DPAC TECHNOLOGIES®
Products & Services for the Integration Age™

WIRELESS PRODUCTS

Airborne™ Wireless LAN Node Module Data Book

DPAC Technologies Confidential

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

LIST OF FIGURES

LIST OF TABLES

This page intentionally left blank

CHAPTER 1
INTRODUCTION

1.1 OVERVIEW

Airborne™ 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 two models (see Table 1).

Table 1. Airborne WLN Module Configurations

Configuration	Description	DPAC Model Number
Airborne 802.11b Wireless LAN Node Module – UART Version	Module with UART firmware and UART interface	WLNB-AN-DP101
Airborne 802.11b Wireless LAN Node Module – SPI Version	Module with SPI (Serial Peripheral Interface) firmware and SPI interface	WLNB-AN-DP102

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
- Built-in TCP/IP and UDP features provide flexible LAN connectivity options
- Built-in Web server enables drop-in LAN and Internet connectivity
- 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 or SPI 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. 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, automotive, 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, Command Line Interface* — describes the Airborne WLN Module command line interface.
- *Appendix B, Power Control* — describes a suggested power supply design.
- *Appendix C, Radio Frequency Channels* — lists radio-frequency channels.
- *Appendix D, 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 book, the following documents are provided on the Evaluation Kit or Developer's Kit CD:

- Airborne™ DLL Programmer's Guide
- Airborne™ Wireless LAN Node Module Evaluation and Development Kit Product Brief
- Airborne™ Wireless LAN Node Module Evaluation and Development Kit Quick Start Guide
- Airborne™ Wireless LAN Node Module Evaluation and Development Kit User's Guide
- Airborne™ Wireless LAN Node Module Firmware Release Notes
- Airborne™ Wireless LAN Node Module Industrial Control Applications
- Airborne™ Wireless LAN Node Module Medical Applications
- Airborne™ Wireless LAN Node Module Product Brief
- Airborne™ Wireless LAN Node Module Transportation-Trucking Applications
- End User License Agreement
- OEM Configuration Tool Release Notes
- VCOM Configuration Utility Release Notes
- VCOM Quick Start Guide
- Other Product Briefs, Release Notes, and Application Notes

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:

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 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 460,800 bps SPI (slave): Can be clocked up to 20 MHz
Data Throughput	UART-to-LAN – 320 Kbps (max) (see Note 5 below) LAN-to-UART – 70 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.

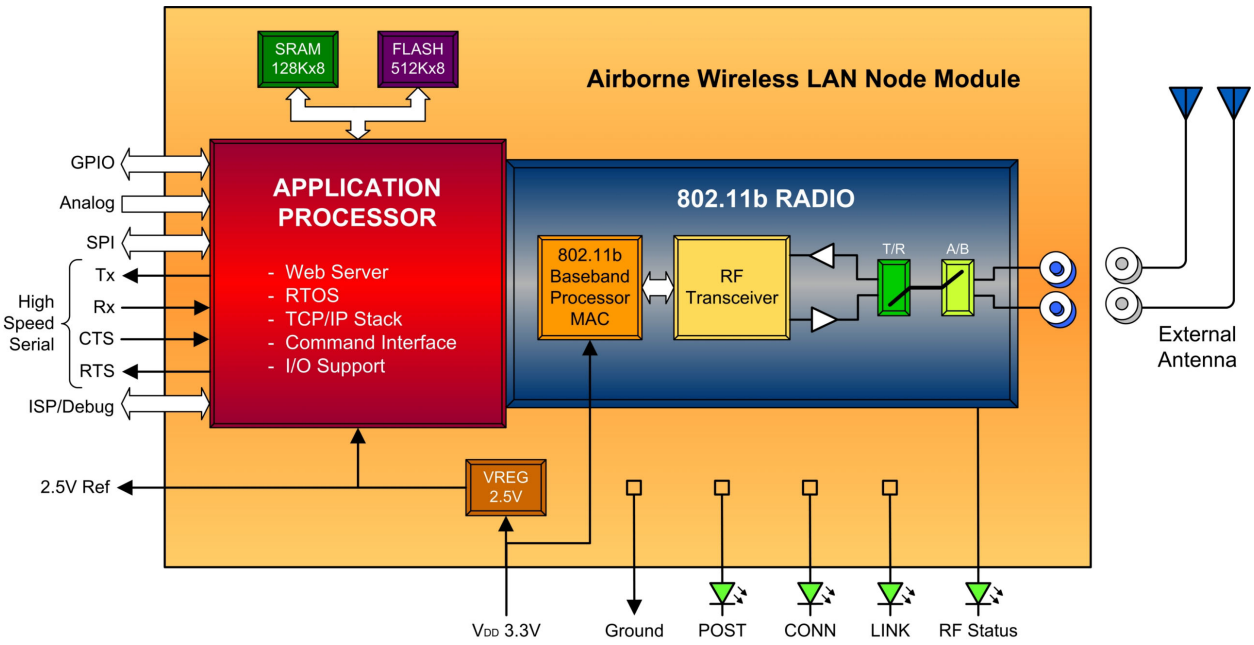


Figure 1. Airborne WLN Module Hardware Block Diagram

Note: 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).

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. 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 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 is 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}). Used as digital output for SPI firmware as Slave data ready interrupt.
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.

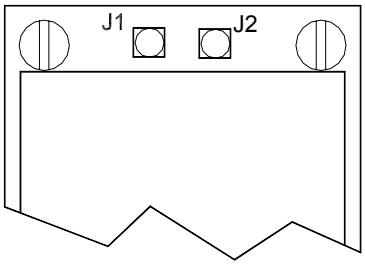


Figure 2. Antenna Connectors

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.

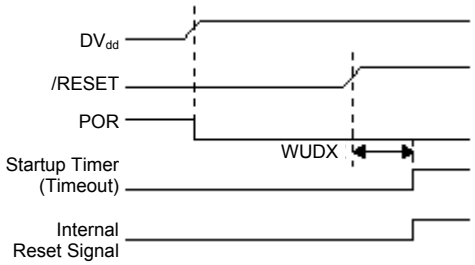


Figure 3. Power-up Sequence (Separate /RESET Signal)

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.

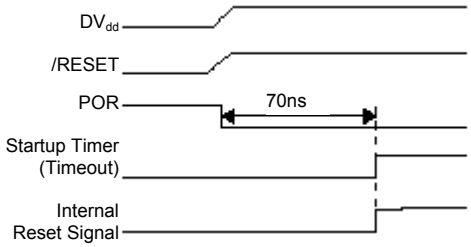


Figure 4. Power-up Sequence (/RESET Tied to DV_{DD})

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.

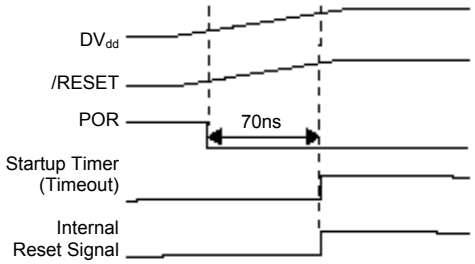


Figure 5. DV_{DD} Rise Time Exceeds Tstartup

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).

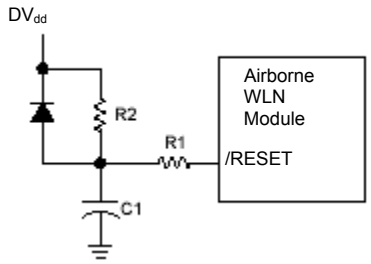


Figure 6. External Reset Circuit

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 52).
- Use the CLI command `reset` (see page 92).
- 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

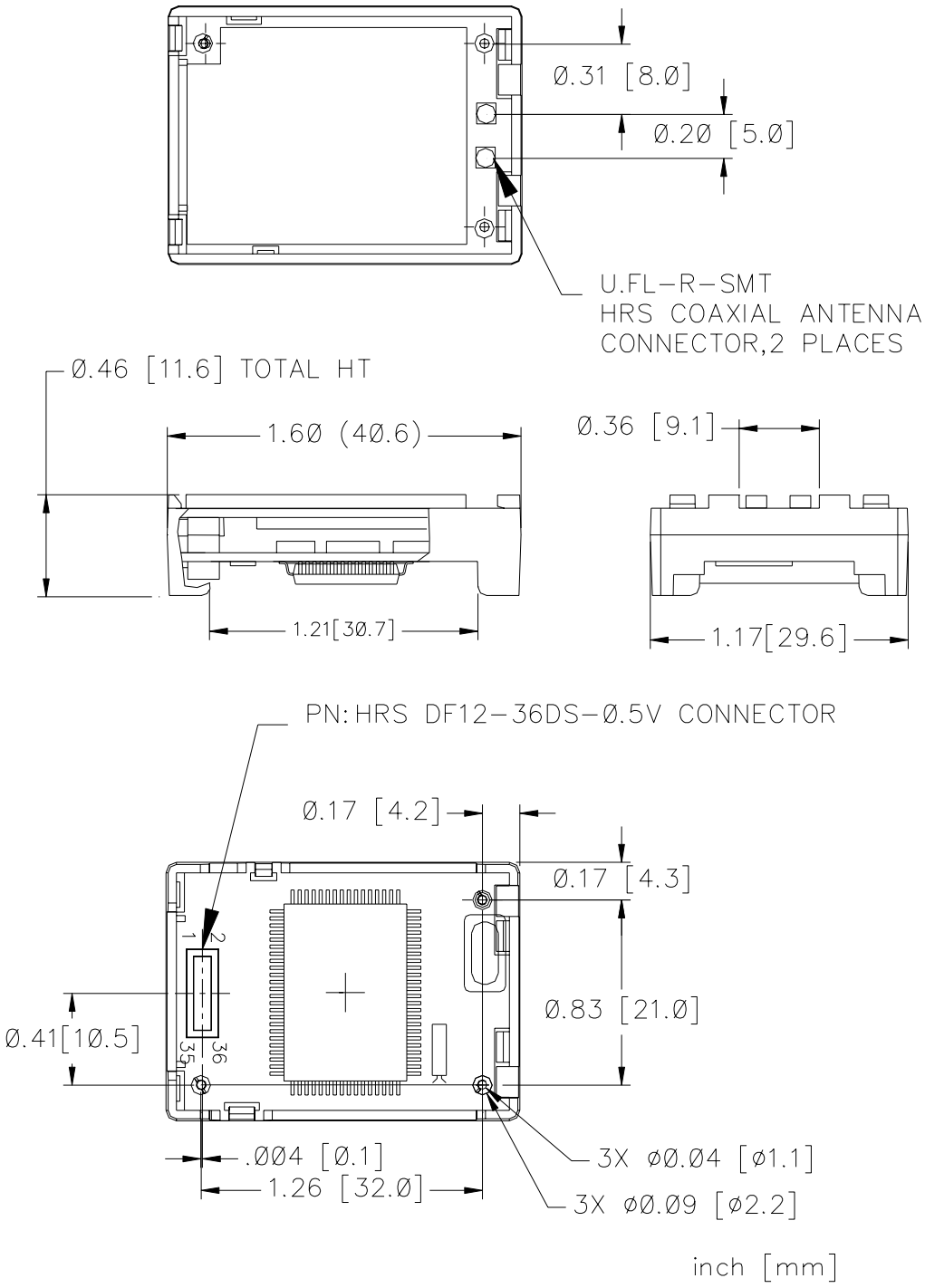


Figure 7. Mechanical Dimensions (Airborne WLN Module)

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.
- 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 capacitances 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.

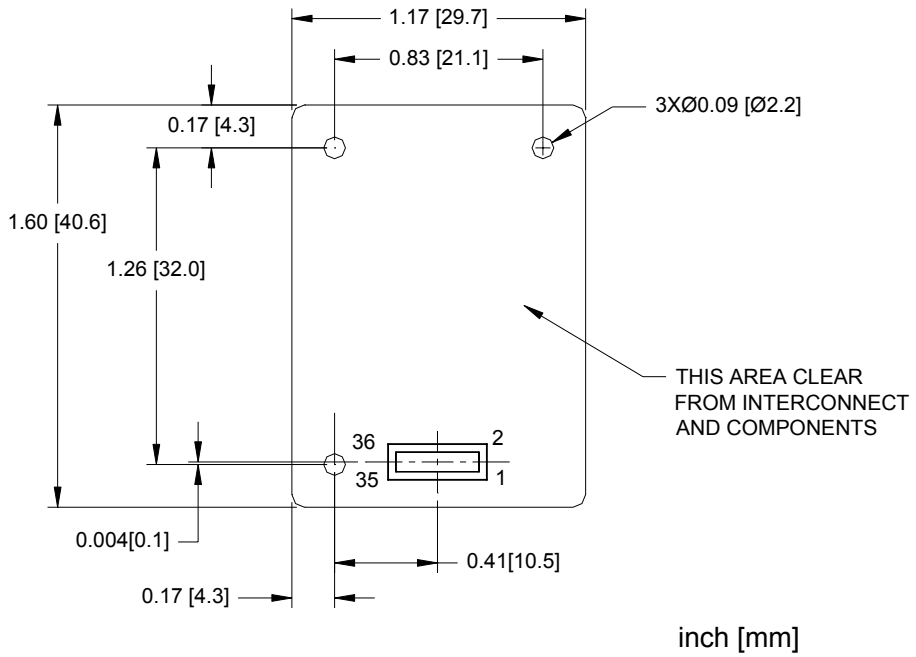


Figure 8. Guidelines for Mounting the Airborne WLN Module

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.

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.

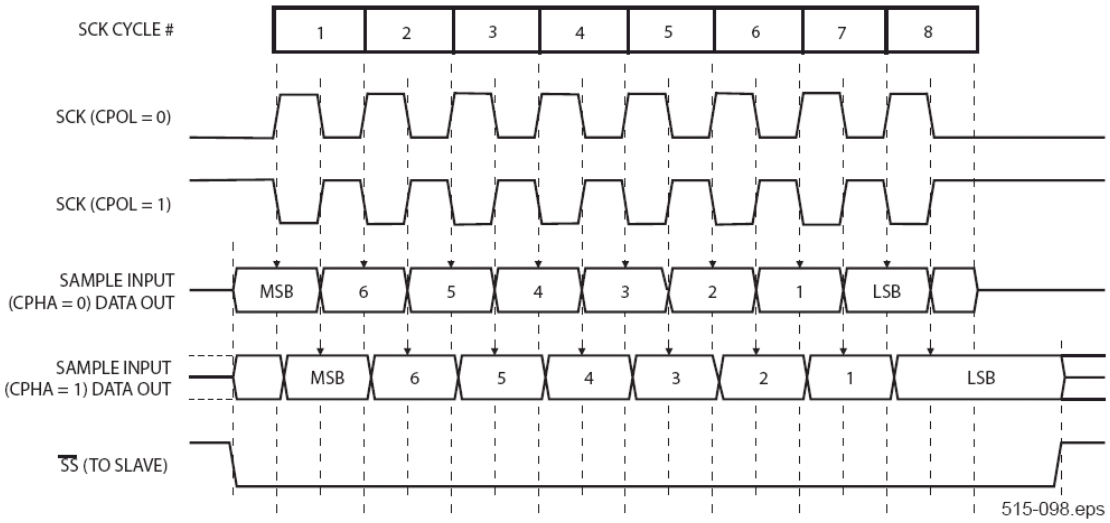


Figure 9. SPI Data Clock Timing

(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 14. 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		

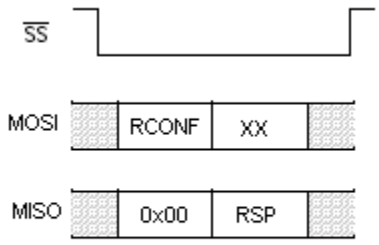


Figure 10. Read Configuration Timing Diagram

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 15. 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.

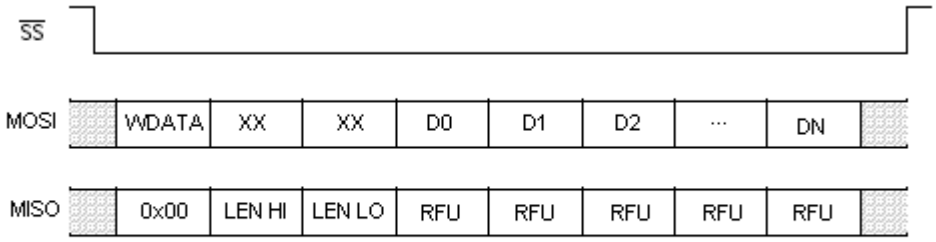


Figure 11. Write Data Timing Diagram

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 16. 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.

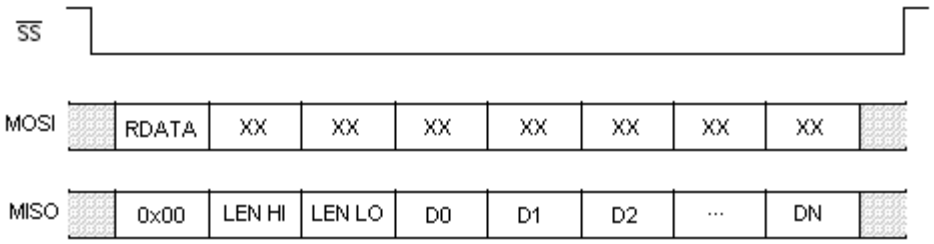


Figure 12. Read Data Timing Diagram

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

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 13).

