QUATECH
A DPAC TECHNOLOGIES COMPANY

Airborne™ Product Family
Command Line Interface (CLI)
Reference Guide

For use with:

WLNG-AN-DP100 Series
WLNG-SE-DP100 Series
WLNG-ET-DP100 Series
ABDG-SE-DP100 Series
ABDG-ET-DP100 Series

Document Number
100-8005-101G

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.

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

Quatech, Inc. Headquarters

QUATECH Inc.
5675 Hudson Industrial Parkway
Hudson, OH 44236
USA

Telephone:	330-655-9000
Toll Free:	800-553-1170
Fax:	330-655-9010
Email:	sales@quatech.com support@quatech.com
Web Site:	www.quatech.com

CONTENTS

LIST OF FIGURES

LIST OF TABLES

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

- *Chapter 1, CLI Overview* — describes how to use the command line interface.
- *Chapter 2, CLI Commands* — provides all of the applicable commands for using the Airborne™ ™ Wireless and Airborne™ Direct™ products.
- *Glossary* — defines the terms associated with the Airborne™ Wireless, AirborneDirect™, and wireless networks in general.

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

CONVENTIONS

The following conventions are used in this document:

Terminology

In this document, the following terms are used:

- "Airborne™ Wireless LAN Node Module" is abbreviated "Airborne™ WLN Module", "WLN", or simply "Module".
- "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 TCP client that communicates with the Airborne™ WLN Module via a wireless network connection.

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.

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.

