port G. Setting it to 1 configures port G to an input. Setting it to 0 configures port G to a digital output. Default is `FF` hex (ports G0 – G7 are input).
GPIO I2C	
I2C Support	Lets you enable or disable I^{2}C support. • `Enabled` = Module is configured for I^{2}C support. • `Disabled`= Module is not configured for I^{2}C support. (*default*)

5.8 NETWORK SERVICES CONFIGURATION PAGE

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

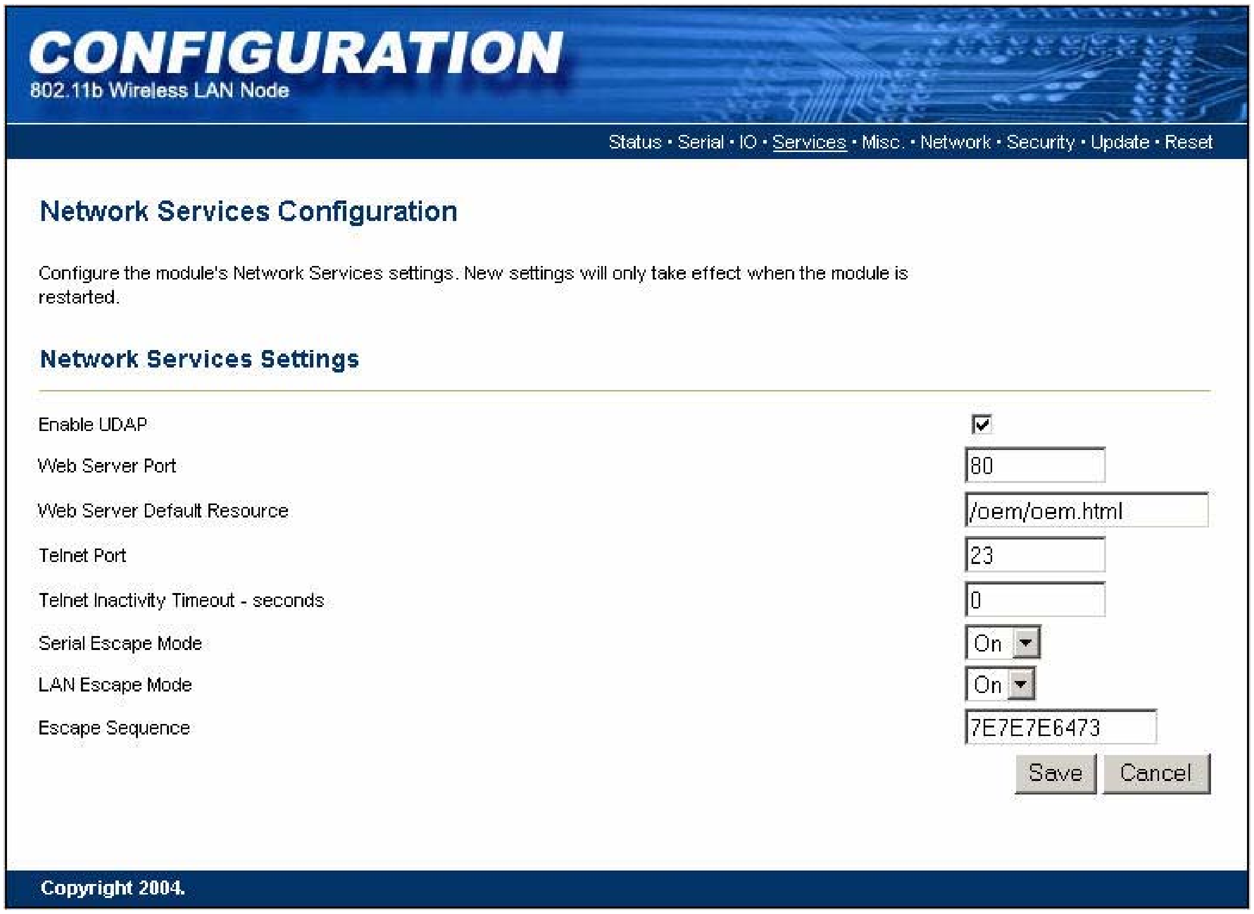


Figure 20. Network Services Configuration Page

Table 20. Network Services Configuration Settings

Parameter	Description
Enable UDAP	When *checked*, enables Universal Data Appliance Protocol (UDAP). This allows the Module 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 Module recognizes or ignores the escape sequence in the data stream. • `On` = Module always looks for the escape sequence in the data stream and reacts to it. • `Off` = Module ignores the escape sequence, allowing the sequence to be embedded in the data stream without concern about having the Module 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 Module'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.

5.9 WLN UART MODEL ONLY — MISCELLANEOUS OEM SETTINGS PAGE

Clicking the **Misc** link in the menu bar displays the Miscellaneous OEM Settings page. In this page, you can enter the Module's OEM version string and discovery name. This page also lets you specify the OEM user name and password, and activate a power-management mode.

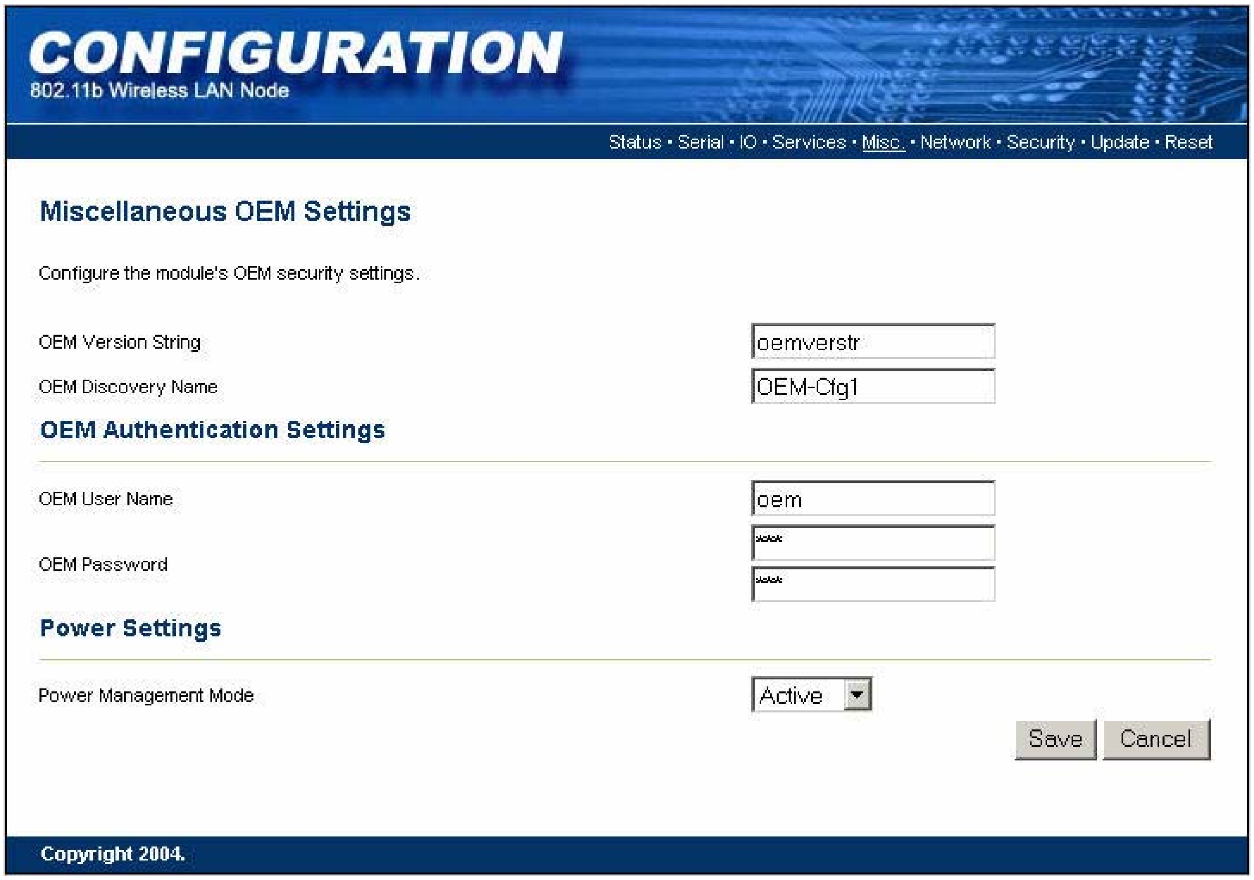


Figure 21. WLN UART MODEL ONLY — Miscellaneous OEM Settings Page

Table 21. WLN UART MODEL ONLY — Miscellaneous OEM Settings

Parameter	Description
Miscellaneous OEM Settings	
OEM Version String	Specifies the OEM version string to be associated with the Module. Default is `oemverstr`.
OEM Discovery Name	Specifies the OEM discovery name to be associated with the Module. Default is `OEM-Cfg1`.
OEM Authentication Settings	
OEM User Name	Specifies the name of the OEM, from 1 to 31 alphanumeric characters. Name is case-sensitive. Default is `oem`.
OEM Password	Two fields where you type and retype the OEM password, from 1 to 31 alphanumeric characters. Password is case-sensitive. For security, each password character appears as an asterisk. Default is `oem`.
Power Settings	
Power Management Mode	Lets you enable or disable the following power-management modes for the Module: • `Active` *(default)* • `Doze` • `Snooze` • `Sleep` • `Off`

5.10 WLN SPI MODEL ONLY — MISCELLANEOUS OEM SETTINGS PAGE

The WLN SPI Miscellaneous OEM Settings page is very similar to the WLN UART Miscellaneous OEM Settings page and differs only in the following area:

- **Power Settings**: area does not exist (*not applicable*).

