

AirborneDirect™

DP5xx/IN5xxx Family User Manual

Revision 1.0

April 2013





International Headquarters

B&B Electronics Mfg. Co. Inc.

707 Dayton Road

Ottawa, IL 61350 USA

Phone (815) 433-5100 -- **General Fax** (815) 433-5105

Website: www.bb-elec.com

European Headquarters

B&B Electronics Ltd.

Westlink Commercial Park

Oranmore, Co. Galway, Ireland

Phone +353 91-792444 -- **Fax** +353 91-792445

Website: www.bb-europe.com

Contents

| | | |
|------|---|----|
| 1.0 | Conventions | 8 |
| 1.1 | Terminology | 8 |
| 1.2 | Notes | 8 |
| 1.3 | Caution..... | 8 |
| 1.4 | File Format | 8 |
| 2.0 | Product Description | 9 |
| 3.0 | Features..... | 10 |
| 4.0 | Device Types | 11 |
| 4.1 | Serial | 11 |
| 4.2 | Ethernet | 11 |
| 4.3 | Serial + Ethernet..... | 11 |
| 4.4 | Enterprise Class | 12 |
| 4.5 | Industrial Class | 12 |
| 5.0 | Block Diagram..... | 14 |
| 6.0 | Pin out and Connectors | 16 |
| 6.1 | Serial Ports..... | 16 |
| 6.2 | Ethernet Port..... | 17 |
| 6.3 | Connector Definition | 18 |
| 6.4 | OEM Reset Switch (Factory Reset)..... | 19 |
| 6.5 | Enterprise Serial Interface Jumpers | 19 |
| 6.6 | Indicator LED's | 20 |
| 7.0 | Electrical & RF Specification..... | 22 |
| 7.1 | AC Electrical Characteristics – Transmitter..... | 24 |
| 7.2 | Performance/Range..... | 24 |
| 8.0 | Antenna..... | 25 |
| 8.1 | Antenna Selection | 25 |
| 8.2 | Host Board Mounted Antenna | 25 |
| 8.3 | Host Chassis Mounted Antenna..... | 26 |
| 8.4 | Embedded Antenna | 26 |
| 8.5 | Antenna Location | 27 |
| 8.6 | Performance..... | 28 |
| 9.0 | Mechanical Outline – Enterprise Class | 30 |
| 10.0 | Mechanical Outline – Industrial Class | 31 |
| 11.0 | Getting Started..... | 32 |
| 11.1 | Unpack the AirborneDirect™ Device..... | 32 |
| 11.2 | Connect AirborneDirect™ to host | 32 |
| 11.3 | Attach Antenna and Power-up the AirborneDirect™ | 32 |
| 12.0 | Configuring Device – Industrial Serial (ABDx-SE-IN5xxx) | 33 |
| 13.0 | Configuring Device – Enterprise Serial (ABDx-SE-DP5xx)..... | 36 |
| 13.1 | Connect a Host Computer | 36 |

| | | |
|--------|--|----|
| 13.2 | Interacting with the AirborneDirect™ device | 36 |
| 13.3 | Determine and Store the Access Point SSID | 37 |
| 13.4 | Determine the Device's IP address | 37 |
| 13.5 | Accessing the Device Using the Web Interface..... | 38 |
| 13.6 | Accessing the Device Using Telnet | 38 |
| 14.0 | Configuring Device – Enterprise/Industrial Ethernet (ABDx-ER-DP5xx/IN5xxx) | 39 |
| 15.0 | Using the Web Interface | 42 |
| 15.1 | Navigation Bar | 43 |
| 15.2 | Feature Links | 44 |
| 15.3 | Navigating the Website..... | 44 |
| 15.4 | Updating a Field | 45 |
| 15.5 | Uploading Certificates..... | 46 |
| 15.6 | Upload Configuration Files..... | 47 |
| 15.7 | Updating Firmware | 48 |
| 16.0 | Express Setup Configuration Page..... | 51 |
| 17.0 | Configuring the Wireless Interface..... | 54 |
| 17.1 | Configuring for Infrastructure Networks | 54 |
| 17.2 | Configuring for AdHoc Networks..... | 54 |
| 18.0 | Configuring the Security Settings..... | 56 |
| 18.1 | Configuring for WEP Security..... | 56 |
| 18.2 | Configuring for WPA-PSK Security | 57 |
| 18.3 | Configuring for WPA2-PSK Security | 58 |
| 18.4 | Configuring for PEAP Security | 59 |
| 19.0 | Configuring Network Settings | 61 |
| 19.1 | Configuring DHCP on WLAN Interface | 61 |
| 19.2 | Configuring DHCP on Ethernet Interface..... | 62 |
| 19.3 | Configuring a Static IP Address on WLAN Interface..... | 63 |
| 19.4 | Configuring a Static IP Address on Ethernet Interface | 64 |
| 20.0 | Configuring Serial Device Server | 66 |
| 20.1 | Configuring Serial Port for Access on Telnet Port..... | 66 |
| 20.2 | Configuring Serial Port 1 for Access on Tunnel Port | 67 |
| 20.3 | Configuring Serial Port 2 for Access on Tunnel Port | 69 |
| 20.4 | Configuring Serial Port 1 as TCP Client..... | 70 |
| 20.5 | Configuring Serial Port 2 as TCP Client..... | 71 |
| 21.0 | Installing and Using the Airborne VirtualCOM Driver | 73 |
| 22.0 | Replacing a Serial Cable | 77 |
| 23.0 | Configuring Ethernet Adapter | 80 |
| 23.1 | Router Functionality | 80 |
| 23.1.1 | Public Network Interface | 81 |
| 23.1.2 | Private Network Interface | 82 |
| 23.2 | Bridge Functionality | 85 |

| | | |
|------|--|-----|
| 23.3 | MAC Cloning | 86 |
| 24.0 | Web Page Overview | 87 |
| | Module Status | 88 |
| | Ethernet Status | 89 |
| | Ethernet DHCP Clients | 90 |
| | Radio Statistics | 91 |
| | Ethernet Statistics | 92 |
| | Express Setup | 93 |
| | WLAN Settings | 94 |
| | WLAN Security Settings | 95 |
| | Network Settings | 97 |
| | Serial Port Settings | 99 |
| | Serial Port 2 Settings | 100 |
| | Connection Settings | 101 |
| | Ethernet Settings | 103 |
| | Wireless Routing Settings | 104 |
| | Ethernet Routing Settings | 105 |
| | Advanced Settings | 106 |
| | Upload Configuration File | 109 |
| | List Configuration File | 110 |
| | Delete Configuration File | 111 |
| | Active Configuration | 112 |
| | User Configuration | 113 |
| | OEM Configuration | 114 |
| | Factory Configuration | 115 |
| | WPA Configuration | 116 |
| | List Certificates | 117 |
| | Upload Certificate | 118 |
| | Delete Certificate | 119 |
| | Network (Home Page) | 120 |
| | Discover Airborne Modules | 121 |
| | Scan for Access Points | 122 |
| | Maintenance (Home Page) | 123 |
| | Update Module Firmware | 124 |
| | Reset Factory Defaults | 125 |
| | Restart Module | 126 |
| | Set System Time | 127 |
| | Blink the POST LED | 128 |
| | Stop Blinking the POST LED | 129 |
| 25.0 | Certification & Regulatory Approvals | 130 |
| 25.1 | FCC Statement | 130 |
| 25.2 | FCC RF Exposure Statement | 130 |
| 25.3 | Information for Canadian Users (IC Notice) | 131 |
| 25.4 | FCC/IC Modular Approval | 131 |
| 25.5 | Regulatory Test Mode Support | 132 |
| 26.0 | Physical & Environmental Approvals | 133 |

Figures

| | |
|--|----|
| Figure 1 - Enterprise AirborneDirect™ Device..... | 12 |
| Figure 2 - Industrial AirborneDirect™ Device..... | 13 |
| Figure 3 - ABDx-ER/SE-DP5xx Block Diagram..... | 14 |
| Figure 4 - ABDx-ER/SE-IN5xxx Block Diagram..... | 15 |
| Figure 5 - DE-9 (DB-9) Connector Pin-out..... | 16 |
| Figure 6 - Ethernet Jack Pin Out..... | 17 |
| Figure 7- Interface Selection Jumpers..... | 20 |
| Figure 8 - Website Login..... | 42 |
| Figure 9 - Default Home Page..... | 43 |
| Figure 10 - Website Navigation Bar..... | 43 |
| Figure 11- Feature Links..... | 44 |
| Figure 12 - Airborne Web Page..... | 45 |
| Figure 13 - Upload Certificate Web page..... | 46 |
| Figure 14 - Upload Configuration Web Page..... | 47 |
| Figure 15 - Firmware Update Page..... | 49 |
| Figure 16 - Firmware Update in Progress..... | 49 |
| Figure 17 - Firmware Update Complete..... | 50 |
| Figure 18 - Express Setup Page..... | 51 |
| Figure 19 - Ethernet Bridge Functionality..... | 80 |
| Figure 20 - Airborne Ethernet Bridge IP Configuration..... | 82 |

Tables

| | |
|--|----|
| Table 1 – Serial Port Pin Definition..... | 16 |
| Table 2 - Serial Ports by Product Class..... | 17 |
| Table 3 - Ethernet Connector Pin Out..... | 17 |
| Table 4 - Connector Description..... | 18 |
| Table 5 - OEM Reset Procedure..... | 19 |
| Table 6 - Enterprise LED Indicators..... | 20 |
| Table 7 - Industrial LED Indicators..... | 21 |
| Table 8- Absolute Maximum Values ¹ | 22 |
| Table 9 - RF Characteristics – 802.11a/b/g/n..... | 22 |
| Table 10 - Supported Data Rates by Band..... | 23 |
| Table 11 - Operating Channels..... | 23 |
| Table 12 - Radio Typical Performance Range..... | 24 |
| Table 13 - Embedded Antenna Options..... | 26 |
| Table 14 - SE-IN5xxx Accessing the Web Interface..... | 33 |
| Table 15 - UART Authentication..... | 36 |
| Table 16 - UART SSID & Authentication..... | 37 |
| Table 17 - UART Determine Module's IP Address..... | 37 |
| Table 18 – ER-DP5xx/IN5xxx Accessing the Web Interface..... | 39 |
| Table 19 - Navigation Bar Items..... | 43 |
| Table 20 - Uploading Certificates..... | 46 |
| Table 21 - Uploading Configurations..... | 47 |
| Table 22 - Updating Firmware..... | 50 |
| Table 23 - Express Page Setup..... | 51 |
| Table 24 - Configuring Wireless Interface - Infrastructure..... | 54 |
| Table 25 - Configuring Wireless Interface - AdHoc..... | 55 |
| Table 26 - Configuring for WEP Security..... | 56 |
| Table 27 - Configuring for WPA Security..... | 57 |
| Table 28 - Configuring for WPA2 Security..... | 58 |
| Table 29 - Configuring for PEAP Security..... | 59 |
| Table 30 - Configuring DHCP - WLAN..... | 61 |
| Table 31 - Configuring DHCP - Ethernet..... | 62 |
| Table 32 - Configuring Static IP - WLAN..... | 63 |
| Table 33 - Configuring Static IP - Ethernet..... | 64 |
| Table 34 – Configure Data Tunnel on Telnet Port..... | 66 |
| Table 35 - Data Tunnel using Telnet Port..... | 67 |
| Table 36 – Configure Data Tunnel on Serial Port 1 Tunnel Port (TCP)..... | 68 |

| | |
|---|-----|
| Table 37 - Data Tunnel using Tunnel Port on Serial Port 1 | 68 |
| Table 38 – Configure Data Tunnel on Serial Port 2 Tunnel Port (TCP) | 69 |
| Table 39 - Data Tunnel using Tunnel Port on Serial Port 2 | 70 |
| Table 40 - Configure Serial Port 1 as TCP Client..... | 70 |
| Table 41 - Configure Serial Port 2 as TCP Client..... | 71 |
| Table 42 - Install VCOM..... | 73 |
| Table 43 - Cable Replacement - Slave Configuration..... | 77 |
| Table 44 - Cable Replacement - Master Configuration | 78 |
| Table 45 - Ethernet Adapter interface Configuration - DHCP..... | 82 |
| Table 46 - Ethernet Adapter interface Configuration - Static IP | 83 |
| Table 47 - Ethernet Adapter interface Configuration..... | 86 |
| Table 48 - Regulatory Approvals | 130 |
| Table 49 - Modular Approval Grant Numbers | 131 |
| Table 50 - Mechanical Approvals..... | 133 |

1.0 Conventions

The following section outlines the conventions used within the document, where convention is deviated from the deviation takes precedence and should be followed. If you have any question related to the conventions used or clarification of indicated deviation please contact B&B Electronics Sales or Wireless Support.

1.1 Terminology

Airborne Enterprise Device Server and AirborneDirect Enterprise Device Server is used in the opening section to describe the devices detailed in this document, after this section the term ***module*** will be used to describe the devices.

1.2 Notes

A note contains information that requires special attention. The following convention will be used. The area next to the indicator will identify the specific information and make any references necessary.



The area next to the indicator will identify the specific information and make any references necessary.

1.3 Caution

A caution contains information that, if not followed, may cause damage to the product or injury to the user. The shaded area next to the indicator will identify the specific information and make any references necessary.



The area next to the indicator will identify the specific information and make any references necessary.

1.4 File Format

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 Acrobat Reader is provided on the Radio Evaluation Kit CD. Should you not have the CD, for the latest version of Adobe Acrobat Reader, go to the Adobe Web site (www.adobe.com).

2.0 Product Description

This guide describes the AirborneDirect™ device servers and wireless adapters from B&B Electronics, Inc. AirborneDirect™ is a fully integrated, 802.11 wireless Local Area Network (LAN) connectivity device designed to provide wireless LAN and Internet connectivity in industrial, scientific, medical, and transportation applications where an existing communications interface already exists. The AirborneDirect family of products supports Serial (RS232/422/485), Ethernet and a combination these interfaces in a range of packaging options.

The AirborneDirect™ product family provides true plug-and-play wireless connectivity. By delivering convenient, easy-to-deploy wireless network connectivity, the device servers and adapters significantly reduce the complexities of wireless system deployment and network implementation. At the same time, users can move equipment without the cost and time associated with wired network drops and environment restrictions. This provides flexibility for seasonal demands, line and staffing changes, and more.

The AirborneDirect™ family includes models with single band or dual band radios: the ABDG supports 802.11b/g and the ABDN supports 802.11a/b/g/n.

The AirborneDirect™ Serial Bridges and device servers provide a simple connection between the 802.11 wireless LAN and three leading serial interfaces: RS-232, RS-422, and RS-485. The Bridge acts transparently between any device using these interfaces and a wireless LAN. Using the B&B Electronics virtual communications port Windows device driver OEMs can communicate with their devices from any workstation on the same network as if the workstation and devices were directly attached through a serial port.

The AirborneDirect™ Ethernet Adapter provides a link between the 802.11 wireless LAN and any Ethernet-ready device with an RJ-45 connector. It acts transparently between the device and a wireless LAN. By integrating AirborneDirect™ into existing and legacy platforms, OEMs can significantly enhance their products by delivering increased value and functionality to their entire customer base.

The Airborne family includes the ability to simultaneously use the serial-to-wireless and Ethernet-to-wireless connectivity in the same unit. This capability provides for multiple connections to the same machine or consolidation of multiple wireless units into a single device.

The AirborneDirect™ products open the world of remote device monitoring and management, as well as wide-area data collection, to any device, machine, or plant that has an external serial or Ethernet connection and a network infrastructure. The development kit provides quick and easy access to the Bridge's configuration and functions, while providing OEMs with a platform to develop their branded solutions. The Bridge also provides the capability to perform firmware upgrades that allow new features to be added quickly and easily, protecting your investment.

The Enterprise family includes the most advanced security support available for the device class in the industry, including WPA, WPA2 and full Enterprise support. The devices can be used with the most advanced WLAN networks being deployed today. The Airborne products are based upon the industry leading Airborne device server and wireless adapter technology from B&B Electronics, providing a fully compatible and familiar device interface across the all product ranges. If you've used one of them, you have used them all.

3.0 Features

- 802.11 WiFi Radio with 32bit ARM9 CPU (128Mb SDRAM, 64Mb Flash)
 - ABDG series supports 802.11b/g
 - ABDN series supports 802.11a/b/g/n
- Integrated Airborne Device Server and Wireless Adapter technology.
- Supports WEP, WPA, WPA2 and 802.1x Supplicant, with Certificates.
- The wireless device server includes integrated:
 - 802.11 Radio Driver
 - TCP/IP stack, UDP, telnet, FTP server
 - Data bridging and buffering
 - Command Line Interface
 - Web interface
 - WPA Supplicant
 - DHCP Server (Ethernet Interface)
 - Firewall and Port Forwarding (Ethernet)
 - FTP Server
- Supports flexible antenna selection.
- Operating Temperature (-40°C to 85°C)
- Storage temp (-40°C to 85°C)
- Industry standard wired connections:
 - D-9 Serial connectors (RS232/422/485)
 - RJ-45 (10/100 Ethernet)
- Multiple host interfaces supported:
 - Single and Dual Serial (RS232/422/485) – up to 921K BAUD
 - 10/100 Ethernet
- Integrated standard and wide range (J1455) Power Supply (5-36VDC)
- Power connector options include 2.1mm Barrel Jack, Terminal Block and custom connectors.
- Power Over Ethernet (PoE) using an 802.3af Class 1 PSE device (ABDx-ER-IN5xx8 models)
- Integrated Site Survey mode.
- Advanced Low power modes.
- Rugged mounting options.
- Virtual COM port driver (WinXP, Vista, Win7)
- Worldwide Regulatory Support (FCC, IC, CE)

4.0 Device Types

This manual covers all variations available in the AirborneDirect™ device family. The following section identifies the different types both functional and classification. In most cases the functional types are available in the listed classifications. If you are not certain which type you have or would like clarify the available options please contact B&B Electronics Sales or Technical support.

4.1 Serial

This device supports a single or dual serial port and provides serial to 802.11 bridging. The serial devices can support one or more of the following serial interface types:

- RS232
- RS422
- RS485

Default configuration on all models is RS232, conversion to RS422/485 requires software configuration and in some models jumper setting changes. These are covered in the following sections.

This device allows the connection of a serial port to an 802.11 network.

4.2 Ethernet

The Ethernet adapter provides a wireless interface to an existing Ethernet port (RJ-45). Depending upon the model of device the connection to the Ethernet port of the host is made via a RJ-45 socket or pigtail with a RJ-45 plug.