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
```

RELATED DOCUMENTATION

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

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

Quatech also offers developer documentation for its AirborneDirect™ products. Please contact Quatech for more information.

CHAPTER 1
CLI OVERVIEW

1.1 OVERVIEW

The Airborne™ WLN Module includes a Command Line Interface (CLI) Server. The CLI Server is the primary user interface for configuring, controlling, and monitoring Airborne™ WLN Modules. Users and OEM applications can establish CLI Sessions to the CLI Server via the serial interface or a TCP connection on the wireless interface.

This document describes the CLI in full. Since different Airborne™ devices differ in functionality, there may be differences in the use of the CLI for particular devices. These differences are clearly identified as part of this document.

1.2 UNDERSTANDING CLI SESSIONS

CLI Sessions established to the CLI Server may operate in one of three modes: CLI, PASS, or LISTEN. Not all modes are supported on all interfaces of the device. A CLI Session established on the serial interface may operate in any of the three modes. CLI Sessions established on the wireless interface are restricted to CLI or PASS Modes.

1.2.1 Connecting to the CLI Server

Users may connect to the CLI Server on the serial interface using a terminal emulation program such as HyperTerminal. The DPAC default settings for the serial interface are:

- Bits per second: 9600
- Data bits: 8
- Stop bits: 1
- Parity: none
- Flow control: none

Users may also connect to the CLI Server on the wireless interface using a TCP client such as Windows Telnet. The Module's CLI Server supports a Telnet connection with the following restrictions:

- 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.

The CLI Server's wireless interface is characterized as follows:

- The CLI Server listens on the TCP port specified by the `wl-telnet-port` parameter. The default is 23.
- The CLI Server inactivity timer is configured via the `wl-telnet-timeout` command.
- The CLI Server uses the `wl-telnet-timeout` value to timeout and close TCP connections that are inactive.
- The CLI Server supports up to three (3) TCP sessions.

1.2.2 CLI Security

The CLI Server supports five (5) levels of security for each CLI Session. The security levels provide a safeguard for the set of CLI commands that may be executed by users. CLI Sessions that are authenticated at a particular security level may execute all CLI commands specified for that security level and below.

The Module's five (5) levels of security are:

- 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 use 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 for CLI Sessions over TCP or the serial interface.

CLI Sessions must execute the CLI command `auth` in order to authenticate the CLI Sessions to another security level. The CLI command definition tables in the following chapter include a column labeled **Ln** that indicates the access level required to execute each command. The CLI command `logout` returns the CLI Session back to security Level 1.

1.2.3 CLI Session Modes

The mode of the CLI Session governs the set of actions allowed in the CLI session. The following are descriptions of each mode:

1.2.4 CLI Mode

CLI Mode is the command processing mode of the CLI Session. CLI Mode allows users and OEM applications to simply execute Airborne™ WLN Module commands as described in the section, "CLI Commands."

A CLI Session may transition into CLI Mode automatically at startup of the CLI Session (if so configured). See section "CLI Session Startup Modes" for details on startup modes.

CLI Sessions may transition manually to CLI Mode from the other modes via the use of the CLI escape processing feature in the CLI Server. See section "CLI Server Escape Processing" for details.

1.2.5 PASS Mode

PASS Mode is an active data bridging mode of the CLI Server. PASS Mode allows the user or OEM application to transfer data between a CLI Session on the wireless interface and the CLI Session on the serial interface.

A CLI Session may transition to PASS Mode automatically at startup of the CLI session (if so configured) or manually from the CLI Mode using the CLI `pass` command. See section "CLI Session Startup Modes" for details on startup modes.

The transition from CLI Mode into PASS Mode differs depending on the attributes of the CLI session. The following is a description of the two PASS Modes:

1.2.6 PASS Mode for the Serial Interface

When the CLI Session on the serial interface attempts a transition to PASS Mode, the CLI Server establishes an outbound connection from the Airborne™ WLN Module to a user-specified TCP server and/or UDP server on the wireless interface. Once a connection is established, data bridging becomes possible between the CLI Session on the serial interface and the TCP Server and/or UDP server. If the connection to the primary TCP server failed, the CLI Server will attempt to connect to a secondary TCP server. If the transition to PASS Mode was triggered by the automatic startup configuration, the CLI Server will use the `wl-retry-time` configuration parameter to continuously retry connection to the servers.

The IP addresses of the primary TCP and UDP servers are configured using `wl-tcp-ip` and `wl-udp-ip` CLI commands. The secondary TCP server is configured using the `wl-tcp-ip2` command. The TCP server port is configured using `wl-tcp-port` and `wl-udp-port` CLI commands. The retry timer is configured using the `wl-retry-time` CLI command. See section "CLI Commands" for more details on these commands.

1.2.7 PASS Mode for the Wireless Interface

When the CLI Session on the wireless interface attempts to transition to PASS Mode, the CLI Server establishes a data bridge to the CLI Session on the serial interface if the following conditions are both true:

- The CLI Session on the serial interface is in LISTEN Mode.
- No other CLI Session on the wireless interface is in PASS Mode.

1.2.8 LISTEN Mode (Serial Interface Only)

LISTEN Mode is a passive data bridging mode of the CLI Session. The LISTEN Mode is only applicable on the serial interface. When the CLI Session on the serial interface enters LISTEN Mode, the Airborne™ WLN Module passively waits for a data bridge to be established over the wireless interface. The data bridge may be initiated using a CLI Session via the PASS Mode or using the tunneling feature. The CLI Session may transition to CLI Mode using CLI Server escape processing. See section "CLI Server Escape Processing" for details.

When the serial interface CLI Session is in LISTEN Mode, the following are possible:

- TCP connections on the wireless interface can use the CLI commands `pass`, `putget` or `putexpect to establish a data bridge`.
- TCP connection can establish a data bridge if tunneling is enabled.

1.2.9 CLI Session Startup Modes

The startup behavior of the CLI Session on each interface is determined as follows:

- The CLI Session on the serial interface startup behavior is determined by the value of the `serial-default` parameter.
- CLI Sessions on the wireless interface using the TCP port specified by `wl-telnet-port` always start in CLI Mode.
- CLI Sessions on the wireless interface using the TCP port specified by the `wl-tunnel-port` or the UDP port specified by `wl-udp-rxport`, always start in PASS Mode. However, if the CLI Session on the serial interface is not in LISTEN Mode, the TCP connection on the `wl-tunnel-port` will be rejected by the Module.

1.2.10 CLI Server Escape Processing

The CLI Server includes an escape processing feature which allows CLI Sessions to transition from PASS or LISTEN (data bridging) Mode back to CLI Mode. Escape processing is configurable to:

- disable escape processing
- process the receipt of a user-defined escape string as an escape signal
- process the receipt of the BREAK signal as an escape signal

When escape processing is disabled, the CLI Server will not parse the data stream for any escape sequence. When escape processing is configured to use an escape string, the CLI Server will perform pattern matching for the user-defined escape string in the data stream. The escape string is a five (5)-character string configurable via the `escape` CLI command. When escape processing is configured to use the BREAK signal, the CLI Server will parse the data stream for the BREAK signal.