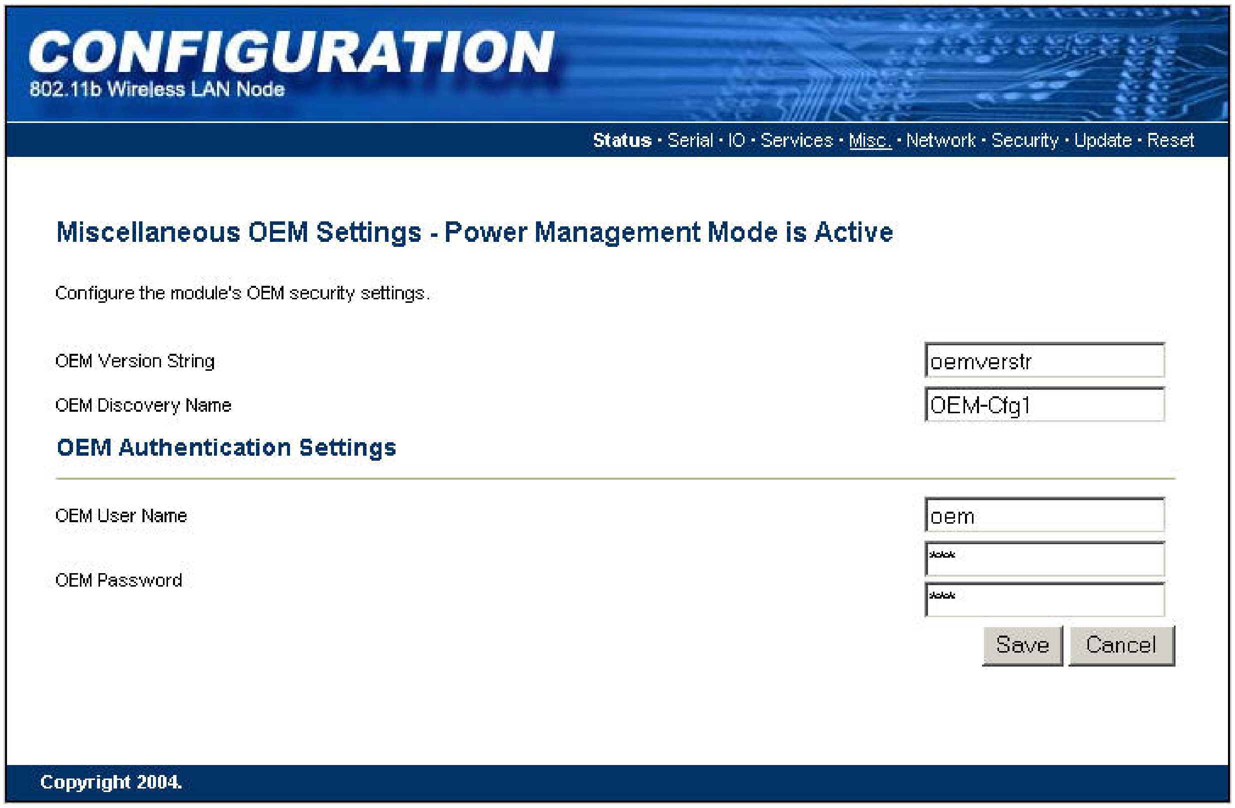


Figure 22. WLN SPI MODEL ONLY — Miscellaneous OEM Settings Page

5.11 WIRELESS NETWORK CONFIGURATION PAGE

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

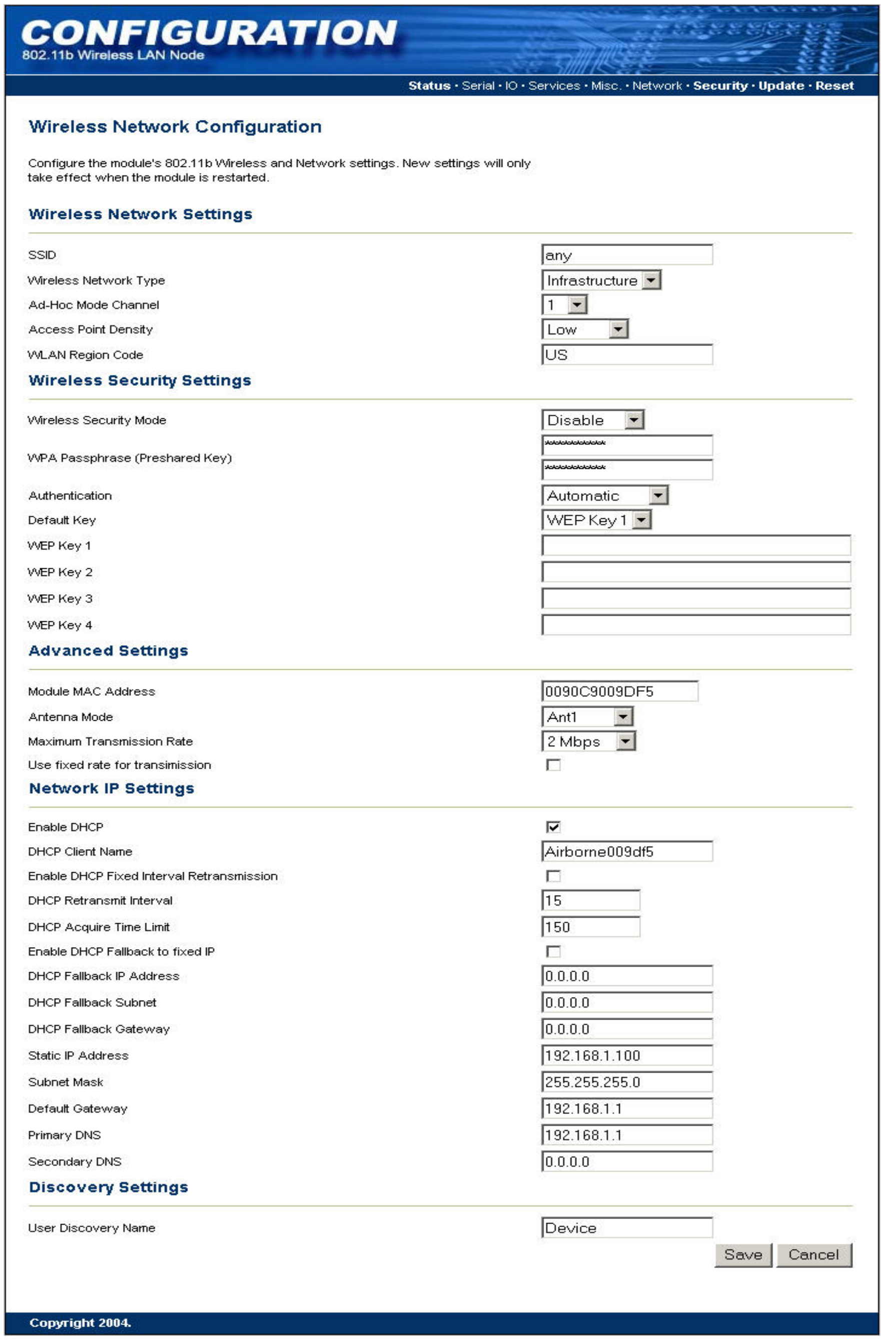


Figure 23. Wireless Network Configuration Page

Table 22. Wireless Network Configuration Settings

Parameter	Description
Wireless Network Settings	
SSID	Service Set Identifier that identifies the Module to connect to an AP. To make this connection, the Module 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 Module 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 Module to look for an AP with which it can maintain the specified rate. A high setting causes the Module 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.
WLAN Region Code	**Module Operation Region** Specifies the wireless channels allowed. This setting only applies when the Module is operating in `Ad Hoc` mode. The AP controls the channel used during `Infrastructure` mode. Default is `US`.
Security Settings	
Wireless Security Mode	Configures the security settings. This command has the same effect as the wl-wep command. `Disable` = security is disabled. (*default*) `wep64` = 64-bit key length (sometimes refered to as 40-bit) `wep128` = 128-bit key length `wpa-psk` = WPA Pre-Shared Key `wpa-leap` = WPA CISCO LEAP