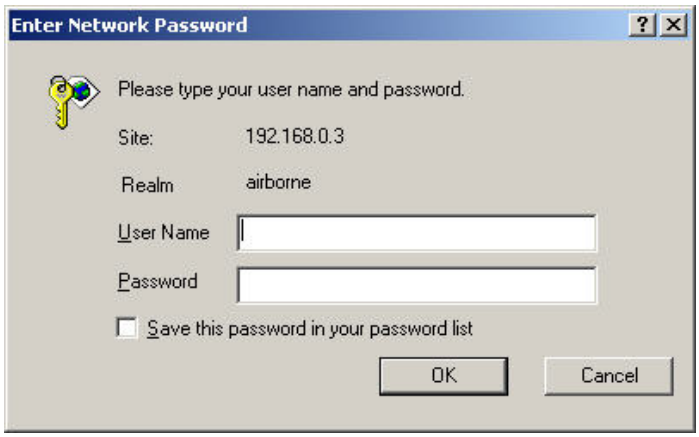


Figure 13. User Name and Password Screen

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 48).

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 (see Table 29 on page 80 for a description of status results)

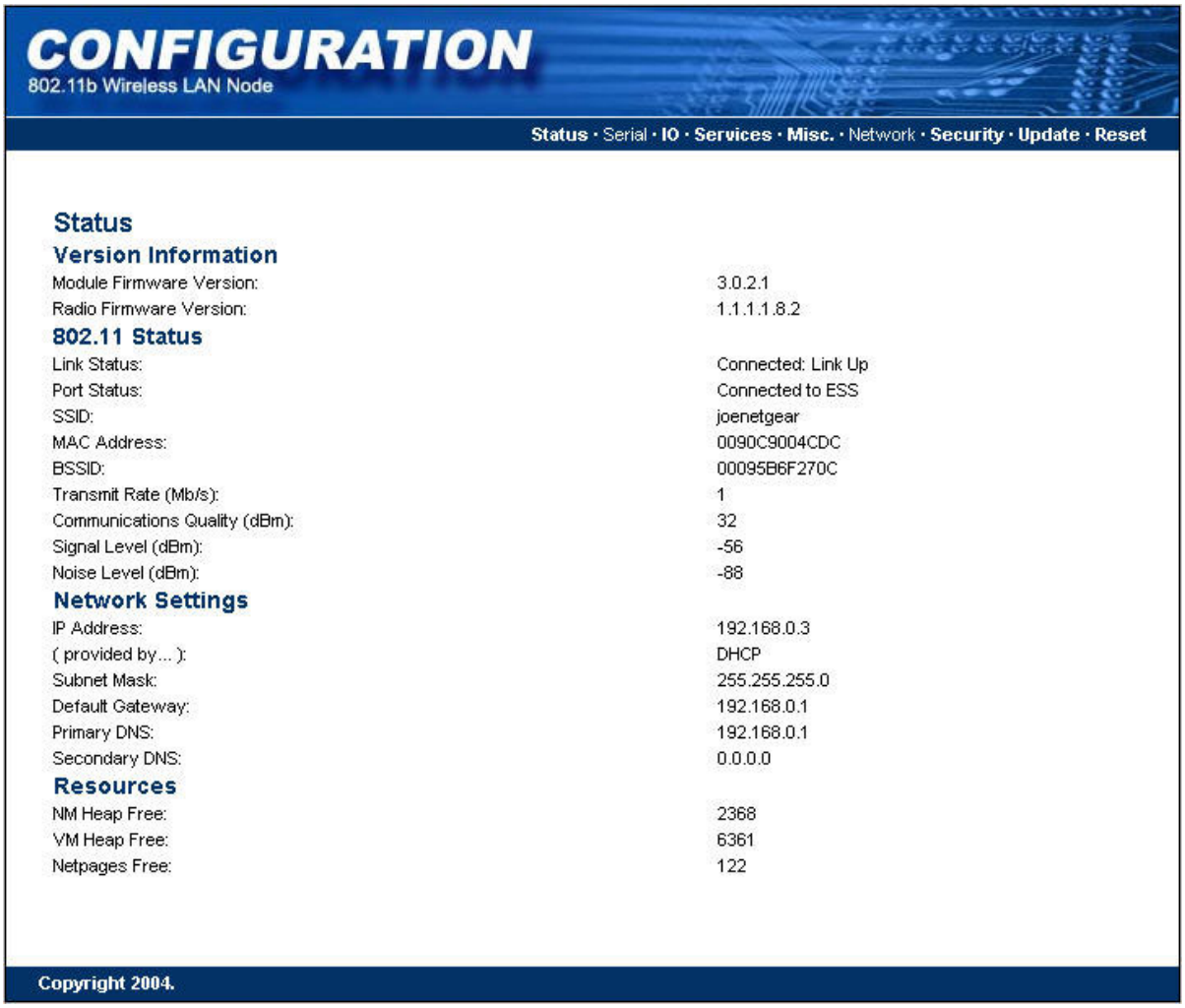


Figure 14. Status Page

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.

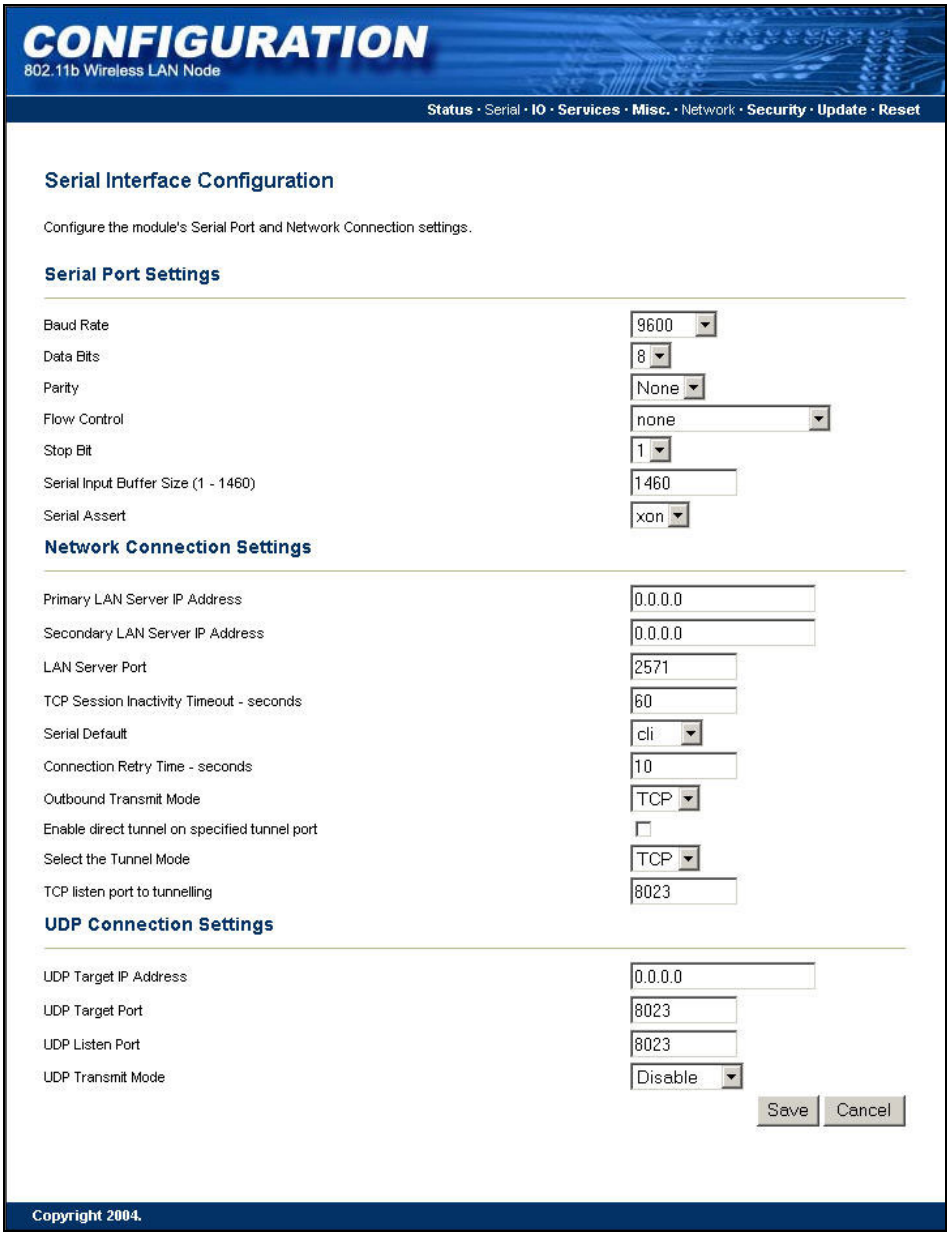


Figure 15. WLN UART Model Only — Serial Interface Configuration Page

Table 17. WLN UART Model Only — Serial Interface Configuration Settings

Parameter	Description
Serial Port Settings	
Baud Rate	300 – 460800 bps Default is 9600. See "High Speed UART Configurations" on page 11.
Data Bits	• 7 • 8 (*default*)
Parity	• None (*default*) • Even • Odd
Flow Control	• none (*default*) • Hardware (RTS/CTS) • Software (XON/XOFF)
Stop Bit	Sets the stop bits to one (1) or two (2). Default is 1.
Serial Input Buffer Size (1 - 1460)	1 - 1460 bytes Default is 1460.
Serial Assert	Allows the serial software flow control to be asserted or deasserted via CLI over TCP. The value committed is also applied to the system at startup. • xoff • xon (*default*)
Network Connection Settings	
Primary LAN Server IP Address	Specifies the IP Address of the primary LAN device to which the 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 17 on page 35)

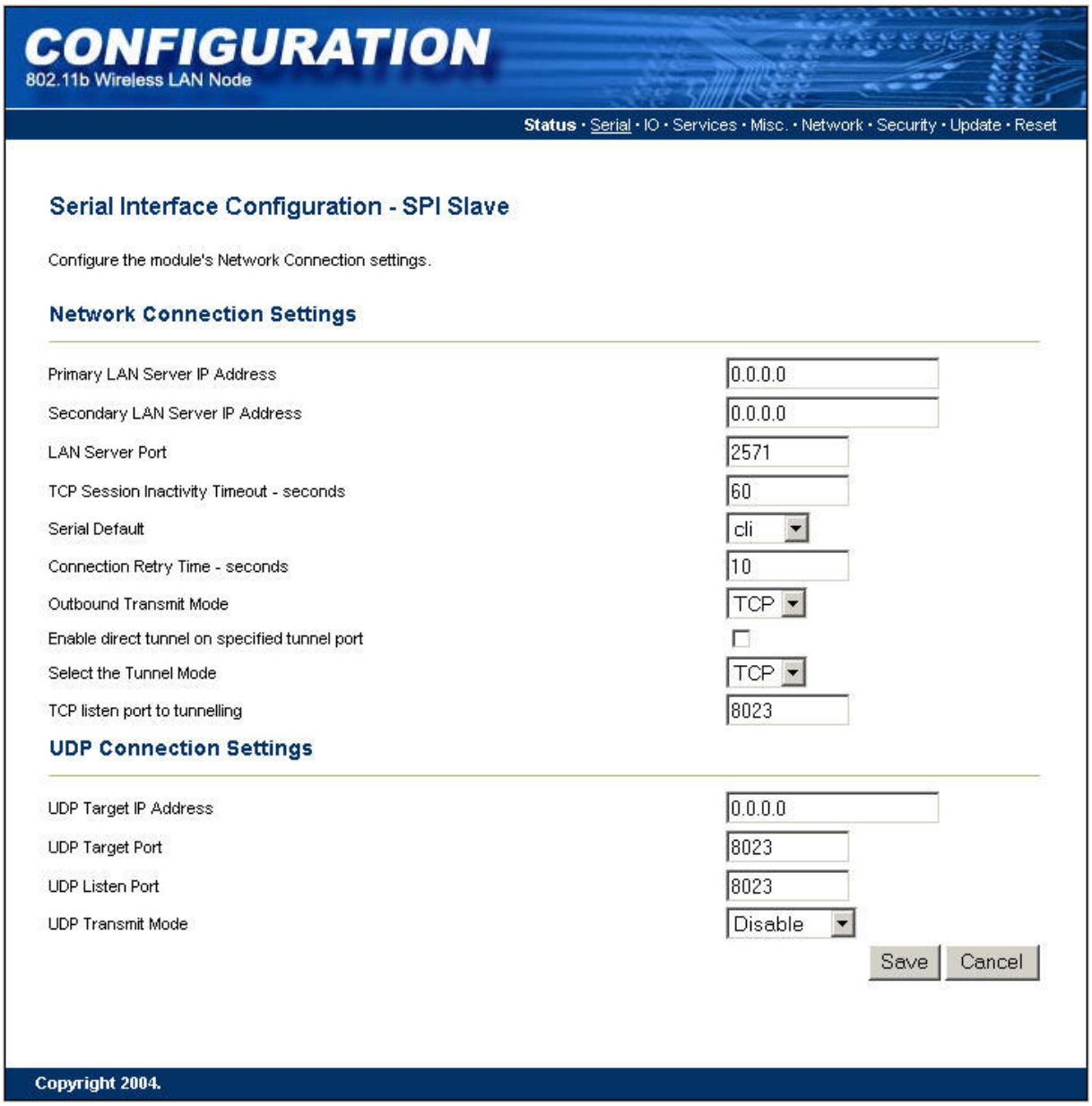


Figure 16. WLN SPI Model Only — Serial Interface Configuration Page

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^2C support.

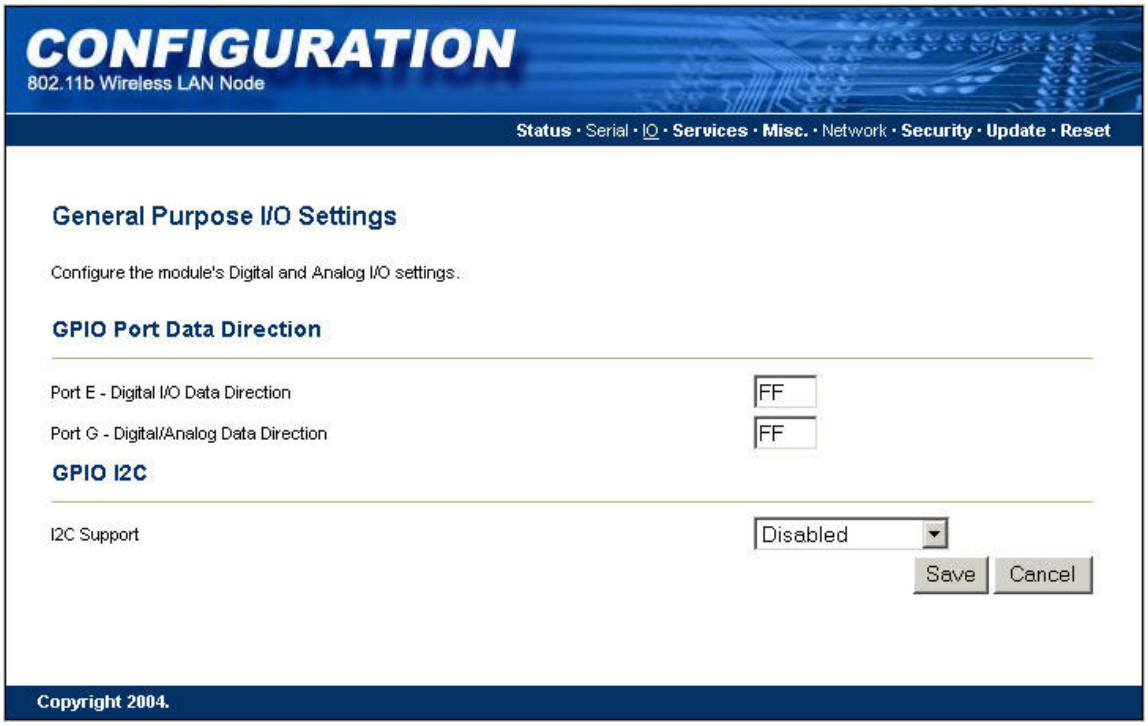


Figure 17. General Purpose I/O Settings Page

Table 18. 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^2C support. • `Enabled` = Module is configured for I^2C support. • `Disabled`= Module is not configured for I^2C 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.

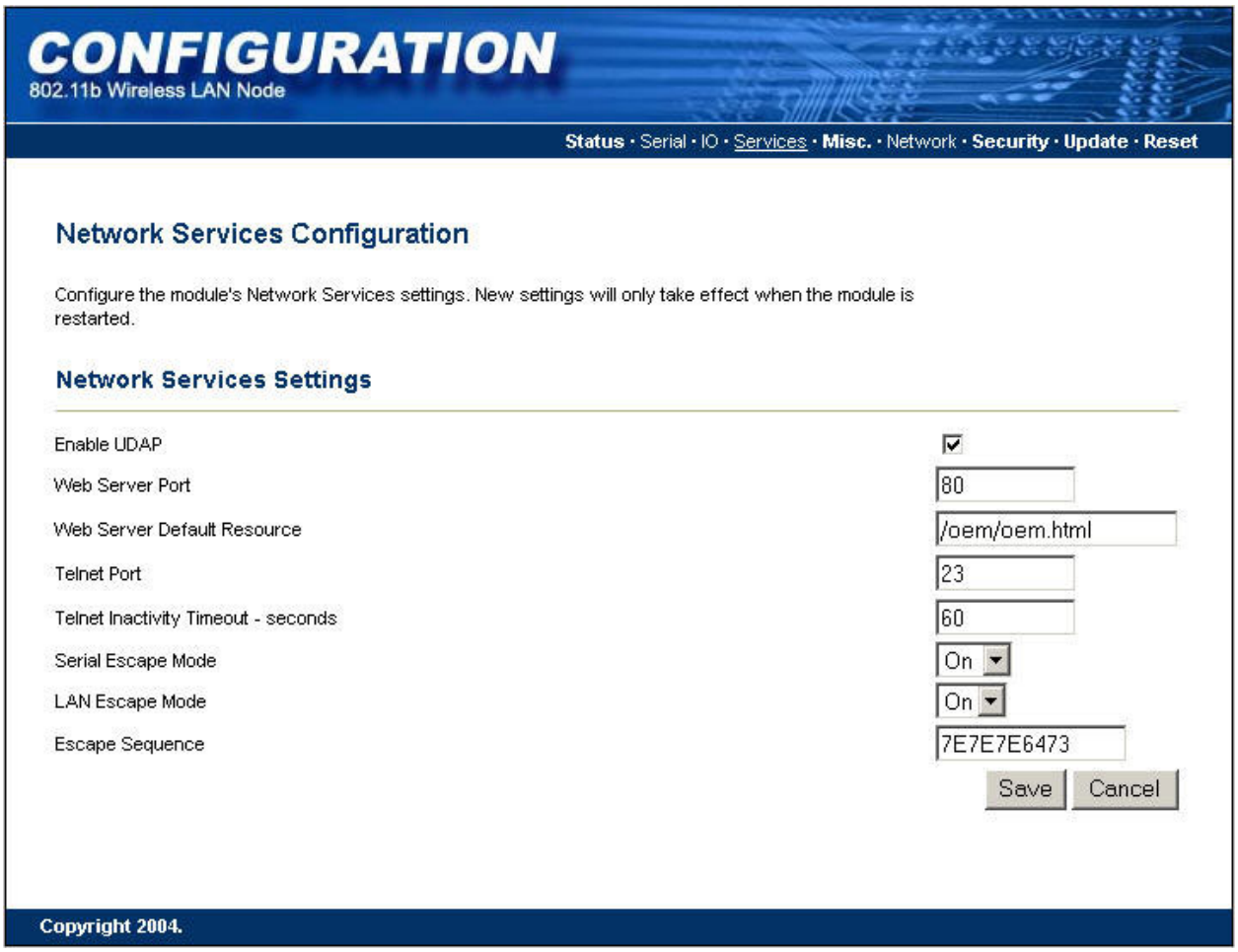


Figure 18. Network Services Configuration Page

Table 19. 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 19. WLN UART MODEL ONLY — Miscellaneous OEM Settings Page

Table 20. 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` For information about these modes, see Table 31 on page 90.