1.2.11 Detecting and Executing the Escape Sequence

Upon detection of the escape sequence, the CLI Server applies the follow rules for transitions of the CLI Session on that interface:

- If the CLI Session is in LISTEN Mode and there is no data bridge established, the CLI Session will transition to CLI Mode and send an "OK" response to the CLI Session.
- If the CLI Session is in LISTEN Mode and there is an active data bridge established, the CLI Server will terminate the active data bridge and the CLI Session will remain in LISTEN Mode. Basically, two escapes are required to transition from active data bridge to CLI mode.
- If the CLI Session is in PASS Mode, the CLI Server will send an "OK" response to the CLI Session and transition to CLI Mode.

The following effects of escape processing require the attention of system implementations:

- If the escape sequence is an escape string, the escape string received on one CLI Session is transmitted to the CLI Session on the other end of the data bridge prior to performing the CLI Session transition. This allows the other end to parse the received data and determine when the data bridge is shutdown.
- If the escape sequence is the BREAK signal, the BREAK received on the serial interface is not transmitted to the wireless interface, but the transition takes place internally.
- The CLI Session that detects the escape sequence will post an "OK" response on its interface if the escape sequence caused the CLI Session to transition to the CLI Mode.
- Escape detection does not close the TCP connection. It only terminates the data bridge. Subsequence use of the `pass` CLI command will re-establish the bridge for that interface.

The CLI Server allows independent configuration of escaping processing for the serial and wireless interfaces. The serial interface escape processing is configurable using the CLI parameter `esc-mode-serial`. The wireless interface escape processing is configurable using the CLI parameter `esc-mode-lan`. See section "CLI Commands" for details on these parameters.

1.3 TYPICAL EVALUATION SYSTEM SETUP

A typical evaluation system includes:

- A Serial Host: A computer connected to the serial port of the Airborne™ WLN Module.
- A LAN Host: A computer that communicates wirelessly with the Module through an Access Point (AP).
- An Access Point.
- An Airborne™ WLN Module.

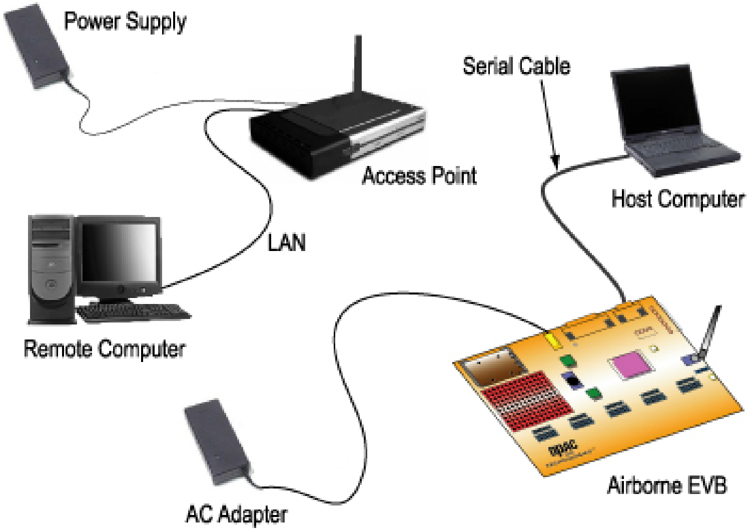

Figure 1. Typical Evaluation System Setup

1.4 DATA BRIDGING

The Airborne™ WLN Module provides data bridging via the PASS and LISTEN Modes of the CLI Session. During data bridging, the raw payload of the incoming TCP or UDP packet is transmitted to the serial interface while the raw data stream from the serial interface is transmitted as the payload of the outgoing TCP or UDP packet.

There are multiple ways to setup a data bridge using the Airborne™ WLN Module. A bridge may be initiated from the Serial Host, from a TCP connection on the `wl-telnet-port`, from a TCP connection on the `wl-tunnel-port`, or from a UDP message on the `wl-udp-rxport`.

Note: Only one CLI Session on the wireless interface may be bridged with the CLI Session on the serial interface at any one time.

1.4.1 Bridging from the Serial Interface

The CLI Session on the serial interface may initiate a data bridge via the use of the `serial-default` parameter set to “pass” or by manually issuing the `pass` CLI command. Prior to establishing the data bridge, the Airborne™ WLN Module must be properly configured to connect to a server on the network that will accept the communications. The following examples illustrate how to configure the Module to initiate a connection to a TCP server:

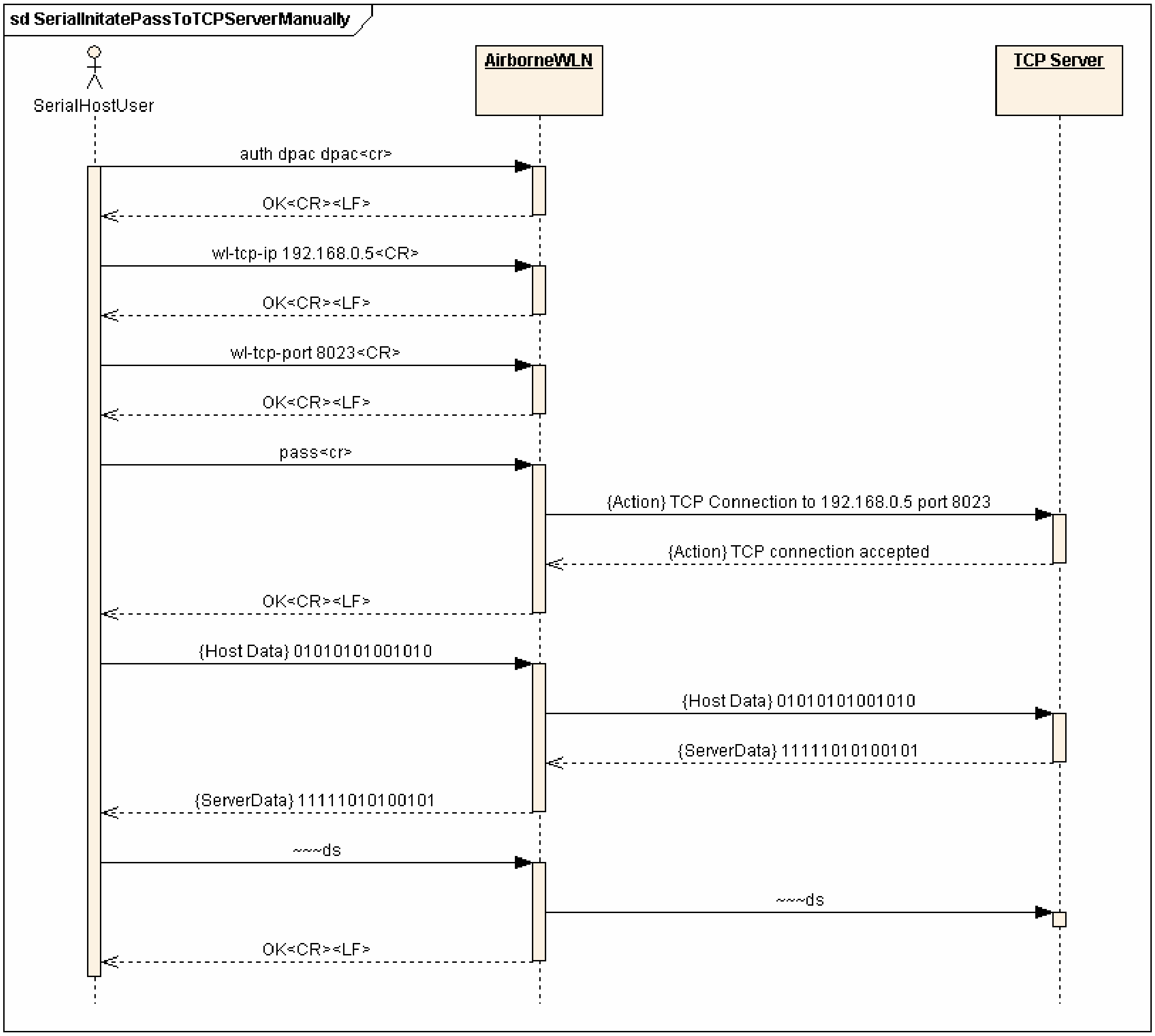
sd SerialInitatePassToTCPServerManually
SerialHostUser
AirborneWLN
TCP Server
auth dpac dpac<cr>
OK<CR><LF>
wl-tcp-ip 192.168.0.5<CR>
OK<CR><LF>
wl-tcp-port 8023<CR>
OK<CR><LF>
pass<cr>
{Action} TCP Connection to 192.168.0.5 port 8023
{Action} TCP connection accepted
OK<CR><LF>
{Host Data} 01010101001010
{Host Data} 01010101001010
{ServerData} 11111010100101
{ServerData} 11111010100101
~~~ds
~~~ds
OK<CR><LF>

Figure 2. Bridging From the Serial Interface Manually Using the `pass` Command

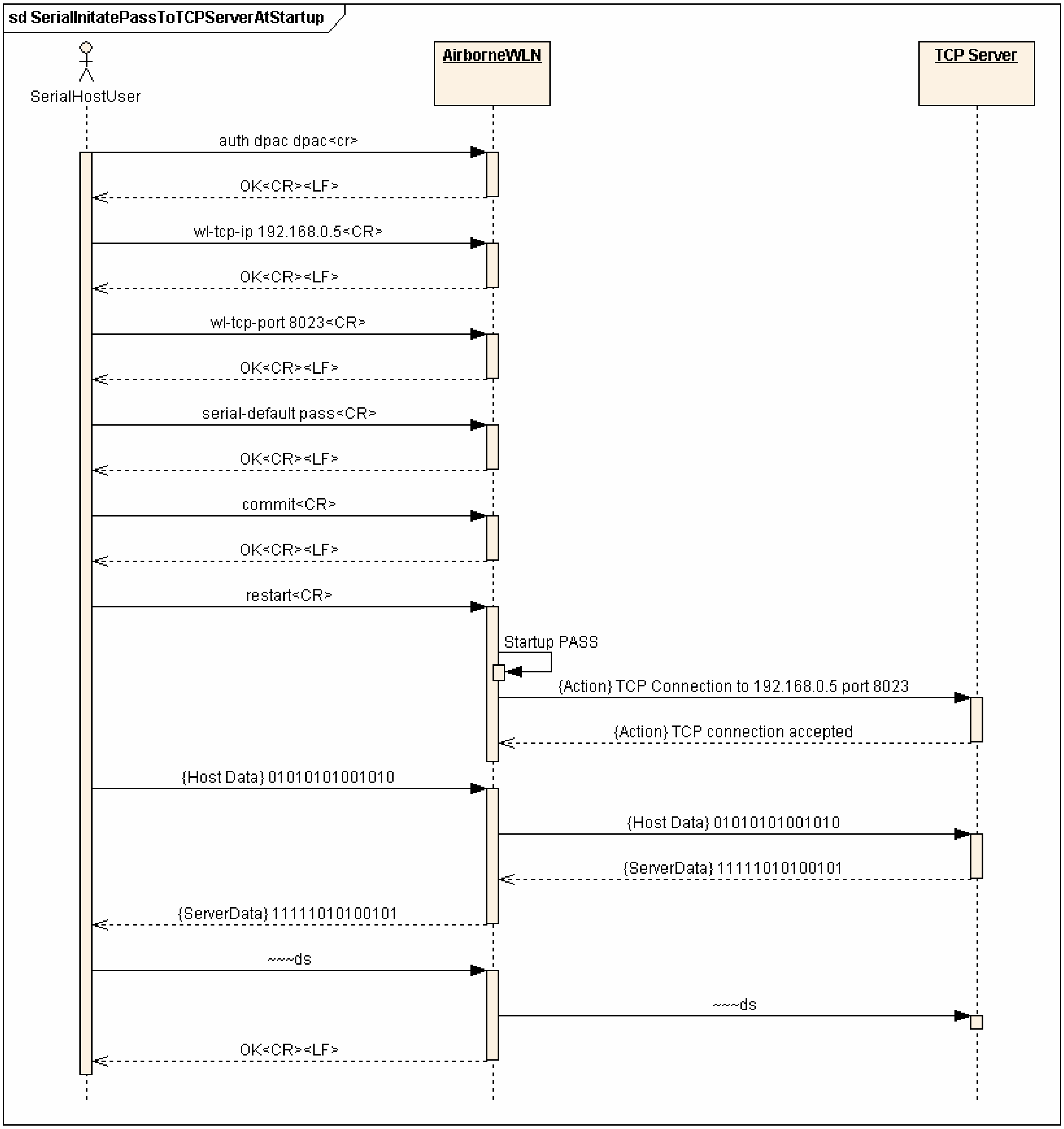
sd SerialInitatePassToTCPServerAtStartup
SerialHostUser
AirborneWLN
TCP Server
auth dpac dpac<cr>
OK<CR><LF>
wl-tcp-ip 192.168.0.5<CR>
OK<CR><LF>
wl-tcp-port 8023<CR>
OK<CR><LF>
serial-default pass<CR>
OK<CR><LF>
commit<CR>
OK<CR><LF>
restart<CR>
Startup PASS
{Action} TCP Connection to 192.168.0.5 port 8023
{Action} TCP connection accepted
{Host Data} 01010101001010
{Host Data} 01010101001010
{ServerData} 11111010100101
{ServerData} 11111010100101
~~~ds
~~~ds
OK<CR><LF>

Figure 3. Bridging From the Serial Interface Automatically at Startup Using the `Serial-Default` Command

1.4.2 Bridging from a TCP connection on the wl-telnet-port

A user or OEM application connected over TCP to the `wl-telnet-port` of the Module may create a data bridge to the serial interface by issuing the `pass` command. The `pass` command will succeed if there is no other data bridge active and the CLI Session on the serial interface is in LISTEN Mode. The following figure illustrates a sequence of commands that create a data bridge from the TCP connection:

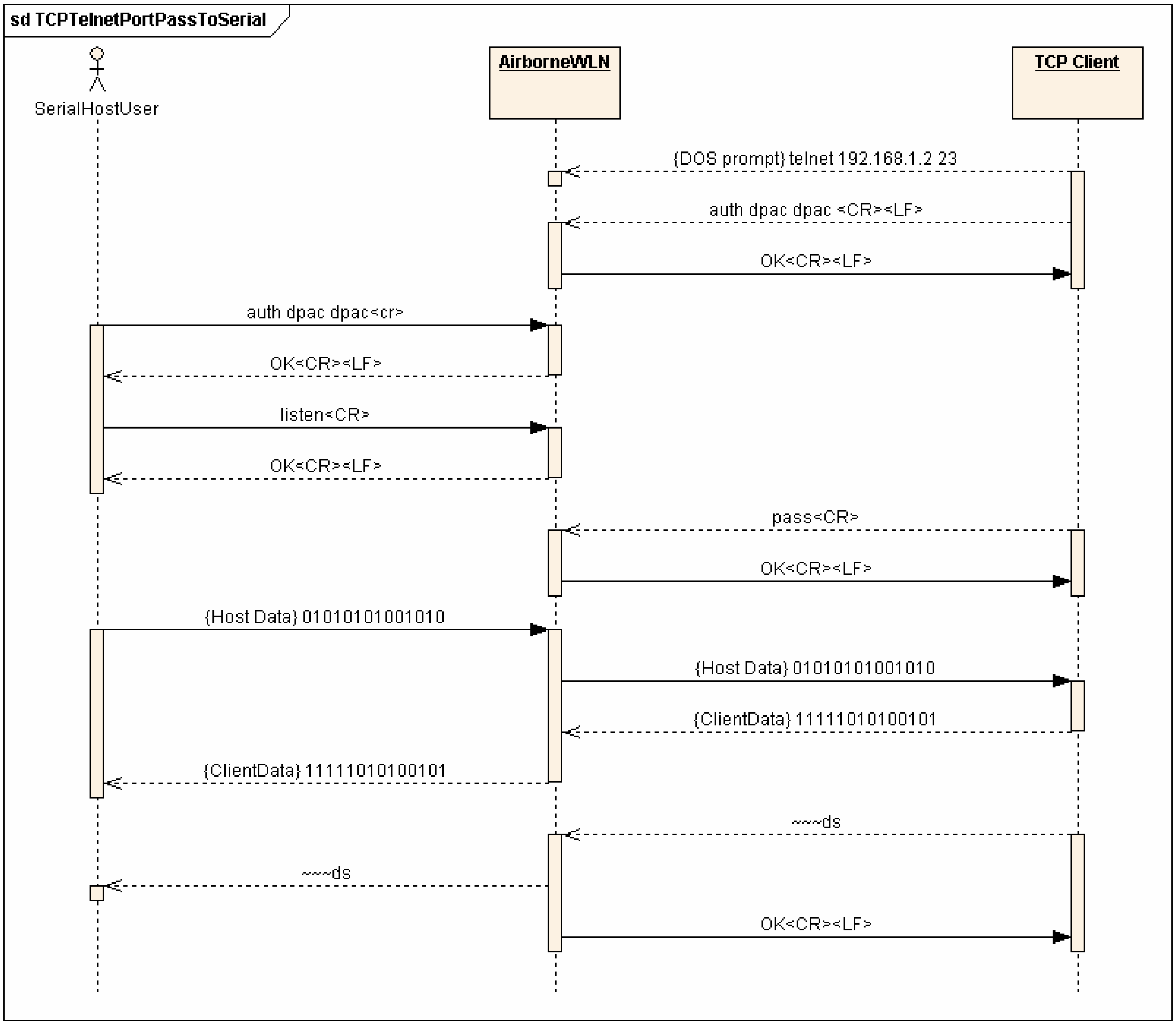
sd TCPTelnetPortPassToSerial
SerialHostUser
AirborneWLN
TCP Client
{DOS prompt} telnet 192.168.1.2 23
auth dpac dpac <CR><LF>
OK<CR><LF>
auth dpac dpac<cr>
OK<CR><LF>
listen<CR>
OK<CR><LF>
pass<CR>
OK<CR><LF>
{Host Data} 01010101001010
{Host Data} 01010101001010
{ClientData} 11111010100101
{ClientData} 11111010100101
~~~ds
~~~ds
OK<CR><LF>

Figure 4. Bridging From a TCP Connection on the `wl-telnet-port`

1.4.3 Bridging from a TCP connection on the wl-tunnel-port

The Module supports a tunneling feature that allows bridging between a specific TCP address/port and the Module's serial port. TCP port tunneling is supported by the `wl-tunnel`, `wl-tcp-mode`, and `wl-tunnel-port` commands. The rules for TCP connections to the `wl-tunnel-port` are as follows:

- `wl-tunnel` must be enabled (set to `1`).
- `wl-tunnel-mode` must be set to `tcp` or `udp`.
- `wl-tunnel-port` must be set to a non-zero value which is not the same as the Web Server port or the telnet port.
- The CLI Session on the serial interface must be in LISTEN Mode.
- There are no other CLI Sessions currently bridged.

If all of the previous conditions are met, this TCP connection will become the active bridge. All data payload will be bridged between the CLI Session on the serial interface and the CLI Session on this TCP port.

Note: The data bridge may terminate for any of the following reasons:

- The `close` CLI command is issued from a secondary TCP CLI Session.
- The other host terminates the TCP connection.
- The connection inactivity timer (specified by `wl-tcp-timeout`) expires.
- Escape sequence detection.

After the data bridge is terminated, the CLI Session on the serial interface remains in LISTEN Mode and escape detection is enabled if configured.

Using the following sequence, a user can configure the Module to operate in TCP tunneling mode:

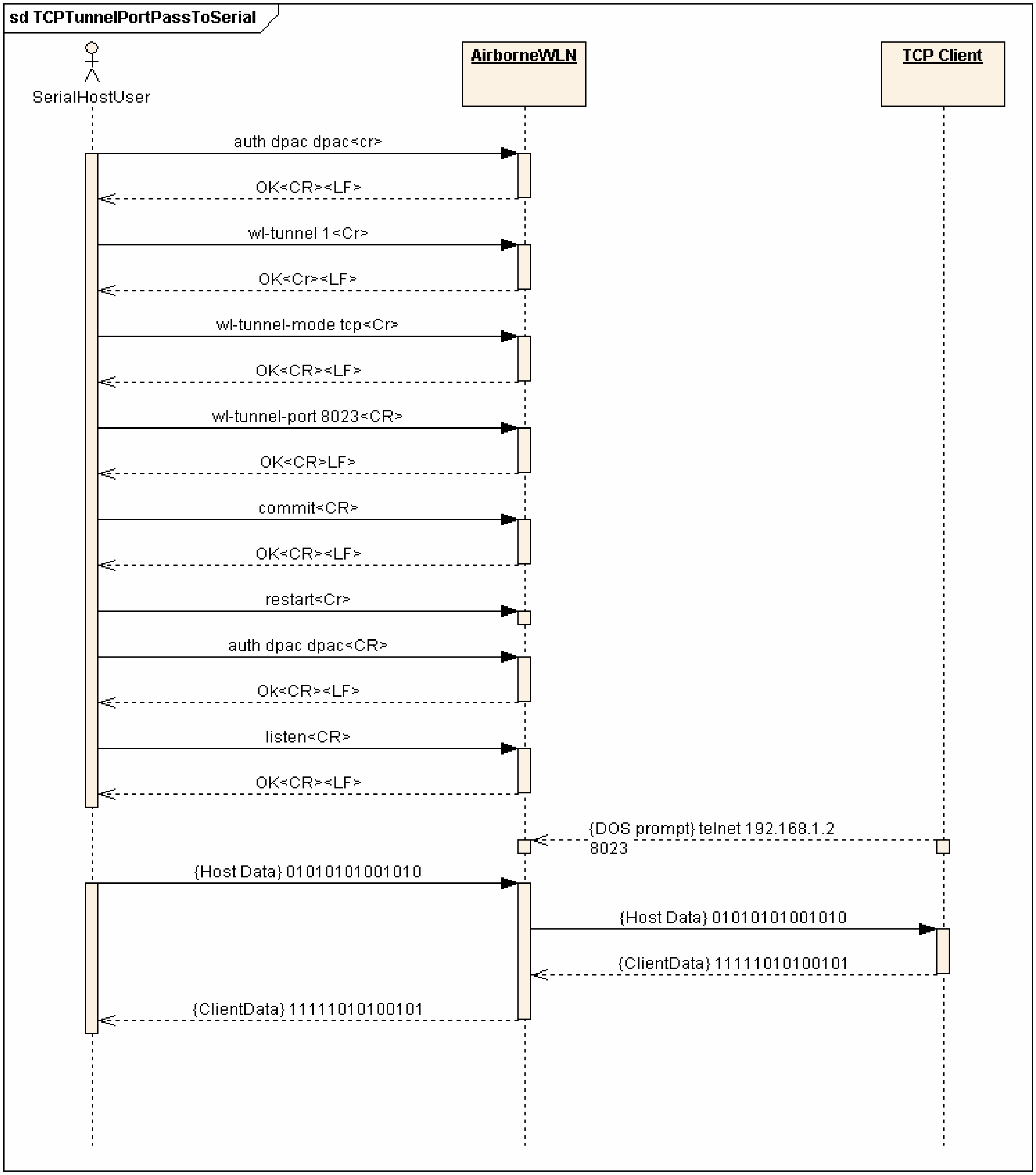

Figure 5. Bridging From a TCP Connection on the `wl-tunnel-port`

1.4.4 Bridging Using UDP

The Module supports UDP tunneling. This allows the Module to forward data from the serial interface to a specific server listening on a specified UDP port or to broadcast a UDP datagram on a specific UDP port. This also allows the Module to forward data received on its specified UDP receive port to the serial interface. The UDP port tunneling feature is configurable via the `wl-tunnel`, `wl-tunnel-mode`, `wl-udp-xmit`, `wl-xmit-type`, `wl-udp-rxport`, `wl-udp-port`, and `wl-udp-ip` CLI commands.

Whenever the CLI Server transitions to PASS Mode either via the startup `serial-default` parameter or the `pass` command, the Module will use the UDP tunneling configurations to operate the UDP data bridge as follows:

- `wl-xmit-type` is used to enable UDP transmission of data from the serial interface.
- `wl-udp-xmit` is used to enable unicast, or broadcast UDP datagram transmission, or both.
- `wl-udp-ip/wl-udp-port` is used to set the UDP transmission destination IP address/port.
- `wl-udp-rxport` sets the UDP port that the Module will receive data on for the bridge.