Parameter	Description
WPA Passphrase	**WPA-PSK** Configure with CLI: 1. `pw-wpa-psk <passphrase><CR>)` followed by `OK<CR><LF>` 2. `commit<CR>` followed by `OK<CR><LF>` Configure from Web: 1. Select wpa-psk as the "Security" option on the Network Services Configuration page, and then click SAVE 2. Enter your WPA passphrase on the Security Configuration page, and then click SAVE.
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`.
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	
Module MAC Address	Specifies the Module's MAC address. Default is factory set. Changing this value may cause unexpected results.
Antenna Mode	Selects the Module's antenna mode: • `Ant1` = uses antenna 1. (*default*) • `Diversity` = uses antenna 1 and antenna 2. Supports receive diversity only.
Maximum Transmission Rate	Specifies the Module's maximum wireless transmission rate. Default is `2 Mbps`.
Use Fixed Rate for Transmission	Sets the 802.11 behavior for Ad Hoc mode. If the `wl-fixed-rate` is set, the Module will indicate only the `wl-rate` value in its becons. This helps prevent Ad Hoc clients from constantly negotiating data rates. Default is `0`.
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 Module'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`.

Parameter	Description
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 `192.168.10.1`
DHCP Fallback Subnet	Sets the fallback subnet mask. Default is `255.255.255.0`
DHCP Fallback Gateway	Sets the fallback gateway address. Default is `0.0.0.0`.
Static IP Address	Specifies the Module'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 Module's subnet mask; up to four octets separated by a period. Default is `255.255.255.0`
Default Gateway	Specifies the Module'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 Module if `Enable UDAP` is *checked* in the Network Services Configuration page (see page 47). Default is `Device`.

5.12 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.

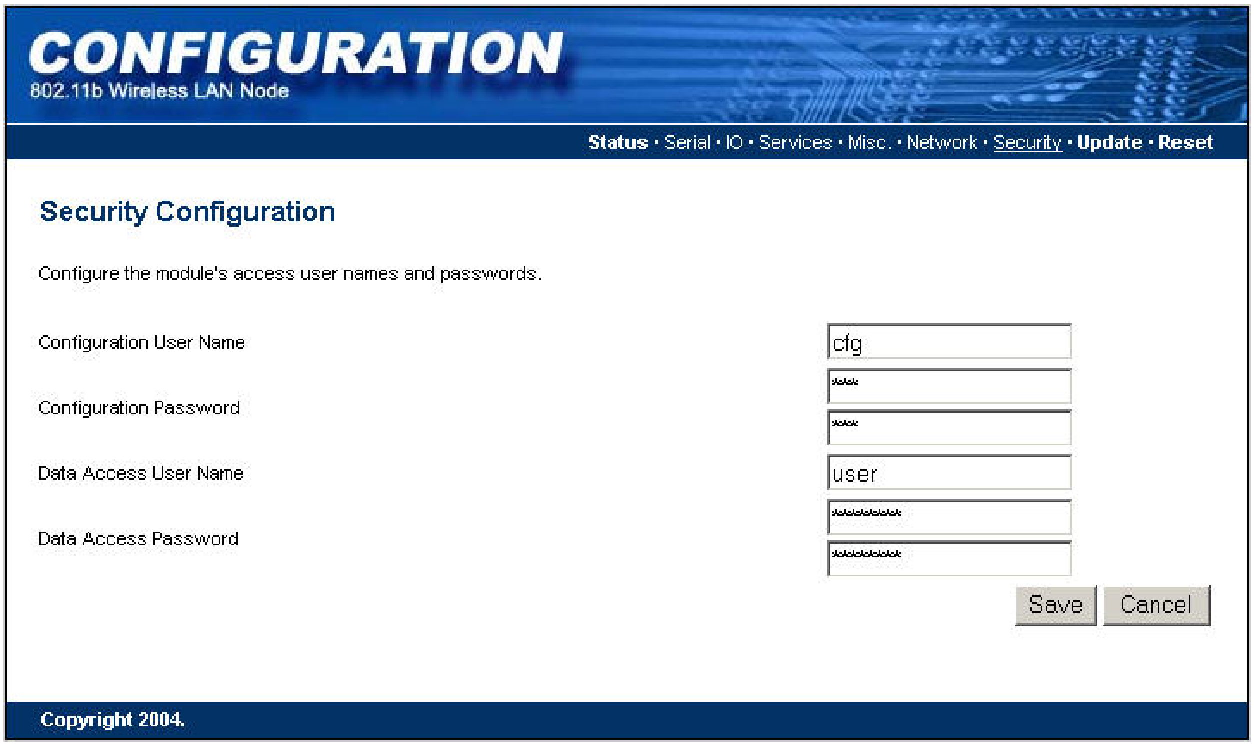


Figure 24. Security Configuration Page

Table 23. 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 Module. 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 Module, from 1 to 31 alphanumeric characters. Password is case-sensitive. For security, each password character appears as an asterisk. Default is `password`.

5.13 FIRMWARE UPDATE PAGE

Clicking the **Update** link in the menu bar displays the Firmware Update page (see Figure 25). This page lets you update the Module firmware.

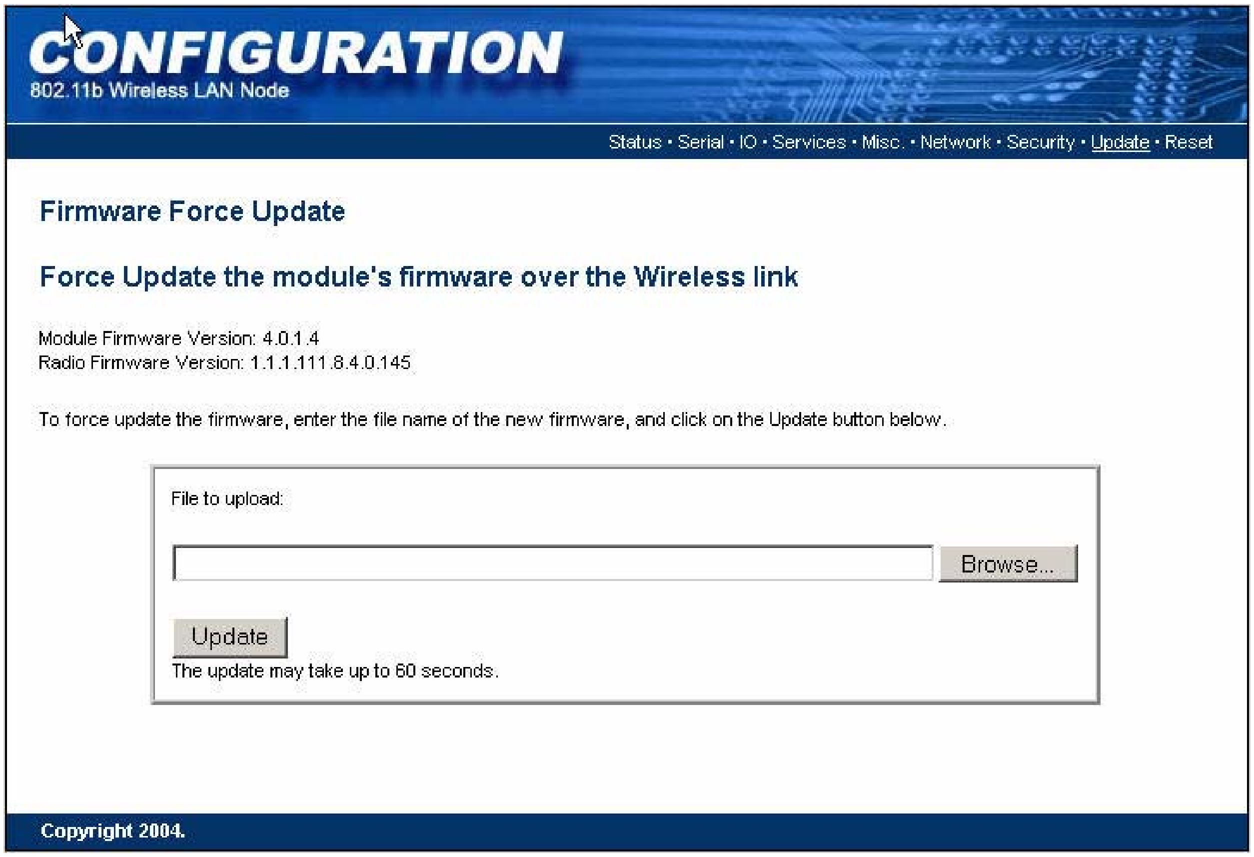


Figure 25. Firmware Update Page

Caution: Updating firmware may cause the Module to stop operating if it is not performed properly. Only advanced users should update firmware. If you encounter problems, contact DPAC Technologies.