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*).

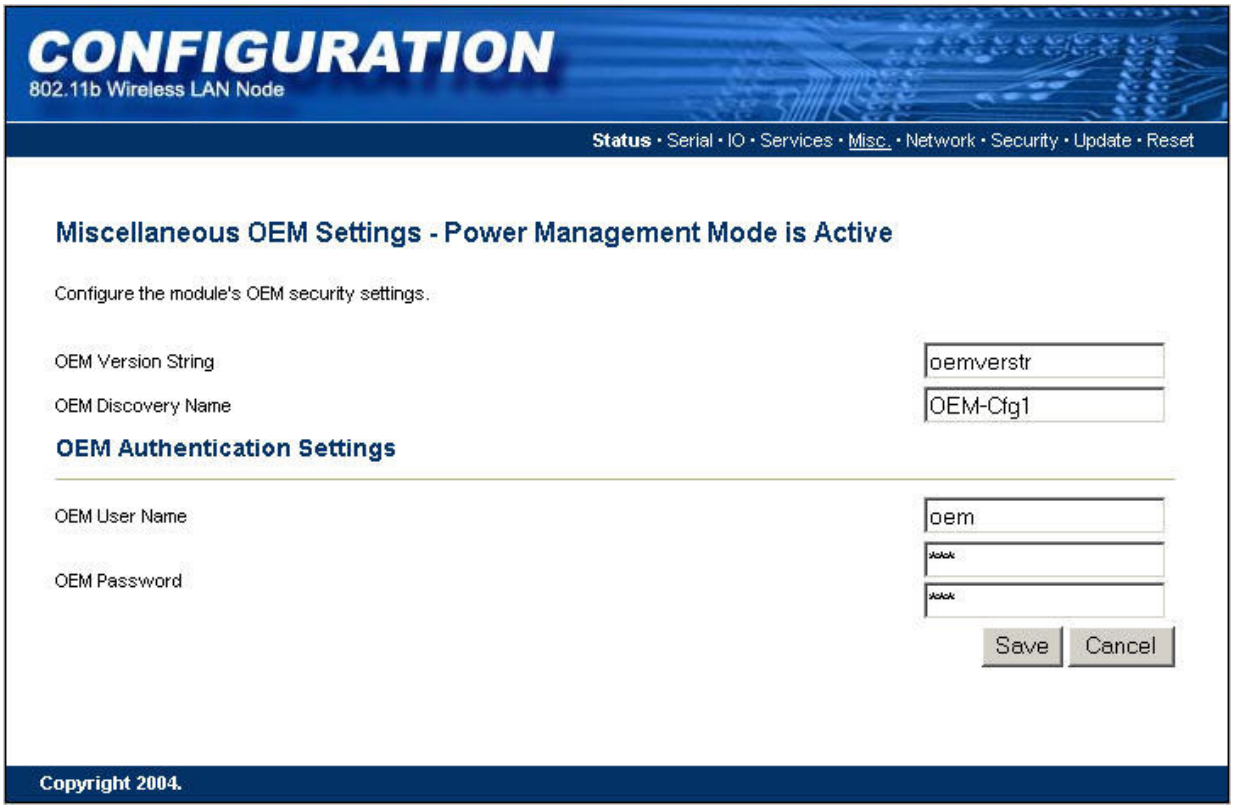


Figure 20. WLN SPI MODEL ONLY — Miscellaneous OEM Settings Page

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, WEP security, advanced, network IP, and discovery settings.

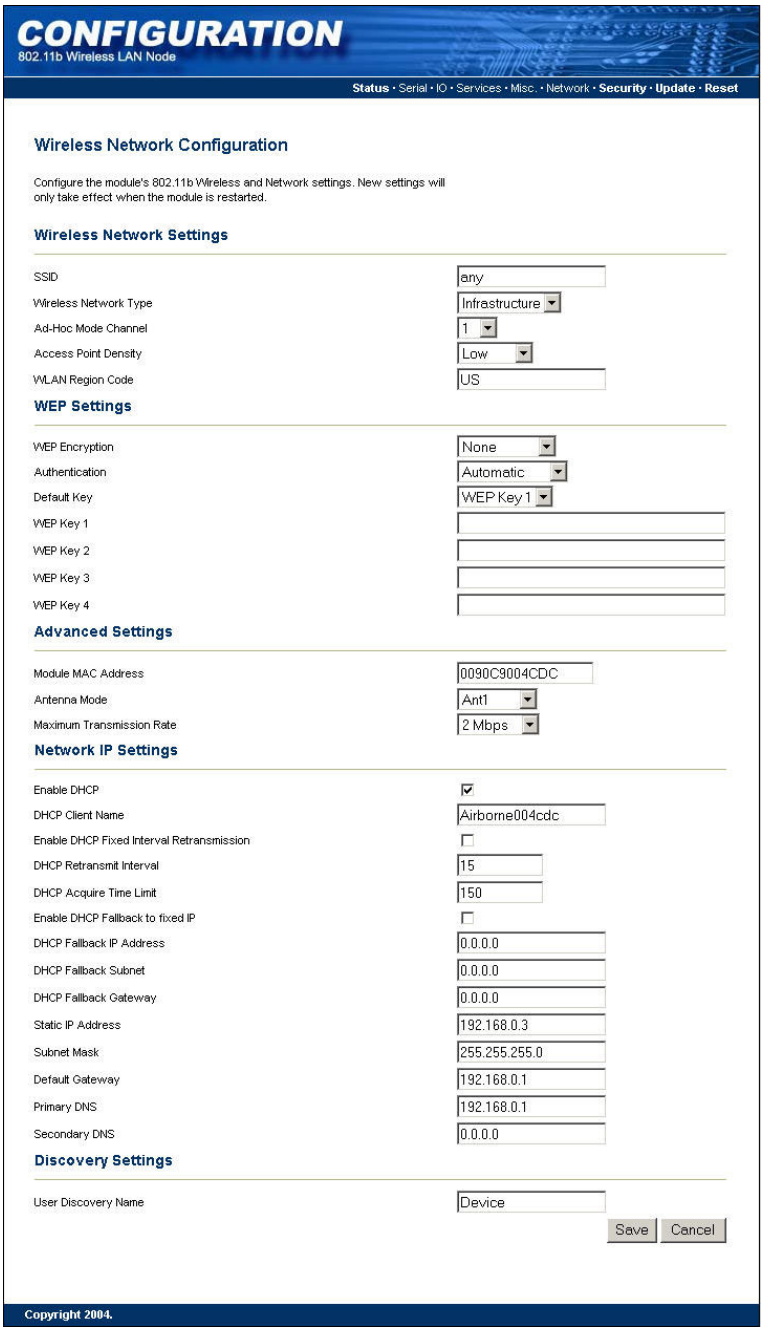


Figure 21. Wireless Network Configuration Page

Table 21. 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. For a list of region country codes, see Table 28 on page 79. Default is `US`.
WEP Settings	
WEP Encryption	Enables or disables WEP security: • `None` (*default*) • `64` = 64-bit key length • `128` = 128-bit key length
Authentication	Enables or disables WEP authentication: • `Automatic` = automatically detects the authentication. (*default*) • `Open System` = communicates the key across the network. • `Shared Key` = allows communication only with devices with identical WEP settings.
Default Key	Selects the default WEP Key from 1 – 4 if `Shared Key` or `Both` is selected for `Authentication`. Default is `WEP Key 1`.

Parameter	Description
WEP Key 1 through 4	Specify up to four WEP key values: • If `WEP Encryption` = `64`, enter 10 hexadecimal digits for each key. • If `WEP Encryption` = `128`, enter 26 hexadecimal digits for each key.
Advanced Settings	
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`.
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`.
DHCP Retransmit Interval	Sets the DHCP retransmission interval to use when `wl-dhcp-mode` is set to fixed. This is an integer with a range of `1-64`. Default is `15`.
DHCP Acquire Time Limit	Sets the number of seconds the DHCP should attempt to acquire an IP address before using the fallback IP address, if `wl-dhcp-fb` is on. An integer with a range of `1-255`. Default is `150`.
Enable DHCP Fallback to fixed IP	Sets the DHCP fallback method off (`0`) or on (`1`). - If `wl-dhcp-fb` is on, after the number of seconds of `wl-dhcp-acqlimit` has been reached, the firmware uses the IP address specified in the `wl-dhcp-fbip`. - If `wl-dhcp-fb` is off, the firmware will not use the fallback method. Default is `0`.
DHCP Fallback IP Address	Sets the fallback IP address. Default is `0.0.0.0`.
DHCP Fallback Subnet	Sets the fallback subnet mask. Default is `0.0.0.0`.
DHCP Fallback Gateway	Sets the fallback gateway address. Default is `0.0.0.0`.
Static IP Address	Specifies the 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`

Parameter	Description
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 39). 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.

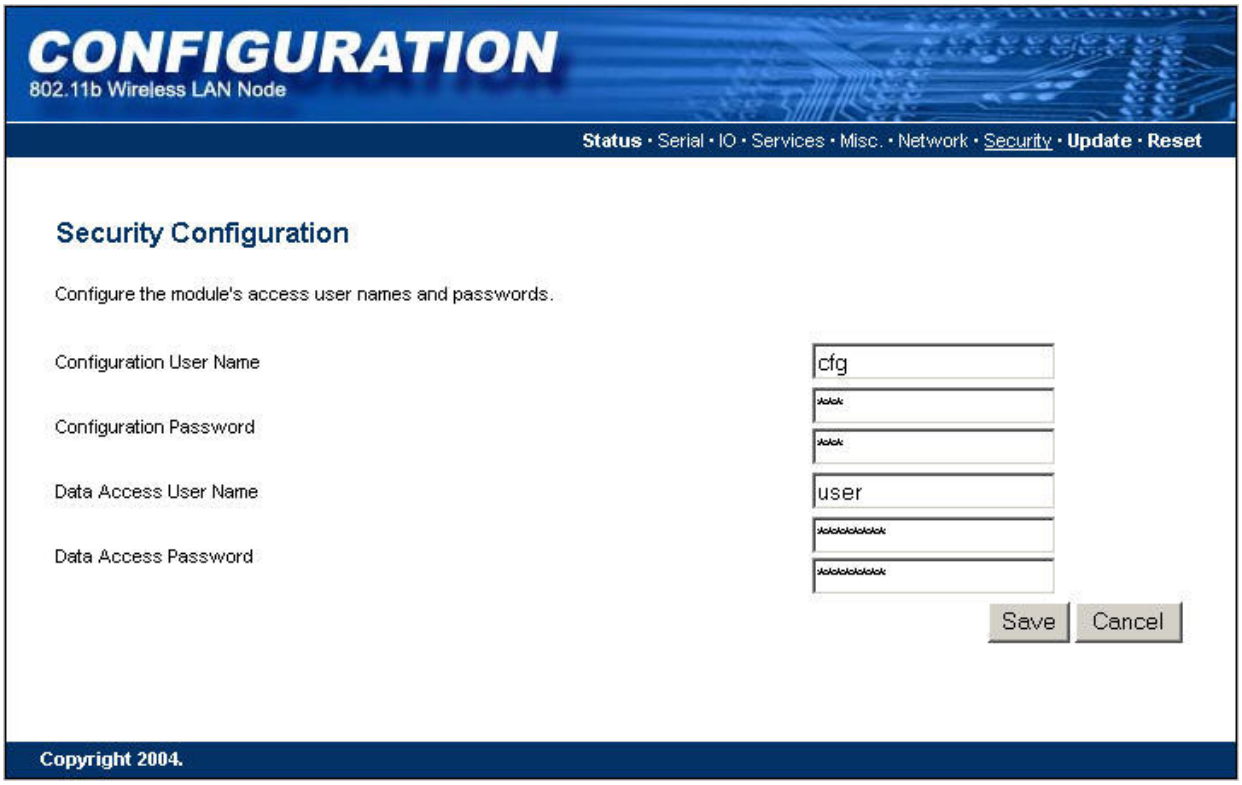


Figure 22. Security Configuration Page

Table 22. 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 23). This page lets you update the Module firmware.

Figure 23. 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:

1. Obtain the updated firmware and make it accessible to a computer connected to the Module.

2. In the menu bar at the top right of the page, click **Update**. The Firmware Update page appears (see Figure 23).

3. 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.

4. Click the **Update** button to update the firmware. The message in Figure 24 appears, asking whether you are sure you want to reprogram the 802.11b interface using the new firmware file.

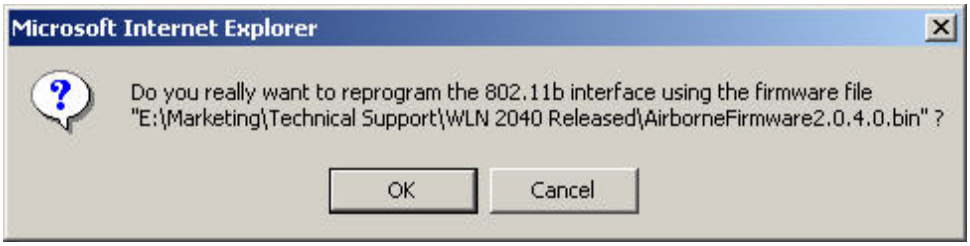


Figure 24. Warning Message Before Updating the Firmware

5. Click **OK** to update the firmware. This process can take up to 60 seconds (see Figure 25).

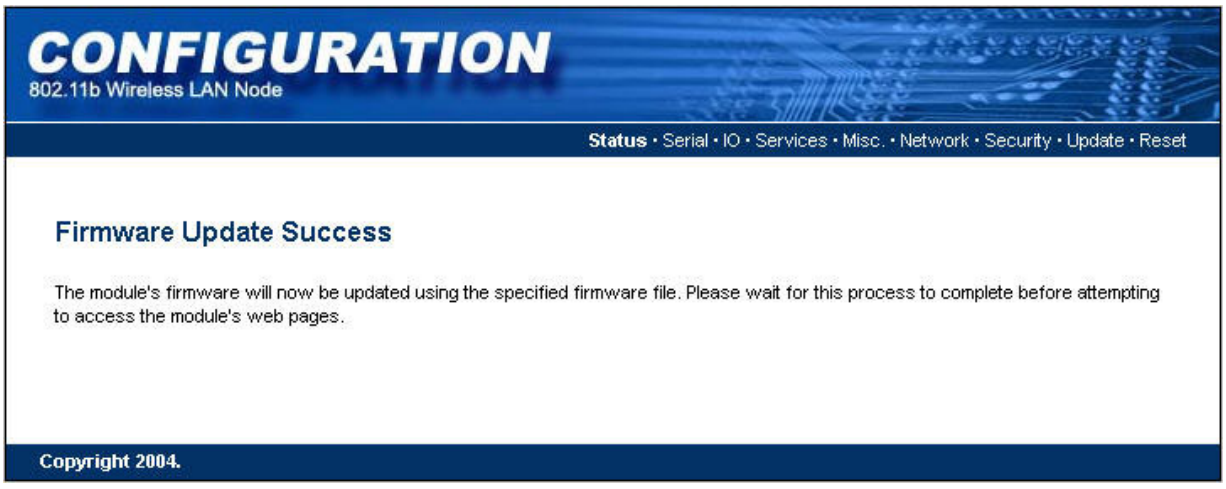


Figure 25. Firmware Update Success Message

5.14 RESET PAGE

Clicking the **Reset** link in the menu bar displays the Reset page (see Figure 26). This page provides a **Restart** button that lets you restart the 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 27 appears. Click **OK** to restart the Bridge or **Cancel** to not restart it.
- If you click the **Defaults** button, the screen in Figure 28 (on page 53) appears. Click **OK** to reset the Bridge to its factory-default settings or **Cancel** to not reset it.