Note: If `wl-xmit-type` is set for “`both`”, then the TCP bridge must remain active for the UDP bridge to remain active. If the TCP server becomes inactive, the UDP bridge will be terminated.

Note: Only the payload of the UDP packets are forwarded to the serial interface. All data received on the serial interface is sent as UDP payload.

1.4.5 Data Bridging with XMODEM Guidelines

Once a data bridge is established, the endpoints may transfer raw binary data. Some systems may choose to apply a protocol such as ZMODEM or XMODEM, etc.
For systems using XMODEM protocol, the following guildelines must be adhered to:

- 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.

Note: These guidelines also apply to the `update` CLI command.

1.6 WIRELESS LAN ROAMING

When configured for Infrastructure mode using the `wl-type` command, the Module supports roaming in accordance with the IEEE 802.11 specification. The following set of commands affect the Module’s roaming capabilities:

Table 1. CLI Commands That Affect Roaming

CLI Commands that Directly Affect Roaming
`wl-type`
`wl-ssid`
`wl-rate`
`wl-security`

The `wl-ssid` command specifies the SSID to use for 802.11 associations. The SSID may be set to the special value “`any`” or to an SSID that matches the SSID of your network.

If `wl-ssid` is set to the value "`any`", the Module will perfrom a scan of APs and attempt to associate with the AP that reports the highest signal quality. In this configuration, the 802.11 roaming feature is not supported. The use of the "`any`" SSID allows the Module to associate with any AP that is in range. Therefore, as the Module becomes mobile, it may associate with an AP that is not in your expected network (as a result, roaming may not work).

If `wl-ssid` is set to a value that is not the "`any`" string, the Module will scan for APs that match the SSID and 802.11 capability information header. If a matching AP is found, the Module will associate. As the Module becomes mobile, it will only roam to APs that match the SSID and 802.11 capability information header.

Roaming is primarily a function of the AP. The APs in your network should monitor the signal strength of the Module and use its Inter Access Point Protocol on your network backbone to transition the Module's association to another AP that is closer to the Module. The role of the Module in roaming is to allow itself to re-associate with the matching AP that is now in range.

The `wl-rate` command affect how readily the Module will disassociate from an AP and associate with another while roaming. 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. 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 frequently to another AP.

1.8 WPA-LEAP SECURITY

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

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

Note: The blank character (space) may not be included in a pass phrase or LEAP password.

1.8.4 Computer Resource Requirements

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

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

1.8.5 System Implementation Considerations

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

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

Symptoms of an unauthenticated client include:

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

Once the WLN is authenticated, additional impacts include:

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

  A WLN configured for LEAP can only roam to APs that support LEAP, roaming, and are connected to the same RADIUS server.
- **Data Throughput and Latency**
  Round trip latency may increase and overall throughput may decrease, due to the additional steps to encrypt or decrypt data.
- **Re-Keying**
  The session key may expire and the authentication process will be executed again causing streaming data to stop until a new key is authorized.

	If Configuring With CLI	
1	`wl-security wpa-psk<CR>`	`OK<CR><LF>`
2	`pw-wpa-psk <passphrase><CR>`	`OK<CR><LF>`
3	`commit<CR>`	`OK<CR><LF>`
4	`restart<CR>`	
5	Module Restarts	

Figure 6. WPA-PSK Sample Security Configuration

	If Configuring With CLI	
1	`wl-security wpa-leap<CR>`	`OK<CR><LF>`
2	`user-leap <username><CR>`	`OK<CR><LF>`
3	`pw-leap <password><CR>`	`OK<CR><LF>`
4	`commit<CR>`	`OK<CR><LF>`
5	`restart<CR>`	
6	Module Restarts	

Figure 7. WPA-LEAP Sample Security Configuration

1.9 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 uppercase or lowercase.
- 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 .

1.10 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**.

1.11 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.

This page left intentionally blank.

CHAPTER 2
CLI COMMANDS

2.1 OVERVIEW

This chapter describes the Airborne™ WLN Module's Command Line Interface (CLI) commands.

The CLI commands are organized into the following categories:

- LAN configuration commands. (page 20)
- Wireless configuration commands. (page 23)
- LAN communication commands. (page 30)
- Escape configuration commands. (page 33)
- UART port configuration commands. (page 34)
- Discovery service commands. (page 35)
- Administration commands. (page 35)
- I/O commands. (page 36)

2.2 CLI COMMANDS

> **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.

The following tables list each CLI command with their corresponding arguments, access level, and description:

2.2.1 LAN Configuration Commands

Command	CLI Arguments	Ln	Description
wl-ip	[IPadrs]	L3*	Configures the static IP address of the Module if the DHCP Client is disabled. Default is `0.0.0.0`.
wl-subnet	[IPadrs]	L3*	Configures the static Subnet Mask of the Module if the DHCP Client is disabled. Default is `255.255.255.0`.
wl-gateway	[IPadrs]	L3*	Configures the static gateway IP address of the Module if the DHCP Client is disabled. Default is `0.0.0.0`.
wl-udap	[<0 | 1>]	L3*	Configures the UDAP Discovery feature to enable or disable. UDAP Discovery is required for discovery of the Module in the subnet by applications like the AEU and the OCT. `0` = disable `1` = enable (*default*)
wl-dhcp	[<0 | 1>]	L3*	Configures the DHCP Client to enable or disable. If the DHCP client is enabled, the Module will use DHCP to obtain an IP configuration. If DHCP fails to obtain the IP configuration, the Module's IP address will be `0.0.0.0`. However, if `wl-dhcp-fb` is enabled, then the values from `wl-dhcp-fbip, wl-dhcp-fbsubnet, wl-dhcp-gateway` will be used as the static IP address, subnet mask and gateway address until the Module is power cycled. `0` = disable `1` = enable (*default*)

wl-ip-source		L3	Method by which current IP address was obtained. This command is read only.
			
			n = IP address invalid
			d = DHCP
			s = static
			f = fallback

wl-dhcp-rel		L3	Releases the current DHCP lease so that wl-dhcp-renew can get a new one.

Command	CLI Arguments	Ln	Description
wl-dhcp-renew		L3	Performs a DHCP renew request to acquire a new IP configuration or update the DHCP lease with the DHCP server.
wl-arp		L3	Causes the unit to produce a gratuitous ARP on the network.
wl-dhcp-client	[string]	L3	Configures the DHCP Client Host Name String to use in the DHCP requests. On some APs, this name is displayed along with the MAC address in the list of attached devices. Up to 31 characters, no spaces. Default is `Airborne™ xxxxxx` where `xxxxxx` are the last six hexadecimal digits of the Module's MAC address.
wl-dns1	[IPadrs]	L3	Configures the Primary DNS Server Address required for DNS lookups with the wl-dns lookup command. If the DHCP Client is enabled, the `wl-dns1` value will be updated (if the DHCP Server provides one). Default is `0.0.0.0`.
wl-dns2	[IPadrs]	L3	Configures the Secondary DNS Server Address. This value is used for DNS lookups, if the lookup fails using the value from `wl-dns1`. If the DHCP Client is enabled, the `wl-dns1` value will be updated (if the DHCP Server provides one). Default is `0.0.0.0`.
wl-dns	string	L2	Performs a DNS lookup using `wl-dns1` and `wl-dns2` as the primary and secondary DNS servers. The input string may be the fully qualified URL or the IP address of the network node. This command returns the IP address that was resolved by the DNS server or an error if not resolved. Responds with the IP address of the URL in a text string format: `xxx.xxx.xxx.xxx`
wl-dhcp-mode	[<0 | 1>]	L3*	Configures DHCP request retransmission mode to either Exponential or Fixed interval. `0` = Exponential interval (default) `1` = Fixed interval