Note: The firmware must come from DPAC Technologies as a `.bin` file and follow the file name format:

`AirborneFirmwarex.x.x.x.bin`

where `x.x.x.x` is the version number of the firmware. For example, the firmware file for the shown version of firmware is:

`DirectSerialFirmware3.0.2.1.bin`

To update firmware in the Module, use the following procedure:

- Obtain the updated firmware and make it accessible to a computer connected to the Module.
- In the menu bar at the top right of the page, click **Update**. The Firmware Update page appears (see Figure 25).
- Under **File to upload**, click the **Browse** button. Then navigate to the firmware file and double-click it. The path and name of the file appear to the left of the **Browse** button.
- Click the **Update** button to update the firmware. The message in Figure 26 appears, asking whether you are sure you want to reprogram the 802.11b interface using the new firmware file.

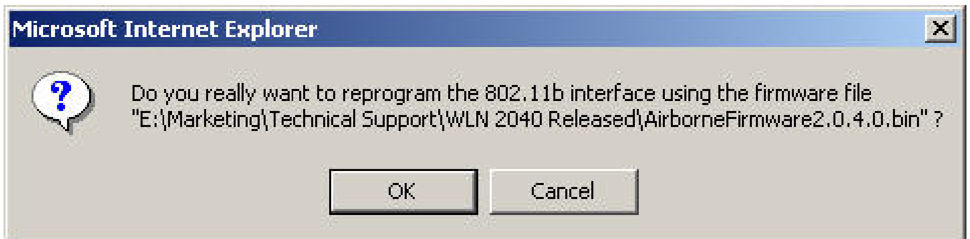


Figure 26. Warning Message Before Updating the Firmware

1. Click **OK** to update the firmware. This process can take up to 60 seconds (see Figure 27).

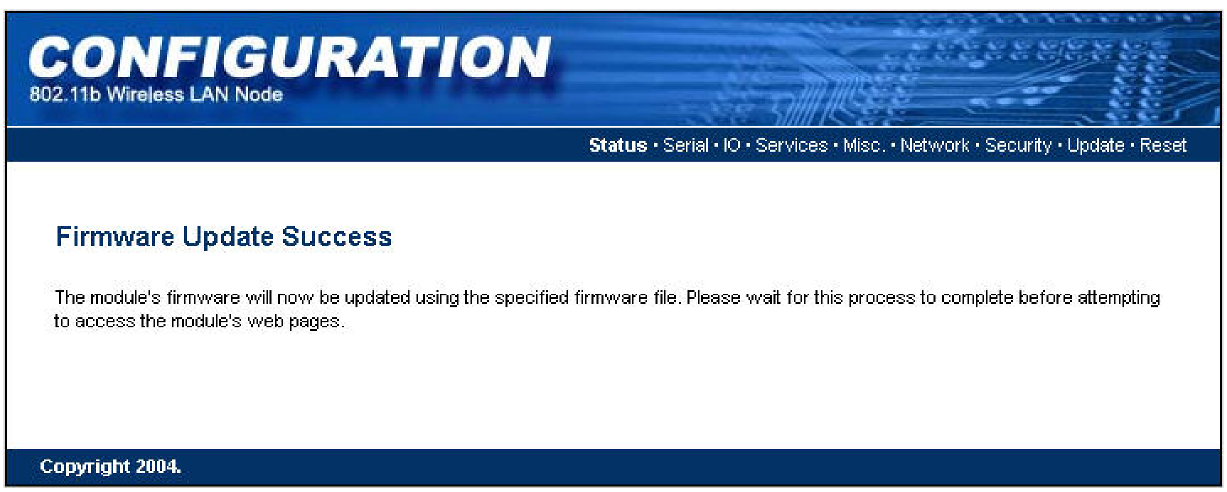


Figure 27. Firmware Update Success Message

5.14 RESET PAGE

Clicking the **Reset** link in the menu bar displays the Reset page (see Figure 28). This page provides a **Restart** button that lets you restart the Module. It also provides a **Defaults** button that discards your custom settings and returns the Module to its factory-default settings.

- If you click the **Restart** button, the screen in Figure 29 appears. Click **OK** to restart the Bridge or **Cancel** to not restart it.
- If you click the **Defaults** button, the screen in Figure 30 (on page 61) appears. Click **OK** to reset the Bridge to its factory-default settings or **Cancel** to not reset it.

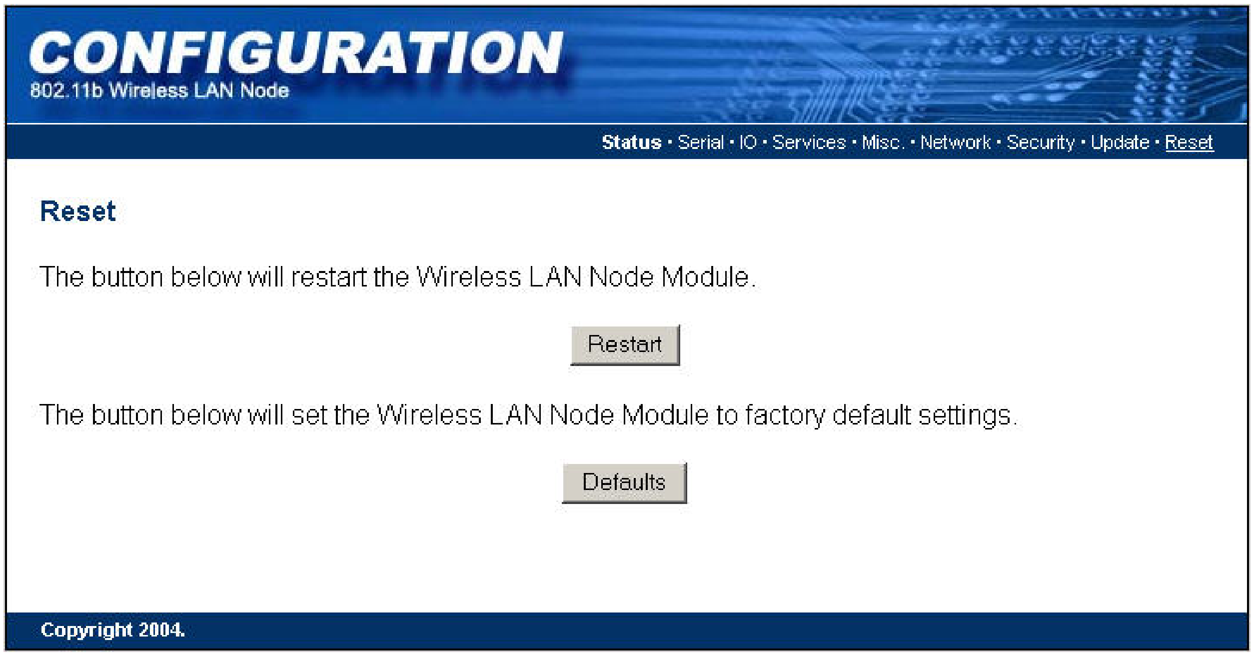


Figure 28. Reset Page

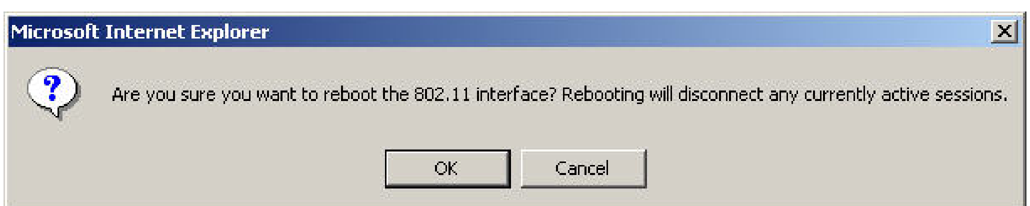


Figure 29. Warning Message After Clicking the Restart Button

Figure 30. Warning Message After Clicking the Defaults Button

This page intentionally left blank

A.1 OVERVIEW

This appendix describes issues associated with external power switches and illustrates a circuit for interfacing and controlling power to the Module from a 5 V system.