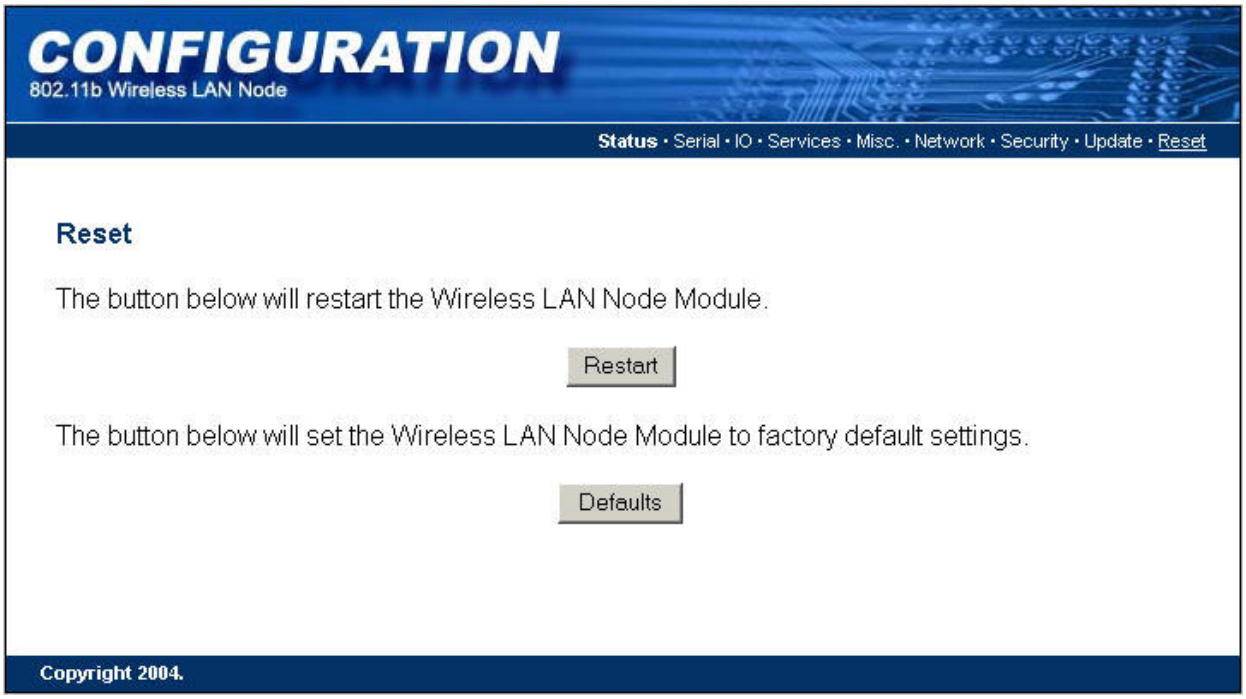


Figure 26. Reset Page

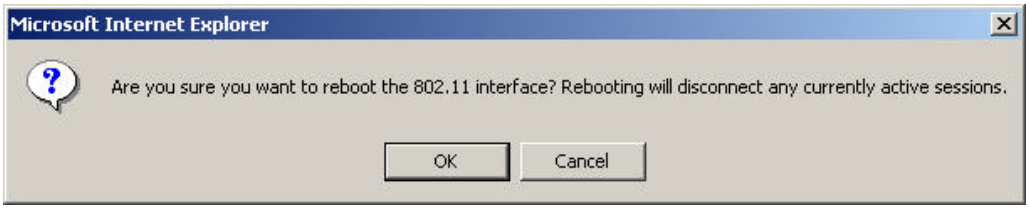


Figure 27. Warning Message After Clicking the Restart Button

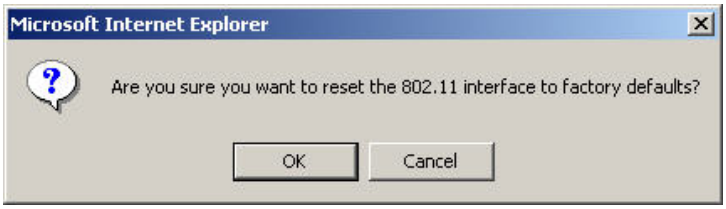


Figure 28. Warning Message After Clicking the Defaults Button

This page intentionally left blank

A.1 OVERVIEW

This appendix describes the Airborne WLN Module's Command Line Interface (CLI) commands. The CLI consists of a set of commands that are supported and executed in the Module. The CLI allows OEM applications to configure, control, and obtain status about the Module, and set up communications via the wireless Local Area Network (LAN).

OEM applications fall into two categories, Host and LAN.

- A Host application refers to an embedded application that communicates with the Module via the Module's serial port.
- A LAN application refers to an application that runs on a computer on the LAN side of the wireless connection.

A.2 TYPICAL SYSTEM

A typical system includes:

- A Serial Host computer connected to the Module's serial port.
- A remote LAN Host that communicates wirelessly with the Module through an Access Point (AP).
- A LAN-based browser with access to the Module via the wireless connection.

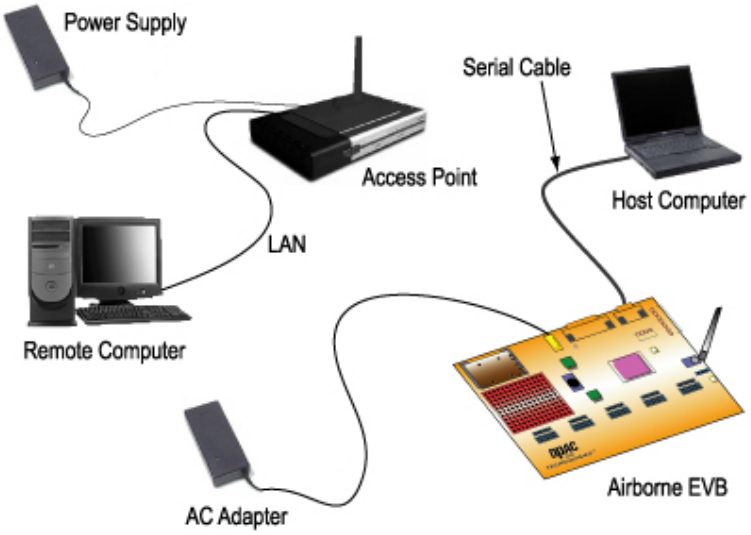


Figure 29. Typical System

A.3 COMMUNICATION METHODS

The following methods can be used to communicate with the Module:

- Using a Serial Host to send CLI commands
- Using a LAN Host to access the Module's Web server and built-in Web pages
- Using a LAN Host to open a TCP connection to send CLI commands

In addition, the Module can initiate a TCP connection to a LAN Host and act as a "pass-through" device that passes received data without acting on it.

The Module responds to a CLI command on the communication channel where the command originated. Commands that forward data to the Host must follow serial interface arbitration rules and modes described later in this appendix.

A.4 USING THE ESCAPE SEQUENCE AND ESCAPE COMMAND

In the following sections, references are made to the "escape sequence" and the "escape command." The escape sequence is a string that switches the Module from data pass-through mode to CLI mode. The default escape sequence is `7E7E7E6473`, which is equivalent to the characters `~~~ds`.

The `escape` command is a CLI command that changes the escape-sequence string, and turns escape-sequence checking on or off. Data-throughput performance can be improved significantly by turning escape-sequence checking off.

A.5 SERIAL INTERFACE ARBITRATION AND MODES

Data can be sent and received across the serial port using one communications session at a time. Examples of sessions that can send and receive data over the serial port are:

- The Serial Host using the serial port in CLI or pass-through mode
- The Web Server CLI interface using `putget` and `putexpect` commands
- A TCP session using `putget` and `putexpect` commands and pass-through mode
- A TCP connection initiated by the Serial Host or LAN Host

The Serial Host has priority over the serial port. If the Serial Host decides it wants to access the port and issues the escape sequence, any other session activity on the serial port ends automatically.

A.6 HOST DEVICE SERIAL PORT OWNERSHIP

When the Serial Host sends an escape sequence to the Module:

- The escape sequence is transmitted through the serial connection.
- Any session currently active on the serial port ends immediately.
- The serial port enters CLI mode.
- The Serial Host is given ownership of the port.

Once the Serial Host owns the serial port, it can access the serial port in several ways:

- As the master of the serial port in CLI mode
- As a master in pass-through mode when the Host has initiated pass-through
- As a slave listening to the serial port for incoming requests in “listen” mode
- As a slave in pass-through mode when another session (Telnet, TCP, or HTTP) has initiated the connection

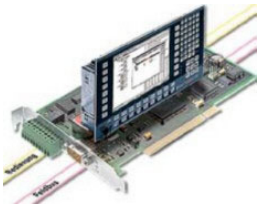
Since the Serial Host has priority of the serial port, it controls the transitions between modes and can temporarily relinquish ownership by issuing the CLI command `listen`. Any time thereafter, the Host can regain ownership by issuing the CLI escape sequence.

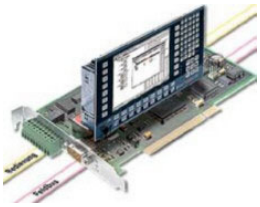
When in listen mode, the Module does not delineate requests or indicate the source of a request. Consequently, the request data must be designed to provide adequate identification so the Host can respond with the appropriate information.

For example, the data in a `putget` or `putexpect` command issued by JavaScript embedded in resident HTML should include enough information so that after the data is forwarded to the Serial Host, the Host can discern the source of the data and respond accordingly. Similarly, the data in a `putget` or `putexpect` command issued by a Serial Host to a LAN Host, and the response data from the LAN Host, should include information that allows each Host to discern the communication source to send corresponding response data.

There is no need to prefix escape characters with an escape prefix. The escape sequence is a fixed-length, 5-byte sequence. The CLI `escape` command can be used to change the escape sequence string. Only one escape is defined for all CLI interfaces.

Table 23. Example of Host-to-Serial (UART or SPI) Port Interaction

	 **Host**	**Airborne WLN Module**
1.	`auth dpac dpac<CR>` Authenticates the connection with the Module.	
2.		`OK<CR><LF>` Indicates that the command executed successfully.
3.	`wl-tcp-ip 192.168.0.5<CR>` Sets the IP address of the LAN Host to which the Serial Host will want to connect.	
4.		`OK<CR><LF>` Indicates that the command executed successfully.
5.	`wl-tcp-port 8023<CR>`	`OK<CR><LF>` Indicates that the command executed successfully.
6.	`wl-tcp-timeout 30<CR>` Continues issuing CLI commands.	
7.		`OK<CR><LF>` Responds to each CLI command.
8.	`pass<CR>` Switches the Module to pass-through mode and makes a connection to the previously defined LAN Host. Data passed between the Serial Host and the LAN Host is tunneled transparently.	
9.		`OK<CR><LF>` Indicates that a connection was made.
10.	`01010101001010` Sends raw binary data.	
11.	01010101001010	Receives data from the LAN Host and forwards it to the Serial Host.
12.	`~~~ds<CR>` Serial Host sends the escape command to exit from pass-through mode and return to CLI mode.	
13.		`OK<CR><LF>` Indicates that the escape command was successful. Returns to CLI mode without ending the TCP connection. Further communication over the serial interface must adhere to the defined CLI command format.

	Host	Airborne WLN Module
		
14.	`close<CR>` Requests the Module to close the TCP connection with the LAN Host.	
15.		`OK<CR><LF>` Responds to CLI command.
16.	`listen<CR>` Releases control of the serial interface. Other LAN Hosts can now establish communication channels with the Serial Host.	

A.7 LAN CLIENT SERIAL PORT OWNERSHIP

The Module does not allow LAN clients to control the serial port permanently. However, if the Serial Host uses the CLI command `listen` to release ownership of the serial port, the Module tunnels the pass-through data from the LAN Host to the Serial Host. The Serial Host can regain ownership of the serial interface at any time and block the LAN client from tunneling data by sending the escape command to the Module. This is useful for configurations where the Host needs to communicate urgent information. When the Serial Host regains ownership while the LAN Host is in pass-through mode, the LAN Host receives the escape command string.

LAN clients using TCP can issue the `pass` command to tunnel data to the Serial Host. However, if the Serial Host owns the serial port by being in CLI or Host-initiated pass-through mode, the Module rejects the LAN Host's pass-through request.

A.8 AIRBORNE WLN MODULE STARTUP

When the Module powers-up, the parameters associated with the CLI command `serial-default` determine how the Module starts up. Factory default is `cli`.

- When set to `cli`, the Module sets the serial port to CLI command mode.
- When set to `pass`, the Module tries to connect to the `wl-tcp-ip` (or `wl-tcp-ip2`) and `wl-tcp-port` LAN server. Once a connection is established, the serial interface is configured to pass-through, as if the Serial Host had issued the CLI command `pass`.
- When set to `listen`, the Module enters a state where a LAN application can initiate a TCP or HTTP connection with the Module and communicate over the serial interface using the `pass`, `putget`, or `putexpect` command.
- When set to `loop`, the Module enters a state where data received on the serial interface is looped back to the Serial Host.

A.9 HOST INTERACTION USING TCP

The serial interface between the Module and the Host operates in master-CLI, slave-listen, master pass-through, or slave pass-through modes. By factory default, the Module starts up in master-CLI mode.

A.9.1 Pass-Through Mode

If the Module has been set to start up in pass-through mode, or is directed into pass-through mode using the CLI command `pass`, it tries to make a TCP connection to the last defined `wl-tcp-ip` (or `wl-tcp-ip2`) and `wl-tcp-port` address settings.

- If the connection is successful, the Module sets the serial interface in pass-through mode.
- If the connection attempt fails, the Module continues to retry at intervals specified by the `wl-retry-time`.

The CLI command `commit` must be issued to write the TCP settings to non-volatile memory.

When the Host sets the Module for pass-through mode:

- The CLI command `pass` causes the Module to open a TCP connection to the LAN application if one is not already open. (A LAN application should be designed to listen on the target TCP port. The LAN application's IP address and TCP port are specified using the CLI commands `wl-tcp-ip`, `wl-tcp-ip2`, and `wl-tcp-port`.)
- The Module sends an `ERROR` response if the connection cannot be opened.
- When the connection is made, all data received on the serial port from the Host is tunneled to the LAN application as TCP payload.

- All data received from the LAN application is tunneled to the Host on the serial interface.
- The Host can return to CLI mode while keeping the TCP connection by issuing the escape sequence. The escape sequence is transmitted to the LAN application.
- The Module buffers sufficient data to ensure proper detection of the escape CLI command.
- The LAN application can end the session by closing the TCP port from the LAN side.
- The Host can end the TCP session by returning to CLI mode and issuing the CLI command `close`.
- If the TCP connection ends for any reason beyond the control of the Host, the Module sends an escape sequence to the Host and returns to CLI mode.
- The Host should always look for the escape sequence.

A.9.2 Detecting and Executing the Escape Sequence

If the Module detects and executes the escape sequence from the Serial Host:

- The escape sequence is transmitted to the LAN application.
- The Module sends an `OK` response to the Serial Host.
- The Serial Host becomes the owner of the serial interface.
- The Module processes data received from the Host as CLI commands.
- The TCP connection established by the prior pass-through mode does not necessarily close unless a timeout occurs, the link is lost, or the Module receives the CLI command `close` on any interface.

A.9.3 Listen Mode

The serial interface can be placed into listen mode when a Serial Host issues the CLI command `listen` or when the serial startup default has been set to listen. The Serial Host is the only device that can issue the CLI command `listen`. When this occurs:

- The Module reverts to listen mode. This mode allows LAN-based TCP (Telnet) or HTTP connections to send `putget` and `putexpect` commands or to place the Module in pass-through mode. The `senddata` content of the CLI commands `putget` and `putexpect` is passed to the Serial Host.
- The Serial Host relinquishes ownership of the serial port, allowing LAN Hosts to establish connections to it.
- The serial port essentially is available as a pass-through channel to the Host.
- The Serial Host can regain control of the serial port and CLI mode at any time by issuing the escape command. The escape command string is transmitted to the LAN Host that is in pass-through mode and has control of the serial port.

A.9.4 Effecting Serial Host-Initiated Data Communications

There are two ways to effect communication of data initiated by the Serial Host:

- **Using pass-through mode:** The TCP connection is kept open until the Serial Host closes the connection. No other interface can initiate pass-through mode or have the Module execute the CLI command `putget` or `putexpect` while the Serial Host-initiated pass-through TCP connection is open or the Serial Host is in CLI mode.
- **Issuing the CLI command `putget` or `putexpect`:** These commands cause the Module to open a TCP connection to the LAN Host and send and receive data. The entire transaction is short and quick, so the Host can switch between CLI mode and listen mode rapidly. By reverting to listen mode, the Host can interact with LAN applications that initiate connections with the Module through the TCP interface.

A.10 TCP SERVER INTERACTION

The Module includes a TCP server that supports multiple TCP connections. There are two ways to establish a TCP connection with the server, CLI mode and Tunnel mode.

The `wl-telnet-timeout` parameter applies to LAN-initiated TCP connections made to the Module. When set to zero, sessions never timeout.

A.10.1 TCP CLI Mode

A connection can be made in CLI mode that allows commands to be sent to the CLI server. In this mode, the TCP client must authenticate itself when logging into the CLI server and the TCP client will have access to the normal CLI interface.

When a TCP connection is initiated from the LAN and established, the connection is transferred to another port number, where the base port is made available for further TCP connections. The factory default TCP port number is 23. You can change this default value using the CLI command `wl-telnet-port`. The Module's TCP server supports three connections or as many as the available memory will support. For example, an active TCP connection that is in pass-through mode can use many memory buffers and significantly limit the actual number of TCP connections.

After a TCP CLI connection is established by a client LAN application:

- The Module starts each TCP session in CLI mode.
- The TCP client can issue CLI commands to the Module over this session, regardless of the mode or state of the Host. The TCP client should expect responses to commands as defined in the CLI commands.
- If the CLI command `putget` or `putexpect` is issued, the `senddata` content of the commands is passed to the Host if the Host set the serial interface to `listen` mode.
- The TCP client can issue a `pass` command to enter pass-through mode with the Host if the Host is in `listen` mode.