wl-dhcp-interval	[<interval in seconds>]	L3*	Configures the DHCP request 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*	Configures the DHCP fallback algorithm. When the DHCP fallback algorithm is enabled, the Module will apply the configuration from `wl-dhcp-fbip`, `wl-dhcp-fbgateway`, and `wl-dhcp-subnet` as the static IP configuration, if the DHCP client has not received its IP configuration after `wl-dhcp-acqlimit` seconds. `0` = Disable DHCP fallback (default for – UART, Direct Serial) `1` = Enable DHCP fallback (default for – SPI, Direct Ethernet)
wl-dhcp-acqlimit	[<number of seconds>]	L3*	Configures the number of seconds that the Module should wait to acquire its IP configuration using DHCP before applying the DHCP fallback algorithm (if enabled). This is an integer with a range of `1-255` seconds. Default is `150`. Note: “0” will turn off IP Fallback.

Command	CLI Arguments	Ln	Description
wl-dhcp-fbip	[<ip address>]	L3*	Configures the IP address used by the DHCP fallback algorithm. Default (UART, Direct Serial) is 192.168.10.1 Default (SPI, Direct Ethernet) is 0.0.0.0
wl-dhcp-fbsubnet	[<subnet mask>]	L3*	Configures the Subnet Mask used by the DHCP fallback algorithm. Default is 255.255.255.0.
wl-dhcp-fbgateway	[<ip address>]	L3*	Configures the gateway address used by the DHCP fallback algorithm. Default is 0.0.0.0.
wl-dhcp-fbauto	<0|1>	L3*	Enabling this will cause the module to set the wl-dhcp-fbip, wl-dhcp-fbgateway, wl-dhcp-fbsubnet, wl-dns1 and wl-dns2 to their current values each time an IP address is successfully DHCP'ed. 0 - disable (default) 1 - enable This will only occur if wl-dhcp-fb is set and the wl-dhcp-acqlimit is not 0 (zero). If wl-dhcp-fbper is not enabled, the current fallback IP address will not be saved across reboots.
wl-dhcp-fbper	<0|1>	L3*	Enabling this will cause the wl-dhcp-fbip, wl-dhcp-fbgateway, wl-dhcp-fbsubnet, wl-dns1 and wl-dns2 to be saved to memory each time it changes. This will make these values persistent across restarts or power cycles. 0 - disable (default) 1 - enable This will only occur if wl-dhcp-fb and wl-dhcp-fbauto are enabled and the wl-dhcp-acqlimit is not 0 (zero).
wl-con-led	<tcp | pass>	L3	Sets the behavior of the Connect LED to toggle on to indicate TCP or PASS mode When set to TCP, the Module will turn on this LED if the Module accepts a TCP connection on the wl-telnet-port or the wl-tunnel-port. It will also turn on this LED if the Module establishes a TCP connection to the wl-tcp-ip or wl-tcp-ip2 target server. When set to PASS, the Module will turn on this LED if a data bridge is active. If the data bridge becomes inactive (because of the escape sequence or loss of connection on the wireless interface), the Module will turn off this LED. Default is tcp.

2.2.2 Wireless Configuration Commands

Command	CLI Arguments	Ln	Description
wl-mac	[aschex]	L4*	Configures the MAC address of the wireless interface. The input is 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-mac-clone	[0 | 1]	L3*	When set to `0`, the Airborne™ will use its MAC address for communications with the access point on the wireless interface. When set to `1`, the Airborne™ will use the MAC address of the first device on the wired interface for communications on the wireless interface. Default is `0`.
wl-type	[string]	L3*	Configures the wireless interface operation type to participate in an infrastructure or peer-to-peer network. `a` = Infrastructure (AP) mode (*default*) `p` = Peer-to-peer (Ad Hoc) mode
wl-chan	[integer]	L2*	Configures the wireless interface Ad Hoc channel number. The channel number is only applicable in Ad Hoc mode. Some channels are restricted in certain countries. OEMs must use only unrestricted channels. Channel range is `1` – `14`. Default is `1`.
wl-ssid	[string]	L3*	Applies the SSID used for 802.11 association. Up to 31 characters. 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. `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.

Command	CLI Arguments	Ln	Description
wl-security	[disable | wep64 |wep128 | wpa-psk | wpa-leap | wpa-leap64 | wpa-leap128 | wpa-psk64 | wpa-psk128]	L3*	**Selects the Wireless Security Method for Authentication and Encryption** This command replaces the `wl-wep` command. When `wl-security` is configured for a value other than `disable`, the value for `wl-wep` is not evaluated for operation. However, when `wl-security` is configured for `disable`, the value of `wl-wep` takes effect. `Disable` = security is disabled. (default) `wep64` = 64-bit key length (sometimes referred to as 40-bit) `wep128` = 128-bit key length `wpa-psk` = WPA Pre-Shared Key `wpa-leap` = WPA CISCO LEAP `wpa-leap64` = Migration mode w/ Cipher suite TKIP+40-bit WEP using EAP (LEAP). *Requires LEAP username and password.* `wpa-leap128` = Migration mode w/ Cipher suite TKIP+128-bit WEP using EAP (LEAP). *Requires LEAP username and password.* `wpa-psk64` = Migration mode w/ Cipher suite TKIP+40-bit WEP using WPA PSK. *Requires WPA Passphrase.* `wpa-psk128` = Migration mode w/ Cipher suite TKIP+128-bit WEP using WPA PSK. *Requires WPA Passphrase.* Default is `disable`.
pw-wpa-psk	<string>	L3*	Configures the Pre-Shared Key used with WPA-PSK security. The input range is 8 to 63 ASCII characters or 64 hex characters. This key must match the key on the AP.
pw-leap	<string>	L3*	Configures the WPA-LEAP password. The LEAP password [1 to 32 characters] must match the LEAP password assigned to the LEAP user on the LEAP server. The LEAP password cannot contain spaces.
user-leap	[string]	L3*	Configures the WPA-LEAP username. The LEAP username [1 to 32 characters] must match the LEAP username assigned on the LEAP server.
wl-auth	[string]	L3*	Configures the authentication type when WEP 64 or 128 is used. `auto` = authenticates using Open Key algorithm (*default*) `open` = authenticates using Open Key algorithm `shared` = authenticates using Shared Key algorithm
wl-def-key	[integer]	L3*	Configures the default WEP key index. This must match the key index configured on the AP. Range is `1 – 4`. Default is `1`.
wl-wpa-format	[0 | 1]	L3*	WPA information Element type selection 0 = Use 802.11i WPA RSN IE (default) 1 = Use legacy WPA RSN IE
wl-key-1	<aschex>	L3*	Sets WEP Key #1 to binary value. [10 or 26 hex digits] – 10 digits for 64 bits, 26 for 128 bits. Default is `00000000000000000000000000`.
wl-key-2	<aschex>	L3*	Sets WEP Key #2 to binary value. [10 or 26 hex digits] – 10 digits for 64 bits, 26 for 128 bits. Default is `00000000000000000000000000`.

Command	CLI Arguments	Ln	Description
wl-key-3	[aschex]	L3*	Sets 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*	Sets 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 (not currently supported) `2` = Ant2 (*default*) `d` = enables receive diversity

wl-scan		L2	Performs a scan for APs and reports 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 `Airborne™ 31` and the SSID is `Airborne™ *`, the Module scans for APs that start with `Airborne™`.
			
			The status report for each found AP is as follows (for a description of these results, see Table 2):
			
			`SSID:             FirstAccessPoint`
			`BSSID:            0006255D537D`
			`signal (dBm):     -56`
			`rate (Mb/s):      0x0014`
			`capabilities:     0x0005`
			`channel:          0x0007`
			`beacon interval:  100`
			`---------------------`
			`SSID:             SecondAccessPoint`
			`BSSID:            0006255D5C2C`
			`signal (dBm):     -55`
			`rate (Mb/s):      0x000A`
			`capabilities:     0x0015`
			`channel:          0x0008`
			`beacon interval:  100`
			`---------------------`

wl-rate	[string]	L3	Configures 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.
			
			`0 = auto (selects best highest rate - default)`
			`1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, or 54`

wl-device		L1	Reports the DPAC-defined Module device type. This may be used by an OEM application to identify the type of device that it is communicating with. The current list of device types reported is:
			`AIRBORNE™`
			`AIRBORNE™ -SPI`
			`DIRECT-ETHERNET`
			`DIRECT-SERIAL`

wl-region	[string]	L3	Specifies the wireless channels allowed. See table 3 for allowed values. Default is `US`.

<table>
<tr><th>Command</th><th>CLI Arguments</th><th>Ln</th><th>Description</th></tr>
<tr><td>wl-status</td><td></td><td>L2</td><td>

Reports abridged Module status. Below is a sample of the report. See Table 4 for a detailed description of the report.