A.2 INTRODUCTION

Several applications, such as long-life battery-powered systems, require Wireless LAN Node (WLN) functionality in a limited-power environment, where there are long intervals between network accesses. When the system is inactive, an absolute minimum power draw from the Module is required. Unfortunately, the Module's low power modes are not always acceptable for these systems.

Other systems have safety or other issues that require a guarantee that the system will not be able to transmit. Since the Module's IEEE 802.11 MAC is under firmware control, the only fail-safe way to guarantee that the system cannot transmit is to disconnect the power.

Issues associated with powering-up systems may not be obvious. For example, the system is held in reset until after the power supply stabilizes, but active systems only see stable power supplies. Unexpected, even undesirable, actions can occur if power is applied to a capacitive circuit. When power is applied, instantaneous inrush currents often exceed 2 amps, even in small systems. Normally, this is not an issue at power-up; however, if a 5 Volt system, designed to accommodate a 500-mA load, gets an instantaneous 2-amp load, the system voltage droops. If this droop exceeds 500 mV, the system voltage exceeds specification and may cause errant operation, and can even reset the system.

This appendix describes how to design a circuit to power the Module safely in a live 5 V system. It addresses the requirements of the power supply and signal isolation, and the power dissipation requirements for an industrial-temperature system.

A.3 LOAD HOT SWAPPING

To understand the problems associated with adding fairly large loads into an active system, it is important to understand the characteristics of the inrush current. Figure 31 shows typical inrush characteristics from the Module. The lower trace is the voltage drop across a 0.82-Ohm resistor on the +5 V supply to the regulator. The upper trace is the Module's +3.3 V supply. The peak inrush current is I = (1.598)/(0.82) = 1.95 A. Adding the measurement resistor limits the inrush current to some extent. In several cases, inrush currents exceeding 2.2 A have been measured.

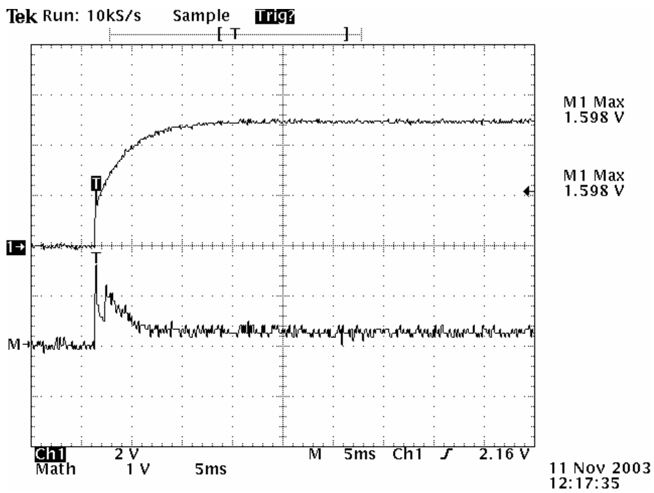


Figure 31. Inrush Current Characteristics

Since the Module's peak operating current is approximately 450 mA, the power budget for the Module is approximately the same. This is satisfactory for an always-on system. For an operating system, however, rapidly switching on the Module and its corresponding inrush requirement can cause system problems.

Figure 32 shows the inrush problem on a 5 V system with a current-limited supply. The lower trace is the system +5 V supply and the upper trace is the Module's +3.3 V supply. With the supply current limited at approximately 500 mA, the power supply falls to 4.16 V. In most systems, this causes a power-fail situation in which the system-supervisor device forces the Host system into reset.

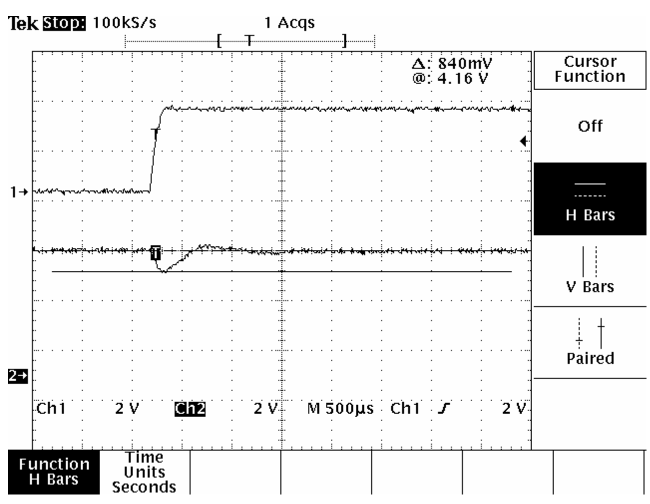


Figure 32. Voltage Droop with Current-Limited Supply

A.4 APPLICATION CIRCUIT

Figure 33 shows a recommended application circuit that can be used to obviate the harmful effects described in this appendix. Table 24 shows the parts associated with the recommended application circuit.

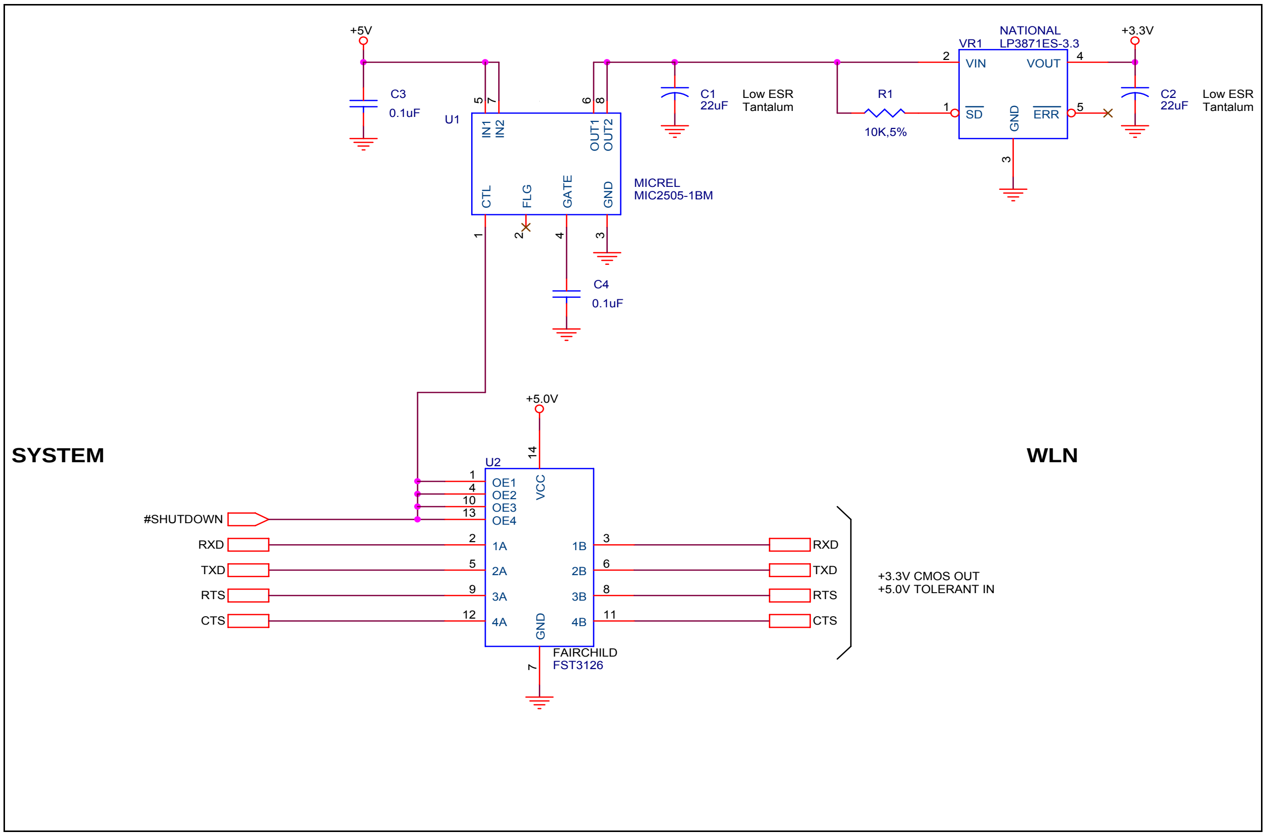


Figure 33. Recommended Application Circuit

Table 24. Parts List for Recommended Application Circuit

Ite m	Qty.	Ref. Des	Description	Manufacturer	Part Number
1	2	C1, C2	Cap, 22 µF, 6.3 V, Tantalum, Low ESR	AVX	TPSB226M06#0600 or equivalent
2	2	C3, C4	Cap, 0.1 µF, 0603, 16 v, Ceramic	Panasonic	ECJ-1VF1C104Z or equivalent
3	1	R1	Res, 10 K, 5%, 0603	Panasonic	ERJ3GEYJ103# or equivalent
4	1	U1	IC, High-side switch	Micrel	MIC2505-1BM
5	1	U2	IC, Bus Switch	Fairchild	FST3126
6	1	VR1	IC, Regulator	National	LP3871ES-3.3

A.4.1 High-Side Switch

The Micrel high-side switch is a single-channel power switch with slow turn-on characteristics. The device's slow turn-on acts as an inrush current limiter and prevents large current spikes from dropping the power supply rail.