- When in pass-through mode, the Module tunnels data between the Host and the TCP client until either side issues the CLI command escape sequence, or until the TCP session is terminated or times out.
- Regardless of which device issues the escape sequence, the sequence is also transmitted to the other side of the connection.
- If the TCP client issues the escape sequence, the TCP server reverts to CLI mode. The Host interface remains in `listen` mode.
- If the Host issues the escape sequence, the escape sequence is transmitted to the TCP client and the TCP client is switched to CLI mode. The Host also enters CLI mode.

A.10.2 TCP Tunnel Mode

If a connection is made using tunnel mode, an immediate pass-through connection is initiated, without requiring authentication or additional commands. The tunnel server bypasses the CLI server and escape sequence checking. The tunnel server supports only one TCP connection on the port specified by the `wl-tunnel-port` parameter.

When a TCP connection is initiated from the LAN to the tunnel port, a pass-through connection is immediately initiated, without having to enter an authorization string or command. This connection is intended for data transfer only and provides no way to escape to CLI mode.

The `wl-tunnel` CLI command enables or disables the tunnel server. The `wl-tunnel-port` CLI command sets the port that the tunnel server monitors for a connection.

A.10.3 TCP Server and Telnet

The TCP server supports a Telnet connection by observing the following limitations:

- Telnet option negotiation should be turned off.
- Telnet commands such as `DO`, `WONT`, and `DON` must not be issued.
- Network Virtual Terminal codes are not supported.
- NUT 7-bit encoding does not allow 8–bit data transfers.

Table 24. Example of TCP Interaction using Telnet

	 **Telnet Client**	 **Airborne WLN Module**
1.	`telnet <WLN IP adrs> <CR>` Connects to the Module TCP server.	
2.		TCP server accepts the connection. The connection is in CLI mode.
3.	`auth dpac dpac<CR>` Authenticates the connection with Module.	
4.		`OK<CR><LF>` Services the command and responds.
5.	`wl-telnet-timeout 0<CR>` Sets the TCP connection timeout to infinite. Applies to subsequent connections, not the current one.	
6.		`OK<CR><LF>` Services the command and responds.
7.	`pass<CR>` Requests entry to pass-through mode. Assumes the Module is in listen mode.	
8.		`OK<CR><LF>` Checks that the Serial Host is in listen mode. Indicates it is OK to transmit pass-through data.
9.	`01010101001` Sends raw data.	Receives the raw data
10.		`01010101001` The Module sends raw data to the Serial Host. The Host sends responding raw data to the Module.
11.		The Module forwards the raw data to the Telnet Client.
12.	`11101010101` Receives the raw data from the Module.	
13.	`~~~ds<CR>` Commands the Module to set the TCP interface back to CLI mode – escape sequence is passed to Host.	
14.		`~~~dsOK<CR><LF>` Sets the interface to CLI mode and `OK`s the Telnet Client request.

A.11 HOST INTERACTION USING UDP

The UDP functions (between the Module and the Host) operate in pass-through mode. By factory default, the Module starts up in master-CLI mode.

A.11.1 Pass-Through Mode

If the Module has been set to start up in pass-through mode, or is directed into pass-through mode using the CLI command `pass`, it will transmit to the UDP target last defined with the `wl-udp-ip` and `wl-udp-port` address settings.

- The UDP functions must be enabled via the CLI commands `wl-udp-xmit`, `wl-xmit-type`.

The CLI command `commit` must be issued to write the UDP settings to non-volatile memory.

When the Host sets the Module for pass-through mode:

- The CLI command `pass` causes the Module to transmit data to the `wl-udp-ip`/`wl-udp-port` target. The module will also broadcast the data if the `wl-udp-xmit` is set to `bcast` or `both`.
- All data received on the serial port from the Host is sent to the `wl-udp-ip`/`wl-udp-port` target as UDP payload.
- All data received from the LAN on the `wl-udp-rxport` is delivered to the Host on the serial interface.
- The Host can return to CLI mode by issuing the escape sequence. The escape sequence is transmitted to the LAN application.
- The Module buffers sufficient data to ensure proper detection of the escape CLI command.
- The Host should always look for the escape sequence.

A.11.2 Detecting and Executing the Escape Sequence

If the Module detects and executes the escape sequence from the Host:

- The escape sequence is transmitted to the LAN application.
- The Module sends an `OK` response to the Host.
- The Host becomes the owner of the serial interface.
- The Module processes data received from the Host as CLI commands.

A.11.3 Using Pass-Through Mode

The UDP functions are kept active until the Host breaks PASS mode.

A.12 UDP INTERACTION

The Module includes UDP support. There are two configuration options to activate UDP. UDP transmit can be enabled either in a “UDP” only or “both” mode.

The `wl-udp-ip, wl-udp-port, wl-udp-xmit, wl-xmit-type, wl-udp-rxport` commands apply to UDP functions for the Module (see section A.21.3 LAN Communication Commands, starting on page 83, for command parameters and descriptions).

A.12.1 UDP Only Mode

A connection can be made in CLI mode that allows commands to be sent to the CLI server. In this mode, the Telnet client must authenticate itself when logging into the CLI server and the Telnet client will have access to the normal CLI interface.

The factory default UDP transmit and receive port number is `8023`. You can change this default value using the CLI commands `wl-udp-port and wl-udp-rxport`.

UDP frames will be passed to the `wl-udp-ip`/`wl-udp-port` address and/or broadcasted if `wl-udp-xmit` is set to `bcast` or both, when the unit is in PASS mode. In addition, UDP frames will be received on the `wl-udp-rxport` when the unit is in PASS mode.

A.12.2 Both Mode

A connection must be made using the TCP tunnel. UDP will transmit and receive UDP frames (like in UDP only mode) when the TCP tunnel is established and active. When the TCP connection closes, UDP operations halt. If the TCP tunnel is active, thereby allocating the serial port, then received UDP datagrams will be dropped.

A.13 XMODEM GUIDELINES

The Module can be placed in pass-through or listen mode using the CLI command `pass` or `listen`, respectively. In these modes, data can pass between the Module and either a Serial Host or a LAN Host. If the XMODEM protocol is used to transfer data in these modes, observe the following guidelines. These guidelines also apply if the CLI command `update` is used to update the Module firmware.

- XMODEM works with 8-bit connections only. If you communicate with the Module via a serial port connection, configure your communication settings as follows:
  Data bits: 8
  Parity: None
  Stop bits: 1

- Run XMODEM with either no flow control or hardware (RTS/CTS) flow control, because the protocol provides no encoding or transparency of control characters. If you run XMODEM with software (XON/XOFF) flow control, your connection will hang. For this reason, configure the flow control parameter in your communication settings to NONE or RTS/CTS, not to XON/XOFF or BOTH.

- During transmission, XMODEM pads files to the nearest 128 bytes. As a result, original file sizes are not retained.

A.14 WEB SERVER INTERFACE

The Module includes a Web Server that responds to HTTP traffic on the wireless interface and, therefore, from the LAN or Internet. The Module includes built-in Web pages. Some of these pages are designed for accessing Module-specific parameters and status, while other pages are designed for OEM product-specific content. All page requests (from a browser, for example) are handled by the Web server, even though the location of the page contents may vary. For example, OEM pages typically obtain content from the Host, but can also obtain content from the Module. Module pages, on the other hand, obtain content only from the Module.

All Web pages on the Module comprise a simple HTML framework with embedded JavaScript. After an HTTP `page get` is issued, the browser executes the JavaScript. The JavaScript is expected to include code that issues HTTP `put`s or `get`s that can include the CLI commands `putget` or `putexpect` to obtain content for Web pages from the Host. The JavaScript can then process and display the data appropriately on the browser.

The JavaScript-initiated connection should be kept open for as short a time as possible to allow other traffic to interleave easily between the JavaScript requests. For this reason, the Module and Host must be readily available to serve OEM page content or interact with other connections.

When the OEM Web pages derive content from the Host:

- The Serial Host must be in listen mode to receive and respond to the CLI command `putget` or `putexpect` or to pass-through data.
- The Module executes the CLI commands `putget` and `putexpect` issued by the remote HTTP client and passes the `senddata` content to the Serial Host.
- Data sent to the Serial Host requesting content must include sufficient identification of the source and context of the requesting data to allow the Serial Host to provide corresponding appropriate return data.

- When using the `putget` and `putexpect` commands, the Serial Host may respond with complete HTML blocked data, which the JavaScript can embed in the Web page.
- It is recommended that only the `putget` or `putexpect` command be used from an embedded JavaScript.

For more information about customizing Module Web pages, refer to the Airborne OEM Configuration Tool documentation or contact DPAC Technologies.

A.15 WIRELESS LAN ROAMING

Roaming is enabled when the Module is set to Infrastructure mode and is disabled for Ad Hoc mode. When configured for Infrastructure mode, the Module supports roaming in accordance with the IEEE 802.11 specification. To enter this mode, use the CLI command `wl-type`. In this mode, you can use the CLI commands in Table 25 to affect the Module's roaming capabilities directly and indirectly.

Table 25. CLI Commands That Affect Roaming

CLI Commands that Directly Affect Roaming	CLI Commands that Indirectly Affect Roaming
`wl-type`	`wl-dhcp`
`wl-ssid`	`wl-dhcp-renew`
`wl-apdensity`	
`wl-rate`	

The `wl-ssid` command lets you specify the AP with which the Module should associate at startup. This command accepts the argument `any` or a valid SSID string. If set to `any`, the Module scans for APs and associates with the AP that has the best signal quality.

The `any` argument does not support roaming. If the Module disassociates from an AP with this argument in effect, the Module does not try to reassociate.

The command `wl-ssid` directs the Module to associate with an AP whose SSID you specify as an argument. The command `wl-ssid` supports roaming. If the Module loses its association with one AP with this command in effect, the Module tries to automatically associate with an AP that has a matching SSID (the WEP security and authentication strings must all match). If DHCP is enabled, a DHCP renew operation is performed with each new association to reconfirm IP address settings.

The `wl-apdensity` and `wl-rate` commands affect how readily the Module will disassociate from an AP and associate with another while roaming. The `wl-apdensity` setting 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. The `wl-rate` setting specifies the Module's maximum wireless data rate, in Mbps. For rates above 1 Mbps the Module may fall back to a lower rate. Note that lower data rates may result in better range, causing the Module to remain connected to the current AP. By increasing the rate, the Module will tend to have reduced range and switch more readily to

another AP. Note that the `wl-apdensity` command requires radio firmware version `1.8.4` or later.

When DHCP is enabled, each reassociation the Module makes with another AP causes the Module to renew its DHCP settings. To determine whether the Module is associated, use the SSID and BSSID values returned by the `wl-status` or `wl-info` command.

A.16 POWER MANAGEMENT MODES — UART MODEL ONLY

The Module supports several power-management modes that can be used to reduce the average current consumption. Use the CLI command `pm-mode` to change the power-management settings. Table 26 summarizes the different settings and their affect.

Table 26. Power Management Modes

Power Management Mode	Association	Wake-Up Methods
Active	Associated	Already awake
Doze	Associated	Wireless data or Serial data
Snooze	Associated	Wireless data or Serial Break
Sleep	Disassociated	Serial Break character
Off	Disassociated	Serial Break character

The IEEE 802.11b standard dictates that the AP can reject requests for Low Power operation, and require the Module to operate in the active mode. The actual current consumption depends on the AP and its low-power support implementation.

Transitions into the Sleep and Off modes are allowed under control of the Serial Host. Snooze is intended for network-initiated activity and waking after a UART Break is received. The Module automatically transitions back to Snooze after 60-to-120 seconds of inactivity. After waking on receipt of a radio packet, the Module transitions back to Snooze immediately after the processor idles.

When in Sleep mode, the Module automatically transitions back to Sleep after 60-to-120 seconds of inactivity following waking on UART activity or Radio Transmit.

From the Off mode, the Module goes to the Active state after receiving a UART Break. It remains in the Active state until the CLI command `pm-mode off` is issued.

A.17 CLI SECURITY

When the Module is accessed from a LAN application through the wireless interface using Telnet, HTTP, or TCP, every transaction is authenticated.

The Module supports five levels of security:

- Level 0 (L0) = connectionless
- Level 1 (L1) = connection, not logged in (*default*)

- Level 2 (L2) = data
- Level 3 (L3) = config
- Level 4 (L4) = OEM
- Level 5 (L5) = MFG

Level 0 is the connectionless access level. Access over UDP will rate this access level. The L0 level provides access to the name query services. It is not an authenticated level.

Level 1 is the default security level when power is applied.

Each security level has access to all security levels below it. For example, Level 2 has access to Level 2, Level 1, and Level 0 commands, but cannot access Level 4 and Level 3 commands.

The user or application must execute the CLI command `auth` before other commands can be accessed. In the CLI command definition tables in the following sections, the **Ln** column indicates the access level required to execute each command. The CLI command `logout` returns the Module to security Level 1.

A.18 CLI CONVENTIONS

The CLI uses the following conventions:

- All commands consist of a string of printable characters, including the command and optional arguments delimited by one or more spaces or tabs. Multiple consecutive spaces or tabs are considered as one delimiter.
- Commands and arguments are case sensitive, except hexadecimal values and port IDs, which can be upper- or lower-case.
- Arguments enclosed within […] are optional.
- All arguments are literal ASCII text, except where indicated.
- Most commands that set the value of a parameter can also obtain the value of the parameter by omitting the argument. Numeric values are returned in aschex format.
- A choice between arguments is indicated with the | character. Only one of the choices can be selected.
- All CLI commands are terminated with a <CR>.
- The maximum length of a CLI command line is 1800 characters, including spaces and terminating characters.
- Argument types include:

– <*string*> – literal ASCII character string without delimiters (no spaces or tabs)

– <*integer*> – value represented as a decimal integer or as “aschex” value in the form 0xhhh…hhh

– <aschex> – one or more pairs of hexadecimal digits with no prefix in the form hhh…hhh

- <*portid*> – an I/O port bit number, from 0 to 7
- <*IPadrs*> - Internet Protocol address string in the format: *nnn.nnn.nnn.nnn*; for example: 192.168.10.3

A.19 ASCHEX VS. BINARY VALUES

Data can be sent to the Module as either binary data or a hexadecimal representation of the actual data being transmitted.

When a LAN device or serial port Host issues a `pass` command, the data is transmitted as binary data. By comparison, when the command `putget` or `putexpect` is issued, the `senddata` content must be encoded as ASCII hexadecimal digit pairs. The data is translated across the Module and received as an ASCII representation of the actual data. This is true whether the transmission initiates from the LAN device or from the Host.

For example, the digits 31 correspond to the ASCII character 1. If you issue a `putget` or `putexpect` command with the `senddata` value of 314151, the destination receives the ASCII characters **1**, **A**, and **Q**.

A.20 COMMAND RESPONSES

The Module responds to CLI commands with a response indicating whether the CLI command was executed successfully. All responses are followed by `<CR><LF>`.

After the Module executes a CLI command successfully, it returns the response:

```
OK
```

Otherwise, it returns an error response. Error responses are returned in the following general format:

```
Error 0xhhhh: error text
```

where the aschex value is the error code.

A.21 CLI COMMANDS

CLI commands are organized into the following categories:

Note: Some CLI commands require the Module to be restarted before they take effect, while others do not. In the following sections, an asterisk (*) in the **Ln** column denotes a command that requires the Module to be restarted. Use the CLI command `commit` to store your current changes to flash memory before restarting; otherwise, changes will be discarded at the next restart.

A.21.1 LAN Configuration Commands

Command	CLI Arguments	Ln	Description
wl-ip	[IPadrs]	L3*	**Static IP Address if DHCP Client is Disabled** Default is `0.0.0.0`.
wl-subnet	[IPadrs]	L3*	**Static Subnet Mask if DHCP Client is Disabled** Default is `255.255.255.0`.
wl-gateway	[IPadrs]	L3*	**Static Default Gateway/Router IP Address** Default is `0.0.0.0`.
wl-udap	[string]	L3*	**UDAP Discovery Enable or Disable** `0` = disable `1` = enable (*default*)
wl-dhcp	[string]	L3*	**DHCP Client Enable or Disable** If DHCP fails, the Module's IP address will be `0.0.0.0`. However, if `wl-dhcp-fb` is enabled, then the value from `wl-dhcp-fbip` will be used. `0` = disable `1` = enable (*default*)

Command	CLI Arguments	Ln	Description
wl-dhcp-renew		L3	**Release Current DHCP Information and Make a New Request**
wl-dhcp-client	[string]	L3	**DHCP Client Host Name String** Up to 31 characters, no spaces. Default is `Airbornexxxxxx` where `xxxxxx` are the last six hexadecimal digits of the Module's MAC address.
wl-dns1	[IPadrs]	L3	**Primary DNS Server Address** 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.
wl-dns2	[IPadrs]	L3	**Secondary DNS Server Address** Sets the secondary DNS server address for DNS lookups when the primary DNS server is unavailable. Default is 0.0.0.0.
wl-dns	string	L2	**Perform DNS Lookup** Performs a DNS lookup for the specified Host name string. The IP address for the Host is returned as an IPadrs string.
wl-dhcp-mode	[<0 | 1>]	L3*	**DHCP Retransmission Mode** Sets the DHCP retransmission mode to either Exponential (`0`) or Fixed interval (`1`). Default is `0`.
wl-dhcp-interval	[<interval in seconds>]	L3*	**DHCP Retransmission Interval** Sets the DHCP retransmission interval (in seconds) to use when `wl-dhcp-mode` is set to fixed. This is an integer with a range of `1-64`. Default is `15`.
wl-dhcp-fb	[<0 | 1 >]	L3*	**DHCP Fallback Method** 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`.
wl-dhcp-acqlimit	[<number of seconds>]	L3*	**DHCP Acquire 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. This is an integer with a range of `1-255`. Default is `150`.
wl-dhcp-fbip	[<ip address>]	L3*	**DHCP Fallback IP Address** Sets the fallback IP address. Default is `0.0.0.0`.
wl-dhcp-fbsubnet	[<subnet mask>]	L3*	**DHCP Fallback Subnet Mask** Sets the fallback subnet mask. Default is `0.0.0.0`.
wl-dhcp-fbgateway	[<ip address>]	L3*	**DHCP Fallback Gateway Address** Sets the fallback gateway address. Default is `0.0.0.0`.