```
Link Status:          Connected
SSID:                 FirstAccessPoint
BSSID:                0006255D537D
signal level (dBm):   -56
noise level (dBm):    -92
current channel:      1
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.

```
Link Status:          Not Connected
SSID:                 FirstAccessPoint
BSSID:                000000000000
signal level (dBm):   -99
noise level (dBm):    -99
current channel:      1
dhcp status:          0x00
```

</td></tr>
<tr><td>wl-info</td><td></td><td>L2</td><td>

Reports more comprehensive Module status. Below is a sample report indicating that the Module is associated. For a detailed description of these results, see Table 4.

```
Module Firmware Version:      4.3.0.19
Radio Firmware Version:       CF8385-5.0.17.p2
Link Status:                  Connected
SSID:                         FirstAccessPoint
MAC Address:                  0090C9004A80
BSSID:                        00095B6F270C
Transmit Rate (Mb/s):         1
Signal Level (dBm):           -41
Noise Level (dBm):            -92
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
```

</td></tr>
</table>

Table 2. Description of `wl-scan` Results

`wl-scan` Result	Description
`Link Status`	**Wireless Local Network Link Status** Connected Not Connected
`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.
`Rate (Mb/S)`	**Allowed 802.11 rates (dBm)** List of allowed bit rates with basic rates denoted by *.
`Current channel`	**Channel currently in use**
`Beacon Interval`	**Beacon Interval**

Table 3. Region Country Codes

Code	Country	Channels
US	United States	1-11
AT	Austria	1-11
AU	Australia	1-11
BR	Brazil	1-11
CA	Canada	1-11
CH	Switzerland and Liechtenstein	1-11
CY	Cyprus	1-11
CZ	Czech Republic	1-11
DE	Germany	1-11
DK	Denmark	1-11
EE	Estonia	1-11
FI	Finland	1-11
GB	Great Britain	1-11
GR	Greece	1-11
HK	Hong Kong	1-11
HU	Hungary	1-11
IE	Ireland	1-11
IS	Iceland	1-11
IT	Italy	1-11
LT	Lithuania	1-11
LU	Luxembourg	1-11
LV	Latvia	1-11
NL	Netherlands	1-11
NO	Norway	1-11
NZ	New Zealand	1-11
PH	Philippines	1-11
PL	Poland	1-11
PT	Portugal	1-11
SE	Sweden	1-11
SI	Slovenia	1-11
SK	Slovak Republic	1-11
CN	China	1-13
ID	Indonesia	1-13
IL	Israel	1-13
IN	India	1-13
KR	Korea	1-13
MY	Malaysia	1-13
SG	Singapore	1-13
BE	Belgium	1-13
TH	Thailand	1-13
TW	Taiwan	1-13
ZA	South Africa	1-13
JP	Japan Wideband	1-14
FR	France	10-13
ES	Spain	10-11

Table 4. Description of `wl-status` & `wl-info` Results

Result	Description
`Module Firmware Version`	**Module Firmware Version**
`Radio Firmware Version`	**Radio Firmware Version**
`Link Status`	**Wireless Local Network Link Status** Connected Not Connected
`SSID`	**Service Set Identifier String**
`Mac Address`	**Mac Address of Airborne Radio**
`BSSID`	**MAC Address of the Responding AP**
`Transmit Rate (Mb/s)`	**Allowed Transmit Rates**
`Signal Level`	**Signal Level (dBm)** The higher (more positive) the number, the stronger the signal.
`Noise Level`	**Average Noise Level (dBm)** The lower (more negative) the number, the quieter the environment.
`IP Address`	**Current IP address**
`Subnet Mask`	**Current Subnet Mask**
`Default Gateway`	**Current Gateway**
`Primary DNS`	**Current Primary DNS**
`Secondary DNS`	**Current Secondary DNS**
`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.

2.2.3 LAN Communication Commands

Command	CLI Arguments	Ln	Description
wl-telnet-timeout	[integer]	L3	Configures the CLI Server connection inactivity timeout. A setting of `0` specifies an infinite timeout. This parameter only applies to new CLI Sessions, not the one issuing the command. The input range is 32 bits unsigned. Default is `0` (seconds).
wl-telnet-port	[integer]	L3*	Configures the TCP port number that the Module CLI Server listens on for a LAN application connection. Default is `23` (decimal).
wl-tunnel	[0 | 1]	L3*	Enables or disables the tunnel capability of the CLI Server. `0` – disables Tunnel connection `1` – enables Tunnel connection Default is `0`.
wl-tunnel-mode	[tcp | udp]	L3*	Configures the protocol that will be used by the CLI Server to tunnel data. `tcp` – sets TCP as the protocol for tunneling `udp` – sets UDP as the protocol for tunneling Default is `tcp`.
wl-tunnel-port	[integer]	L3*	Configures the CLI Server tunneling port for TCP. The CLI Server will process TCP connection requests on this port as a request to open a CLI Session in PASS Mode. The range of the input is 16 bits unsigned. Default is `8023`.
listen		L2	Sets the CLI session to LISTEN Mode when issued on the serial interface. This command is not applicable on the wireless interface. See "Understanding CLI Sessions" for details on this command.
wl-retry-time	[integer]	L3	Configures the interval (in seconds) between attempts to establish a TCP connection with a LAN TCP server when the `serial-default` configuration is set to PASS Mode. The range of this input is 32 bits unsigned. Default is `60` (seconds).
wl-tcp-timeout	[integer]	L3	Configures the inactivity timeout (in seconds) for TCP connections initiated by the CLI Session on the serial interface using the `pass` or `serial-default` commands. A value of zero sets an infinite timeout. This parameter applies only to newer sessions. The range of this input is 32 bits unsigned. Default is `0 (`seconds).
wl-tcp-port	[integer]	L3	Configures the TCP port number to use when the CLI Session on the serial interface initiates a TCP connection with the `pass` or `serial-default` commands. This value must match the TCP port on which the target server specified by `wl-tcp-ip` is listening. The range of this input is 16 bits unsigned. Default is `2571` (decimal).