The device supports a 10/100 Ethernet interface with auto configuration. Manual control of the interface is possible through the web or CLI interface.

4.3 Serial + Ethernet

This device allows for simultaneous connection of Serial and Ethernet ports. Providing the same functionality on each port that is available on the individual devices, it is possible to maintain network based connections to both the Ethernet and Serial ports without compromise of functionality or performance.

Each interface can be configured and operated independently of the others. Connection to the serial port can be made via both the wireless and Ethernet ports supporting redundant network connectivity for high reliability applications.

4.4 Enterprise Class

The enterprise class product provides the best cost vs. performance in the AirborneDirect™ product family. The packaging is compact and designed to fit with non-industrial applications and markets. The product class supports the full industrial operating temperature range and the complete set of functional capabilities of the Airborne™ Device Server and Wireless Adapter technology.

Figure 1 - Enterprise AirborneDirect™ Device



The Enterprise class product range includes devices that support a single serial port and an Ethernet device.

The enterprise class product is ideal for the following application types:

- Medical equipment.
- Point-of-Sale devices.
- CNC/DNC equipment.
- Time clocks.
- Scales.
- Data collection devices.
- Vehicle diagnostics.

The Enterprise Class products require a 5VDC power supply.

4.5 Industrial Class

Developed to support the demands of the industrial and automotive environments, the features of the Industrial Class products offer a more flexible and rugged alternative to the enterprise class devices. The product class supports the full industrial operating temperature range and the complete set of functional capabilities of the Airborne Device Server and Wireless Adapter technology.

Figure 2 - Industrial AirborneDirect™ Device

The family includes a metal enclosure and a wide range power supply capable of exceeding the SAE J1455 power supply requirements.

The enterprise class product is ideal for the following application types:

- CNC/DNC equipment.
- Vehicle diagnostics.
- Telematics.
- Remote monitoring and management.
- Industrial control.

The Industrial class of products includes Ethernet only, Serial only and the dual (Serial+Ethernet) capability. Some models support Power over Ethernet (PoE) when connected to an 802.3af Class 1 PSE device.

5.0 Block Diagram

The following outlines the block diagram for the devices:

Figure 3 - ABDx-ER/SE-DP5xx Block Diagram

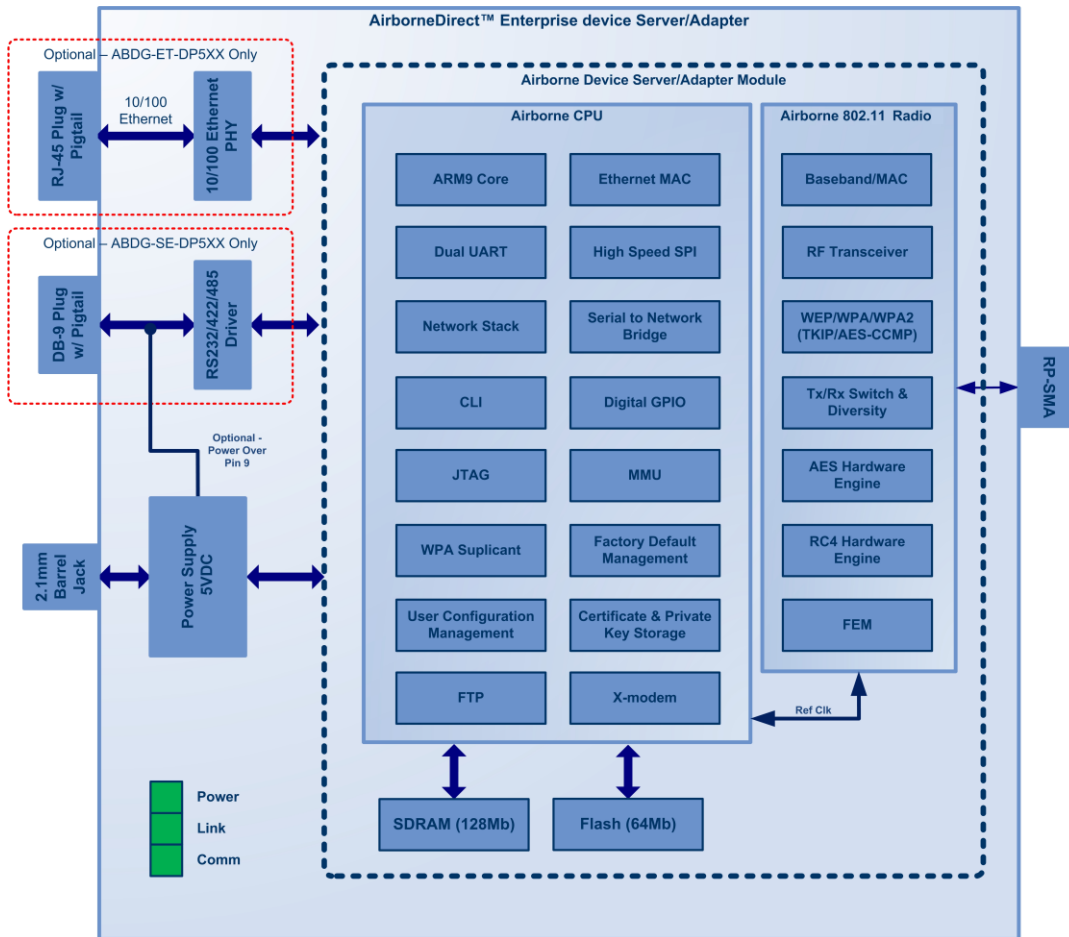
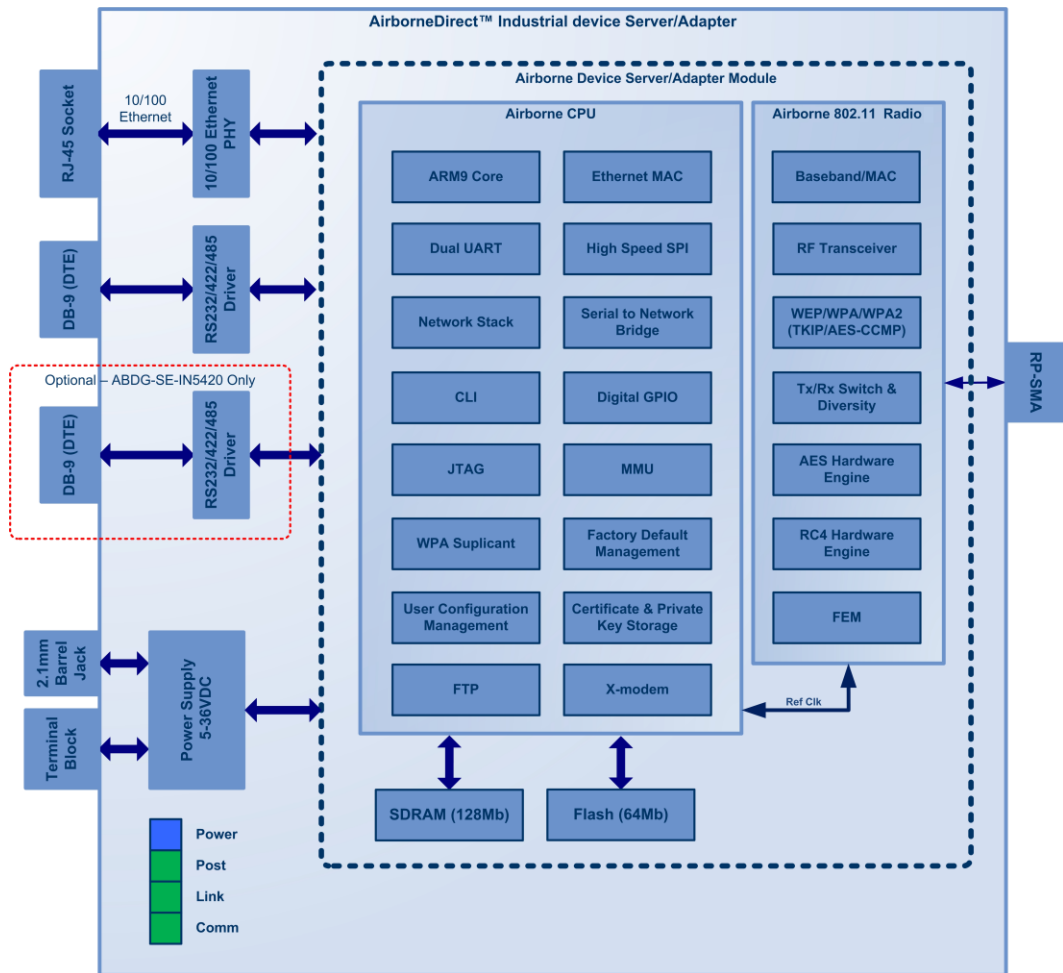


Figure 4 - ABDx-ER/SE-IN5xxx Block Diagram



6.0 Pin out and Connectors

Pin definition is dependent upon the device type selected. The following defines the pin outs for the individual interfaces.

6.1 Serial Ports

The AirborneDirect™ units support either a single or dual serial port configuration. The Port pin out can change depending upon the interface configuration chosen, Table 1 shows the pin out for the interface selected.

Figure 5 - DE-9 (DB-9) Connector Pin-out

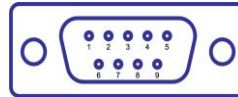


Table 1 – Serial Port Pin Definition

| Pin | RS232 (DTE) | RS232 w/ Power on pin 9 ² | RS422 | RS485 |
|-----|-------------|---|------------|-------------------------------|
| 1 | No Connect | No Connect | No Connect | No Connect |
| 2 | RxD | RxD | RxD+ | Connect to pin 3 ³ |
| 3 | TxD | TxD | TxD+ | TxD+/RxD+ |
| 4 | No Connect | No Connect | No Connect | No Connect |
| 5 | GND | GND | GND | GND |
| 6 | No Connect | No Connect | RxD- | Connect to pin 9 ³ |
| 7 | RTS | RTS | No Connect | No Connect |
| 8 | CTS | CTS | No Connect | No Connect |
| 9 | No Connect | 5VDC (Input) | TxD- | TxD-/RxD- |



1. For 2-wire operation, the user must externally connect pin 3 to pin 2 and pin 6 to pin 9.
2. Power on pin 9 only available on Enterprise devices (ABDx-SE-DP501).
3. Only required on Industrial products (ABDx-SE-IN54XX)

Table 2 shows the availability of the serial ports and available interface types by product class.

Table 2 - Serial Ports by Product Class

| Device Class | Port 1 | Port 2 |
|--------------|---|-------------------------|
| Enterprise | RS232 RS422 (4-wire) RS485 (2-wire) | N/A |
| Industrial | RS232 RS422 (4-wire) RS485(2-wire) | N/A |
| | RS232 RS422 (4-wire) RS485(2-wire) | RS232 RS422 (4-wire) |

The Port 1 and Port 2 interfaces support the following configurations:

- BAUD: 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 57600, 115200, 230400, 460800, 921600
- Flow Control: None, Hardware (CTS/RTS), Software (XON/XOFF)
- Port 1 Default settings: 9600, 8, N, 1, No Flow Control.
- Port 2 Default settings: 9600, 8, N, 1, No Flow Control.

6.2 Ethernet Port

The AirborneDirect™ Ethernet devices support a single interface. This is a 10/100Mbps interface that supports auto negotiation and cross-over cabling. The interface also supports both half and full duplex for 10Mbps and 100Mbps. Table 3 shows the interface pin out.

In some Industrial models, the Ethernet port supports Power over Ethernet (PoE) when connected to an 802.3af Class 1 PSE device. Both Mode A (MDI and MDI-X) and Mode B powering schemes are supported (Table 3a).

Figure 6 - Ethernet Jack Pin Out

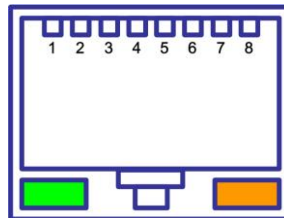


Table 3 - Ethernet Connector Pin Out

| Pin | RJ45 Socket (Industrial) | RJ45 Plug (Enterprise) |
|-----|--------------------------|------------------------|
| 1 | TxD+ | RxD+ |
| 2 | TxD- | RxD- |
| 3 | RxD+ | TxD+ |
| 4 | NC | NC |
| 5 | NC | NC |

| Pin | RJ45 Socket (Industrial) | RJ45 Plug (Enterprise) |
|------------|---|------------------------|
| 6 | RxD- | TxD- |
| 7 | NC | NC |
| 8 | NC | NC |
| Green LED | Valid TCP/IP connection made with Airborne Adapter: Off No TCP/IP connection On Valid TCP/IP Connection | N/A |
| Yellow LED | Power-on Self Test (POST): Off Not powered or has failed POST On Passed POST | N/A |

Table 3a - PoE Pinout Alternatives

| Pin | Alternate A (MDI-X) | Alternate A (MDI) | Alternate B (All) |
|-----|---------------------|--------------------|--------------------|
| 1 | Negative V_{PSE} | Positive V_{PSE} | |
| 2 | Negative V_{PSE} | Positive V_{PSE} | |
| 3 | Positive V_{PSE} | Negative V_{PSE} | |
| 4 | | | Positive V_{PSE} |
| 5 | | | Positive V_{PSE} |
| 6 | Positive V_{PSE} | Negative V_{PSE} | |
| 7 | | | Negative V_{PSE} |
| 8 | | | Negative V_{PSE} |

6.3 Connector Definition

There are a total of five connectors used by the AirborneDirect™ family. Which connectors are available on your product depend upon the model you purchased. The definition for the connectors is common to all product classes. Table 4 provides definitions for the connectors.

Table 4 - Connector Description

| Type | Description | Product Class |
|----------|---------------------------|------------------------|
| Serial | DE-9 Connector Male | Enterprise, Industrial |
| Ethernet | RJ45 Plug | Enterprise |
| Ethernet | RJ45 Socket | Industrial |
| Antenna | RP-SMA | Enterprise, Industrial |
| Power | 2.1mm Barrel Jack | Enterprise, Industrial |
| Power | 2 Position Terminal Block | Industrial |

6.4 OEM Reset Switch (Factory Reset)

All AirborneDirect™ devices support the ability to reset the configuration back to OEM defaults. This is useful when a device has been incorrectly configured and has lost the ability to communicate on any of the available ports, preventing access to one of the configuration interfaces and blocking your ability to recover the device by correcting the configuration.

The following Table 5 describes the sequence for OEM resetting the AirborneDirect™ devices. All devices use the same process however the location of the OEM reset switch varies between the product families.

Table 5 - OEM Reset Procedure

| | |
|----------|---|
| 1 | Disconnect or turn off the power supply. |
| 2 | Press the OEM reset (factory reset) button. This may require the use of a small narrow object, it is important that this object is not sharp as it may cause damage to the unit. |
| 3 | While holding the OEM button pressed reapply power to the unit. |
| 4 | Hold the OEM reset button for 5-6 seconds after power has been applied. |
| 5 | Release the OEM reset button. |
| 6 | The device will restart with the installed OEM defaults. If no OEM Configuration is applied the device will return to B&B Electronics factory defaults. See section 15.6 on use of OEM factory configurations. |

The location of the OEM reset button for the Enterprise devices is on the back of the enclosure, underneath the label near the pigtail. The Industrial devices OEM reset button is on the Ethernet/Power end of the box next to the 2.1mm barrel connector (See section 10.0)

6.5 Enterprise Serial Interface Jumpers

The Enterprise Serial device server supports RS232/422/485 interface drivers, as well as power over pin 9. Selection of these options is made through both the web interface and hardware jumpers. Figure 7 shows the interface selection jumpers for the different interface types.

Figure 7- Interface Selection Jumpers

| | | |
|------------------------------------|---|--|
| RS-232 Cable Sense | 1 | |
| RS-232 Power Pin 9, Cable Sense | 1 | |
| RS-422 w/ Termination | 1 | |
| RS-485 w/ Termination | 1 | |

The jumper selections must be made while the device is unpowered and before being used in the final application.



The interface type selected by the interface jumpers in Figure 7 must match the selected configuration for the **Configuration | Serial Port Settings | Serial Interface Type** setting in the web interface.

6.6 Indicator LED's

The devices provide indicator LED's to provide feedback on the state of the device. These are a useful tool during installation and troubleshooting.

Table 6 - Enterprise LED Indicators

| LED | Color | Airborne Device State |
|-------|-------|---|
| POWER | | Adapter is not powered. |
| | | Adapter failed Power On Self Test (POST) and is not configured for wireless communication. |
| | | Adapter passed POST but is not configured for wireless network communication. |
| | | Adapter passed post and is configured for wireless communication. |
| LINK | | Adapter is not powered. |
| | | (Periodic Blinking) Adapter is searching for a valid network (Access Point) that matches device's configuration. |
| | | Adapter has successfully associated with an Access Point. |
| COMM | | If Power LED is also Off then Adapter is not powered. If Power LED is On then either: <ul style="list-style-type: none"> A physical connection detected on Serial/Ethernet cable. No TCP session from wireless interface has been established. |
| | | No physical Serial/Ethernet connection has been detected. |
















| LED | Color | Airborne Device State |
|-----|---|--|
| |  | (Blinking – OFF/Red) A physical Serial/Ethernet connection has been detected and there is traffic across the interface. No TCP connection to the adapter has been established on the wireless interface. |
| |  | A TCP connection to the adapter from the wireless interface has been established but no physical connection on the Serial/Ethernet interface has been detected. |
| |  | (Blinking – Green/Orange) A physical Serial/Ethernet connection has been detected and there is Serial/Ethernet traffic across the interface. A TCP connection to the adapter has been established (On WLAN or Ethernet interface). |
| |  | A physical Serial/Ethernet connection has been detected. A TCP connection to the adapter has been established from the WLAN or Ethernet interface but no traffic has been detected. |

Table 7 - Industrial LED Indicators

| LED | Color | Airborne Device State |
|-------|---|--|
| POWER |  | Adapter is not powered. |
| |  | Adapter is powered. |
| POST |  | Adapter is not powered. |
| |  | Adapter failed Power On Self Test (POST) and is not configured for wireless communication. |
| |  | Adapter passed POST but is not configured for wireless network communication. |
| |  | Adapter passed post and is configured for wireless communication. |
| LINK |  | Adapter is not powered. |
| |  | (Periodic Blinking) Adapter is searching for a valid network (Access Point) that matches device's configuration. |
| |  | Adapter has successfully associated with an Access Point. |
| COMM |  | If Power LED is also Off then Adapter is not powered. If Power LED is On then: <ul style="list-style-type: none"> No TCP session from WLAN or Ethernet interface has been established. |
| |  | A TCP connection to the adapter has been established from the Wireless or Ethernet interfaces but no traffic has been detected. |

7.0 Electrical & RF Specification

Table 8- Absolute Maximum Values¹

| Parameter | Min | Max | Unit |
|---|-----|------|------|
| Maximum Supply Voltage - Enterprise | 4.5 | 5.5 | VDC |
| Maximum Supply Voltage - Industrial | 5.0 | 36 | VDC |
| PoE 802.3af Class1 – Industrial (IN5xx8 models) | 37 | 57 | VDC |
| Power Dissipation | | 3.00 | W |
| Operating Temperature Range | -40 | 85 | °C |
| Storage Temperature | -40 | 85 | °C |

Note: 1. Values are absolute ratings, exceeding these values may cause permanent damage to the device.