A.21.2 Wireless Configuration Commands

Command	CLI Arguments	Ln	Description
wl-mac	[aschex]	L4*	**Wireless Ethernet MAC** Six bytes aschex. The address specified by the argument temporarily overwrites the factory value when the Module starts up. If the `reset` command is issued, the Module reverts to the factory-set MAC address at startup. **Use with caution.** Set at the DPAC factory.
wl-type	[string]	L3*	**Wireless Network Type** `a` = Infrastructure (AP) mode (*default*) `p` = Peer-to-peer (Ad Hoc) mode In Infrastructure mode, the `wl-ssid` parameter controls the Module's automatic AP roaming behavior at startup. In peer-to-peer mode, the `wl-chan` parameter controls the radio channel the Module uses at startup.
wl-chan	[integer]	L2*	**Wireless Ad Hoc Channel Number** Applies to peer-to-peer Ad Hoc mode only. Channel range is 1 – 14. Default is `1`.
wl-ssid	[string]	L3*	**Apply SSID** Up to 31 characters, no spaces. In Infrastructure mode, the SSID controls which AP the Module connects to and affects the Module's roaming behavior. In Ad Hoc mode, the SSID defines the network name for the ad hoc devices. Only the devices with the same SSIDs can connect to each other. The Module must be restarted for the setting to take effect. `any` = the Module associates with the AP that has the best signal quality, regardless of the AP's WEP, DHCP, authentication, or other capabilities. Roaming is not supported. (*default*) `<other_value>` = the Module associates with the AP matching the SSID that has the best signal quality. Roaming is supported.
wl-wep	[integer]	L3*	**WEP Security – Number of Bits** `0` = WEP security is disabled. (*default*) `64` = 64-bit key length `128` = 128-bit key length
wl-auth	[string]	L3*	**WEP Authentication** `auto` = automatically detects the authentication. (*default*) `open` = authenticates using Open Key algorithm. `shared` = authenticates using Shared Key algorithm.
wl-def-key	[integer]	L3*	**Set Default WEP Key** Selects the default WEP key. Range is 1 – 4. Default is `1`.
wl-key-1	[aschex]	L3*	**Set WEP Key 1 to Binary Value** [10 or 26 hex digits] – 10 digits for 64 bits, 26 for 128 bits. Default is `0000000000000000000000000000`.
wl-key-2	[aschex]	L3*	**Set WEP Key 2 to Binary Value** [10 or 26 hex digits] – 10 digits for 64 bits, 26 for 128 bits. Default is `0000000000000000000000000000`.

Command	CLI Arguments	Ln	Description
wl-key-3	[aschex]	L3*	**Set WEP Key 3 to Binary Value** [10 or 26 hex digits] – 10 digits for 64 bits, 26 for 128 bits. Default is `00000000000000000000000000`.
wl-key-4	[aschex]	L3*	**Set WEP Key 4 to Binary Value** [10 or 26 hex digits] – 10 digits for 64 bits, 26 for 128 bits. Default is `00000000000000000000000000`.
wl-ant	[string]	L3*	**Antenna Selection** `1` = Ant1 (*default*) `2` = Ant2 (not currently supported) `d` = enables receive diversity

wl-scan	[string]	L2	**Scan for APs and Report Status**
			If [string] is specified, AP SSIDs that match the string are listed. Partial matching SSIDs are listed when the * wildcard is appended to string. For example, if APs have an SSID of `Airborne31` and the SSID is `Airborne*`, the Module scans for APs that start with `Airborne`.
			
			Status report for each found AP is as follows. For a description of these results, refer to Table 27 on page 78.
			
			`SSID: FirstAccessPoint`
			`BSSID: 0006255D537D`
			`signal (dBm): -56`
			`noise (dBm): -92`
			`rate (KB/s): 0x0014`
			`capabilities: 0x0005`
			`channel: 0x0007`
			`----------`
			`SSID: SecondAccessPoint`
			`BSSID: 0006255D5C2C`
			`signal (dBm): -55`
			`noise (dBm): -80`
			`rate (KB/s): 0x000A`
			`capabilities: 0x0015`
			`channel: 0x0008`
			`----------`

wl-apdensity	[string]	L3	**Module 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. Note: Requires radio firmware version 1.8.4 or higher.
wl-rate	[string]	L3	**Wireless Communication Rate** Specifies the maximum wireless data rate for the Module, in Mbps. For rates above 1 Mbps, the Module may fall back to a lower rate. Lower data rates may result in better range. `1` = 1 Mbps `2` = 2 Mbps (*default*) `5.5` = 5.5 Mbps `11` = 11 Mbps Note: Requires radio firmware version 1.8.4 or higher.

Command	CLI Arguments	Ln	Description

wl-device		L1	**Module Device Type**
			Returns a string describing the Module firmware type.
			`AIRBORNE`
			`AIRBORNE-SPI`
			`DIRECT-ETHERNET`
			`DIRECT-SERIAL`

wl-region	[string]	L3	**Module Operation Region** Specifies the wireless channels allowed. The parameter must be one of the ISO standard two-letter codes listed in Table 28 on page 79. The setting applies only when the Module is in Ad Hoc mode. In Infrastructure mode, the AP determines the channel used. Default is `US`.

wl-status		L2	**Report Abridged Module Status**
			The following example shows a response if the Module is associated with an AP. For a description of these results, refer to Table 29 on page 80.
			`SSID: FirstAccessPoint`
			`BSSID: 0006255D537D`
			`signal (dBm): -56`
			`noise (dBm): -92`
			`quality: (dBm): 57`
			`rate (KB/s): 0x0014`
			`link status: 0x05`
			`port status: 0x0004`
			`dhcp status: 0x02`
			The following example shows a response if the Module is not associated. The SSID and BSSID values are valid if the Module is disassociated from an AP and can be used to determine this condition.
			`SSID: non-spec`
			`BSSID: 444444444444`
			`signal (dBm): -73`
			`noise (dBm): -73`
			`quality: (dBm): 0`
			`rate (KB/s): 0x0014`
			`link status: 0x00`
			`port status: 0x0002`
			`dhcp status: 0x00`

Command	CLI Arguments	Ln	Description

wl-info		L2	**Report Comprehensive Module Status**
			The following example shows a response if the Module is associated with an AP. For a description of these results, refer to Table 29 on page 80.
			
			`Firmware Version: 2.0.2.0`
			`MAC Firmware Version: 1.7.6`
			`Link Status: 1`
			`Port Status: 4`
			`SSID: FirstAccessPoint`
			`MAC Address: 0090C9004A80`
			`BSSID: 00095B6F270C`
			`Transmit Rate (Mb/s): 1`
			`Signal Level (dBm): -41`
			`Noise Level (dBm): -92`
			`Communications Quality (dBm): 51`
			`IP Address: 192.168.0.5`
			`Subnet mask: 255.255.255.0`
			`Default gateway: 192.168.0.1`
			`Primary DNS: 0.0.0.0`
			`Secondary DNS: 0.0.0.0`
			`NM Heap Free: 2415`
			`VM Heap Free: 6685`
			`Netpages Free: 122`
			`Up Time (Sec): 2183`

wl-tally		L2	**Report Radio/MAC Performance Statistics**
			For a description of these results, refer to Table 30 on page 81.
			
			`TxUnicastFrames: 0x0002`
			`TxMulticastFrames: 0x0000`
			`TxFragments: 0x0012`
			`TxUnicastOctets: 0x02D8`
			`TxMulticastOctets: 0x0000`
			`TxDeferredTransmissions: 0x0261`
			`TxSingleRetryFrames: 0x0000`
			`TxMultipleRetryFrames: 0x0000`
			`TxRetryLimitExceeded: 0x0068`
			`TxDiscards: 0x0000`
			`RxUnicastFrames: 0x0007`
			`RxMulticastFrames: 0x007C`
			`RxFragments: 0x0083`
			`RxUnicastOctets: 0x0198`
			`RxMulticastOctets: 0x28FE`
			`RxFCSErrors: 0x0007`
			`RxDiscardsNoBuffer: 0x0000`
			`TxDiscardsWrongSA: 0x0000`
			`RxDiscardsWEPUndecryptable: 0x0000`
			`RxMessageInMsgFragments: 0x0000`
			`RxMessageInBadMsgFragments: 0x0000`

Table 27. Description of wl-scan Results

`wl-scan` Result	Description
`SSID`	**Service Set Identifier String**
`BSSID`	**MAC Address of the Responding AP**
`Signal`	**Signal Level (dBm)** The higher (more positive) number indicates a stronger signal.
`Noise`	**Average Noise Level (dBm)** The lower (more negative) number indicates a quieter environment.
`Rate`	**Raw Wireless Data Rate** `0x0A` = 1 Mbps `0x14` = 2 Mbps `0x37` = 5.5 Mbps `0x6E` = 11 Mbps
`Capabilities`	**Capabilities** Bits 1-0: AP Extended Service Set 01 = Infrastructure mode. 10 = Ad Hoc (peer-to-peer) mode. Bits 3-2: Contention Free Polling Bits Bit 4: Privacy 0 = WEP disabled. 1 = WEP enabled. Bit 5: Preamble Used 0 = use normal preamble. 1 = use short preamble. Bit 6: Data Rates 0 = use normal rates for 802.11b. 1 = supports high data rate. Bit 7: Channel Agility 0 = do not use channel agility. 1 = use channel agility. Bits 8-15: Reserved
`Channel`	**Channel Number (1 to 14)**

Table 28. Region Country Codes

Code	Country	Code	Country	Code	Country
AF	Afghanistan	GH	Ghana	PK	Pakistan
AX	Åland Islands	GI	Gibraltar	PW	Palau
AL	Albania	GR	Greece	PS	Palestinian Territory
DZ	Algeria	GL	Greenland	PA	Panama
AS	American Samoa	GD	Grenada	PG	Papua New Guinea
AD	Andorra	GP	Guadeloupe	PY	Paraguay
AO	Angola	GU	Guam	PE	Peru
AI	Anguilla	GT	Guatemala	PH	Philippines
AQ	Antarctica	GN	Guinea	PN	Pitcairn
AG	Antigua and Barbuda	GW	Guinea-Bissau	PL	Poland
AR	Argentina	GY	Guyana	PT	Portugal
AM	Armenia	HT	Haiti	PR	Puerto Rico
AW	Aruba	HM	Heard Island and McDonald Islands	QA	Qatar
AU	Australia	VA	Holy See (Vatican City State)	RE	Réunion
AT	Austria	HN	Honduras	RO	Romania
AZ	Azerbaijan	HK	Hong Kong	RU	Russian Federation
BS	Bahamas	HU	Hungary	RW	Rwanda
BH	Bahrain	IS	Iceland	SH	Saint Helena
BD	Bangladesh	IN	India	KN	Saint Kitts and Nevis
BB	Barbados	ID	Indonesia	LC	Saint Lucia
BY	Belarus	IR	Iran, Islamic Republic of	PM	Saint Pierre and Miquelon
BE	Belgium	IQ	Iraq	VC	Saint Vincent and the Grenadines
BZ	Belize	IE	Ireland	WS	Samoa
BJ	Benin	IL	Israel	SM	San Marino
BM	Bermuda	IT	Italy	ST	Sao Tome and Principe
BT	Bhutan	JM	Jamaica	SA	Saudi Arabia
BO	Bolivia	JP	Japan	SN	Senegal
BA	Bosnia and Herzegovina	JO	Jordan	CS	Serbia and Montenegro
BW	Botswana	KZ	Kazakhstan	SC	Seychelles
BV	Bouvet Island	KE	Kenya	SL	Sierra Leone
BR	Brazil	KI	Kiribati	SG	Singapore
IO	British Indian Ocean Territory	KP	Korea, Democratic People's Republic of	SK	Slovakia
BN	Brunei Darussalam	KR	Korea, Republic of	SI	Slovenia
BG	Bulgaria	KW	Kuwait	SB	Solomon Islands
BF	Burkina Faso	KG	Kyrgyzstan	SO	Somalia
BI	Burundi	LA	Lao People's Democratic Republic	ZA	South Africa
KH	Cambodia	LV	Latvia	GS	South Georgia and the South Sandwich Islands
CM	Cameroon	LB	Lebanon	ES	Spain
CA	Canada	LS	Lesotho	LK	Sri Lanka
CV	Cape Verde	LR	Liberia	SD	Sudan
KY	Cayman Islands	LY	Libyan Arab Jamahiriya	SR	Suriname
CF	Central African Republic	LI	Liechtenstein	SJ	Svalbard and Jan Mayen
TD	Chad	LT	Lithuania	SZ	Swaziland
CL	Chile	LU	Luxembourg	SE	Sweden
CN	China	MO	Macao	CH	Switzerland
CX	Christmas Island	MK	Macedonia, The Former Yugoslav Republic of	SY	Syrian Arab Republic
CC	Cocos (Keeling) Islands	MG	Madagascar	TW	Taiwan (Republic of China)
CO	Colombia	MW	Malawi	TJ	Tajikistan
KM	Comoros	MY	Malaysia	TZ	Tanzania, United Republic of
CG	Congo	MV	Maldives	TH	Thailand
CD	Congo, The Democratic Republic of the	ML	Mali	TL	Timor-Leste
CK	Cook Islands	MT	Malta	TG	Togo
CR	Costa Rica	MH	Marshall Islands	TK	Tokelau
CI	Côte d'Ivoire	MQ	Martinique	TO	Tonga
HR	Croatia	MR	Mauritania	TT	Trinidad and Tobago

Table 28. Region Country Codes

Code	Country	Code	Country	Code	Country
CU	Cuba	MU	Mauritius	TN	Tunisia
CY	Cyprus	YT	Mayotte	TR	Turkey
CZ	Czech Republic	MX	Mexico	TM	Turkmenistan
DK	Denmark	FM	Micronesia, Federated States of	TC	Turks and Caicos Islands
DJ	Djibout	MD	Moldova, Republic of	TV	Tuvalu
DM	Dominica	MC	Monaco	UG	Uganda
DO	Dominican Republic	MN	Mongolia	UA	Ukraine
EC	Ecuador	MS	Montserrat	AE	United Arab Emirates
EG	Egypt	MA	Morocco	GB	United Kingdom
SV	El Salvador	MZ	Mozambique	US	United States
GQ	Equatorial Guinea	MM	Myanmar	UM	United States Minor Outlying Islands
ER	Eritrea	NA	Namibia	UY	Uruguay
EE	Estonia	NR	Nauru	UZ	Uzbekistan
ET	Ethiopia	NP	Nepal	VU	Vanuatu
FK	Falkland Islands (Malvinas)	NL	Netherlands		Vatican City State see Holy See
FO	Faroe Islands	AN	Netherlands Antilles	VE	Venezuela
FJ	Fiji	NC	New Caledonia	VN	Viet Nam
FI	Finland	NZ	New Zealand	VG	Virgin Islands, British
FR	France	NI	Nicaragua	VI	Virgin Islands, U.S.
GF	French Guiana	NE	Niger	WF	Wallis and Futuna
PF	French Polynesia	NG	Nigeria	EH	Western Sahara
TF	French Southern Territories	NU	Niue	YE	Yemen
GA	Gabon	NF	Norfolk Island		Zaire see Congo, The Democratic Republic of the
GM	Gambia	MP	Northern Mariana Islands	ZM	Zambia
GE	Georgia	NO	Norway	ZW	Zimbabwe
DE	Germany	OM	Oman		

Table 29. Description of wl-status & wl-info Results

Result	Description
`SSID`	**Service Set Identifier String**
`BSSID`	**MAC Address of the Responding AP**
`Signal`	**Signal Level (dBm)** The higher (more positive) the number, the stronger the signal.
`Noise`	**Average Noise Level (dBm)** The lower (more negative) the number, the quieter the environment.
`Quality`	**Communications Quality (dBm)** This is a measure of the signal-to-noise ratio. A higher value indicates better quality.
`Rate`	**Raw Wireless Data Rate** `0x0A` = 1 Mbps `0x14` = 2 Mbps `0x37` = 5.5 Mbps `0x6E` = 11 Mbps
`Link Status`	**Wireless Local Network Link Status** `0` = Association not yet completed `1` = Connected `2` = Disconnected `3` = AP change `4` = AP out of range `5` = AP in range `6` = Association failed

Table 29. Description of wl-status & wl-info Results

Result	Description
`Port status`	**Current MAC Port Connection Status** `1` = Disabled `2` = Searching for initial connection `3` = Connected to IBSS `4` = Connected to ESS `5` = Out of range (in ESS) `8` = Started Host AP
`DHCP status`	**DHCP Status** `0` = DHCP is disabled. `1` = DHCP is in the process of leasing an address. `2` = DHCP has leased an address.
`NM Heap Free`	**Native Memory** Number of bytes free in native memory.
`VM Heap Free`	**Virtual Memory** Number of bytes free in virtual memory.
`Netpages Free`	**Network Data Buffers** Number of network data buffers free. A page (buffer) contains 256 bytes.
`Up Time`	**Up Time** Time, in seconds, since the Module was restarted or rebooted.