Adding C4 (0.1 μF ceramic capacitor) on the GATE input of U1 slows the device's switching time. This slow turn-on of the switch, together with the internal current limiter of the MIC2505, acts as a current limiter to prevent the full impact of the inrush on the system. The chosen value of C4 sets the turn-on delay to approximately 375 ms.

A.4.2 Voltage Regulator

The voltage regulator, VR1, is an ultra-fast low-drop-out linear regulator. The device's high-speed characteristics are essential for the fast load-changes the Module requires when transmitting.

In this application, the regulator also provides a Power Supply Ripple Rejection Ratio (PSRR) between the +5 V input and the +3.3 V output of 73 dB (typical). This further isolates the Module transmitter and receiver from system noise.

It is important for the voltage regulator to have the proper input and output capacitors. The National LP3871 requires a minimum of 10 μF for each of the input and output capacitors, while the output capacitor requires an ESR of <5 Ω. When selecting an alternate voltage regulator, pay attention to the input and output load requirements.

In an extremely power-limited application, a Switch Mode Power Supply (SMPS) is preferred instead of the linear supply shown. The current linear regulator is approximately 66% efficient (2.4 W input to 1.6 W output). An SMPS tuned for the application can be more than 80% efficient, saving roughly 0.5 W that is currently being dissipated as heat in VR1.

A.4.3 Bus Switch

The Bus Switch, U1, guarantees that no signal will be applied to the Module when the power supply is shut down. Given the nature of CMOS input-protection devices (reverse-biased diodes from the input to VCC and GND), any signal on the input conducts through the input protection device onto VCC of the Module. While it may not provide enough current to operate the Module, it may provide sufficient power to prevent proper initialization and startup of the Module when power is applied.

While this circuit shows only the serial port signals (RXD, TXD, RTS, and CTS) being isolated, all signals between the Module and the system must be isolated using a similar device.

A.4.4 Circuit Performance

Figure 34 shows the characteristics of the implemented circuit. The lower trace is the system's +5 V supply, current limited at 500 mA. The upper trace is the Module's 3.3 V supply. The voltage sag on the +5 V system supply (lower trace) is limited to 0.24 V, keeping it within +5.0 ±5% range for proper system operation.

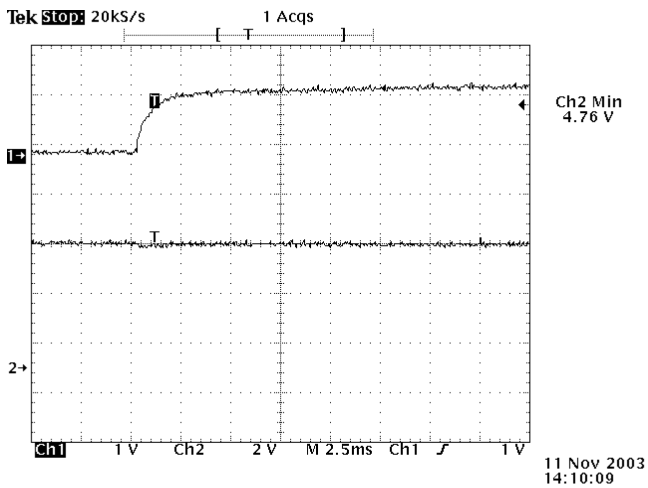


Figure 34. Circuit Soft-start Characteristics

A.4.5 Off Current

When the Module is shut down (#SHUTDOWN=0), the total current is given by:

$$I_{OFF} = I_{L\text{-}U1} + I_{L\text{-}U2}$$

Where the worst-case leakage currents are:

$$I_{L\text{-}U1} = 5\ \mu A$$
$$I_{L\text{-}U2} = 3\ \mu A$$

Giving a total leakage current of:

$$I_{OFF} = 5\ \mu A + 3\ \mu A$$
$$= 8\ \mu A$$

A.4.6 Thermal Characteristics

For industrial-temperature applications, ensure that all components will operate correctly over the entire -40°C to +85°C operating range. By design, the Bus Switch (U2) is guaranteed over the industrial temperature range. The High-Side switch (U1) and the Voltage Regulator (VR1), however, handle all the WLN current. Exercise care to ensure the devices stay within normal operating parameters.

The total power dissipation of U1 is given by:

$$P_D = (R_{ON})\, I_{OUT}^2 + (V_{IN})\, I_{LEAK}$$

For this application:

V_{IN}	= 5.25 V	(maximum of 5.0 ±5%)
R_{ON}	= 0.06 Ω	(maximum)
I_{OUT}	= 480 mA	(WLN data sheet maximum)
I_{LEAK}	= 5 µA	(MIC2505 data sheet maximum)

Giving a total power dissipation in U1 of:

$$\begin{aligned} P_D &= (0.06\ \Omega)\ 0.480^2\ \text{A} + (5.25\ \text{V})\ 5\ \mu\text{A} \\ &= 0.014\ \text{W} + 26\ \mu\text{W} \\ &= 0.014\ \text{W} \end{aligned}$$

The device junction temperature within U1 is given by:

$$T_J = T_A + \Theta_{JA}(P_D)$$

Rearranging for the ambient temperature:

$$T_A = T_J - \Theta_{JA}(P_D)$$

For this application:

T_J	= 125°C	(MIC2505 data sheet maximum)
ΘJA	= 160°C/W	(8-pin SOP package)

Giving a maximum ambient operating temperature for U1 of:

$$\begin{aligned} T_A &= 125°\text{C} – 160°\text{C/W}\ (.014\ \text{W}) \\ &= 122.8°\text{C maximum} \\ &\geq 85°\text{C} \end{aligned}$$

The total power dissipation of VR1 is given by:

$$P_D = (V_{IN} - V_{OUT})\, I_{OUT} + (V_{IN})\, I_{GND}$$

For this application:

V_{IN}	= 5.25 V	(maximum of 5.0 ±5%)
V_{OUT}	= 3.20 V	(minimum of 3.3 ±3%)
I_{OUT}	= 480 mA	(WLN data sheet maximum)
I_{GND}	= 15.0 mA	(LP3871 data sheet maximum)

Giving a total power dissipation in VR1 of:

$$P_D = (5.25\ \text{V} – 3.20\ \text{V})\ 0.480\ \text{A} + (5.25\ \text{V})\ 0.0150\ \text{A}$$

$= 0.984\ W + 0.079\ W$
$= 1.06\ W$

The device junction temperature within VR1 is given by:

$$T_J = T_A + \Theta_{JA}(P_D)$$

Rearranging for the ambient temperature:

$$T_A = T_J - \Theta_{JA}(P_D)$$

For this application:

$T_J = 125°C$ (LP3871 data sheet maximum)
$\Theta_{JA} = 35°C/W$ (TO-263 package mounted to 1-in^2 of 1-oz. copper)

Giving a maximum ambient operating temperature for VR1 of:

$T_A = 125°C – 35°C/W\ (1.06\ W)$
$= 87.9°C$ maximum
$\geq 85°C$

This application operates properly in an industrial-temperature environment.

This page intentionally left blank

IEEE 802.11 wireless nodes, like your Airborne WLN Module, 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.

Note: The available channels supported by wireless products in various countries are different.

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.

Table 25. 802.11b Channel Frequencies

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

This page intentionally left blank

APPENDIX C
WLN ETHERNET BRIDGE

C.1 OVERVIEW

The Airborne™ Wireless LAN Node Module (WLN) is available with firmware that provides Ethernet Bridge functionality. The Ethernet Bridge is designed to connect devices with wired Ethernet (10Base-T) connectivity to a LAN using the WLN Module's IEEE 802.11 Wireless LAN capability.

The Ethernet Bridge firmware changes the operation of the Wireless LAN Node Module to that of an Ethernet Bridge. Specific I/O ports on the Ethernet Bridge Module provide a 10Base-T Ethernet connectivity. The firmware is also used in the AirborneDirect™ Ethernet Bridge product. For the functionality of the AirborneDirect™ Ethernet firmware, see the AirborneDirect™ Ethernet User's Guide.