Table 9 - RF Characteristics – 802.11a/b/g/n

| Symbol | Parameter | Rate (Mb/s) | Min | Average dBm / mW | | Peak dBm / mW | | Units |
|----------------------|-------------------------------|------------------------------|----------------------|---------------------|------|----------------------|--|-------|
| P _{OUTB} | Transmit Power Output 802.11b | 11, 5.5, 2, 1 | | 15.0 | 31.6 | | | dBm |
| P _{OUTG} | Transmit Power Output 802.11g | 6, 9, 12, 18, 24, 36, 48, 54 | | 12.6 | 18.2 | | | dBm |
| P _{OUTA} | Transmit Power Output 802.11a | 6, 9, 12, 18, 24, 36, 48, 54 | | 17.0 | 50.1 | | | dBm |
| P _{RSENB} | Receive Sensitivity 802.11b | 11 | | -86 | | | | dBm |
| | | 1 | | -92 | | | | |
| P _{RSENG} | Receive Sensitivity 802.11g | 54 | | -72 | | | | dBm |
| | | 36 | | -78 | | | | |
| | | 18 | | -84 | | | | |
| | | 6 | | -89 | | | | |
| P _{RSENA} | Receive Sensitivity 802.11a | 54 | | -74 | | | | dBm |
| | | 36 | | -80 | | | | |
| | | 18 | | -86 | | | | |
| | | 6 | | -90 | | | | |
| F _{RANGEBG} | Frequency Range | | 2412 | | | 2484 | | MHz |
| F _{RANGEA} | Frequency Range 802.11a | | 4910 5150 5470 | | | 4990 5350 5825 | | MHz |



The transmit power is automatically controlled by the device for minimum power consumption.

The transmit power at the antenna connector is listed in Table 9 above (±2dBm)..

Table 10 - Supported Data Rates by Band

| Band | Supported Data Rates (Mb/s) |
|-----------|-------------------------------------|
| 802.11b | 11, 5.5, 2, 1 |
| 802.11a/g | 54, 48, 36, 24, 18, 12, 9, 6 |
| 802.11n | 65, 58.5, 42, 39, 26, 19.5, 13, 6.5 |

Table 11 - Operating Channels

| Band | Region | Freq Range (GHz) | No. of Channels | Channels |
|------------------------|-----------|--|-----------------|---|
| 802.11b ^{1,2} | US/Canada | 2.401 - 2.473 | 11 | 1 – 11 |
| | Europe | 2.401 - 2.483 | 13 | 1 – 13 |
| | Japan | 2.401 - 2.495 | 14 | 1 – 14 |
| 802.11g ^{1,2} | US/Canada | 2.401 - 2.473 | 11 | 1 – 11 |
| | Europe | 2.401 - 2.483 | 13 | 1 – 13 |
| | Japan | 2.401 - 2.483 | 13 | 1 – 13 |
| 802.11a ³ | US/Canada | 5.15 - 5.35, 5.725 - 5.825 | 13 | 36,40,44,48,52,56,60,64,149,153,157, 161,165 |
| | Europe | 5.15 - 5.35, 5.47 - 5.725 | 19 | 36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140 |
| | Japan | 4.91 – 4.99, 5.15 - 5.35, 5.47 - 5.725 | 23 | 36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140,184, 188,192,196 |
| | China | 5.725 - 5.825 | 5 | 149,153,157,161,165 |



1. Only channels 1, 6 and 11 are non-overlapping.
2. Channel 14 is non-overlapping (Japan only).
3. Channel count denotes number of non-overlapping channels. Channels shown represent non-overlapping channel numbers.

7.1 AC Electrical Characteristics – Transmitter

Transmit power is automatically managed by the device for minimum power consumption. The transmit power at the RF connector is listed in Table 9 for 802.11a/b/g Modes (all rates).

7.2 Performance/Range

The following table illustrates the typical data rates, performance and range the device is capable of providing using an omni-directional antenna.

Table 12 - Radio Typical Performance Range

| Data Rate | Typical Outdoor Distance | |
|----------------|--------------------------|--|
| | (Unity gain antenna) | (2dBi antenna gain on each end for B/G mode) |
| 1.0 Mb/s | 240m | 380m |
| 11.0 Mb/s | 135m | 215m |
| 6Mb/s 802.11g | 135m | 215m |
| 6Mb/s 802.11a | 49m | 155m |
| 54Mb/s 802.11g | 12m | 19m |
| 54Mb/s 802.11a | 4.5m | 14m |

Ranges are affected by receiver sensitivity; transmit power, free-space path loss, antenna gain, and link margin. Actual range will vary from those stated. Non-line-of-site applications will result in typical values less than shown above.

The Data Rate is the supported connection rate for the wireless link, the actual data throughput for the link will be less than the stated data rates.

8.0 Antenna

The unit supports antenna connection through a single Hirose U.FL connector, located on the top surface of the radio next to the RF shielding.

Any antenna used with the system must be designed for operation within the 2.4GHz ISM band and specifically must support the 2.412GHz to 2.482GHz for 802.11b/g, the 5GHz ISM band and must specifically support 5.1GHz to 5.9GHz for 802.11a operation. They are required to have a VSWR of 2:1 maximum referenced to a 50 Ω system impedance.

8.1 Antenna Selection

The Airborne radio supports a number of antenna options, all of which require connection to the U.FL connectors on the radio. Ultimately the antenna option selected will be determined by a number of factors, including consideration of the application, mechanical construction and desired performance. Since the number of possible combinations is endless we will review some of the more common solutions in this section. If your application is not covered during this discussion please contact Technical Support for more specific answers.

The available antenna connections include:

- Host board mounted antenna
- Host Chassis mounted antenna
- Embedded antenna

In addition to the above options, location and performance need to be considered. The following sections discuss these items.

8.2 Host Board Mounted Antenna

Host board mounted requires that an antenna connection is physically mounted to the host system board. It also requires that the host board include a U.FL connector to allow a U.FL to U.FL coaxial lead to connect from the radio to the host board. It will then require 50 Ω matched PCB traces to be routed from the U.FL connector to the antenna mount.

There are several sources for the U.FL to U.FL coaxial cable these include Hirose, Sunridge and IPEX. Please contact B&B Electronics for further part numbers and supply assistance.

This approach can simplify assembly but does require that the host system configuration can accommodate an antenna location that is determined by the host PCB. There are also limitations on the ability to seal the enclosure when using this approach.

This approach also restricts the selection of available antenna. When using this approach, antennas that screw or press fit to the PCB mount connector must be used. There are many options for the antenna connector type, however if you

wish to utilize the FCC/IC modular approval the connector choice must comply with FCC regulations. These state that a non-standard connector, e.g. RP-TNC/RP-SMA, is required. TNC/SMA connectors are not allowed.

8.3 Host Chassis Mounted Antenna

Host Chassis mounted antennas require no work on the host PCB. They utilize an antenna type called 'flying lead'. There are two types of flying leads; one which provides a bulkhead mounted antenna connector and one which provides a bulk head mounted antenna. The type you choose will be determined by the application.

A flying lead system connects a U.FL coaxial lead to the radio's U.FL connector. The other end of the coax is attached to either a bulkhead mounted antenna connector or directly to an antenna that has an integrated bulkhead mount.

In either of the two cases, the use of this approach significantly reduces the antenna system development effort and provides for greater flexibility in the available antenna types and placement in the host system chassis.

When using the flying lead antenna (integrated bulk head mounting), there are no connector choice restrictions for use with the FCC/IC modular certification. However if the flying lead connector is used, the same restrictions as identified for the Host Mounted Antenna apply.

There are many suppliers of flying lead antenna and connectors. B&B Electronics' Airborne Antenna product line offers a range of antenna solutions.

8.4 Embedded Antenna

Use of Embedded antenna can be the most interesting approach for M2M, industrial and medical applications. Their small form factor and absence of any external mounting provides a very compelling argument for their use. There is a downside to this antenna type and it comes with performance. Antenna performance for all of the embedded options will, in most cases, be less than that achievable with external antenna. This does not make them unusable; it will impact choice of antenna type and requires more focus on placement.

The three main embedded antenna types are PCB embedded, chip (PCB mounted) and flying lead; each has its advantages and disadvantages (See Table 13).

Table 13 - Embedded Antenna Options

| Antenna Type | Features | | | |
|--------------|----------|---------|--------------|-------------|
| | Cost | Size | Availability | Performance |
| PCB Embedded | Lowest | Largest | Custom | Poor |
| Chip | Low | Small | Standard | Poor |
| Flying Lead | Low | Small | Standard | Fair |

PCB Embedded – This approach embeds an antenna design into the host PCB. This approach is very common with add-in WiFi cards (CF, PCMCIA, SDIO, etc.) as it requires no external connections and is the cheapest production approach. The lower production cost requires significant development cost and lack of performance and flexibility.

Chip – The integration of a chip antenna is simple and requires a relatively small footprint on the host system, however, it does suffer from the same limitations of flexibility and performance seen with the PCB embedded approach. There are relatively large numbers of suppliers of this type of antenna; there is also a range of configuration and performance options.

Flying Lead – This approach is similar to the flying lead solution for external antennas. The difference is that the form factors are smaller and provide a range of chassis and board mounting options, all for internal use. This approach suffers less from the performance and flexibility limitations of the other approaches, since the location of the antenna is not determined by the host PCB design. The assembly of a system using this approach maybe slightly more complex since the antenna is not necessarily mounted on the host PCBA.

8.5 Antenna Location

The importance of this design choice cannot be over stressed. It can in fact be the determining factor between success and failure of the WiFi implementation.

There are several factors that need to be considered when determining location:

- Distance of Antenna from radio
- Location of host system
 - Proximity to RF blocking or absorbing materials
 - Proximity to potential noise or interference
 - Position relative to infrastructure (Access Points or Laptops)
- Orientation of host system relative to infrastructure
 - Is it known
 - Is it static

To minimize the impact of the factors above the following things need to be considered during the development process:

- Minimize the distance between the radio and the location of the antenna. The coaxial cable between the two impacts the Transmit Power and Receive Sensitivity negatively. B&B Electronics recommends using 1.32-1.37mm outer diameter U.FL coaxial cables.
- Minimize the locations where metal surfaces come into contact or are close to the location of the antenna.
- Avoid locations where RF noise, close to or over lapping the ISM bands, may occur. This would include microwave ovens and wireless telephone systems in the 2.4GHz and 5.0GHz frequency range.
- Mount the antenna as high on the equipment as possible.

- Locate the antenna where there is a minimum of obstruction between the antenna and the location of the Access Points. Typically Access Points are located in the ceiling or high on walls.
- Keep the main antenna's polarization vertical, or in-line with the antenna of the Access Points. 802.11 systems utilize vertical polarization and aligning both transmit and receive antenna maximizes the link quality.

Even addressing all of the above factors does not guarantee a perfect connection, however with experimentation an understanding of the best combination will allow a preferred combination to be identified.

8.6 Performance

Performance is difficult to define as the appropriate metric changes with each application or may indeed be a combination of parameters and application requirements. The underlying characteristic that, in most cases, needs to be observed is the link quality. This can be defined as the bandwidth available over which communication between the two devices can be performed. The lower the link quality the less likely the devices can communicate.

Measurement of link quality can be made in several ways: Bit Error Rate (BER), Signal to Noise (SNR) ratio, Signal Strength, and may also include the addition of distortion. The link quality is used by the radio to determine the link rate. Generally as the link quality for a given link rate drops below a predefined limit, the radio will drop to the next lowest link rate and try to communicate using it.

The reciprocal is also true. If the radio observes good link quality at one rate it will try to move up to the next rate to see if communication can be sustained using it. It is important to note that for a given position the link quality improves as the link rate is reduced. This is because as the link rate drops the radios Transmit power and Receive sensitivity improve.

From this it can be seen that looking at the link rate is an indirect way of assessing the quality of the link between the device and an Access Point. You should strive to make the communication quality as good as possible in order to support the best link rate. However be careful not to *over specify* the link rate. Consider your application's bandwidth requirements and tailor your link rate to optimize the link quality. For example, the link quality for a location at 6Mb/s is better than it would be for 54Mb/s. If the application only needs 2Mb/s of data throughput, the 6Mb/s rate would provide a better link quality.

Aside from the radio performance, there are a number of other things that contribute to the link quality. These include the items discussed earlier and choices made when looking at the overall antenna gain. The antenna gain contributes to the Equivalent Isotropically Radiated Power (EIRP) of the system. This is part of an overall measurement of the link quality called link margin.

Link Margin provides a measure of all the parts of the RF path that impact the ability of two systems to communicate. The basic equation looks like this:

$$\text{EIRP (dB)} = \text{TxP} + \text{TxA} - \text{TxC}$$

$$\text{Link Margin (dB)} = \text{EIRP} - \text{FPL} + (\text{RxS} + \text{RxA} - \text{RxC})$$

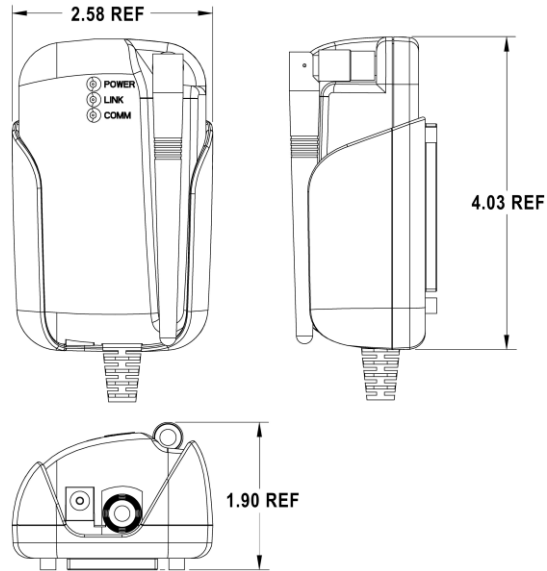
Where:

- TxP = Transmitter output power (dBm)
- TxA = Transmitter antenna gain (dBi)
- TxC = Transmitter to Antenna coax cable loss (dB)
- FPL = Free Path Loss (dB)
- RxS = Receiver receive sensitivity (dBm)
- RxA = Receiver antenna gain (dBi)
- RxC = Receiver to Antenna coax cable loss (dB)

This is a complex subject and requires more information than is presented here, B&B Electronics recommends at reviewing the subject and evaluating any system at a basic level.

It is then possible, with a combination of the above items and an understanding of the application demands, to achieve a link quality optimized for the application and host design. It is important to note that this is established with a combination of hardware selection, design choices and configuration of the radio.

9.0 Mechanical Outline – Enterprise Class



Antenna Connector: **RP-SMA (Reverse Polarity – SMA)**

Requires 2.4GHz/5GHz ISM band antenna, 50 input impedance, RP-SMA connector

Serial Connector: **DB-9M (Male)**

Requires DB-9 (Female)

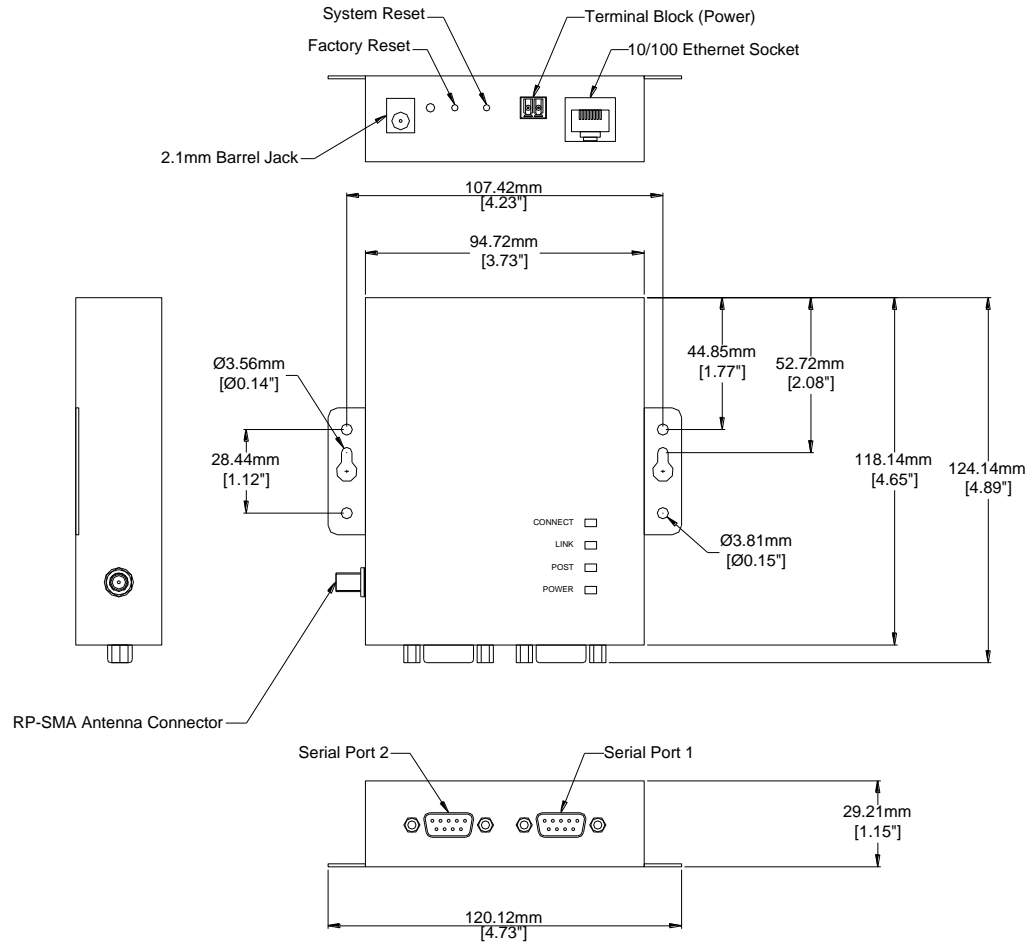
Ethernet Connector: **RJ-45 Plug**

Requires RJ-45 socket, 10/100 Ethernet interface

Power Connector: **2.1mm Barrel Jack**

Requires 2.1mm ID, 5.5mm OD, +5VDC center pin.