Table 30. Description of wl-tally Results

`wl-tally` Result	Description
`TxUnicastFrames`	Total number of successfully transmitted MAC Service Data Units (MSDUs) for which the Destination Address is a unicast MAC address. This implies having received an acknowledgment to all associated MAC Protocol Data Unit (MPDUs).
`TxMulticastFrames`	Total number of successfully transmitted MSDUs for which the Destination Address is a multicast MAC address (including the broadcast MAC address). When operating as a station in an ESS, these frames are directed to the AP. This implies having received an acknowledgment to all associated MPDUs.
`TxFragments`	Total number of successfully delivered Data or Management MPDUs. This includes directed MPDUs transmitted and being ACKed, as well as non-directed MPDUs transmitted.
`TxUnicastOctets`	Total number of octets transmitted successfully as part of a successfully transmitted unicast MSDUs (see Tal.TxUnicast). These octets include the MAC Header and Frame Body [std 7.1.2] of all associated fragments.
`TxMulticastOctets`	Total number of octets transmitted successfully as part of a successfully transmitted multicast (including broadcast) MSDUs. These octets include the MAC Header and Frame Body [std 7.1.2] of all associated fragments.
`TxDeferredTransmissions`	Number of MSDUs for which one or more (or a fragment of one or more) transmission attempt(s) was deferred to avoid a collision.
`TxSingleRetryFrames`	Number of MSDUs successfully transmitted after one retransmission (based on the total of all associated fragments).
`TxMultipleRetryFrames`	Number of MSDUs successfully transmitted after more than one retransmission (based on the total of all associated fragments).

Table 30. Description of wl-tally Results

wl-tally Result	Description
TxRetryLimitExceeded	Number of times an MSDU was not transmitted successfully because the retry limit (either the ShortRetryLimit or the LongRetryLimit) was reached, due to no acknowledgment or CTS received.
TxDiscards	Number of transmit requests discarded to free buffer space. This tally increments when one of the following occurs: • Transmit packet queued is too long on one of the transmit queues, due to many retries and defers, or otherwise not being able to transmit (for example, scanning). • Transmit packet queued is too long on the Power-Save queue (for a station in IBSS, the destination station did not respond to ATIM; for an AP, the station did not poll or wake up in time).
RxUnicastFrames	Total number of successfully received MSDUs with a unicast MAC address as the destination address.
RxMulticastFrames	Total number of successfully received MSDUs with a multicast MAC address (including the broadcast MAC address) as the destination address.
RxFragments	Total number of successfully received MPDUs of type data or management.
RxUnicastOctets	Total number of octets received successfully as part of unicast MSDUs. These octets include the MAC Header and Frame Body [std 7.1.2] of all associated fragments.
RxMulticastOctets	Total number of octets received successfully as part of multicast (including broadcast) MSDUs (see TxMulticast). These octets include the MAC Header and Frame Body [std 7.1.2] of all associated fragments.
RxFCSErrors	Number of MPDUs considered to be destined for this station (Address1 matches) received with an FCS error. This does not include “items” received with an incorrect CRC in the Physical Layer Convergence Protocol header. These are not considered MPDUs.
RxDiscardsNoBuffer	Number of received MPDUs discarded due to a lack of buffer space.
TxDiscardsWrongSA	Number of transmit requests discarded due to an incorrect source address (Source Address does not equal OwnMACAddress). This applies only to a station with a BSS port.
RxDiscardsWEPUndecryptable	Number of received MPDUs, with the WEP subfield in the Frame Control field set to one, discarded because it should not have been encrypted or because the receiving station did not implement the privacy option.
RxMessageInMsgFragments	Total number of MPDUs of type Data or Management received successfully, while there was another good reception occurring above the carrier-detect threshold (the message-in-message path #1 in the RF modem).
RxMessageInBadMsgFragments	Total number of Data or Management MPDUs received successfully, while there was another reception occurring above the carrier-detect threshold with a bad or incomplete PLCP preamble and header (the message-in-message path #2 in the RF modem).

A.21.3 LAN Communication Commands

Command	CLI Arguments	Ln	Description
wl-telnet-timeout	[integer]	L3	**TCP Server Session Inactivity Timeout** Specifies the TCP connection inactivity timeout. A setting of 0 specifies an infinite timeout. Applies to a new session. 32 bits unsigned. Default is `60` (seconds).
wl-telnet-port	[integer]	L3*	**TCP Server Port Number** Specifies the TCP port number the Module listens on for a LAN application connection. The TCP server does not support Telnet commands (see Section A.10). 16 bits unsigned. Default is `23` (decimal).
wl-tunnel	[0 | 1]	L3*	**TCP Server (Tunnel) Enable or Disable** Enables or disables the tunnel server capability. The Tunnel Server is accessible from a LAN application and bypasses access to the CLI, and therefore immediately enters `pass` mode without requiring authentication. A TCP connection is refused or UDP data is not passed if the Serial Host is not in `listen` or `pass` mode, or if an existing TCP pass action is in progress, or if a TCP Tunnel connection is already established. `0` – disables Tunnel connection. `1` – enables Tunnel connection. Default is `0`.
wl-tunnel-mode	[tcp | udp]	L3*	**TCP Server Tunnel Protocol** Sets the IP protocol that will be used to convey data on the Tunnel port to TCP or UDP. A TCP connection is refused or UDP data is not passed if the Serial Host is not in `listen` or `pass` mode, or if an existing TCP pass action is in progress, or if a TCP Tunnel connection is already established. `tcp` – Enables TCP Tunnel data communication. `udp` – Enables UDP Tunnel data communication. Default is `tcp`.
wl-tunnel-port	[integer]	L3*	**TCP Server (Tunnel) Port Number** Defines the TCP port the Tunnel server will listen on for an inbound TCP connection. 16 bits unsigned. Default is `8023`.
listen		L2	**Set Module to Listen Mode** Module accepts connections or exchanges from other interfaces such as LAN TCP. The Module must be in `listen` mode for a LAN application to pass data through the serial interface. The CLI only accepts this command from the Serial interface, or the `serial-default` command can be used to set the startup state to `listen` mode. If a connection is already open, an error is returned.

Command	CLI Arguments	Ln	Description
wl-http-port	[integer]	L3	**Web Server Port Number** Sets the port number on which the Module's Web server will listen for HTTP connections. 16 bits unsigned. Default is `80` (decimal).
wl-http-def	[string]	L3	**Default Web Page** Sets the directory path for the default Web page. Default is `/oem/oem.html` (all lower case and case sensitive).
wl-retry-time	[integer]	L3	**Outbound TCP Connection Retries Interval** Defines the delay, in seconds, between attempts to establish a TCP connection with a LAN TCP server. 32 bits unsigned. Default is `60` (seconds).
wl-tcp-timeout	[integer]	L3	**Outbound TCP Inactivity Timeout for Serial Host-Initiated TCP Connection** Specifies the inactivity timeout in seconds. A value of zero sets an infinite timeout. Applies to a new session. 32 bits unsigned. Default is `60` (seconds).
wl-tcp-port	[integer]	L3	**Outbound TCP Port Number for Serial Host-Initiated TCP Connection** Specifies the TCP port number to use when the Host initiates a TCP connection with a remote server. 16 bits unsigned. Default is `2571` (decimal).
wl-tcp-ip	[IPadrs]	L3	**Outbound TCP IP Address for Serial Host-Initiated TCP Connection** TCP IP address to use when the Host initiates a TCP connection with a remote server. Default is `0.0.0.0`.
wl-tcp-ip2	[IPadrs]	L3	**Outbound TCP IP Secondary Address for Serial Host-Initiated TCP Connection** Secondary TCP IP address to use when the Host initiates a TCP connection with a LAN device. If the address defined by `wl-tcp-ip` is unavailable, a connection is attempted at this secondary address. When the address is `0.0.0.0`, a secondary connection is not attempted. Default is `0.0.0.0`.

Command	CLI Arguments	Ln	Description
pass		L2	**Enter Data Pass-Through Mode** Enter pass-through mode and open a TCP connection if one is not already open. The CLI responds with OK when a successful connection is made. If the CLI responds with ERROR, the Module remains in CLI mode (see section A.9). When issued from a LAN application, the Serial Host must be in `listen` mode to establish a connection. When issued from a Serial Host application, the Module uses the `wl-tcp-ip` or `wl-tcp-ip2`, `wl-tcp-port`, `wl-retry-time` and `wl-tcp-timeout` parameters to make the TCP connection. The Module will try the `wl-tcp-ip` address first and if it fails, tries `wl-tcp-ip2`. If both fail, an error message is returned. When the serial-default is set to `pass`, at restart, the module will try the `wl-tcp-ip` address and if it fails, tries `wl-tcp-ip2`. If both fail, the module waits the `wl-retry-time` and repeats the steps over again, continuously. Escape to CLI mode ends the retries. UDP must be allowed by the `wl-xmit-type` CLI command for pass-mode to convey UDP packets. The `pass` mode enables the module to transfer serial data to the wireless network as either UDP unicast or UDP broadcast packets, whichever was specified with the `wl-udp-xmit` CLI command. The Module will listen for incoming LAN unicast and broadcast UDP packets on the specified UDP listen port and transfer that data to the serial port only when the `wl-xmit-type` is set to UDP. UDP Unicast packets will be sent to the address and port specified in the `wl-udp-port` and `wl-udp-ip` CLI commands. When `wl-xmit-type` is set to `both` and the outgoing TCP connection initiated by the `pass` command fails, neither TCP nor UDP data will be sent or received. Also, when set to `both`, and a TCP connection succeeds, UDP packets may only be sent from the serial interface to the wireless LAN (not received).
putget	<integer1> <integer2> <aschex>	L2	**Module Connects (if required) to IP Address and Port Number** The Module transfers binary <aschex> data to a remote IP application and waits for <integer1> bytes of returned data or times out after <integer2> seconds. Excess bytes are discarded. After the command completes, the connection remains in CLI mode. The command can be issued from a LAN application (Serial in listen mode) or from a Serial Host application. <integer1>= number of bytes, from 0 -1800 bytes max. <integer2>= timeout, 32 bit unsigned, seconds. <aschex> = senddata, up to the max length of the command line. Example: **`putget 10 60 aef32bc89d`**`<CR><LF>`

Command	CLI Arguments	Ln	Description
putexpect	<integer1> <integer2> <aschex1> <aschex2>	L2	**Module Connects (if required) to IP Address and Port Number** The Module transfers binary <aschex> data to a remote IP application and waits for <integer1> bytes of returned data or times out after <integer2> seconds or the <aschex> terminator is recognized. Excess bytes are discarded. After the command completes, the connection remains in CLI mode. The command can be issued from a LAN application (Serial in listen mode) or from a Serial Host application. <integer1> = maximum number of bytes, 0 – 1800 bytes max. <integer2>= timeout, 32 bit unsigned seconds <aschex1> = senddata, up to max length of command line <aschex2> = terminator, 16 bytes maximum Example: **`putexpect 64 60 aef32bc89d 646464`**`<CR><LF>`
close		L3	**Close a TCP Connection Initiated by the Serial Host** The command can be sent from any interface. A connection initiated by a LAN application (TCP and HTTP) must be managed by that application.
wl-udp-ip	<IP address>	L3	**Outbound UDP 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`.
wl-udp-port	[integer]	L3	**Outbound UDP Port Number** 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).
wl-udp-rxport	[integer]	L3	**UDP Server (Tunnel) Port Number** 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).
wl-udp-xmit	[disable | ucast | bcast | both]	L3	**Outbound UDP Mode** Sets the mode for outbound UDP transmissions. `disable` – disables outbound UDP packet transmission `ucast` – enables UDP unicast only `bcast` – 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`.

Command	CLI Arguments	Ln	Description
wl-xmit-type	[tcp | udp | both]	L3	**Outbound TCP and UDP Traffic Selection** Selects the type of outbound traffic that will be transmitted. `tcp` – only TCP traffic is allowed outbound. `udp` – only UDP traffic is allowed outbound – use the `pass` command to enable data transmission. `both` – both TCP and UDP traffic are transmitted – when data is sent through the serial interface, it will be transmitted in TCP and UDP packets. The module must be set to `pass` mode to enable the transmission of outbound UDP traffic. Default is `tcp`.

A.21.4 Escape Configuration Commands

Command	CLI Arguments	Ln	Description
esc-mode-serial	<string>	L2	**Set Serial 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 Serial interface. `off` = disables Serial escape checking `on` = enables Serial escape string checking `brk` = enables Serial escape on UART Break checking Default is `on`.
esc-mode-lan	<string>	L2	**Set TCP (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. `off` = disables LAN escape checking `on` = enables LAN escape string checking Default is `on`.
esc-str	<aschex>	L2	**Set Escape String to Specified Value** The escape string applies to the Serial and LAN escape-checking modes if they are set to on. The string must be 5 bytes (10 aschex digits). Default is `7E7E7E6473`, which is equivalent to `~~~ds`.
escape	[aschex | off]	L2	**Set Escape Sequence to the Specified Value** Must be five bytes (10 aschex digits). Can be set to a desired sequence or be disabled with the `off` argument. Instead of using this command, use the CLI commands `esc-mode-serial`, `esc-mode-lan`, and `esc-mode-str` described above. Default is `7E7E7E6473`, which is equivalent to `~~~ds`.

A.21.5 UART Port Configuration Commands

Command	CLI Arguments	Ln	Description
apply-cfg	<serial>	L3	**Apply Serial Port Configuration** Applies the serial port settings immediately, without requiring a restart. Serial configuration settings must be committed if they are to apply after a restart. Serial port settings that applied are: `bit-rate`, `data-bits`, `parity`, `flow`, and `input-size`.
bit-rate	[string]	L3*	**Serial Port Bit-Rate in Bits per Second (bps)** Acceptable values are: `300`, `600`, `1200`, `2400`, `4800`, `9600`, `14400`, `19200`, `28800`, `38400`, `57600`, `115200`, `230400`, and `460800`. Default is `9600` bps.
clear-buf		L3	**Clear Buffer** Issued after a `serial-assert` to clear all data that is buffered in the Module.
data-bits	[string]	L3*	**Serial Port Data Bits** `7` `8` (*default*)
flow	[string]	L3*	**Serial Port Flow Control** `n` = no flow control (*default*) `h` = enable hardware (RTS, CTS) `s` = enable software (DC1 - Xon, DC3 - Xoff)
input-size	[integer]	L4	**Serial Input Buffer Size** Sets a threshold at which the serial input buffer will be flushed through the TCP connection. Size range is `1` to `1460` bytes. Default is `1460` (bytes). If using software flow control, the input size range is `5` to `1460` bytes.
parity	[string]	L3*	**Serial Port Parity** `n` = none (*default*) `e` = even `o` = odd
serial-assert	[xon |xoff]	L3	**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. Default is `xon`.
serial-default	[string]	L4*	**Set the Module's Startup Serial Interface Mode** `pass` = Module connects to LAN device with the IP address specified by the `wl-tcp-ip` or `wl-tcp-ip2` and `wl-tcp-port` commands and enters pass-through mode. `cli` = Module sets serial interface in CLI mode. (*default*) `listen` = Module sets serial interface in listen mode. `loop` = Serial interface is placed into loopback mode.

Command	CLI Arguments	Ln	Description
stop-bit	[1 | 2]	L3	**Set the Number of Stop Bits** Sets the stop bits to one or two. Default is `1`.

A.21.6 Power Management Command — UART MODEL ONLY

Command	CLI Arguments	Ln	Description
pm-mode	[string]	L3	**Power Management Mode** Sets the Module's power-management mode. Parameters are active, doze, snooze, sleep, and off. Default is `active`. For more information, see Table 31.

Table 31. Description of Power Management Parameters

Mode	CPU	OSC/PLL	Radio	Wakeup
Active	On	On	On	None
Doze	Stop	On	Low Power	UART traffic, or directed or broadcast radio packet
Snooze	Stop	Off	Low Power	UART Break, or directed or broadcast radio packet
Sleep	Stop	Off	Very low power (see Note 1)	UART Break
Off (see Note 2)	Off	Off	Very low power (see Note 1)	UART Break

Note 1: In the current version, the radio does not completely shut off. Instead, it is set in as low a power state as possible short of being Off. In future releases, the radio will enter a true Off state.

Note 2: In the current version, the Off mode yields the same results as sleep mode. In future releases, the Off mode will be implemented as described in the table above.

A.21.7 Discovery Service Commands

Command	CLI Arguments	Ln	Description
name-manuf	[string]	L5	**Discovery Name: Manufacturer** 31 characters Default is `DPAC-Airborne-A`.
name-oem	[string]	L4	**Discovery Name: OEM** 31 characters] Default is `OEM-Cfg1`.
name-device	[string]	L3	**Discovery Name: Device** 31 characters] Default is `Device`.

A.21.8 Administration Commands

Command	CLI Arguments	Ln	Description
commit		L3	**Commit System Configuration Parameters to Flash Memory**

auth	[string1 string2]	L1	**Log into the Module**
			Persistent until logout or restart, not persistent across restart.
			`string1 = user ID`
			`string2 = password`
			If no arguments are given, reports security level as `L1`, `L2`, `L3`, `L4`, or `L5`.

ver-fw		L1	**Firmware Version String** [31 characters].
ver	[string]	L4	**OEM Version String** [31 characters] If no argument is given, the current `oemverstr` is returned for any security level. The `ver` command can be issued from a L1 security level without an argument. Default is `oemverstr`.
user-manuf	[string]	L5	**Level 4 User ID** [31 characters] Default is `dpac`.
user-oem	[string]	L4	**Level 3 User ID** [31 characters] Default is `oem`.
user-cfg	[string]	L3	**Level 2 User ID** [31 characters] Default is `cfg`.
user	[string]	L2	**Level 1 User ID** [31 characters] Default is `user`.
pw-manuf	<string>	L5	**Level 4 Password** [31 characters] Default is `dpac`.
pw-oem	<string>	L4	**Level 3 Password** [31 characters] Default is `oem`.
pw-cfg	<string>	L3	**Level 2 Password** [31 characters] Default is `cfg`.
pw	<string>	L2	**Level 1 Password** [31 characters] Default is `password`.
logout		L1	**Return to Level 1**
restart		L2	**Restart Firmware** All system configuration parameters that have been changed must be committed to flash memory using the `commit` command before issuing this command; otherwise, the changes will be lost after restart.
update		L2	**Update Module Firmware** Prompts for an Airborne firmware image file. The transfer uses the XMODEM protocol (refer to “XMODEM Guidelines” on page 66). After the update is completed, the Module restarts automatically. Execute this command from the Serial interface, with hardware handshake enabled (not soft handshake).