The Ethernet Bridge Module model number is:

WLNB-ET-DP101	Airborne™ Ethernet Bride Module

The Ethernet Bridge firmware enables the Wireless LAN Node Module to act as a transparent bridge between an Ethernet 10Base-T wired connection and a Wireless LAN connection. The Bridge conveys IEEE 802.3 Ethernet packets in either direction. The Bridge includes a TCP/IP stack, which provides for two ways to provision and configure the Bridge: (1) an HTTP web interface or, (2) by a TCP socket connection. The HTTP interface includes built-in web pages that allow the Bridge to be configured. The TCP server provides another way to configure the Bridge using the built-in Command Line interface (CLI). The Ethernet Bridge CLI includes a subset of the WLN CLI commands – please refer to the latest WLN CLI Reference Guide for a list of the applicable commands.

C.2 ETHERNET BRIDGE MODULE PIN ASSIGNMENTS

The Ethernet Bridge Module I/O connections are available through the Module's 36-pin Hirose connector, and are identical to the WLN Module with the following noted exceptions. Specific I/O lines are driven to provide 10Base-T interface functionality, and some of the status lines, typically used to drive LEDs, have modified operation. The following table indicates the Ethernet Module's significant I/O connections and their function.

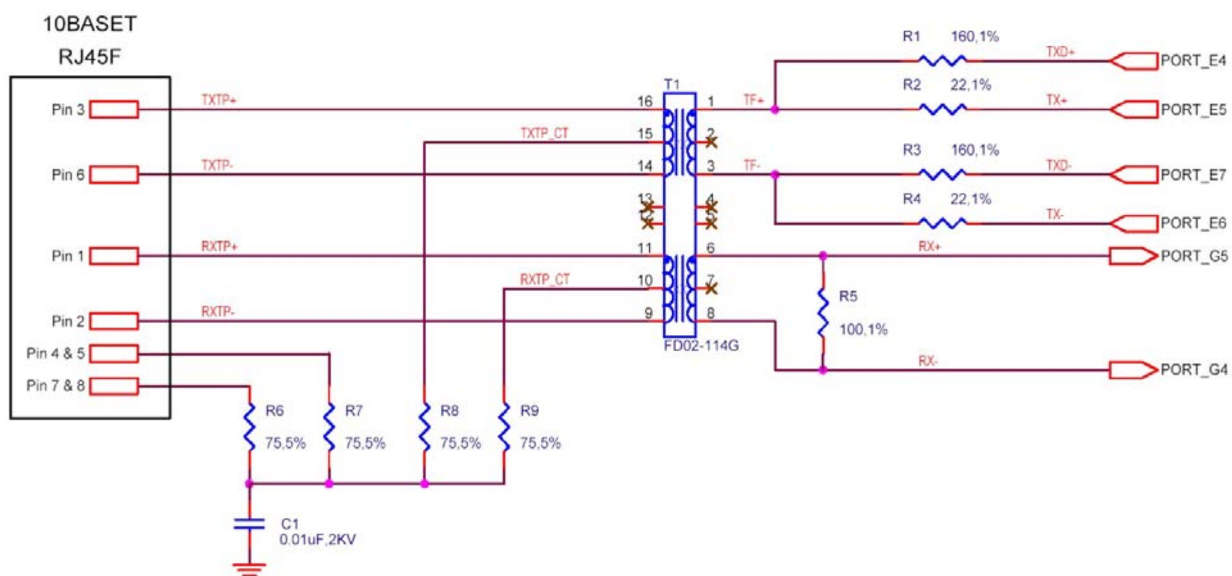
The remaining WLN I/O lines are not available for any other use since the Ethernet Bridge firmware does offer the capability to use them.

Table 26. WLN Module Ethernet-Specific Pin Assignments

WLN Pin	WLN Signal	Ethernet Signal	Direction	Description
14	G4	RX-	I	Differential negative side input
13	G5	RX+	I	Differential positive side input
32	E4	TXD+	O	Differential positive side output with pre-emphasis
30	E5	TX+	O	Differential positive side output
29	E6	TX-	O	Differential negative side output
31	E7	TXD-	O	Differential negative side output with pre-emphasis

I/O lines G4 and G5 are used as digital inputs and may not exceed 2.4V.
I/O lines E4 – E7 are used as digital outputs with outputs not exceeding 3.3V.

For proper interface with 10Base-T signals, it is recommended the I/O signals drive a transformer/filter as indicated in the following schematic. The RJ-45F connector is for reference and typically an embedded design will route the 10Base-T signals directly to the embedded host Ethernet connections.



T1 – recommended transformer/filter: Halo FD02-114G
C1 – use lower voltage part when 10Base-T connections are not made to external connector.

Figure 35. Recommended Magnetics Schematic

C.3 STATUS PORTS SIGNAL ASSIGNMENT

Table 27. WLN Ethernet Module Status Ports

Pin	Signal	Status	Description
25	F0	POST	Bridge passed Power-On-Self-Test, ready for operation
27	F2	RF LINK	Bridge has associated with an AP or ad hoc peer
26	F3	CONFIG	Bridge has obtained an IP address via DHCP or provided as Static
23	F6	CONNECT	A TCP socket connection from a WLAN or wired Client device has been made with the Bridge's TCP/IP stack
35	/RF_LED	RADIO ACTIVITY	Blinks when radio is not connected and is scanning Solidly on when radio is connected or associated

C.4 DESIGN GUIDELINES

In addition to the Design Guidelines specified for the Wireless LAN Node Module, the Ethernet Bridge Module should adhere to the following design guidelines:

- Make sure that **NO** copper and traces on all layers are present under the magnetics –prevents magnetic induction into the circuitry.
- Place R5 as close to the magnetics as possible.
- Place R1 as close to module as possible.
- All traces to and from the magnetics should be designed for an impedance of 100Ω.
- Keep the transmit traces separated from the receive traces, and where possible place the one or the other end on a different layer.
- Route differential pairs together and keep them parallel to one another. Also, do not separate them around parts or across PCB layers.

This page intentionally left blank

The following tables outline the steps to set-up a wireless cable replacement connection between two serial ports, using the Airborne WLN products. This connection relies upon a type of peer-to-peer wireless network call an AdHoc. This network type does not require an Access Point.

Table 28. Slave Configuration and Set-up

	Description	Setting	Webpage	CLI Command
1	Set the SSID of the unit to the name of the AdHoc network	AdHoc Network Name	Network	`wl-ssid AdHocNetwork`
2	Set network type to AdHoc (Infrastructure is default)	AdHoc	Network	`wl-type p`
3	Set AdHoc Channel	1	Network	`wl-chan 1`
4	Disable DHCP	Disable	Network	`wl-dhcp 0`
5	Assign a static IP	192.168.10.150	Network	`wl-ip 192.168.10.150`
6	Assign a network mask	255.255.255.0	Network	`wl-subnet 255.255.255.0`
7	Enable the Direct tunnel	Enable	Serial	`wl-tunnel 1`
8	Assign the tunnel port (8023 is the default and there is no need to change it)	8023	Serial	`wl-tunnel-port 8023`
9	Set the tunnel mode to TCP (this is default) - Assumes setting up a TCP/IP connection between the devices	TCP	Serial	`wl-tunnel-type tcp`

10	Configure the serial port settings to match the attached system	Baud Rate = 9600
		Data Bits = 8
		Parity = None
		Flow Control = Hardware (RTS/CTS)
		Stop Bits = 1
			Serial	`Bit-rate 9600`
				`data-bits 8`
				`parity n`
				`flow h`
				`stop-bit 1`

11	Set serial default mode to LISTEN (CLI is default)	Listen	Serial	`serial-default listen`
12	Save the settings and restart the unit.	Save and Restart	Reset	`commit` `restart`

Note: All parameters values are included for the purpose of demonstration only. Although valid, they should be changed to meet the application requirements.

Table 29 - Master Configuration and Set-up

	Description	Setting	Webpage	CLI Command
1	Set the SSID of the unit to the name of the AdHoc network	AdHoc Network Name	Network	`wl-ssid [AdHoc Network Name]`
2	Set network type to AdHoc (Infrastructure is default)	AdHoc	Network	`wl-type p`
3	Set AdHoc Channel	1	Network	`wl-chan 1`
4	Disable DHCP	Disable	Network	`wl-dhcp 0`
5	Assign a static IP (Slave address + 1)	192.168.10.151	Network	`wl-ip 192.168.10.151`
6	Assign a network mask	255.255.255.0	Network	`wl-subnet 255.255.255.0`
7	Set the Primary LAN Server IP Address to match the slaves static IP address	192.168.10.150	Serial	`wl-tcp-ip 192.168.10.150`
8	Set the LAN Server port to match the tunnel port on the slave	8023	Serial	`wl-tcp-port 8023`

9	Configure the serial port settings to match the attached system	Baud Rate = 9600
		Data Bits = 8
		Parity = None
		Flow Control = Hardware (RTS/CTS)
		Stop Bits = 1
			Serial	`Bit-rate 9600`
				`data-bits 8`
				`parity n`
				`flow h`
				`stop-bit 1`

10	Set serial default mode to PASS (CLI is default)	Pass	Serial	`serial-default pass`
11	Save the settings and restart the unit.	Save and Restart	Reset	`commit` `restart`

Note: All parameters values are included for the purpose of demonstration only. Although valid, they should be changed to meet the application requirements.