10.0 Mechanical Outline – Industrial Class



- Antenna Connector: **RP-SMA (Reverse Polarity – SMA)**
Requires 2.4GHz/5GHz ISM band antenna, 50 input impedance, RP-SMA connector
- Serial Connector: **DB-9M (Male)**
Requires DB-9F (Female)
- Ethernet Connector: **RJ-45 Socket**
Requires RJ-45 plug, 10/100 Ethernet interface
- Power Connector: **2.1mm Barrel Jack**
Requires 2.1mm ID, 5.5mm OD, +5VDC center pin.
- Power Connector: **Terminal Block (2 connector)**
Requires 16-30 AWG gauge wire.

11.0 Getting Started

11.1 Unpack the AirborneDirect™ Device

Unpack the AirborneDirect™ Device and compare the package contents with the items listed on the front of the included Quick Start Guide. If any item is missing or damaged, contact B&B Electronics immediately.

Contact details can be found at www.B&B Electronics.com/support.

11.2 Connect AirborneDirect™ to host

Connect the Airborne Direct unit to a system capable of configuring it. The preferred initial connection depends upon the class and type of product:

Serial – Enterprise: Connect to a serial port on the host or through a serial to USB adapter.

Serial – Industrial: Connect the RJ-45 socket to a RJ-45 socket using a CAT 5 Ethernet cable.

Ethernet – Enterprise: Connect to an RJ-45 socket on the host.

Ethernet – Industrial: Connect the RJ-45 socket to a RJ-45 socket using a CAT 5 Ethernet cable.

11.3 Attach Antenna and Power-up the AirborneDirect™

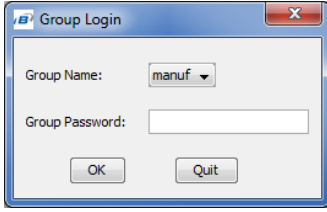
Attach the supplied antenna to the RP-SMA connector on the AirborneDirect™ unit. Connect the supplied AC adapter to the power connector. If using your own power supply make sure the correct power connector type and polarity are being used, verify the appropriate voltage to be applied by checking Table 8 for the correct product class. Confirm that the device is receiving power by verifying that the POST LED is lit when the supply is applied.

12.0 Configuring Device – Industrial Serial (ABDx-SE-IN5xxx)

The following describes initial connection to an AirborneDirect™ Serial Device Server (ABDx-SE-IN5xxx). If you have an Ethernet device (ABDx-ER-DP5xx/IN5xxx), please go to section 14.0. If you have purchased a SE-DP5xx device please go to section 13.0 for the set-up instructions.

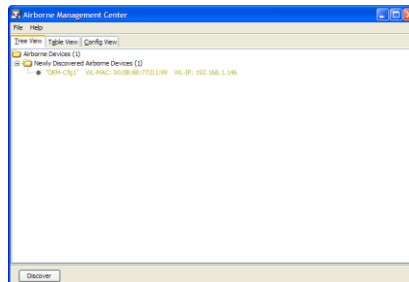
The instructions in Table 14 provide step-by-step instructions for configuration of the ABDx-SE-IN5xxx product family.

Table 14 - SE-IN5xxx Accessing the Web Interface

| | |
|----------|--|
| 1 | Open the AirborneDirect™ packaging and locate the Install CD. |
| 2 | Place the CD in the CD/DVD drive of the laptop or desktop you will be using to configure the AirborneDirect™ device. Follow the on screen directions for installation of the appropriate device software and documentation. |
| 3 | Connect the Ethernet cable on ABDx to an Ethernet port on the laptop or desktop system. |
| 4 | Apply power to the ABDx-SE-IN5xxx. |
| 5 | <p>The unit will boot and display one of the following LED patterns:</p> <p>ABDx-SE-IN5xxx</p> <p>COMM: ● Off</p> <p>LINK : ● Red</p> <p>POST: ● Orange</p> <p>POWER: ● Blue</p> |
| 6 | <p>Run the Airborne Management System application. This was installed during the CD installation and a menu item will be found in the Airborne folder located in the programs directory of your system.</p> <p>When the application opens the following dialog will be displayed:</p>  <p>Select Group Name: manuf and enter Group Password: dpac</p> |

7

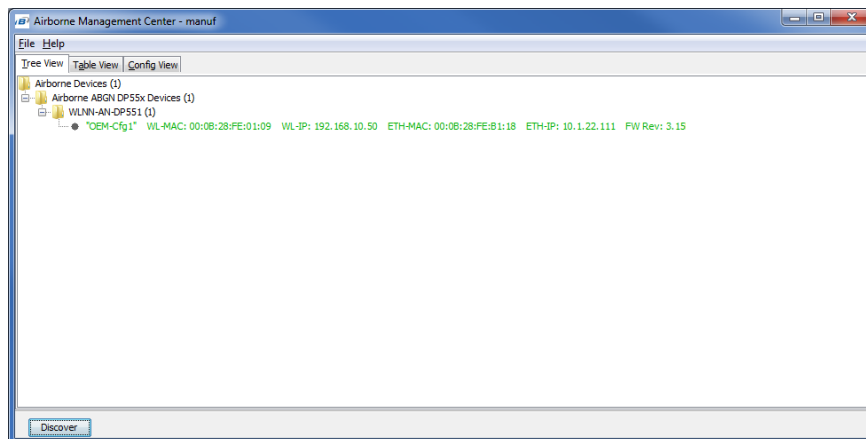
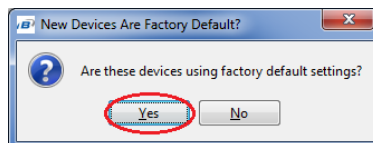
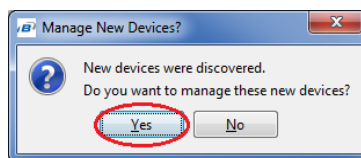
The AMC will load and discover the attached device.



If the unit is not detected please verify that your firewall is disabled. Run a "Discover", if the unit is still not being detected, close down AMC and restart it by doing a Right Click on the AMC icon and select "Run as administrator".

8

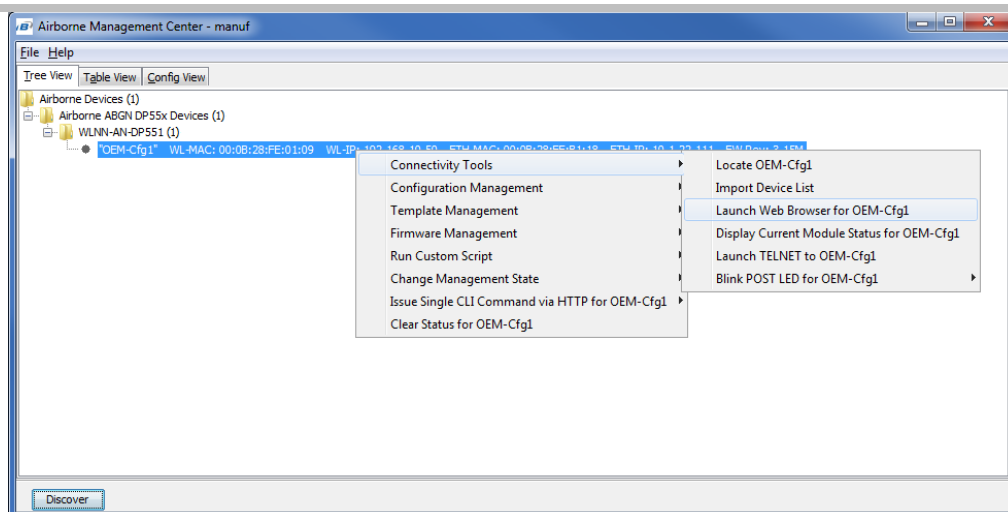
Manage Your Device



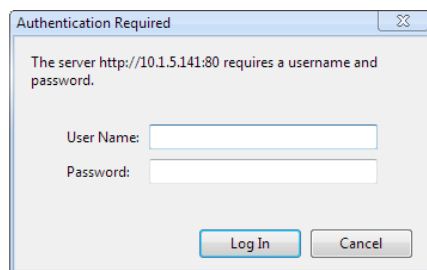
9

The devices status will move to managed and the device will be displayed under the device type/group it belongs too. Right click the device and then:

1. Select **Connectivity Tools**
2. Select **Launch Web Browser for OEM-Cfg1**



Username= "dpac"
Password = "dpac"



Opening web page shows adapter status.

10

Links to the available configuration options are identified in the left hand menu. The top menu bar provides access to different operations that can be performed by the AirborneDirect™ device. See section 15.0 for a full description of how to use the web interface.

Using Express Setup:

11

If this is the first time you have configured the device the Express Setup page will be displayed, please refer to section 16.0 to continue set-up of the device.

If this is not the first time please move to section to update the configuration

12

When the **Reboot** button is pressed the unit will restart and install new settings. This may take 15-20 seconds. Please refresh the web interface after the boot cycle has completed.

13

When configured correctly the LED pattern should match the following:

| ABDx-SE-IN5xxx | No TCP Connection | TCP Connection |
|----------------|-------------------|----------------|
| COMM: | ● Off | ● Green |
| LINK : | ● Green | ● Green |
| POST: | ● Green | ● Green |
| POWER: | ● Blue | ● Blue |

14

To use the adapter on the wireless network, address all traffic to the IP address of the wireless interface of the ABDx-SE- IN5xxx. This address is listed in the home page of the web interface.

13.0 Configuring Device – Enterprise Serial (ABDx-SE-DP5xx)

The ABDx-SE-DP5xx family does not have an Ethernet port for initial configuration so initial configuration can be performed through the serial port. To do this it is necessary to connect using the serial connector.

13.1 Connect a Host Computer

Connect the serial pigtail connector to the serial port on a host computer.



It may be necessary to use a gender changed that includes a Null Modem adapter.

13.2 Interacting with the AirborneDirect™ device

On the Host computer, use a terminal emulation program to interact with the device issuing B&B Electronics Command Line Interface (CLI) commands. CLI commands let you request status or change parameter settings. Press the Enter key (<CR>) after each command line you type. After the module starts, type the following CLI command to log in (you must log in before CLI commands can be recognized):

Table 15 - UART Authentication

| CLI Command | Description |
|--|---|
| <code>Send Break Sequence</code> | <p>The serial port starts up in a listen mode waiting for a request for a data tunnel. To access the CLI mode in which set-up can take place the break sequence must be sent.</p> <p>The default break sequence for the device is <code>~ABD</code></p> <p>The sequence must be sent with no trailing characters.</p> <p>If received correctly the device will respond <code>OK</code>.</p> |
| <code>auth dpac dpac <CR></code> | <p>The module responds with <code>OK</code>, indicating that it executed the command successfully. (If you did not receive <code>OK</code>, check the settings in your terminal emulation program).</p> |



You will have to break into CLI mode and log into the module after any reset or restart.

13.3 Determine and Store the Access Point SSID

On the Host computer, use the terminal emulation program to type the following CLI commands in the order shown:

Table 16 - UART SSID & Authentication

| CLI Command | Description |
|---------------------------------------|--|
| <code>wl-scan<CR></code> | The module scans for APs and returns information on each one it discovers. Note the SSID value that is returned, as you will need to enter it when configuring the device in the next steps. |
| <code>wl-ssid [SSID]<CR></code> | Associates the module with the network name [SSID] you specify. [SSID] is the value returned by the wl-scan command. |
| <code>commit<CR></code> | Stores the information to flash memory. |
| <code>restart</code> | Restarts the device and installs the new settings. |

If your access point has security enabled, you will also need to use the CLI to enter those parameters (See the Enterprise CLI Reference Guide for details). That setup is outside the scope of this user guide, which assumes that the AP being tested with has no security.

After issuing the commands, the unit will restart and apply the network settings. Once restarted the LINK LED will stop blinking and go solid. If DHCP is enabled on the network the POWER and LINK LED's will turn solid green.

13.4 Determine the Device's IP address

On the Host computer, use the terminal emulation program to type the following CLI commands:

Table 17 - UART Determine Module's IP Address

| CLI Command | Description |
|--|---|
| Send Break Sequence | The serial port starts up in a listen mode waiting for a request for a data tunnel. To access the CLI mode in which set-up can take place the break sequence must be sent. The default break sequence for the device is <code>~ABD</code> The sequence must be sent with no trailing characters. If received correctly the device will respond OK. |
| <code>auth dpac dpac <CR></code> | Authenticate with the device server. |
| <code>wl-ip<CR></code> | The module returns the IP address assigned to it by the DHCP server. |

13.5 Accessing the Device Using the Web Interface

See section 15.0.

13.6 Accessing the Device Using Telnet

On the Remote computer, use a terminal emulation program to start a Telnet session. To connect to the device using TCP/IP, use the IP address obtained in section 13.4 to connect on port 23.

The terminal emulator will attempt to connect to the IP address; if successful you will now be able to use the WLAN interface for configuration of the device through either CLI or web.

For more information on the full CLI command set please refer to the Airborne Enterprise Command Line Reference Manual.

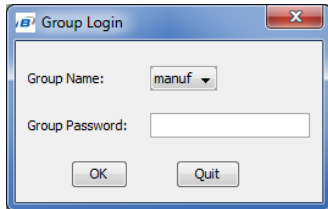


The above process can be achieved by any of the available Terminal Emulation programs. Please follow the specific applications requirements to make the TCP/IP connection and authenticate with the module.

14.0 Configuring Device – Enterprise/Industrial Ethernet (ABDx-ER-DP5xx/IN5xxx)

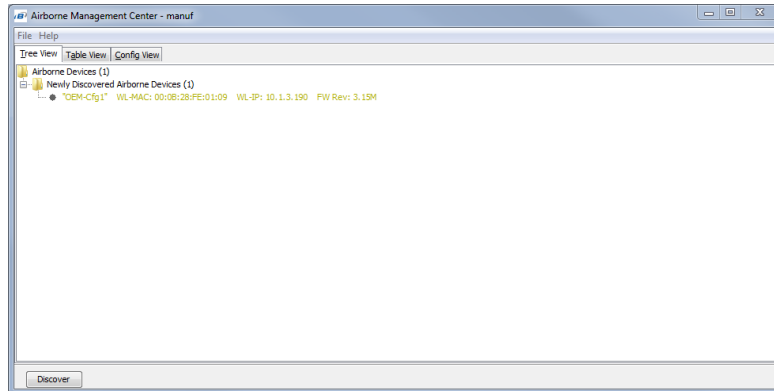
The following instructions describe how access the AirborneDirect™ Ethernet device and web interface for initial configuration of the unit.

Table 18 – ER-DP5xx/IN5xxx Accessing the Web Interface

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------------|---|---------------------------|----------------------------------|-----------------------|--------|---------|---------|--------|---------|---------------------------|-------|-------|-------|-----------------------|--|--|-------|-------|--|--------|-------|--|-------|----------|--|--------|--------|--|
| 1 | Open the AirborneDirect™ packaging and locate the Install CD. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Place the CD in the CD/DVD drive of the laptop or desktop you will be using to configure the AirborneDirect™ device. Follow the on screen directions for installation of the appropriate device software and documentation. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Connect the Ethernet cable on ABDx to an Ethernet port on the laptop or desktop system. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Apply power to the ABDx-ER-DP5xx/IN5xxx. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | <p>The unit will boot and display one of the following LED patterns:</p> <table><tr><td>ABDx-ER-DP5xx</td><td><i>Associated (Open Network)</i></td><td><i>Not Associated</i></td></tr><tr><td>POWER:</td><td>● Green</td><td>● Green</td></tr><tr><td>LINK :</td><td>● Green</td><td>● Red (Periodic Blinking)</td></tr><tr><td>COMM:</td><td>● Red</td><td>● Red</td></tr><tr><td>ABDx-ER-IN5xxx</td><td></td><td></td></tr><tr><td>COMM:</td><td>● Off</td><td></td></tr><tr><td>LINK :</td><td>● Off</td><td></td></tr><tr><td>POST:</td><td>● Orange</td><td></td></tr><tr><td>POWER:</td><td>● Blue</td><td></td></tr></table> | ABDx-ER-DP5xx | <i>Associated (Open Network)</i> | <i>Not Associated</i> | POWER: | ● Green | ● Green | LINK : | ● Green | ● Red (Periodic Blinking) | COMM: | ● Red | ● Red | ABDx-ER-IN5xxx | | | COMM: | ● Off | | LINK : | ● Off | | POST: | ● Orange | | POWER: | ● Blue | |
| ABDx-ER-DP5xx | <i>Associated (Open Network)</i> | <i>Not Associated</i> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| POWER: | ● Green | ● Green | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LINK : | ● Green | ● Red (Periodic Blinking) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| COMM: | ● Red | ● Red | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ABDx-ER-IN5xxx | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| COMM: | ● Off | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LINK : | ● Off | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| POST: | ● Orange | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| POWER: | ● Blue | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | <p>Run the Airborne Management System application. This was installed during the CD installation and a menu item will be found in the Airborne folder located in the programs directory of your system.</p> <p>When the application opens the following dialog will be displayed:</p>  <p>Select Group Name: manuf and enter Group Password: dpac</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | |

7

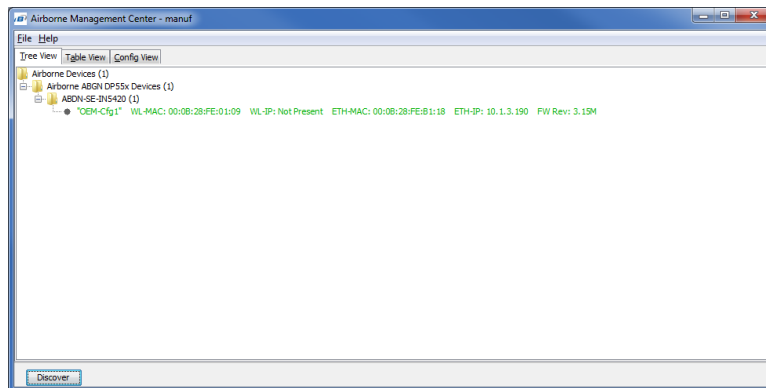
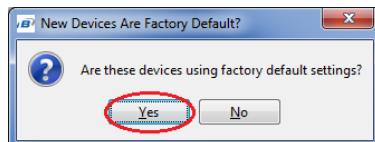
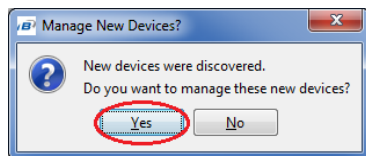
The AMC will load and discover the attached device.