Command	CLI Arguments	Ln	Description
wl-tcp-ip	[IPadrs]	L3	Configures the primary target server IP address to use when the CLI Session on the serial interface initiates a TCP connection with the `pass` or `serial-default` commands. If this IP address is empty or the connection is unsuccessful, the CLI Server will attempt a connection to `wl-tcp-ip2` as a secondary target server. Default is `0.0.0.0`.
wl-tcp-ip2	[IPadrs]	L3	Configures the secondary target server IP address to use when the CLI Session on the serial interface initiates a TCP connection with the `pass` or `serial-default` commands. If the CLI Server can not connect to the primary target server, the CLI Server will attempt connection to `wl-tcp-ip2` as a secondary target server. Default is `0.0.0.0`.
pass		L2	Creates a data bridge between the wireless and serial interfaces. The behavior of the `pass` command depends on a number of factors including the interface on which the command was issued and the mode of operation of the CLI Session on the serial interface. See “PASS Mode for the Serial Interface” for details on this command when issued in a CLI Session on the serial interface. See “PASS Mode for the Wireless Interface” for details on this command when issued in a CLI Session on the wireless interface.
putget	<integer1> <integer2> <aschex>	L2	Performs a binary <aschex> data transfer to a target server or to the CLI Session on the serial interface. The operation 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>`
putexpect	<integer1> <integer2> <aschex1> <aschex2>	L2	Performs a binary <aschex> data transfer to a target server or to the CLI Session on the serial interface. The operation 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	Closes a TCP connection initiated by the Serial Host with the `pass` or `serial-default` commands. It also closes the TCP tunnel connection on the `wl-tunnel-port`.

Command	CLI Arguments	Ln	Description
wl-udp-ip	<IP address>	L3	Configures the IP address to use when the Serial Host wishes to send UDP data packets to a remote UDP listener/server. This command can be changed dynamically without saving and restarting. Default is: `0.0.0.0`.
wl-udp-port	[integer]	L3	Configures the UDP port number to use when the Serial Host wishes to send UDP unicast data packets to a remote listener/server. This command can be changed dynamically without saving and restarting. Default is: `8023` (decimal).
wl-udp-rxport	[integer]	L3	Configures 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	Configures the outbound UDP transmission mode. `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`.
wl-xmit-type	[tcp | udp | both]	L3	Configures the outbound TCP and UDP traffic transmission protocols. `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`.

2.2.4 Escape Configuration Commands

Command	CLI Arguments	Ln	Description
esc-mode-serial	<string>	L2	Configures the escape-processing mode for the CLI Session on the serial interface. See “CLI Server Escape Processing” for details on escape processing. `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	Configures the escape-processing mode for the CLI Session on the wireless interface. See “CLI Server Escape Processing” for details on escape processing. `off` = disables LAN escape checking. `on` = enables LAN escape string checking. Default is `on`.
esc-str	<aschex>	L2	Configures the global five (5)-character escape string used for the serial or wireless interface if escape checking is configured for string mode on any of the interfaces. The string must be five (5) bytes (10 aschex digits). Default is `7E7E7E6473`, which is equivalent to `~~~ds`. AbD Serial Default is `FF7E414244`, which is equivalent to `ÿ~ABD`.
escape	[aschex | off]	L2	[Deprecated] Sets the escape string sequence to a 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`. Default is `7E7E7E6473`, which is equivalent to `~~~ds`.

2.2.5 UART Port Configuration Commands — NOT FOR ABD ETHERNET

Command	CLI Arguments	Ln	Description
apply-cfg	<serial>	L3	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 applied are: `bit-rate, data-bits, parity, flow`, and `input-size`.
bit-rate	[string]	L3*	Configures the bit-rate of the serial interface 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	Executes the clear buffer feature. When issued after a `serial-assert` command, it clears all data that is buffered in the Module.
data-bits	[string]	L3*	Configures the serial port data bits. `7` `8` (*default*)
flow	[string]	L3*	Configures the 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	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.
intf-type	[rs232 | rs422 | rs485]	L3*	Sets the serial interface for RS-232, RS-422, or RS-485 communications. Default is `rs232`.
parity	[string]	L3*	Configures the serial port parity. `n` = none (*default*) `e` = even `o` = odd
serial-assert	[xon |xoff]	L3	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. This command requires software flow control to be configured. Default is `xon`.
serial-default	[string]	L4*	Sets the default mode for the CLI Session on the serial interface. The CLI Server will transition to the specified mode on the serial interface at system startup. `pass` = The CLI Session on the serial interface will transition to PASS Mode at system startup. See “PASS Mode for the Serial Interface” for a decription of the transition of the serial interface to PASS Mode. `cli` = The CLi Session on the serial interface will startup in CLI Mode. (*default*) `listen` = The CLI Session on the serial interface will startup in LISTEN Mode.
stop-bit	[1 | 2]	L3	Configures the number of stop bits to use on the serial interface. Default is `1`.

2.2.7 Discovery Service Commands

Command	CLI Arguments	Ln	Description
name-manuf	[string]	L5	Configures the Discovery Name: Manufacturer. 31 characters, no spaces. Default is `DPAC-Airborne™ -A`.
name-oem	[string]	L4	Configures the Discovery Name: OEM. 31 characters, no spaces. Default is `OEM-Cfg1`.
name-device	[string]	L3	Configures the Discovery Name: Device. 31 characters, no spaces. Default is `Device`.

2.2.8 Administration Commands

Command	CLI Arguments	Ln	Description

auth	[string1 string2]	L1	Logs into the Module. The authentication provided by this login is persistent until a logout or restart command is issued. The login is not persistent across a restart.
			`string1 = user ID`
			`string2 = password`
			If no arguments are given, reports security level as `L1`, `L2`, `L3`, `L4`, or `L5`.

commit		L3	Commits the system configuration parameter to non-voliatile memory. Use this command after making parameter changes if you want to retain your parameter after a system power cycle.
cfg-dump		L3	Dumps complete configuration in CLI command format to console screen.
ver-fw		L1	Reports the DPAC firmware version. String [31 characters].
ver-radio		L1	Reports the radio firmware version. String [31 characters].
ver	[string]	L4	Configures an OEM version. String [31 characters] , no spaces. If no argument is given, the current `oemverstr` is returned for any security level. The `ver` command can be issued from an L1 security level without an argument. Default is `oemverstr`.
user-manuf	[string]	L5	Configures the Level 5 User ID [31 characters, no spaces]. Default is `dpac`.
user-oem	[string]	L4	Configures the Level 4 User ID [31 characters, no spaces]. Default is `oem`.
user-cfg	[string]	L3	Configures the Level32 User ID [31 characters, no spaces]. Default is `cfg`.
user	[string]	L2	Configures the Level 2 User ID [31 characters, no spaces]. Default is `user`.
pw-manuf	<string>	L5	Configures the Level 5 Password [31 characters, no spaces]. Default is `dpac`.
pw-oem	<string>	L4	Configures the Level 4 Password [31 characters, no spaces]. Default is `oem`.

Command	CLI Arguments	Ln	Description
pw-cfg	<string>	L3	Configures the Level 3 Password [31 characters, no spaces]. Default is `cfg`.
pw	<string>	L2	Configures the Level 2 Password [31 characters, no spaces]. Default is `password`.
logout		L1	Return to Level 1.
restart		L2	Restarts the Module firmware, reinitializing everything in the system like a power cycle. All system configuration parameters that have not been saved with the `commit` command will be reinitialized to system defaults. All connections on the wireless interface will be disconnected abruptly.
update		L2	Updates the Module's firmware using XMODEM. When using terminal emulation software on a workstation as the serial host, the terminal emulation software may prompt the user for the filename to proceed. However, if used in an embedded system, the XMODEM protocol will complete the transaction. Please see "Data Bridging with XMODEM Guidelines" for more details. After the update is completed, the Module restarts automatically. Execute this command from the serial interface, with hardware handshake enabled (not soft handshake).
time		L2	Reports the number of seconds that the Module has been operational. The accuracy of the internal timer is not guaranteed when power modes are active.
reset		L3	Restores all system configurations to the OEM defaults. This has the same effect as using the "factory reset" button at power-up.

2.2.9 I/O Commands — WLN ONLY

Command	CLI Arguments	Ln	Description
io-read	e | f<portid>	L2	Reads the 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	Writes a value to digital I/O port <num>. <portid> = a bit number from `0-7` (or as allowed by the Signal Assignments tables in the Airborne™ Wireless LAN Node Module Data Book), 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	Sets 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.

Command	CLI Arguments	Ln	Description
io-dir-g	[integer]	L2	Sets 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	Sets 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.
adc-read	g<portid>	L2	Reads analog input port. The returned value's range is an unsigned integer 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.

2.2.12 CLI Commands by Model

The following table lists every CLI command in alphabetical order:

Note: Unless otherwise noted as **N/A** (Not Applicable), the information in the following table applies to the WLN Module, Airborne™ Direct® Serial Bridge, and Airborne™ Direct® Ethernet Bridge.