As long as the slave device is on and is waiting for the connection, the master will boot and establish a TCP/IP connection with the slave. The slave will accept the connection and a serial-to-serial data tunnel will be established between the two units. Once the tunnel is established data can be sent between the two devices.

D.1 INFRASTRUCTURE NETWORK CONSIDERATIONS

If you want to use Infrastructure mode, there are a couple of modifications:

- The SSID must match the AP you want to you (step 1 in Table 28. Slave Configuration and Set-up& Table 29)
- Leave the network type as Infrastructure (step 2 in Table 28. Slave Configuration and Set-up & Table 29).

If you are using static IP addresses no further changes are required to the set-up. If not, you will need to do a couple of things:

- Enable DHCP (default).
- Find out the IP address assigned to the slave unit by the DHCP server. To do this you can look at the wireless routers attached devices table, search for the device using the Airborne Evaluation Utility (AEU) or guess (if the device has been on the network before in all likelihood the DHCP server has assigned it the same IP address).

Once you have found the IP address this needs to be used in the Primary LAN Server IP field (step 7 in Table 29).

Again as long as the Slave is on and associated with the AP, the devices will establish a TCP/IP connection and bridge data between the serial ports.

This glossary provides a definition 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 Module 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 Module 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 Module.
LEAP	Lightweight Extensible Authentication Protocol developed by Cisco. LEAP provides username/password-based authentication between a wireless client and a RADIUS server. It is one of several protocols used with the IEEE 802.1X standard for LAN port access control.
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.
RADIUS	Remote Authentication Dial In User Service. A backend server that performs authentication using Extensible Authentication Protocol (EAP). This server is required by the IEEE 802.1X security standard.
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.
TKIP	Temporal Key Integrity Protocol and is used in encryption. TKIP is an IEEE 802.11i standard and an enhancement to WEP security.
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 Module that provides 802.11 LAN connectivity.
WLN SPI	This is the model of the Airborne Module that uses an SPI to interface to a Host device.
WLN UART	This is the model of the Airborne Module that uses a serial UART to interface to a Host device.
WPA	Wi-Fi Protected Access. It addresses all known Wired Equivalent Privacy (WEP) vulnerabilities. WPA uses RC4 for encryption and TKIP for key management. It includes a message integrity mechanism commonly called Michael or MIC.
WPA-LEAP	Wi-Fi Protected Access - Light Extensible Authentication Protocol, an implementation based on the IEEE 802.11i 2004 and IEEE 802.1X 2001 standards, which includes the LEAP protocol for initial key assignment.
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key, an implementation based on the IEEE 802.11i 2004 and IEEE 802.1X 2001 standards, where the PSK is stored on the client.

A

A/B Diversity Switch, 11
Accessing the Web interface, 39
Additional Literature, 4
Airborne wireless lan node module, 7
Airborne Wireless LAN Node Module
    block diagram, 9
Airborne Wireless LAN Node Module
    antenna pin assignments, 15
    antenna signal descriptions, 15
    Design Guidelines, 18
    features, 1
    hardware description, 9
    host pin assignments, 11
    host signal descriptions, 11
    package, 21
    Reset, 15
Airborne Wireless LAN Node Module operation
    electrical characteristics, 22
    factory restart, 17
    performance range, 24
    power-up, 17
Analog inputs, 10
Application Circuit for Power Control
    performance, 67
Application processor, 9
Applications, 2
ASLIP, 27

B

Block diagram
    Airborne Wireless LAN Node Module, 9
Bus Switch, 66

C

CD, 4
Circuit board layout practices, 25
Circuit Performance, 67
Configurations, 1
Connections
    WLN SPI, 20
    WLN UART, 19
Conventions
    manual, 3

D

Design Guidelines
    general design guidelines, 18
    SPI design guidelines, 18
Developer Documentation, 4
Digital inputs, 10
Documentation
    related, 4
DPAC Technologies
    Web Site, 4

E

Electrical characteristics, 22
EMI / RFI GUIDELINES, 26
External antenna connections, 11

F

Factory restart, 17
Features
    Airborne Wireless LAN Node Module, 1
Firmware Update Page, 58
Flash, 10

G

General Design Guidelines, 18
General Purpose I/O Settings page, 46
General purpose input/output, 10
Glossary, 81

H

Hardware description, 9
    802.11 Media Access Control, 10
    A/B Diversity Switch, 11
    analog inputs, 10
    application processor, 9
    digital inputs, 10
    external antenna connections, 11
    Flash, 10
    general purpose input/output, 10
    high-speed and low-speed serial UART, 11
    power supply, 11
    serial ports, 10
    SPI, 11
    Static Random Access Memory, 10
    Transmit/Receive Switch, 10
High Speed serial UART, 11
High-Side Switch, 66

I

IEEE 802.11 baseband RF purpose input/output, 10
IEEE 802.11 Media Access Control, 10
Inrush Current Characteristics, 64

K

Key, 53

L

Layout practices
- circuit board, 25
- EMI / RFI GUIDELINES, 26
- Module mounting guidelines, 25
- Overview, 25

Load hot swapping, 63
Low Speed serial UART, 11

M

Module mounting guidelines, 25

N

Navigating through the Web interface, 40
Network Services Configuration page, 47

O

Off Current, 67

P

Package configuration
- Airborne Wireless LAN Node Module, 21
- WLN SPI, 20
- WLN UART, 19

Parts List for Recommended Power Control Application Circuit, 65
PDF Files, 4
Performance range, 24
Pin assignments
- Airborne Wireless LAN Node Module, 11
- antenna, 15

Power control, 63
- Introduction, 63
- load hot swapping, 63
- Recommended application circuit, 65

Power Control
- inrush current characteristics, 64

Power supply, 11
Power-up, 17

R

Radio Frequency Channels, 71
Recommended application circuit for power control, 65
Recommended Application Circuit for Power Control
- parts list, 65

Recommended circuit for power control, 65
Recommended Circuit for Power Control
- parts list, 65

Related documentation, 4
Related Documentation, 4
Reset Page, 60

S

Security Configuration Page, 56
SERIAL PERIPHERAL INTERFACE, 35
SERIAL PERIPHERAL INTERFACE (spi)
- OVERVIEW, 35
- SPI Hardware Configuration, 35
- SPI Logical Interface, 36
- SPI Standard Support Summary, 35

Serial ports, 10
Signal descriptions
- Airborne Wireless LAN Node Module, 11
- antenna, 15

Specifications, 8
SPI, 11
SPI (SERIAL PERIPHERAL INTERFACE), 35
SPI Design Guidelines, 18
Static Random Access Memory, 10
STATUS page, 40

T

Thermal Characteristics, 68
Transmit/Receive Switch, 10

V

Voltage Regulator, 66

W

Web interface
- accessing, 39
- Firmware Update Page, 58
- General Purpose I/O Settings page, 46
- navigating, 40
- Network Services Configuration page, 47
- Reset Page, 60
- STATUS page, 40
- Wireless Network Configuration page, 52
- Wireless Security Configuration Page, 56
- WLN SPI Model only — Miscellaneous OEM Settings page, 51
- WLN SPI Model only — Serial Interface Configuration page, 45
- WLN UART Model only — Miscellaneous OEM Settings page, 49
- WLN UART Model only — Serial Interface Configuration page, 42

WEB Interface
- OVERVIEW, 39

Web Site, 4
Wireless Network Configuration page, 52
WLN SPI
- package, 20

WLN SPI Connections, 20
WLN SPI Model only — Miscellaneous OEM Settings page, 51

WLN SPI Model only — Serial Interface Configuration
page, 45
WLN UART
package, 19
WLN UART Connections, 19
WLN UART Model only — Miscellaneous OEM
Settings page, 49
WLN UART Model only — Serial Interface
Configuration page, 42
WPA-LEAP Security, 29
WPA-LEAP Security Configuration Page, 29

7321 Lincoln Way
Garden Grove, California 92841
Tel: 714.898.0007
www.dpactech.com

39L3702-01
REV. E 1/25/2006 JN