If the unit is not detected please verify that your firewall is disabled. Run a "Discover", if the unit is still not being detected, close down AMC and restart it by doing a Right Click on the AMC icon and select "Run as administrator".

8

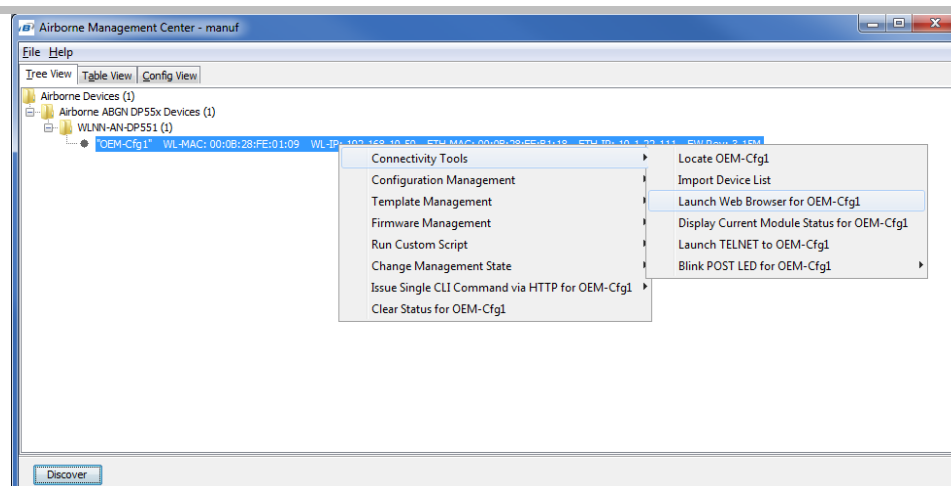
Manage Your Device



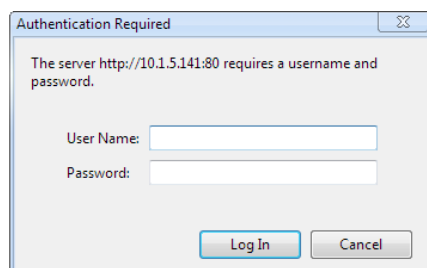
9

The devices status will move to managed and the device will be displayed under the device type/group it belongs too. Right click the device and then:

3. Select **Connectivity Tools**
4. Select **Launch Web Browser for OEM-Cfg1**



Username= "dpac"
Password = "dpac"



Opening web page shows adapter status.

10

Links to the available configuration options are identified in the left hand menu. The top menu bar provides access to different operations that can be performed by the AirborneDirect™ device. See section 15.0 for a full description of how to use the web interface.

Using Express Setup:

11

If this is the first time you have configured the device the Express Setup page will be displayed, please refer to section 16.0 to continue set-up of the device.

If this is not the first time please move to section to update the configuration

12

When the **Reboot** button is pressed the unit will restart and install new settings. This may take 15-20 seconds. Please refresh the web interface after the boot cycle has completed.

13

When configured correctly the LED pattern should match the following:

ABDx-ER-DP5xx

POWER: ● Green
LINK : ● Green
COMM: ● Red

ABDx-ER-IN5xxx

COMM: ● Off
LINK : ● Green
POST: ● Green
POWER: ● Blue

No TCP Connection

TCP Connection

● Green
● Green
● Green
● Blue

14

To use the adapter on the wireless network, address all traffic to the IP address of the wireless interface of the ABDx-ER-DP5xx/IN5xxx. This address is listed in the home page of the web interface.

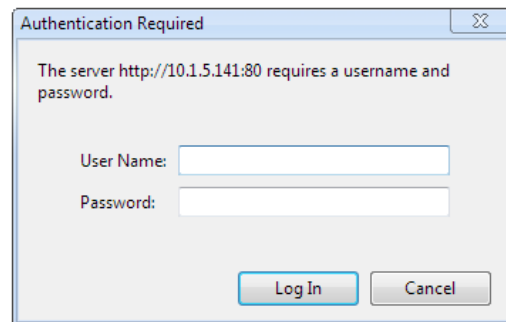
15.0 Using the Web Interface

The AirborneDirect™ Device Servers and Wireless Adapters include a web interface that provides access to module status, parameter modification and certificate and configuration file management. To use the web interface follow the steps outlined in section 14.0 to establish the IP address of the module. Once the IP address is known open a web browser and enter the IP address of the module in the URL window.

The web interface currently supports Internet Explorer v6.0 thru 9.0, Firefox v3.x+, Opera v9.6+, Chrome v4.0+ and Safari v5.0.5+.

When the authentication request is returned enter:

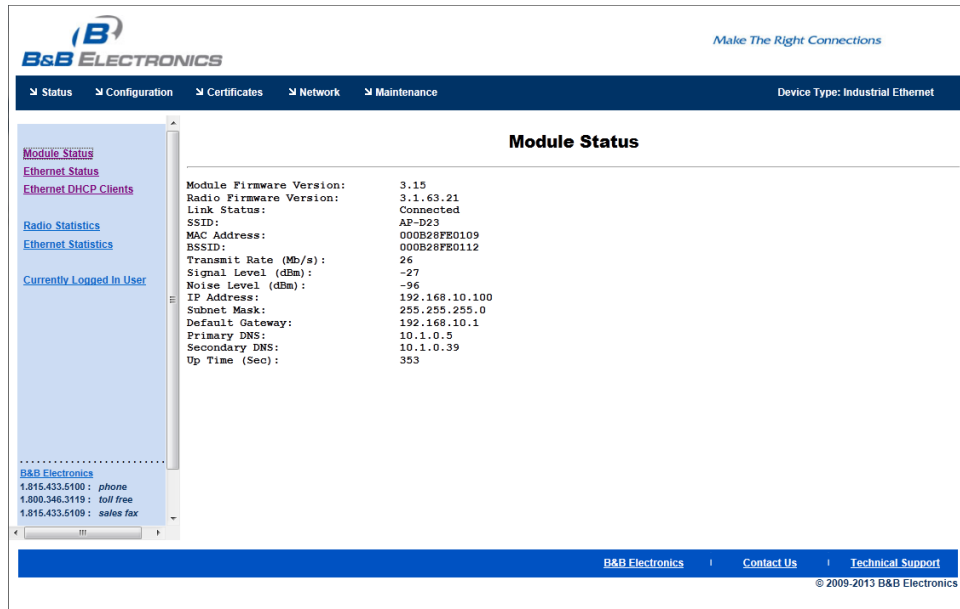
Figure 8 - Website Login



Username: dpac
Password: dpac

After successfully authenticating with the module, you will be logged into the web server. If this is the first time you have accessed the device the Express Setup page will be displayed see section 16.0 for configuration of the device using this page. If you have previously configured the device the default home page will be displayed (See Figure 9), from here you can update device settings if required. A quick overview of the web interface follows.

Figure 9 - Default Home Page



15.1 Navigation Bar

Figure 10 - Website Navigation Bar



Table 19 - Navigation Bar Items

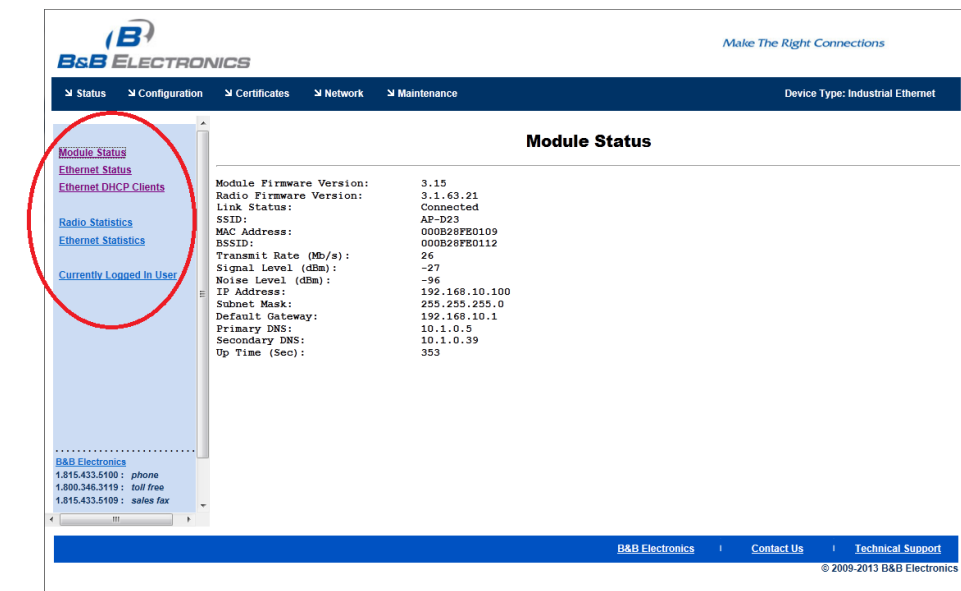
| Title | Description |
|---------------|---|
| Status | Provides status and performance characteristics for the network interfaces available. Includes connection status, radio and Ethernet statistics. |
| Configuration | Allows viewing and configuration of all the interface settings including wireless LAN, network connectivity, security, FTP client, serial port and web server. Includes the interface for delivery of OEM and user configuration files, as well as management and viewing of current configurations. |
| Certificates | This menu item provides the interface for certificate delivery and management. Included in this section are the abilities to view resident certificates, upload and delete certificates. |

| Title | Description |
|-------------|--|
| Network | <p>With this section it is possible to locate other Airborne Device Server modules on the current network.</p> <p>It is also possible to scan for available Access Points.</p> |
| Maintenance | <p>This section allows the updating of the modules firmware. You can also revert the device settings to OEM defaults and restart the module remotely.</p> <p>The module locate function is also enabled in this section.</p> |

15.2 Feature Links

Each Navigation Bar link has a set of Features/Fields it allows access to. These are different for each Navigation option and change for different device selections. The Feature Links are located in the left hand panel of the web page (See Figure 11).

Figure 11- Feature Links



15.3 Navigating the Website

A standard web page looks like Figure 12. The navigation bar runs along the top of the page, page specific feature links are list in the left hand pane of the page and the specific parameters are shown in the main display panel.

Figure 12 - Airborne Web Page

To select any of the items, move your cursor over the item and press the Left Hand mouse button. The items in the Navigation bar and the Feature Links are hyperlinks and will cause the mouse cursor to change from an arrow pointer to a finger pointer when placed over them.

To find out what a specific field does move the cursor over the field and hover for approximately a second. A help balloon will appear and will provide details on the function of the field and its valid range of values.

15.4 Updating a Field

To update a field, select the field by pressing the Left Hand mouse button. Then either type in the appropriate content or select from the pull down menu.

Once you have finished modifying parameters, scroll to the bottom of the page and press the **Commit** button. The page will then indicate the changes have been completed successfully, you can then return to the configuration page by pressing the **Reload** button or restart the module by pressing the **Reboot** button.




Note that the changes to the parameters will not be applied until a module restart (reboot) has been completed.

Before the **Commit** button has been pressed, all modified fields can be returned to their original state by pressing the **Cancel** button.

15.5 Uploading Certificates

Adding certificates to the Airborne Device Server module is very easy when using the web interface.

Figure 13 - Upload Certificate Web page

**B&B ELECTRONICS**

Make The Right Connections

▼ Status

▼ Configuration

▼ Certificates

▼ Network

▼ Maintenance

Device Type: Industrial Ethernet

[Upload Certificate](#)
[List Certificates](#)
[Delete Certificate](#)

1.815.433.5100 : phone
1.800.346.3119 : toll free
1.815.433.5109 : sales fax

Upload a Certificate to the Module

Select a Certificate File to upload and save on the module:

◀

111

▶

[B&B Electronics](#)

|

[Contact Us](#)

|

[Technical Support](#)

© 2009-2013 B&B Electronics

Table 20 - Uploading Certificates

| Step | Description |
|--|---|
| <i>Navigation Bar</i> Select Certificates | You will see a list of certificates currently resident on the module when you enter the Certificate File List window. |
| <i>Feature Link</i> Select Upload Certificates | You will see a window open with field to enter the location of the certificate you want to upload. |
| Press Browse... Button | <p>This will open a dialog box in which you can locate the certificate you wish to upload to the module. Select the Certificate file and press Open.</p> <p>This will return you to the Certificate Upload window and will have entered the location and file name of the certificate you wish to upload in the field next to the Browse... button.</p> |
| Press Upload Certificate | You will then see a notice that the certificate has been successfully uploaded to the module. |
| Press List certificates Files | This will show the current certificates resident on the module and will include the file just uploaded. |

15.6 Upload Configuration Files

The Airborne Device Server module supports User, Encrypted and OEM configuration files for provisioning the module. Delivery of these configuration files can be performed through the web interface. A full description of these files can be found in the Airborne CLI manual.

To upload configuration files follow the steps in Table 21.

Figure 14 - Upload Configuration Web Page

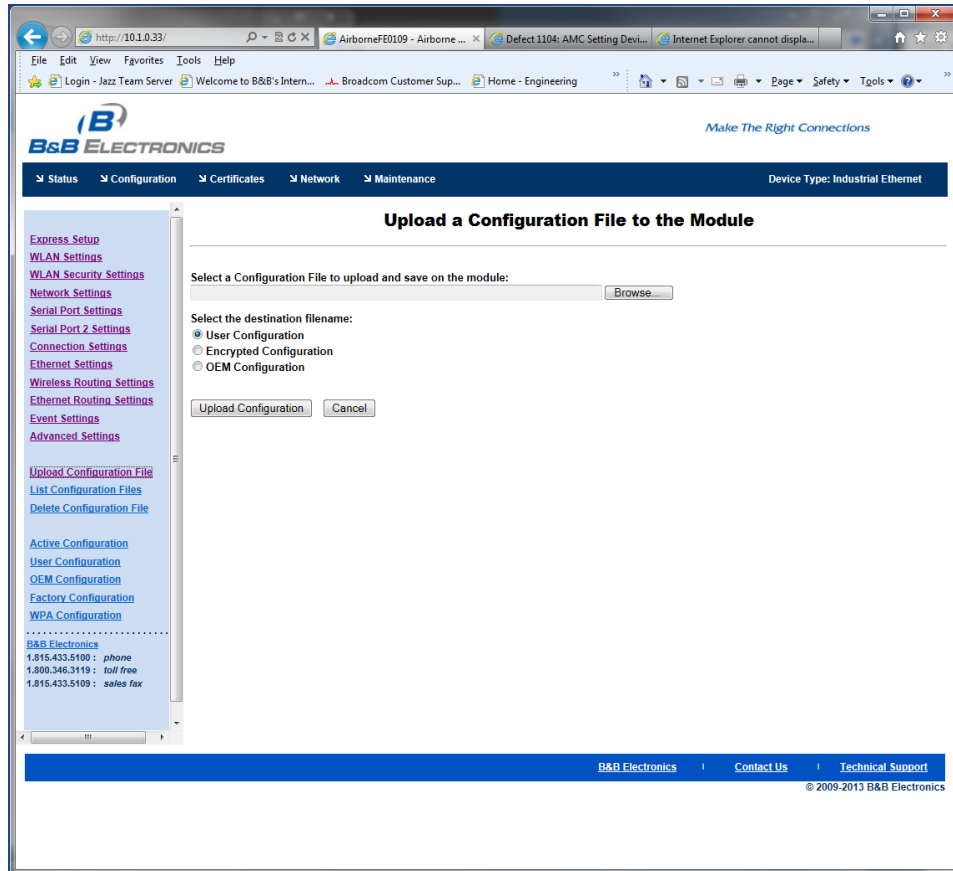



Table 21 - Uploading Configurations

| Step | Description |
|--|---|
| <i>Navigation Bar</i> Select Configuration | You will see major WLAN parameters displayed. |
| <i>Feature Link</i> Select Upload Configuration File | You will see a window open with field to enter the location of the configuration you want to upload, along with a choice of User, Encrypted or OEM Configuration. |

| Step | Description |
|---|--|
| Press Browse... Button | This will open a dialog box in which you can locate the file you wish to upload to the module. Select the configuration file and press Open . This will return you to the Configuration Upload window and will have entered the location and name of the file you wish to upload in the field next to the Browse... button. |
| Select User, Encrypted or OEM Configuration | This defines the configuration you are installing. Only the OEM Configurations will survive a factory reset. |
| Press Upload Configuration | You will then see a notice that the configuration has been successfully uploaded to the module. |
| Press List Configuration Files | This will show the current configuration files resident on the module and will include the file just uploaded. |



Uploading a configuration file will overwrite any configuration file already stored on the module. This will cause a change in configuration when a module restart is performed.

IMPORTANT: Confirm that the OEM or USER settings in the configuration files will allow the user to communicate with the module after the upload and a restart has been completed.

15.7 Updating Firmware

The module's firmware may be updated using the web interface. Please refer to Table 22 for the procedure to do this.

Updating the firmware will not alter any existing configuration files or certificates loaded on the module.

You will first need to obtain the version of firmware you wish to install from the B&B Electronics website or B&B Electronics technical support. The firmware will be a binary image file (.img) and indicate the version of the firmware in the file name.

Once you have obtained the firmware, save the firmware image to a location on the system you are browsing the module from, or a location accessible to the system you are browsing the module from.

Figure 15 - Firmware Update Page

B&B ELECTRONICS *Make The Right Connections*

▼ Status ▼ Configuration ▼ Certificates ▼ Network ▼ Maintenance Device Type: Industrial Ethernet

Upload Firmware to the Module

Current Firmware Version = 3.15

Select the firmware image file to load and then click "Load New Firmware"

[Update Module Firmware](#)
[Reset to Factory Defaults](#)
[Restart Module](#)

[Set System Time](#)

[Blink the POST LED](#)
[Stop Blinking the POST LED](#)

[Change Module Personality](#)

[Upload Script File](#)
[List Script Files](#)
[Display Script File](#)
[Delete Script File](#)
[Run Script File](#)

.....

B&B Electronics
1.815.433.5100 : phone
1.800.346.3119 : toll free
1.815.433.5109 : sales fax

.....