Table 5. Parameter Keywords

Parameter Keyword	WLN UART	AbD Serial	AbD Ethernet	WLN SPI
adc-read		N/A	N/A	
apply-cfg			N/A	N/A
auth				
bit-rate			N/A	N/A
cfg-dump				
clear-buf			N/A	N/A
close			N/A	
commit				
data-bits			N/A	N/A
escape			N/A	
esc-mode-serial			N/A	
esc-mode-lan			N/A	
esc-str			N/A	
flow			N/A	N/A
input-size			N/A	N/A
Intf-type	N/A		N/A	N/A
io-dir		N/A	N/A	
io-dir-e		N/A	N/A	
io-dir-g		N/A	N/A	
io-read		N/A	N/A	
io-write		N/A	N/A	

Parameter Keyword	WLN UART	AbD Serial	AbD Ethernet	WLN SPI
listen			**N/A**	
logout				
name-device				
name-manuf				
name-oem				
parity			**N/A**	**N/A**
pass			**N/A**	
putget			**N/A**	
putexpect			**N/A**	
pw				
pw-cfg				
pw-manuf				
pw-oem				
pw-leap				
pw-wpa-psk				
reset				
restart				
serial-assert			**N/A**	**N/A**
serial-default			**N/A**	
stop-bit			**N/A**	**N/A**
time				
update			**N/A**	
user				
user-cfg				
user-leap				
user-manuf				
user-oem				
ver				
ver-fw				
wl-ant		**N/A**	**N/A**	

Parameter Keyword	WLN UART	AbD Serial	AbD Ethernet	WLN SPI
wl-auth				
wl-chan				
wl-con-led			**N/A**	
wl-def-key				
wl-device				
wl-dhcp				
wl-dhcp-acqlimit				
wl-dhcp-client				
wl-dhcp-fb				
wl-dhcp-fbgateway				
wl-dhcp-fbip				
wl-dhcp-fbsubnet				
wl-dhcp-interval				
wl-dhcp-mode				
wl-dhcp-renew				
wl-dhcp-rel				
wl-dhcp-fbauto				
wl-dhcp-fbper				
wl-dns				
wl-dns1				
wl-dns2				
wl-gateway				
wl-info				
wl-ip				
wl-ip-source				
wl-key-1				
wl-key-2				
wl-key-3				
wl-key-4				

Parameter Keyword	WLN UART	AbD Serial	AbD Ethernet	WLN SPI
wl-mac				
wl-mac-clone	**N/A**	**N/A**		**N/A**
wl-rate				
wl-region				
wl-retry-time			**N/A**	
wl-scan				
wl-security				
wl-ssid				
wl-status				
wl-subnet				
wl-tcp-ip			**N/A**	
wl-tcp-ip2			**N/A**	
wl-tcp-port			**N/A**	
wl-tcp-timeout			**N/A**	
wl-telnet-port				
wl-telnet-timeout				
wl-tunnel			**N/A**	
wl-tunnel-port			**N/A**	
wl-tunnel-mode			**N/A**	
wl-type				
wl-udap				
wl-udp-ip			**N/A**	
wl-udp-port			**N/A**	
wl-udp-rxport			**N/A**	
wl-udp-xmit			**N/A**	
wl-wpa-format				
wl-xmit-type			**N/A**	

2.3 CLI ERROR CODES AND MESSAGES

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

Table 6. CLI Error Codes

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
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
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

GLOSSARY

This is a glossary of wireless terminology.

4-Way Handshake	A connection method where each side of the connection acts independently (four packets are exchanged between the supplicant and the authenticator) and is required to successfully complete the WPA authentication process.
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.
Authentication Server	An entity providing authentication service to the authenticator. It may be co-located with an authenticator (e.g., as in a Cisco 1200 Access Point), but is usually an external server (e.g., RADIUS).
Authenticator	The entity that requires the entity on the other end of the link to be authenticated.
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.
EAP	Extensible Authentication Protocol, a general protocol supporting multiple authentication methods used between the client and the authenticator. The 802.1X standard specifies encapsulation methods for transmitting EAP messages so they can be carried over different media.
EAPOL	EAP over LAN, an 802.1X delivery mechanism used in authentication. EAPOL encapsulates EAP messages between the supplicant and the authenticator.
ESS	Each set of wireless devices communicating directly with each other is called a basic service set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). A Service Set Identifier (SSID) is the 1-32 byte alphanumeric name given to each ESS.
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.

IEEE 802.1X	IEEE standard for port-based network control. 802.1X provides multiple methods to authenticate devices attached to a LAN port and functions with both wired and wireless LAN media. 802.1X is based on the Extensible Authentication Protocol (EAP), and features dynamic distribution and management of session keys. A RADIUS server is required for this security standard.
IEEE 802.11i	IEEE security standard officially ratified in June 2004 as part of the 802.11 family. 802.11i was tested and certified for interoperability by the Wi-Fi Alliance. In addition to improved encryption, this standard contains the 802.1X standard, improving key management and user authentication.
Independent Basic Service Set Network (IBSS Network)	An IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations. This type of network is often referred to as an Ad Hoc network because it can be constructed quickly without too much planning.
Infrastructure mode	A client setting providing connectivity to an Access Point. As compared to Ad Hoc mode, where PCs communicate directly with each other, clients set in Infrastructure mode all pass data through a central Access Point. The Access Point not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad Hoc and Access Point.
LAN application	A software application that runs on a computer that is attached to a LAN, Intranet, or the Internet, and uses various protocols to communicate with the Module.
LEAP	Lightweight Extensible Authentication Protocol developed by Cisco. LEAP provides username/password-based authentication between a wireless client and a RADIUS server. It is one of several protocols used with the IEEE 802.1X standard for LAN port access control.
Local Area Network	A system of connecting PCs and other devices within the same physical proximity for sharing resources such as Internet connections, printers, files, and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.
Media Access Control (MAC) Layer	One of two sub-layers that make up the Data Link Layer of the OSI reference model. The MAC layer is responsible for moving data packets to and from one network node to another across a shared channel.
MPDU	MAC Protocol Data Unit, the unit of data exchanged between two peer MAC entities using the services of the physical layer (PHY).
MSDU	MAC Service Data Unit, information that is delivered as a unit between MAC service Access Points (SAPs).
Peer-to-peer network	A wireless or wired computer network that has no server, central hub, or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an Access Point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.
PSK	Pre-Shared Key and is used in authentication. This is a shared key between the station and the AP and is entered as a passphrase.

RADIUS	Remote Authentication Dial In User Service. A backend server that performs authentication using Extensible Authentication Protocol (EAP). This server is required by the IEEE 802.1X security standard.
RS-232	An EIA standard that specifies up to 20 Kbps, 50 foot serial transmission between computers and peripheral devices.
RTOS	An operating system implementing components and services that explicitly offer deterministic responses, and therefore allow the creation of real-time systems. An RTOS is characterized by the richness of the services it provides, the performance characteristics of those services, and the degree that those performance characteristics can be controlled by the application engineer (to satisfy the requirements of the application).
Service Set Identifier (SSID)	An identifier attached to packets sent over the wireless LAN that functions as a "password" for joining a particular radio network (BSS). All radios and Access Points within the same BSS must use the same SSID or their packets will be ignored.
SPI	Short for Serial Peripheral Interface, a full-duplex serial interface for connecting external devices using four wires. SPI devices communicate using a master/slave relationship over two data lines and two control lines.
Supplicant	The entity being authenticated by the authenticator and desiring access to the services of the authenticator.
Telnet	A virtual terminal protocol used (e.g., with the Internet) to enable users to log into a remote Host.
TKIP	Temporal Key Integrity Protocol and is used in encryption. TKIP is an IEEE 802.11i standard and an enhancement to WEP security.
Transceiver	A device for transmitting and receiving packets between the computer and the medium.
Transmission Control Protocol (TCP)	A commonly used protocol for establishing and maintaining communications between applications on different computers. TCP provides full-duplex, acknowledged, and flow-controlled service to upper-layer protocols and applications.
UDP	Short for User Datagram Protocol, UDP is a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages or sending streaming data (e.g., video) over a network.
Wide Area Network (WAN)	A communication system of connecting PCs (and other computing devices) across a large local, regional, national, or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered wireless LANs.
Wi-Fi	Wi-Fi is a name for 802.11 wireless network technology.
Wi-Fi Alliance	A non-profit international association formed in 1999 to certify interoperability of wireless LAN products based on the IEEE 802.11 specification.
Wired Equivalent Privacy (WEP)	A security protocol for wireless LANs defined in the IEEE 802.11 standard. WEP is designed to provide the same level of security as a wired LAN.

WLAN	Also referred to as a wireless LAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes and provide network connectivity.
WLN	Short for Wireless LAN Node, this is the Airborne™ Module that provides 802.11 LAN connectivity.
WLN Module	Module Airborne™ Wireless LAN Node Module.
WLN UART	This is the model of the Airborne™ Module that uses a serial UART to interface to a Host device.
WPA	Wi-Fi Protected Access. It addresses all known Wired Equivalent Privacy (WEP) vulnerabilities. WPA uses RC4 for encryption and TKIP for key management. It includes a message integrity mechanism commonly called Michael or MIC.
WPA-LEAP	Wi-Fi Protected Access - Light Extensible Authentication Protocol, an implementation based on the IEEE 802.11i 2004 and IEEE 802.1X 2001 standards, which includes the LEAP protocol for initial key assignment.
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key, an implementation based on the IEEE 802.11i 2004 and IEEE 802.1X 2001 standards, where the PSK is stored on the client.

This page left intentionally blank.

100-8005-101G
Revision 1.01
April 2007