Command	CLI Arguments	Ln	Description
time	[integer]	L2	**Set/Get the current Run Time** Sets or gets the current `time_t` returned by the `time()` `POSIX` function, representing the number of seconds since 00:00:00 January 1, 1970 (non-persistent). At startup, the Module time starts ticking from 0. The accuracy of the internal timer is not guaranteed when power modes are active.
reset		L3	**Reset All Settings to OEM Defaults**

A.21.9 Digital I/O Commands

Command	CLI Arguments	Ln	Description
io-read	e | f<portid>	L2	**Read Digital I/O Port** <port id> = a bit number from `0-7`. Returns the state of the I/O port. Example: `io-read e4`
io-write	e | g<portid> <num>	L2	**Write Digital Value to Digital I/O Port <num>** <portid> = a bit number from `0-7` or as allowed by Tables 4 through 7 (see page 13) if the direction has been set as output. <num> = `0` or `1`. Writing to a bit position that has been configured as an input has no effect. Writing to port g3 has no effect.
io-dir-e	[integer]	L2	**Set the Direction of Port E I/O Bits to Input or Output** 8 bits, bit setting of `1` = Input, `0` = Output. Bits 3-0 = don't care. Bits 7-4 = must be `0` or `1`. Default is all inputs. Requires restart to take effect.
io-dir-g	[integer]	L2	**Set the Direction of Port G I/O Bits to Input or Output** 8 bits `1` = Input `0` = Output A bit set as an input is an analog input and `adc-read` is used to read the bit value. Setting port G3 as output has no effect. Default is all inputs.
io-dir	e | g<portid> [in | out]	L2	**Set the Direction of Port to Input or Output** Applies setting dynamically, without requiring a restart. Bit restrictions are the same as for the `io-dir-e` and `io-dir-g` commands above.

A.21.10 Analog Input Command

Command	CLI Arguments	Ln	Description
adc-read	g<portid>	L2	**Read Analog Input Port** Range of returned value is 0x0000 (`0`) to 0x03FF (`1023`), in integer steps. Valid if bit position is set as a port G input. <port id> is `0` through `7`. If the port is set as an output using `io-dir-g` and as a logic 0 output, reading returns result code `0`. If set as a logic 1 output, reading returns a result close to `1023`.

A.21.11 I^2C Interface Commands

Command	CLI Arguments	Ln	Description
i2c	[0 | 1]	L2*	**I^2C Enable** Enables the function and allocation of the I^2C interface on pins E4 and E7. `0` = I^2C disabled, ports E4/E7 are GPIO. `1` = I^2C enabled, ports E4/E7 are SCL/SDA. Default is `0`.
i2c-write	<addr> <control> <data>	L2	**I^2C Bus Data Write** Performs a write to an I^2C device, including control byte and data byte with appropriate Start/Ack/Stop flag generation. `addr` = an integer, device address `control` = an integer, control byte `data` = an integer, data byte
i2c-read	<addr>	L2	**I^2C Bus Data Read** Performs a read of an I^2C device, including the appropriate Start/Ack/Stop flag generation. `addr` = an integer, address Data read is returned an integer.
i2c-put	<data> <flag>	L2	**I^2C Bus Put Data Byte** Writes a data byte to the I^2C bus following flag assertion. `data` = an integer. `flag` = an integer (Figure 30, on page 94, shows the definitions for this byte).
i2c-get	<flag>	L2	**I^2C Get Data Byte** Returns an integer of the last value in the receiving buffer. `flag` = an integer (Figure 30, on page 94, shows the definitions for this byte).
i2c-isbusy		L2	**I^2C Bus Check for Bus Busy** Returns the status of the I^2C bus for access by the Module. `FREE` = bus is available for access. `BUSY` = another master is utilizing the bus.
i2c-chkack		L2	**I^2C Bus Check for ACK** Returns the ACK status of the last operation `OK` = ACK is received. `FAILED` = no ACK has been received.

Bit	7	6	5	4	3	2	1	0
Flag	0	0	0	0	NON	ACK	STOP	START

Flag is an array of bits represented in an integer.
A minimum of one flag must be present.

Figure 30. I²C Bus Put Data Byte

A.21.12 FCC Test Commands

The Airborne Wireless LAN Node (WLN) Module can be set to operate in modes suitable for meeting FCC test requirements. In particular, FCC tests require that the module be placed into a continuous transmit mode and several characteristics of the output (such as power level, modulation, channel, data rate, and data pattern) must be configurable. FCC testing also requires a way to test the transceiver in a receive-only mode to provide a way to scan emissions.

A.21.12.1 Using the `wl-tx-test` CLI Command

The WLN command line interface includes the `wl-tx-test` CLI command that provides the means to set the WLN in the desired transmit modes.

When submitted, the command will immediately enable continuous data pattern transmission. The best way to terminate the transmit test is to reset or power cycle the module.

The command syntax is as follows (parameters are separated by a space):

```
wl-tx-test <modulation> <weight> <ant> <power> <chan> <rate> <pattern>
```

Where parameters are defined as:

Table 32. FCC Test Command `wl-tx-test` Parameters

Parameter	Values	Notes
`<modulation>`	`0` | `1`	Turns modulation off or on
`<weight>`	`0` = USA | `1` = Japan	Modulation weighting
`<ant>`	`0` = J1 antenna only `1` = J1 primary, J2 Rx diversity	For transmit set to `1`
`<power>`	Power Level in `0xnn` format	(See the following Power Levels table: Table 33 on page 96.)
`<chan>`	Channel in range `1` to `14`	Sets the 802.11b channel number – see the following Channel Frequencies table for the corresponding frequency: Table 34 on page 96.

Parameter	Values	Notes
<daterate>	0 = 1 Mbps 1 = 2 Mbps, 2 = 5.5 Mbps 3 = 11 Mbps	Sets wireless data rate Frame preamble is not transmitted
<datapattern>	16 bit data pattern in 0xnnnn format	Data pattern is transmitted continuously. For example, if 0xa010 is specified, the bit sequence would be (spaces added for clarity): 1010 0000 0001 0000 1010 0000 0001 0000…

Special Note:

1. Power and Pattern parameters must be in Hex format (i.e., preceded by the 0x nomenclature).
2. When testing channel 1, the command must be issued twice on the CLI.

A.21.12.2 Using the wl-rx-test CLI Command

The wl-rx-test CLI command sets the module into a receive-only mode and disables the transmitter. This test is useful for checking emissions from the module with the transmitter disabled.

The command syntax is:

```
wl-rx-test <chan> <rate>
```

This command invokes a continuous receive state.

where:

<chan> : integer 1 to 14 - receive channel - see Table 34 (on page 96) for the corresponding frequency.

<rate> : integer - transmit rate for test - 0 = 1 Mbps, 1 = 2 Mbps, 2 = 5.5, Mbps, 3 = 11 Mbps

Table 33. Power Levels

Desired Tx Power Level	Hex Power Level	Measured Power @ J1 (dBm)
0	0x00	19.64
10	0x0a	19.45
20	0x14	18.39
30	0x1e	17.32
40	0x28	16.12
50	0x32	14.70
60	0x3c	12.82
70	0x46	10.72
80	0x50	8.42
90	0x5A	6.00
100	0x64	3.50
110	0x6E	0.88
120	0x78	-1.83

Table 34. 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

A.22 CLI ERROR CODES AND MESSAGES

The following table lists the CLI hexadecimal error codes and their meanings.

Hex Code	Error Message
0x23	An unknown error has occurred
0xf801	Invalid parameter
0xf802	Command not recognized
0xf803	Operation timed out
0xf804	Invalid character
0xf805	Insufficient memory
0xf806	Not authorized
0xf807	Parameter length invalid
0xf808	Command not implemented
0xf809	File not found
0xf80a	Invalid port
0xf80b	Port busy
0xf80c	Invalid user or password
0xf80d	Timeout waiting for update file
0xf80e	Update file error
0xf80f	Update cancelled
0xf810	Invalid XMODEM Packet Sequence
0xf811	Processing another inquiry
0xf812	Unable to connect to server
0xf813	Command not allowed in script
0xf814	Join failed
0xf815	Join in progress
0xf816	Port assigned to another service
0xf818	Socket Busy

Hex Code	Error Message
0xf819	Insufficient socket memory
0xf81a	No IP route
0xf81b	Socket not connected
0xf81c	No TCP data
0xf81d	DNS: Transaction failed
0xf81e	DNS: Hostname not found
0xf81f	DNS: Internal error
0xf820	DNS: Invalid Hostname
0xf821	DNS: Server not configured
0xf823	Upgrade header failure
0xf824	I2C: read failed
0xf825	I2C: write failed
0xf826	I2C: chkack failed
0xf827	I2C: protocol disabled
0xf828	I2C: GPIO pin reserved for I2C
0xf829	I2C: communication timeout
0xf82d	Mixed use of Legacy Escape command
0xf82e	TCP outbound configuration invalid
0xf832	SPI read failed
0xf833	SPI write failed
0xf834	SPI dir failed
0xf835	SPI pin in use

This page intentionally left blank

B.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.

B.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.

B.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.

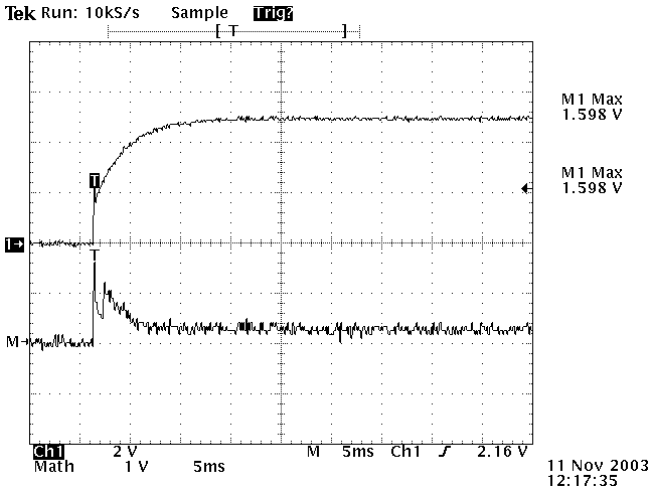


Figure 31. Inrush Current Characteristics

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.

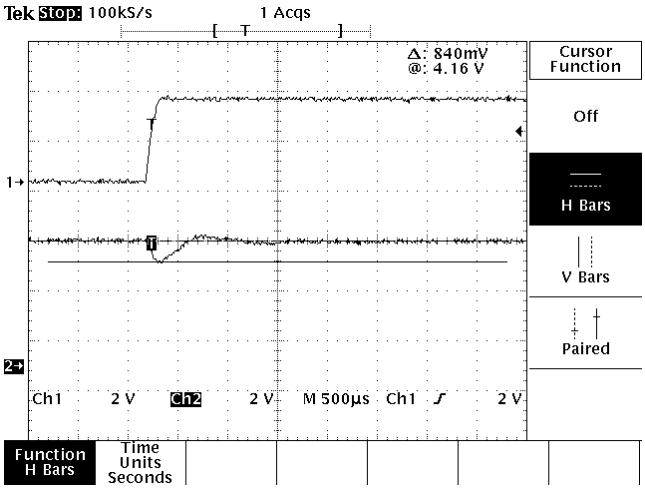


Figure 32. Voltage Droop with Current-Limited Supply

B.4 APPLICATION CIRCUIT

Figure 33 shows a recommended application circuit that can be used to obviate the harmful effects described in this appendix. Table 35 shows the parts associated with the recommended application circuit.

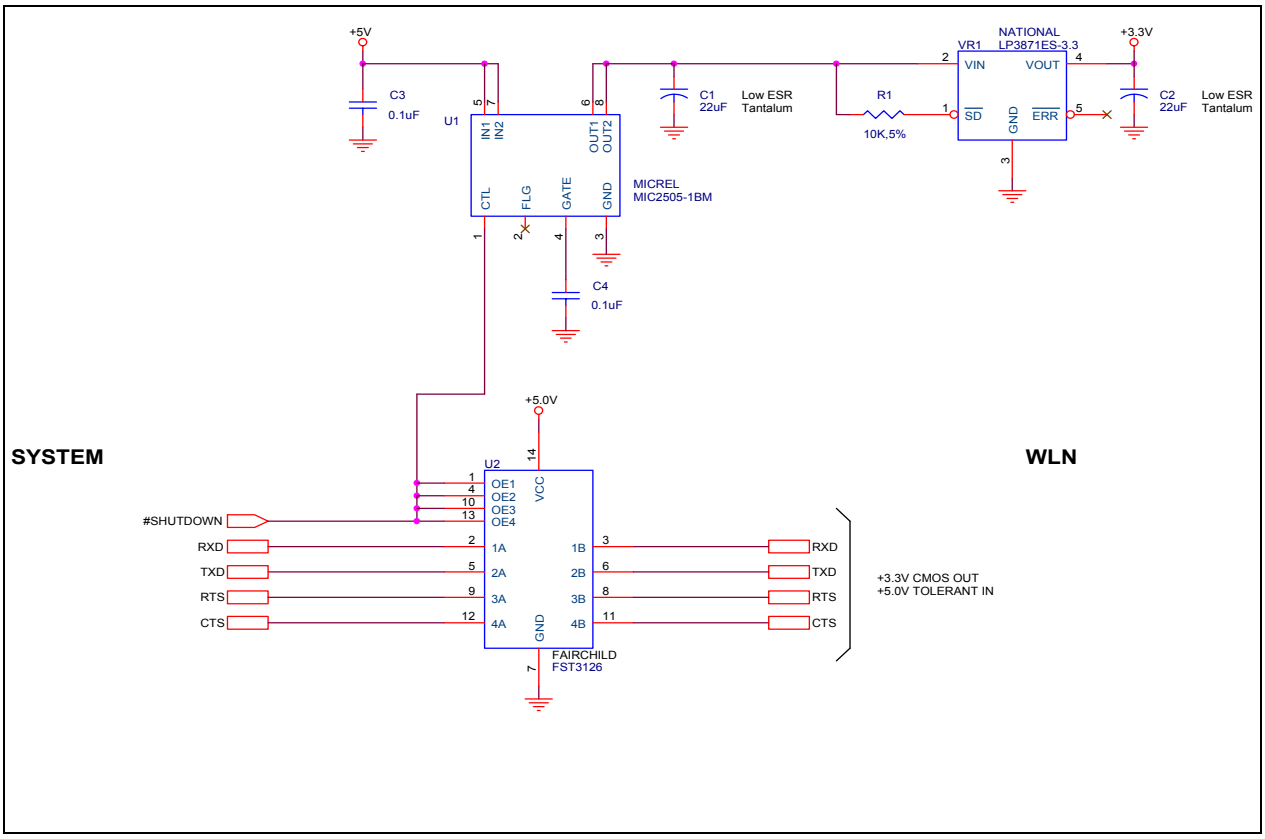


Figure 33. Recommended Application Circuit

Table 35. Parts List for Recommended Application Circuit

Item	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

B.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.

B.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.

B.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.

B.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.

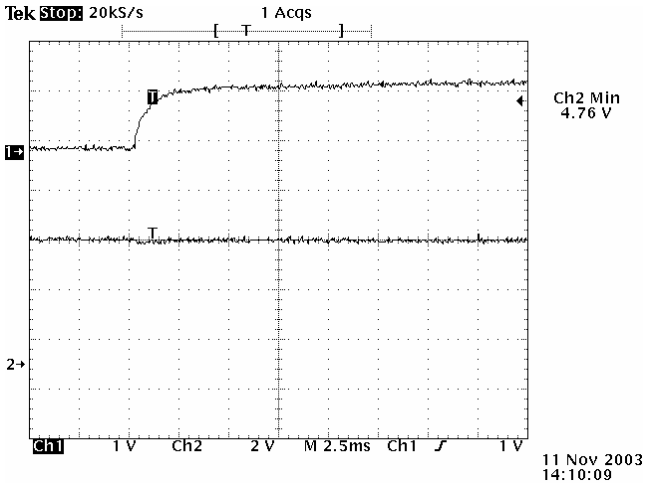


Figure 34. Circuit Soft-start Characteristics

B.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:

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

$= 8\ \mu A$

B.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:

$$P_D = (0.06\ \Omega)\ 0.480^2\ A + (5.25\ V)\ 5\ \mu A$$
$$= 0.014\ W + 26\ \mu W$$
$$= 0.014\ W$$

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:

$$T_A = 125°C - 160°C/W\ (.014\ W)$$
$$= 122.8°C\ \text{maximum}$$
$$\geq 85°C$$

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:

$$P_D = (5.25\ V - 3.20\ V)\ 0.480\ A + (5.25\ V)\ 0.0150\ A$$
$$= 0.984\ W + 0.079\ W$$
$$= 1.06\ W$$

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)
Θ_{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

APPENDIX C
RADIO FREQUENCY CHANNELS

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.

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 D
GLOSSARY

This appendix provides a glossary of wireless terminology.

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

Command Line Interface (CLI)	A method of interacting with the Airborne WLN 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.
Local Area Network	A system of connecting PCs and other devices within the same physical proximity for sharing resources such as Internet connections, printers, files, and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.
Media Access Control (MAC) Layer	One of two sub-layers that make up the Data Link Layer of the OSI reference model. The MAC layer is responsible for moving data packets to and from one network node to another across a shared channel.
MPDU	MAC Protocol Data Unit, the unit of data exchanged between two peer MAC entities using the services of the physical layer (PHY).

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

WLAN	Also referred to as a wireless LAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes and provide network connectivity.
WLN	Short for Wireless LAN Node, this is the Airborne 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.

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

DPAC Technologies Confidential

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

39L3702-01
REV. D 10/25/2004 JR