[B&B Electronics](#) | [Contact Us](#) | [Technical Support](#)
© 2009-2013 B&B Electronics

Figure 16 - Firmware Update in Progress

B&B ELECTRONICS *Make The Right Connections*

▼ Status ▼ Configuration ▼ Certificates ▼ Network ▼ Maintenance Device Type: Industrial Ethernet

Flashing Firmware in the Module

Transferring the firmware file
File retrieved successfully - Flashing the module

This should take approximately 90 seconds

Do not turn off the power!

[Update Module Firmware](#)
[Reset to Factory Defaults](#)
[Restart Module](#)

[Set System Time](#)

[Blink the POST LED](#)
[Stop Blinking the POST LED](#)

[Change Module Personality](#)

[Upload Script File](#)
[List Script Files](#)
[Display Script File](#)
[Delete Script File](#)
[Run Script File](#)

.....

B&B Electronics
1.815.433.5100 : phone
1.800.346.3119 : toll free
1.815.433.5109 : sales fax

.....

[B&B Electronics](#) | [Contact Us](#) | [Technical Support](#)
© 2009-2013 B&B Electronics

Figure 17 - Firmware Update Complete

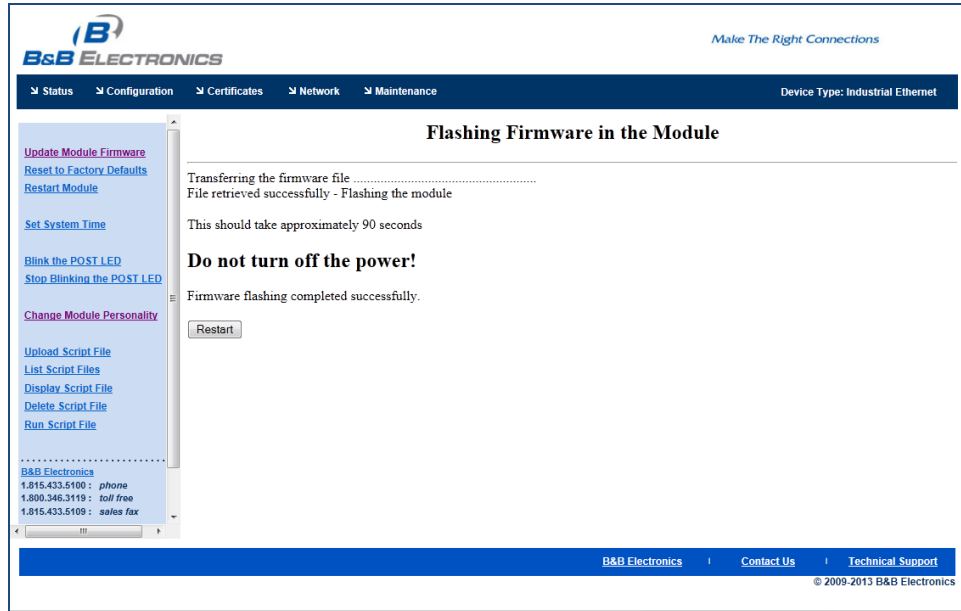


Table 22 - Updating Firmware

| Step | Description |
|--|---|
| Navigation Bar Select Maintenance | This will open a window showing the current module status. |
| Feature Link Select Update Module Firmware | You will see a window open with field to enter the location of the module firmware you want to upload. The current firmware version number is displayed at the top of the page. |
| Press Browse... Button | This will open a dialog box in which you can locate the firmware image you wish to upload to the module. Select the firmware image file and press Open . This will return you to the Upload Firmware window and will have entered the location and file name of the firmware image you wish to upload in the field next to the Browse... button. |
| Press Load New Firmware | You will then see a notice that the firmware upload has begun (Error! Reference source not found.). When the upload has been completed successfully and the firmware updated w window indicating this will be shown (Figure 17). |
| Press Reboot | This will restart the module and the new firmware will be loaded. |



DO NOT REMOVE POWER FROM THE MODULE DURING THE FIRMWARE UPDATE.

This may cause the device to become non-operational. If this happens please contact B&B Electronics Technical Support.

16.0 Express Setup Configuration Page

When the device's web interface is accessed for the first time an Express Setup page will be shown. This page is designed to allow a quick device set-up by presenting the most popular device configuration options in a single location. For more advanced configurations the full set of options are available in the feature links (left-hand column).

The Express Setup web page will display the necessary fields based upon the selections made during configuration. The Express Setup page looks like (Figure 18):

Figure 18 - Express Setup Page

To configure the device for operation each field must be configured correctly. The following steps should be taken to configure the device (Note: not all fields will be visible):

Table 23 - Express Page Setup

| Step | Description |
|---|--|
| Navigation Bar Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| Feature Link Select Express Setup | This step is optional. If this is the first time the device has been configured this page will automatically be displayed. |

| Step | Description |
|--|--|
| Select Discovery OEM Device Name | <p>This parameter allows you to name the device uniquely or group into a functional set. When device discovery is used this name identifies the found device.</p> <p>If you wanted to uniquely identify the device you could mark it with a label e.g. Dev1, and then enter Dev1 in this field. When the device is found it will identify itself as Dev1.</p> <p>Alternately you could indicate the type of equipment the device is attached to e.g. Haas TL-2 (CNC Turning Center), by giving the unit a name like Haas_TL_2. When discovered you can then identify the device you are accessing.</p> <p>Enter the text string is you wish to change the default value. This field is optional.</p> |
| Select Radio Startup Mode | Select On from the drop down menu for the radio to operate. |
| Select Wireless LAN Connection Type | <p>If you are using Access Points make sure this is set to Infrastructure from the drop down menu.</p> <p>If you want to use AdHoc set this accordingly. Additional settings may be required to fully configure for AdHoc mode, these are covered if section 17.2.</p> |
| Select SSID | Enter the name of the wireless network you wish to access. This field is case sensitive. |
| Select Wireless LAN Security Type | <p>Select the security type the wireless network you wish to access is using.</p> <p>Depending upon the option you choose you may have to enter additional information. Once you have selected the security type the required inputs will be displayed. All displayed fields must be completed.</p> <p>If the security type is not in the available selections more are available in the <i>WLAN Security Settings</i> page. If you choose to use this page make sure you commit the change before selecting the <i>WLAN Security Settings</i> page.</p> |
| Select WLAN DHCP | <p>If your WLAN network uses DHCP to assign IP addresses to the wireless clients, select Enabled from the drop down menu.</p> <p>If you are using static IP addresses select disabled from the drop down menu. WLAN Static IP and WLAN Subnet Mask will need to be entered.</p> |
| Select Ethernet DHCP | <p>If the Ethernet network connected to the Ethernet port uses DHCP to assign IP addresses to the wired clients, you should select Enabled from the drop down menu.</p> <p>If you are using static IP addresses you should select Disabled from the drop down menu. Ethernet Static IP and Ethernet Subnet Mask will need to be entered.</p> <p>Important: This field is only used if the Ethernet interface is set as a client (default for Serial devices). If set as a router the field is ignored. See section 21.0 for a full description of configuring the unit as an Ethernet router.</p> |
| Select WLAN Static IP | <p>This field defines the static IP address for the wireless interface.</p> <p>This address is only used if the WLAN DHCP is disabled or DHCP failed.</p> <p>Default: 192.168.10.1</p> |
| Select WLAN Subnet Mask | <p>This field defines the subnet mask used by the wireless interface.</p> <p>This mask is only used if the WLAN DHCP is disabled or DHCP failed.</p> <p>Default: 255.255.255.0</p> |

| Step | Description |
|--|--|
| Select Ethernet Static IP | This field defines the static IP address for the Ethernet interface. When configured as a serial device server (Ethernet interface is in client mode) this address is only used if the Ethernet DHCP is disabled or DHCP failed. Default: 192.168.2.100 |
| Select Ethernet Subnet Mask | This field defines the subnet mask used by the Ethernet interface. When configured as a serial device server (Ethernet interface is in client mode) this mask is only used if the Ethernet DHCP is disabled or DHCP failed. Default: 255.255.255.0 |
| Select Ethernet Gateway Address | This field defines the gateway IP address used by the Ethernet interface. When configured as a serial device server (Ethernet interface is in client mode) this mask is only used if the Ethernet DHCP is disabled or DHCP failed. Default: 192.168.2.1 |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Express Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. If the network is using DHCP then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses it will be necessary to configure the network interface, see the next step. |

The web interface supports advanced configuration of the device through the additional pages available. The following sections provide guidance on how to use these pages for specific configurations.

17.0 Configuring the Wireless Interface

The following section will outline how to configure the wireless interface for both infrastructure and AdHoc networks.

17.1 Configuring for Infrastructure Networks

Infrastructure networks use Access Point and/or Wireless Routers to provide wireless access to a network. Each wireless network is identified by a name referred to as the SSID (**S**ervice **S**et **I**Dentifier). To configure the device with the necessary parameters to operate with an Infrastructure network use the following steps.

Table 24 - Configuring Wireless Interface - Infrastructure

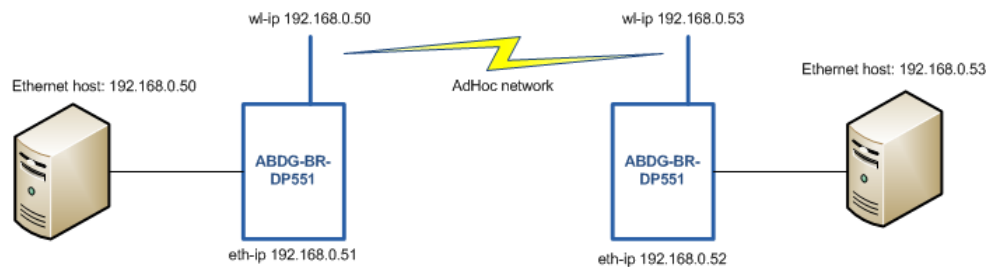
| Step | Description |
|---|--|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select WLAN Settings | This step is optional. The default home page for the Configuration link in the Navigation Bar is WLAN Settings . |
| Select Radio Startup Mode | Select On from the drop down list. |
| Select Wireless LAN Connection Type | Select the Infrastructure form the drop down list. |
| Select SSID | Enter the name of the wireless network you want the device to use. This cannot include spaces. |
| Select Wireless LAN Region | Select the most appropriate region for the deployment location of the device. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the WLAN Settings page. |
| <i>Feature Link</i> Select WLAN Security Settings | The wireless interface is now configured however most wireless networks use security to protect the network and users from unauthorized use. Selecting WLAN Security Settings will allow us to configure the devices security settings for the network. This is covered in section 18.0. |

17.2 Configuring for AdHoc Networks

AdHoc networks use peer-to-peer connection to create a local wireless network. These can be useful when no infrastructure (AP) is available. Each wireless network is identified by a name referred to as the ESSID (Extended Service Set Identifier). To configure the device with the necessary parameters to operate with an AdHoc use the following steps.

Table 25 - Configuring Wireless Interface - AdHoc

| Step | Description |
|---|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select WLAN Settings | This step is optional. The default home page for the Configuration link in the Navigation Bar is WLAN Settings . |
| Select Radio Startup Mode | Select On from the drop down list. |
| Select Wireless LAN Connection Type | Select the AdHoc form the drop down list. |
| Select Wireless LAN Channel | This determines the 802.11 channel that the device will use when it establishes a connection with another device in the AdHoc network. Select a channel that is clear, i.e. one which has no other 802.11 network using it. It is not necessary for all devices in a single AdHoc network to have the same channel number selected. |
| Select SSID | Enter the name of the wireless network you want the device to use. This cannot include spaces. |
| Select Wireless LAN Region | Select the most appropriate region for the deployment location of the device. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the WLAN Settings page. |
| <i>Feature Link</i> Select WLAN Security Settings | The wireless interface is now configured however most wireless networks use security to protect the network and users from unauthorized use. Selecting WLAN Security Settings will allow us to configure the devices security settings for the network. This is covered in section 18. |
| <i>Feature Link</i> Select Network Settings | The wireless interface is now configured however most AdHoc networks do not have a DHCP server available to provide IP address to the devices in the network. It therefore necessary to assign a static IP address to the wireless interface. Selecting Network Settings will allow us to configure the device with a static IP address. This is covered in section 19.0. A bridge unit will require static IP addresses. |



18.0 Configuring the Security Settings

Almost all 802.11 networks will use some sort of security to protect the network from unauthorized use. There are many types of security options available. The following section will cover how to configure the device for the most popular options. If your security configuration is not covered, further details can be found in the Airborne Enterprise CLI Reference Manual.

18.1 Configuring for WEP Security

Although an old protocol WEP is still used by many networks. The Airborne device supports many variations of WEP however we will only cover the most popular in the following table. If the basic 64 or 128 bit WEP configuration does not work please refer to the Airborne Enterprise CLI Reference Manual for the other options available.

Table 26 - Configuring for WEP Security

| Step | Description |
|---|--|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select WLAN Security Settings | The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed. |
| Select Wireless LAN Security | Select WEP64 or WEP128 from the drop down list. The options identify the length of the key that will be used with the security protocol. |
| Select Authentication Type | Select Auto from the drop down list. This field should not need to be changed. Only modify if you have been specifically told to by the network administrator. |
| Select Default WEP Key | Select the key number that matches the selection used by the AP's in the wireless network. This must match for authentication to be successful. There must be a valid key in the selected key number field. |
| Select WEP Key 1 - 4 | Select the key field that matches the one selected in Default WEP Key field. Enter the key exactly as it is entered into the AP. If WEP64 is selected the key length is 10 digits. If WEP128 is selected the key length is 26 digits. More than one key field can be completed. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the WLAN Settings page. Select this if you have further configuration options to change. |

| Step | Description |
|---|--|
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. If the network is using DHCP then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses it will be necessary to configure the network interface, see the next step. |
| <i>Feature Link</i> Select Network Settings | The wireless interface is now configured however if the WLAN network does not have a DHCP server available to provide IP address to the device, it necessary to assign a static IP address to the wireless interface. Selecting Network Settings will allow us to configure the device with a static IP address. This is covered in section 19.0. |

18.2 Configuring for WPA-PSK Security

This security type is a very popular type and is easy to configure. Most often used in SOHO and home environments, some enterprise networks do use it.

Table 27 - Configuring for WPA Security

| Step | Description |
|---|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select WLAN Security Settings | The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed. |
| Select Wireless LAN Security | Select WPA-PSK from the drop down list. |
| Select WPA Protocol Version | Select Auto from the drop down list. This field should not need to be changed. Only modify if you have been specifically told to by the network administrator. |
| Select WPA/WPA2 Pre Shared Key (PSK) | Enter the PreShared Key used by the AP. The PSK is case sensitive and must be entered exactly as it is in the AP. The PSK cannot include spaces. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the WLAN Settings page. Select this is you have further configuration options to change. |

| Step | Description |
|---|--|
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. If the network is using DHCP then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses it will be necessary to configure the network interface, see the next step. |
| <i>Feature Link</i> Select Network Settings | The wireless interface is now configured however if the WLAN network does not have a DHCP server available to provide IP address to the device, it necessary to assign a static IP address to the wireless interface. Selecting Network Settings will allow us to configure the device with a static IP address. This is covered in section 19.0. |

18.3 Configuring for WPA2-PSK Security

This security type is a very popular type and is easy to configure. Most often used in SOHO and home environments, WPA2-PSK is starting to be widely used by enterprise networks.

Table 28 - Configuring for WPA2 Security

| Step | Description |
|---|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select WLAN Security Settings | The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed. |
| Select Wireless LAN Security | Select WPA2-PSK from the drop down list. |
| Select WPA/WPA2 Pre Shared Key (PSK) | Enter the PreShared Key used by the AP. The PSK is case sensitive and must be entered exactly as it is in the AP. The PSK cannot include spaces. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the WLAN Settings page. Select this is you have further configuration options to change. |

| Step | Description |
|---|--|
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. If the network is using DHCP then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses it will be necessary to configure the network interface, see the next step. |
| <i>Feature Link</i> Select Network Settings | The wireless interface is now configured however if the WLAN network does not have a DHCP server available to provide IP address to the device, it necessary to assign a static IP address to the wireless interface. Selecting Network Settings will allow us to configure the device with a static IP address. This is covered in section 19.0. |

18.4 Configuring for PEAP Security

This security type is a very popular type for enterprise networks. Actual use of the security protocol requires the network is using a RADIUS server for device authentication, depending upon the security policies of the network this protocol supports authentication with and without a CA certificate.

The Airborne device supports PEAPv0 using both WPA (TKIP) and WPA2 (AES-CCMP) encryption. The device will automatically use the most appropriate encryption type to obtain authentication to the WLAN.

Table 29 - Configuring for PEAP Security

| Step | Description |
|---|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select WLAN Security Settings | The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed. |
| Select Wireless LAN Security | Select PEAP from the drop down list. |
| Select EAP Identity | Enter the RADIUS server account name provided by the network administrator. If a Windows domain server is being used for authentication the server domain must be included in the EAP Ident field |
| Select EAP Password | Enter the RADIUS server account password for the EAP Ident . |
| Select EAP Phase 1 String | Enter <code>peaplabel=0</code> |
| Select EAP Phase 1 String | Enter <code>auth=MSCHAPV2</code> |

| Step | Description |
|---|---|
| Select CA Certificate Filename | <p>Enter the name of the Certificate Authority (CA) certificate stored on the device.</p> <p>Storing Certificates on the device is cover in section 15.5.</p> <p>If the network security does not require the use of a CA certificate this field should be left blank.</p> |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the WLAN Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | <p>Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect.</p> <p>If the network is using DHCP then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network.</p> <p>If the network is using static IP addresses it will be necessary to configure the network interface, see the next step.</p> |
| <i>Feature Link</i> Select Network Settings | <p>The wireless interface is now configured however if the WLAN network does not have a DHCP server available to provide IP address to the device, it necessary to assign a static IP address to the wireless interface.</p> <p>Selecting Network Settings will allow us to configure the device with a static IP address. This is covered in section 19.0.</p> |

19.0 Configuring Network Settings

Once the device is authenticated to a wireless network communication is possible, however before TCP/IP connectivity can be achieved the device must obtain a valid IP address on the WLAN and/or Ethernet interface.

The Airborne device supports both DHCP and Static IP addressing for both the WLAN and Ethernet interfaces. The following sections cover the correct configuration for both DHCP and Static IP addressing on the interfaces.

When the Ethernet interface is in client mode DHCP can be used on either the WLAN or Ethernet interface but not on both interfaces at the same time.

The Ethernet interface configuration only applies when the interface is in client mode and is being used by a serial device server. The configuration of the Ethernet interface when being used with the Ethernet adapter (ABDx-ER) products is covered in section 21.0.



The Ethernet configuration sections do not apply to devices that do not have an available Ethernet port; these include but are not limited to the ABDx-SE-DP5xx product families.

19.1 Configuring DHCP on WLAN Interface

DHCP enabled on the WLAN interface is the default configuration for the Ethernet devices. For serial devices the default is DHCP disabled on the WLAN interface. It requires that there is a DHCP server on the WLAN network the device has authenticated to and that the necessary network policies will allow the server to lease an address to the Airborne™ device.

Table 30 - Configuring DHCP - WLAN

| Step | Description |
|---|--|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Network Settings | The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed. |
| Select WLAN DHCP | Select Enabled from the dropdown menu. |
| <i>Optional</i> Select WLAN DHCP Name | Provides a method of uniquely identifying the device in the DHCP lease table on the DHCP server. The default name is AirborneXXXXXX , where XXXXXX matches the last 6 octets of the WLAN interface MAC address. |
| Press Commit [Button] | Saves changes to the device. |

| Step | Description |
|--|--|
| <i>Optional</i> Press Reload [Button] | Reloads the Network Settings page. Select this if you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated the network should lease an IP address to the WLAN interface and IP connectivity is possible over the WLAN network. |

19.2 Configuring DHCP on Ethernet Interface

DHCP enabled on the Ethernet interface is the default configuration for the serial devices. The Ethernet interface must be in client mode for this setting to be used.

The Airborne Device does not support the ability to enable DHCP on the WLAN and Ethernet interfaces simultaneously (when in client mode). Only one may have DHCP enabled at a time. The other interface must be configured to use a static IP address.

Table 31 - Configuring DHCP - Ethernet

| Step | Description |
|--|--|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Ethernet Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields, setting the mode of operation for the Ethernet interface is done in this page. |
| Select Ethernet Role | Select Client from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Ethernet Settings page. |
| <i>Feature Link</i> Select Network Settings | The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed. |
| Select Ethernet DHCP | Select Enabled from the drop down menu. |
| <i>Optional</i> Select WLAN DHCP Name | Provides a method of uniquely identifying the device in the DHCP lease table on the DHCP server. The default name is AirborneXXXXXX , where XXXXXX matches the last 6 hexadecimal digits of the Ethernet interface MAC address. |

| Step | Description |
|--|--|
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Network Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated the network should lease an IP address to the WLAN interface and IP connectivity is possible over the WLAN network. |

19.3 Configuring a Static IP Address on WLAN Interface

Static IP addresses on the WLAN interface is the default configuration for serial devices. It is important to verify the address being entered is unique to the device when on the network.

Table 32 - Configuring Static IP - WLAN

| Step | Description |
|---|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Network Settings | The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed. |
| Select WLAN DHCP | Select Disable from the drop down menu. |
| Select WLAN Static IP Address | Enter the assigned static IP address. The address must be in the format: XXX.XXX.XXX.XXX |
| Select Subnet Mask | Enter the subnet mask for the network. The mask must be in the format: XXX.XXX.XXX.XXX |
| Select Gateway IP Address | Enter the assigned Gateway IP address. The address must be in the format: XXX.XXX.XXX.XXX |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Network Settings page. Select this is you have further configuration options to change. |

| Step | Description |
|--|---|
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated the network will use the assigned static IP address on the WLAN interface making IP connectivity possible over the WLAN network. |

19.4 Configuring a Static IP Address on Ethernet Interface

This is not the default configuration for the Ethernet interface. It is important to verify the address being entered is unique to the device when on the network.

The Airborne Device does not support the ability to enable DHCP on the WLAN and Ethernet interfaces simultaneously (when in client mode). Only one may have DHCP enabled at a time, the other interface must be configured to use a static IP address.

Table 33 - Configuring Static IP - Ethernet

| Step | Description |
|--|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Ethernet Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields, setting the mode of operation for the Ethernet interface is done in this page. |
| Select Ethernet Role | Select Client from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Ethernet Settings page. |
| <i>Feature Link</i> Select Network Settings | The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed. |
| Select Ethernet DHCP | Select Disable from the drop down menu. |
| Select Ethernet Static IP Address | Enter the assigned static IP address. The address must be in the format: XXX.XXX.XXX.XXX |
| Select Ethernet Subnet Mask | Enter the subnet mask for the network. The mask must be in the format: XXX.XXX.XXX.XXX |

| Step | Description |
|--|---|
| Select Ethernet Gateway IP Address | Enter the assigned Gateway IP address. The address must be in the format: XXX.XXX.XXX.XXX |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Network Settings page. Select this if you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated the network will use the assigned static IP address on the Ethernet interface making IP connectivity possible over the Ethernet network. |

20.0 Configuring Serial Device Server

The ABDx-SE-DP5xx/IN5xxx devices are shipped preconfigured for use as Serial Device Servers. All that is required is configuration of the WLAN parameters and security protocols; however the following section will cover the full configuration of a Serial Device Server to aid in the installation and deployment of the units.

If the Windows Virtual COM port driver is being used with the device, configure only the WLAN network parameters and security protocols through the web interface. All other parameters will be controlled by the VCOM driver. Installation and configuration of the VCOM driver is covered in section 21.0.

The following section shows how to manually configure the unit to accept TCP/IP connections and automatically set-up a data tunnel with one of the serial ports. The configuration is independent of the source of the request, as the tunnel ports are available to both the WLAN and Ethernet interfaces.

The Airborne devices support conditional tunnel binding based upon rules included in the configuration. The major options will be included.

20.1 Configuring Serial Port for Access on Telnet Port

A data tunnel can be made using the device's telnet port as the network connection port. This does require authenticating with the device and manually initiating the tunnel connection. Configuring the device to support this approach to establishing a data tunnel is covered in the following table.

Table 34 – Configure Data Tunnel on Telnet Port

| Step | Description |
|--|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Connection Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page. |
| Select Telnet Port | Enter the port number you wish to use for a telnet (TCP/IP) connection to the device. The default 23 should only be changed if your application requires access to port 23 for another purpose. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Connection Settings page. |

| Step | Description |
|--|--|
| <i>Feature Link</i> Select Serial Port 1 Settings/Serial Port 2 Settings | The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration, setting the default mode of operation for the serial interface is done in this page. |
| Select Serial CLI Default Mode | Select Listen from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Serial Port X Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated the network it is possible for a TCP/IP connection to be made on the Telnet port. |

To establish a data tunnel and gain access to the serial data from the WLAN or Ethernet interface follow the steps in Table 35.

Table 35 - Data Tunnel using Telnet Port

| Step | Description |
|---------------------------------|--|
| Open TCP socket to device | Using the WLAN IP Address and configured telnet port number. |
| Authenticate with device | <code>auth dpac dpac</code> Any user level above L5 can authenticate with the unit. Device responds <code>OK</code> |
| Open data tunnel to serial port | <code>pass-x</code> Where <code>x</code> can be <code>p1</code> , <code>p2</code> or <code>any</code> . <code>p1</code> or <code>p2</code> binds to the indicated serial port, as long as the serial port is in listen mode and does not already have a data tunnel open. <code>any</code> binds to the first serial port which is in listen mode and does not already have a data tunnel open. |

20.2 Configuring Serial Port 1 for Access on Tunnel Port

A data tunnel can be made using the devices tunnel port as the network connection port. This does not require authenticating with the device and automatically initiates the tunnel connection. Configuring the device to support this approach to establishing a data tunnel is covered in the following table.

Table 36 – Configure Data Tunnel on Serial Port 1 Tunnel Port (TCP)

| Step | Description |
|---|--|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Connection Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page. |
| Select Tunnel Enabled | Select Enabled . |
| Select Tunnel Port | Enter the port to be used for the tunnel. Default is 8023 , this should only be changed if a port is already defined for the application server or it is already being used by another service. |
| Select Tunnel Mode | Select TCP from drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Connection Settings page. |
| <i>Feature Link</i> Select Serial Port Settings | The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration, setting the default mode of operation for the serial interface is done in this page. |
| Select Serial CLI Default Mode | Select Listen from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Serial Port Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated the network it is possible for a TCP/IP connection to be made on the Telnet port. |

To establish a data tunnel and gain access to the serial data from the WLAN or Ethernet interface follow the steps in Table 37.

Table 37 - Data Tunnel using Tunnel Port on Serial Port 1

| Step | Description |
|---------------------------|---|
| Open TCP socket to device | Using the WLAN IP Address and configured tunnel port number for Serial Port 1 (Default 8023). |

20.3 Configuring Serial Port 2 for Access on Tunnel Port

A data tunnel can be made using the devices tunnel port as the network connection port. This does not require authenticating with the device and automatically initiates the tunnel connection. Configuring the device to support this approach to establishing a data tunnel is covered in the following table.

Table 38 – Configure Data Tunnel on Serial Port 2 Tunnel Port (TCP)

| Step | Description |
|---|--|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Connection Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page. |
| Select Tunnel Enabled – Serial Port 2 | Select Enabled . |
| Select Tunnel Port – Serial Port 2 | Enter the port to be used for the tunnel. Default is 8024 , this should only be changed if a port is already defined for the application server or it is already being used by another service. |
| Select Tunnel Mode – Serial Port 2 | Select TCP from drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Connection Settings page. |
| <i>Feature Link</i> Select Serial Port 2 Settings | The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration, setting the default mode of operation for the serial interface is done in this page. |
| Select Serial CLI Default Mode | Select Listen from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Serial Port 2 Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated the network it is possible for a TCP/IP connection to be made on the Telnet port. |

To establish a data tunnel and gain access to the serial data from the WLAN or Ethernet interface follow the steps in Table 39.

Table 39 - Data Tunnel using Tunnel Port on Serial Port 2

| Step | Description |
|---------------------------|---|
| Open TCP socket to device | Using the WLAN IP Address and configured tunnel port number for Serial Port 2 (Default 8024). |

20.4 Configuring Serial Port 1 as TCP Client

In this mode the device will attempt to initiate a TCP connection to a network based server and establish a data tunnel with Serial Port 1 on a successful network connection.

Table 40 - Configure Serial Port 1 as TCP Client

| Step | Description |
|---|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Connection Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page. |
| Select TCP Port | Enter the port on which the target server is listening for TCP connections. |
| Select TCP Timeout | Enter the inactivity timeout in seconds, after which the device will close the open data tunnel on Serial Port 1. The default 0 disables the timeout. |
| Select TCP Retry Time | Enter the period (in seconds) the device should use to retry establishing the TCP connection to the target server. |
| Select Primary TCP Target Server IP Address | Enter the IP address of the primary target server. The address must be in the format: XXX.XXX.XXX.XXX |
| <i>Optional</i> Select Secondary TCP Target Server IP Address | Enter the IP address of the secondary target server. The address must be in the format: XXX.XXX.XXX.XXX This address will be used if the initial attempts to connect to the primary server fail. This field is optional. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Connection Settings page. |

| Step | Description |
|---|--|
| <i>Feature Link</i> Select Serial Port 1 Settings | The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration, setting the default mode of operation for the serial interface is done in this page. |
| Select Serial CLI Default Mode | Select Pass from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Serial Port 1 Settings page. Select this if you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated to the network the device will attempt to make a TCP connection with primary target server, using the configured port number. |

20.5 Configuring Serial Port 2 as TCP Client

In this mode the device will attempt to initiate a TCP connection to a network based server and establish a data tunnel with Serial Port 2 on a successful network connection.

Table 41 - Configure Serial Port 2 as TCP Client

| Step | Description |
|--|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Connection Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page. |
| Select TCP Port – Serial Port 2 | Enter the port on which the target server is listening for TCP connections. |
| Select TCP Timeout – Serial Port 2 | Enter the inactivity timeout in seconds, after which the device will close the open data tunnel on Serial Port 1. The default 0 disables the timeout. |
| Select TCP Retry Time – Serial Port 2 | Enter the period (in seconds) the device should use to retry establishing the TCP connection to the target server. |

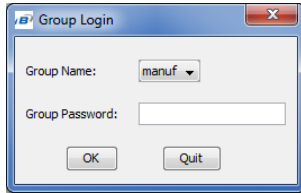
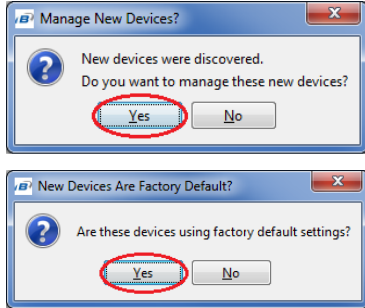
| Step | Description |
|---|---|
| Select Primary TCP Target Server IP Address – Serial Port 2 | Enter the IP address of the primary target server. The address must be in the format: XXX.XXX.XXX.XXX |
| <i>Optional</i> Select Secondary TCP Target Server IP Address – Serial Port 2 | Enter the IP address of the secondary target server. The address must be in the format: XXX.XXX.XXX.XXX This address will be used if the initial attempts to connect to the primary server fail. This field is optional. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Connection Settings page. |
| <i>Feature Link</i> Select Serial Port 2 Settings | The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration, setting the default mode of operation for the serial interface is done in this page. |
| Select Serial CLI Default Mode | Select Pass from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Serial Port 2 Settings page. Select this if you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Once authenticated to the network it the device will attempt to make a TCP connection with primary target server, using the configured port number. |

21.0 Installing and Using the Airborne VirtualCOM Driver

B&B Electronics supplies with its serial devices a virtual COM port device driver for the Microsoft Windows operating system. This driver acts as a Virtual COM port for applications requiring the use of a COM port for data communication. The driver redirects serial data to a TCP/IP connection between the host computer and target Airborne™ device.

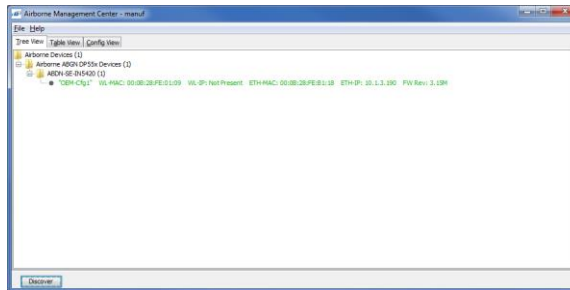
Installation of the VCOM driver is done using the Airborne Management Center™ (AMC). The following Table 42 identifies the steps to complete the process of installing the VCOM driver for a specific device. Once installed the host system will have additional COM ports through which the system may communicate with the device attached to the serial port on the Airborne™ device.

Table 42 - Install VCOM

| | |
|---|--|
| 1 | <p>Run the Airborne Management System application. This was installed during the CD installation and a menu item will be found in the Airborne folder located in the programs directory of your system.</p> <p>When the application opens the following dialog will be displayed:</p>  <p>The dialog box is titled 'Group Login'. It has a 'Group Name' dropdown menu with 'manuf' selected, a 'Group Password' text field, and 'OK' and 'Quit' buttons.</p> <p>Select Group Name: manuf and enter Group Password: dpac</p> |
| 2 | <p>The AMC will load and discover the attached devices. Manage your device.</p>  <p>Two dialog boxes are shown. The first is titled 'Manage New Devices?' and asks 'New devices were discovered. Do you want to manage these new devices?' with 'Yes' and 'No' buttons. The 'Yes' button is circled in red. The second is titled 'New Devices Are Factory Default?' and asks 'Are these devices using factory default settings?' with 'Yes' and 'No' buttons. The 'Yes' button is circled in red.</p> |

3

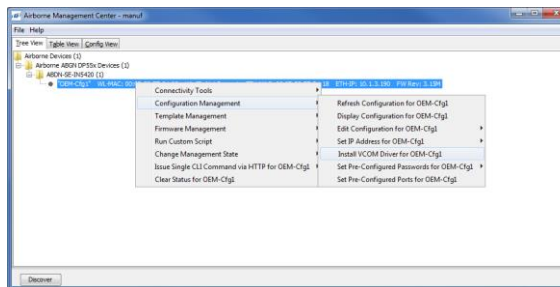
Managed devices will show up under the device type heading they belong to. To install a VCOM driver the device MUST have a serial port.



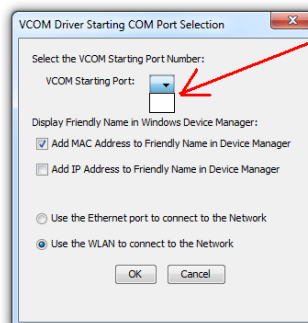
4

The status of the device will move to managed and it will be displayed under the device type/group it belongs too. To install the VCOM driver, right click the target device:

1. Select **Configuration Management**
2. Select **Install VCOM Driver for OEM-Cfg1**



Note: if the port selection box doesn't have any ports listed; cancel the install, close AMC, then restart AMC by right-clicking the icon and clicking "Run as administrator".



5

The VCOM driver will then be installed. When completed the following message will be seen in the lower right-hand corner.



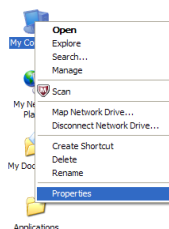
6

The installed VCOM ports are now available for use.

7

To identify the VCOM ports right click **My Computer**.

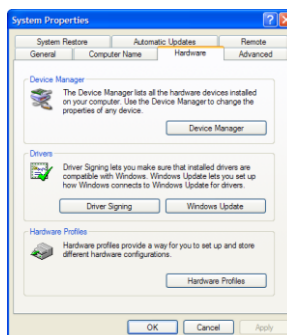
Select **Properties**.



8

Select the **Hardware** tab.

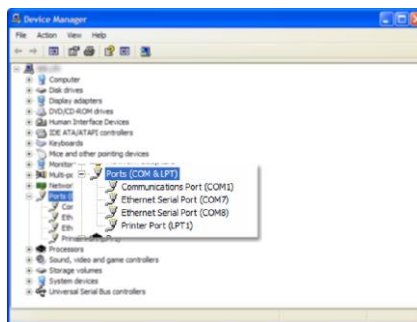
Select the **Device Manager** button.



9

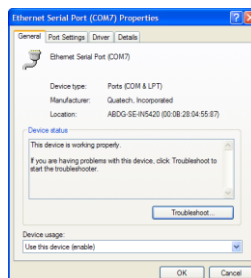
Select the **Ports (COM & LPT)** group and the list of available COM ports will be shown. The VCOM ports will be identified as **Ethernet Serial Port (COMx)**, where **x** will be an integer. This **COMx** reference identifies the VCOM to be used.

Note that if your unit is a dual serial port device, two VCOM ports will have been created.



10

To identify which VCOM port is assigned to which device, right click the **Ethernet Serial Port** and select **Properties**.



The **Location** label identifies the MAC address of the associated Airborne device.



Do not change the WLAN IP address settings for the Airborne device which is using the VCOM driver. Changing the IP address of the device will cause the VCOM driver not to function. It will need to be reinstalled if this occurs.

22.0 Replacing a Serial Cable

The serial device servers can be configured to act as a cable replacement using either an AdHoc or Infrastructure network. In this application you will need two (2) B&B Electronics Serial device servers. Once configured the two devices will automatically connect and make a virtual serial connection between the two serial ports across the 802.11 network.

To establish the cable replacement one device will be the master and one the slave. It does not matter which end of the serial connection is which. The master initiates the network connection and the slave waits for the master to connect. The following Table 43 and Table 44 identify the required configurations for the Master and Slave. The configuration is for a single serial port, the same configuration can be used with those devices that support two serial connections.

The configurations in Table 43 and Table 44 use an AdHoc network. An infrastructure network can be used as long as static IP configuration is used for the slave device.

Table 43 - Cable Replacement - Slave Configuration

| Step | Description |
|--|---|
| <i>Configure the device to use an AdHoc network</i> | See section 17.2 After the Commit at the end of the configuration press the Reload Button. |
| <i>Configure the device to use a static IP address on the WLAN interface</i> | See section 19.3 After the Commit at the end of the configuration press the Reload Button. |
| <i>Configure the device to listen for a connection on the tunnel port</i> | See section 20.2 After the Commit at the end of the configuration press the Reload Button. |
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of Interface and Network Parameters. |
| <i>Feature Link</i> Select Serial Port Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page. |
| Select Serial Port Bit Rate | Select the appropriate bit rate to match the serial port the device will be connected to. |
| Select Parity | Select the parity setting to match the serial port the device will be connected to, from the drop down list. |
| Select Data Bits | Select the number of data bits to match the serial port the device will be connected to, from the drop down list. |
| Select Stop Bits | Select the number of stop bits to match the serial port the device will be connected to, from the drop down list. |
| Select Flow Control | Select the flow control option to match the serial port the device will be connected to, from the drop down list. |
| <i>Optional</i> Select Serial Assert | Select the option to match the serial port the device will be connected to, from the drop down list. This is only required if software flow control has been selected. |
| Press Commit [Button] | Saves changes to the device. |

| Step | Description |
|--|--|
| Press Reload [Button] | Reloads the WLAN Settings page. |
| <i>Optional</i> Press Reload [Button] | Reloads the Serial Port Settings page. Select this if you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device is rebooted it will create an AdHoc network with the name you gave the SSID. As long as the network is in range the wireless interface will connect. |

Table 44 - Cable Replacement - Master Configuration

| Step | Description |
|--|--|
| <i>Configure the device to use an AdHoc network</i> | See section 17.2 After the Commit at the end of the configuration press the Reload Button. |
| <i>Configure the device to use a static IP address on the WLAN interface</i> | See section 19.3 After the Commit at the end of the configuration press the Reload Button. |
| <i>Configure the device to listen for a connection on the tunnel port</i> | See section 20.2 After the Commit at the end of the configuration press the Reload Button. |
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of Interface and Network Parameters. |
| <i>Feature Link</i> Select Serial Port Settings | The serial port must be configured to work with the target device. This is a page showing the configuration options for the serial port. |
| Select Serial Port Bit Rate | Select the appropriate bit rate to match the serial port the device will be connected to. |
| Select Parity | Select the parity setting to match the serial port the device will be connected to, from the drop down list. |
| Select Data Bits | Select the number of data bits to match the serial port the device will be connected to, from the drop down list. |
| Select Stop Bits | Select the number of stop bits to match the serial port the device will be connected to, from the drop down list. |
| Select Flow Control | Select the flow control option to match the serial port the device will be connected to, from the drop down list. |
| <i>Optional</i> Select Serial Assert | Select the option to match the serial port the device will be connected to, from the drop down list. This is only required if software flow control has been selected. |
| Select Serial CLI Default Mode | Select Pass from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the WLAN Settings page. |

| Step | Description |
|--|---|
| <i>Feature Link</i> Select Connection Settings | <p>The target device configuration must be configured to make sure the master device connects to the correct slave.</p> <p>A page showing the configuration options for TCP/IP and UDP connections to and from the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.</p> |
| Select TCP Port | <p>This is the target port for the TCP connection on the slave device. This should be set to the listen port assigned during the configuration of the slave. The default for the listen port is 8023.</p> |
| Select TCP Timeout | <p>This parameter allows the device to close the TCP socket to the slave should the connection be lost. The default of 0 disables the timeout.</p> <p>The timeout setting should be based upon the period of time a connection would not be used. It should at least exceed the worst case of the data period.</p> |
| Select Primary TCP Target Server IP Address | <p>Enter the static IP address that was given to the slave device during configuration.</p> |
| Select Outbound Transmit Type | <p>This is the outbound transmission protocol.</p> <p>Set this to TCP from the drop down list.</p> |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the WLAN Settings page. |
| <i>Optional</i> Press Reload [Button] | Reloads the Serial Port Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will create an AdHoc network with the name you gave the SSID. As long as the network is in range the wireless interface will connect. |

23.0 Configuring Ethernet Adapter

The ABDx-ER-DP5xx/IN5xxx devices are shipped preconfigured for use as an Ethernet adapter. All that is required is configuration of the WLAN parameters and security protocols; however the following section will cover the full configuration of an Ethernet Device to aid in the installation and deployment of the units.

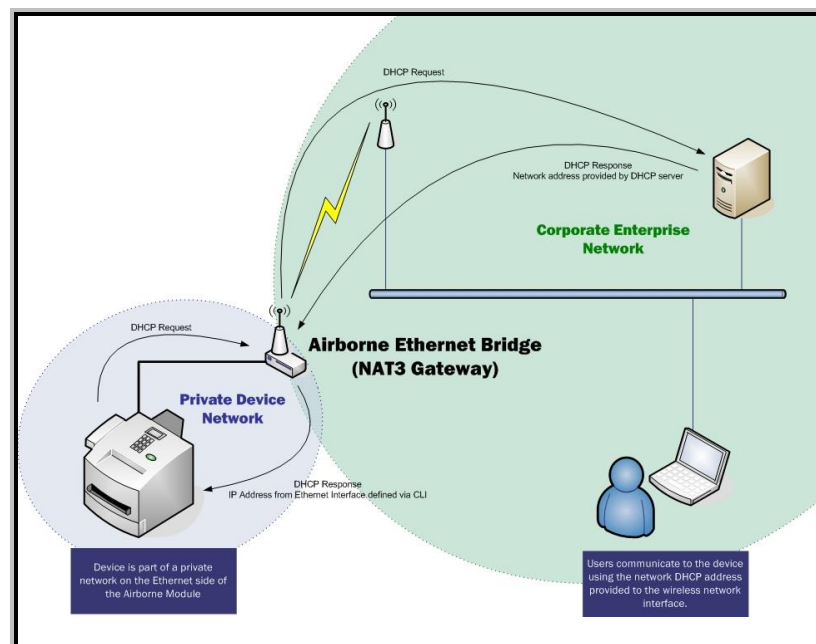
The Airborne Ethernet adapter (ER) is a fully functional NAT Level 3 router, supporting a public IP address for the WLAN interface and a private network for the attached devices on the Ethernet interface. When configured as a Bridge adapter, it disables routing and bridges all packets between the Ethernet and wireless interfaces.

23.1 Router Functionality

Network Address Translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. In the case of a NAT Level 3 device, the modification of the packet headers provides for a translation between a single public IP address (that of the WLAN interface) and the IP address of the devices on the private network (Ethernet interface).

The Airborne Adapter WLAN interface is considered the public address and will be the point of contact on the target network (see Figure 19). This interface supports all the wireless and network authentication requirements including support for WPA2-Enterprise. It can acquire an IP address through both DHCP or user configured static IP. Configuration, association and authentication are handled entirely by the Airborne Bridge and require no interaction from the wired host on the private network.

Figure 19 - Ethernet Bridge Functionality



The Private network is the wired interface provided by the bridge. This interface includes a DHCP server and supports dynamic and static IP address assignment. This means any Ethernet client supporting DHCP can be connected to the wired interface without any configuration changes. The private network host can communicate with the Airborne Adapter using the bridge's Ethernet IP address on the private network.

The Airborne Ethernet Adapter supports NAT Level 3 and as such provides the following advantages over the more traditional bridge functionality:

- A single network IP address on the public network. This simplifies management of the devices on the network.
- A single point of authentication. The Airborne device handles authentication for the public network, this means a single point of contact for all security interaction, simplifying deployment for the network.
- Zero security footprint on the private network host.
- Support for DHCP and static IP on the private network. This capability allows the host to be shipped without any configuration changes.
- Port forwarding. Allows you to decide if web page, telnet or FTP access should be forwarded to the private network or handled by the Airborne Bridge.
- Plug-n-Play. In most cases all that is required for full functionality is configuration of the wireless interface for the target network. This can be done before deployment to minimize deployment time and complexity.

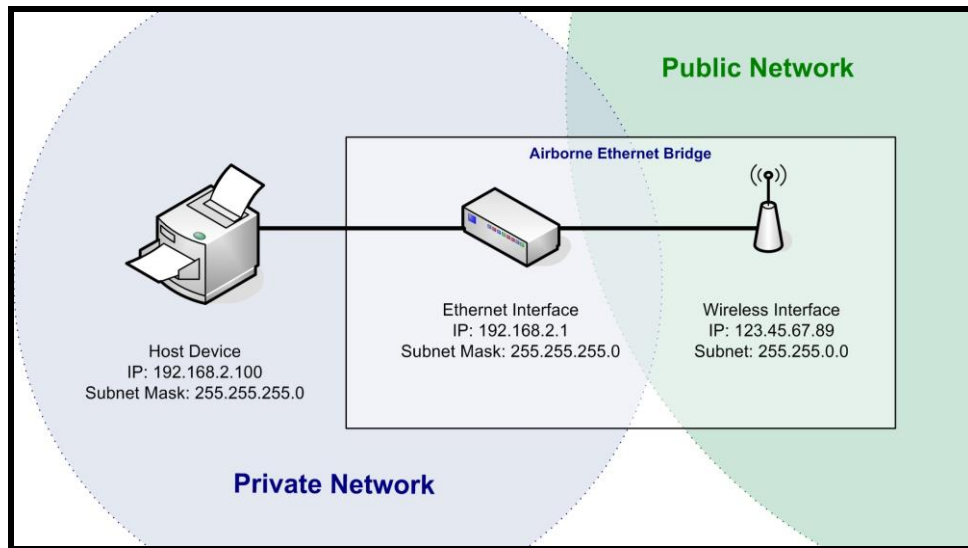
23.1.1 Public Network Interface

The public network interface is the Airborne Adapter WLAN port. This interface must be configured to associate and authenticate with the target network. Configuration of this interface is covered in section 17.0.

The public address becomes the target address for all accesses to the host device connected to the private network. In the example shown in Figure 20, any device on the public network wanting to communicate with the Host device (IP: 192.168.2.100), would use the IP address 123.45.67.89, the Airborne Ethernet Adapter will forward all traffic to the private address 192.168.2.100.

The network infrastructure will show the MAC and IP address of the Airborne Adapter WLAN interface as the network presence, as a consequence of this all traffic will be identified as being from or to this address.

Figure 20 - Airborne Ethernet Bridge IP Configuration



The public network interface supports the Airborne™ discovery protocol and will respond to discovery requests issued on the public network.

23.1.2 Private Network Interface

The private network interface is on the Ethernet port of the Airborne Adapter. The interface supports multiple Ethernet clients with either a static or DHCP sourced IP addresses. The configuration of this interface is covered in Table 45 and Table 46.

Table 45 - Ethernet Adapter interface Configuration - DHCP

| Step | Description |
|--|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Ethernet Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields, setting the mode of operation for the Ethernet interface is done in this page. |
| Select DHCP Server Enabled | Select Enable from drop down menu. |
| Select Ethernet Role | Select Router from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Ethernet Settings page. |

| Step | Description |
|---|--|
| <i>Feature Link</i> Select Network Settings | <p>The wireless interface and security must be configured before configuring the network settings.</p> <p>A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed.</p> |
| Select Ethernet Static IP Address | <p>Enter a valid IP address. This address will be the first IP address leased. If more than one is leased they will increment from this address.</p> <p>The subnet of the address must be different than the WLAN interface subnet.</p> <p>The address must be in the format: XXX.XXX.XXX.XXX</p> <p>This is also the default address all incoming traffic on the WLAN interface is routed to.</p> |
| Select Ethernet Subnet Mask | <p>Enter the subnet mask for the private network.</p> <p>The mask must be in the format: XXX.XXX.XXX.XXX</p> |
| Select Ethernet Gateway IP Address | <p>Enter a valid Gateway IP address. This is the Static IP address of the Ethernet interface on the private network. This must be in the same subnet as the Ethernet Static IP Address.</p> <p>The address must be in the format: XXX.XXX.XXX.XXX</p> |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Network Settings page. Select this is you have further configuration options to change. |
| <i>Optional</i> Press Restart [Button] | <p>Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect.</p> <p>The Ethernet interface will have leased IP addresses to the Ethernet clients and the Ethernet interface would have taken the Ethernet Gateway IP Address. Access to the public network from the private network is now possible.</p> |

Unless your public network is using the default 192.168.2.XX subnet you should not change the Ethernet parameters.


Table 46 - Ethernet Adapter interface Configuration - Static IP

| Step | Description |
|--|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |

| Step | Description |
|--|---|
| <i>Feature Link</i> Select Ethernet Settings | The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields, setting the mode of operation for the Ethernet interface is done in this page. |
| Select DHCP Server Enabled | Select Disable from drop down menu. |
| Select Ethernet Role | Select Router from the drop down menu. |
| Press Commit [Button] | Saves changes to the device. |
| Press Reload [Button] | Reloads the Ethernet Settings page. |
| <i>Feature Link</i> Select Network Settings | The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed. |
| Select Ethernet Static IP Address | Enter the static IP address of the Ethernet client attached to the devices Ethernet port. The subnet of the address must be different than the WLAN interface subnet. The address must be in the format: XXX.XXX.XXX.XXX This is also the default address all incoming traffic on the WLAN interface is routed to. |
| Select Ethernet Subnet Mask | Enter the subnet mask for the private network that matches the subnet mask on the Ethernet client. The mask must be in the format: XXX.XXX.XXX.XXX |
| Select Ethernet Gateway IP Address | Enter a valid Gateway IP address. This is the Static IP address of the Ethernet interface on the private network. This must be in the same subnet as the Ethernet Static IP Address , but a different address. The address must be in the format: XXX.XXX.XXX.XXX This address should be entered into the Gateway parameter for the Ethernet clients on the private network. |
| Press Commit [Button] | Saves changes to the device. |
| <i>Optional</i> Press Reload [Button] | Reloads the Network Settings page. Select this is you have further configuration options to change. |

| Step | Description |
|--|--|
| <i>Optional</i> Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. Access to the public network from the private network is now possible. |

The private network supports the Airborne™ discovery protocol (UDAP) and will respond to discovery requests.



The subnet for the private network IP addresses (Ethernet Client and Gateway) and public IP address (WLAN), obtained by the module via the wireless interface, **MUST NOT** be the same.

Failure to observe this requirement will result in unpredictable behavior of the adapter.

When attempting to make an out-bound connection to a device on the public network, the public network IP address of the device should be used e.g. In Figure 20 the client with address 192.168.2.100 wants to connect to an FTP server, with the address of 123.45.67.99, on the public network to perform a firmware download. The FTP address that would be used in the **Configuration/Advanced Settings** FTP Server Address or Name would be 123.45.67.99. Note that this is not within the subnet of the Ethernet client, however the NAT router will do the necessary address translations and packet header manipulations to ensure the out-bound and in-bound connections are maintained.

Any traffic between the Airborne Ethernet Adapter's Ethernet interface and Ethernet client, on the private network, will not be broadcast on the public network unless it is directed at the public network.

For most users there will be no modification of the private network settings needed and if the target Ethernet client uses DHCP to obtain an IP address, no change in configuration will be required either.

23.2 Bridge Functionality

When the Adapter is a bridge, the Ethernet and 802.11 interfaces will be bridged together. All packets received on either interface will be forwarded to the other interface. Both interfaces reside on the same network, there are no Private and Public networks. The Ethernet IP configuration is used and the 802.11 IP configuration is ignored. The 802.11 interface will assume the IP address of the first ethernet network client that has traffic sent across the bridge.

When acting as a bridge, the Adapter is still listening on the configured ports for remote access to the Adapter. If traffic to any of the configured ports (http, telnet, ftp, ssh, etc) need to pass through the module, then the ports need to be reconfigured to use non-default settings.

Table 47 - Ethernet Adapter interface Configuration

| Step | Description |
|---|---|
| <i>Navigation Bar</i> Select Configuration | You will see a group of fields under the banner of WLAN Parameters. |
| <i>Feature Link</i> Select Express Setup | A page showing the range of basic Wireless and Ethernet options and fields. |
| Select Ethernet Role | Select Router from the drop down menu. |
| Select Ethernet Static IP Address | Enter the static IP address for the Ethernet network. The IP address should be on the same subnet as the other network clients. The address must be in the format: XXX.XXX.XXX.XXX |
| Select Ethernet Subnet Mask | Enter the subnet mask for the private network that matches the subnet mask of the Ethernet client and network. The mask must be in the format: XXX.XXX.XXX.XXX |
| Optional Select Web Server Port | Enter a different value for this port if you want normal Web Server traffic that uses port 80 to pass through the adapter. |
| Optional Select Telnet Port | Enter a different value for this port if you want normal telnet traffic that uses port 23 to pass through the adapter. |
| Optional Select Internal FTP Server Listen Port | Enter a different value for this port if you want normal FTP traffic that uses port 21 to pass through the adapter. |
| Optional Select Secure Shell Server (SSH) Port | Enter a different value for this port if you want normal SSH traffic that uses port 22 to pass through the adapter. |
| Press Commit [Button] | Saves changes to the device. |
| Press Restart [Button] | Restarts the device. After the device as rebooted it will attempt to authenticate to the configured wireless network. As long as the network is in range the wireless interface will connect. |

23.3 MAC Cloning

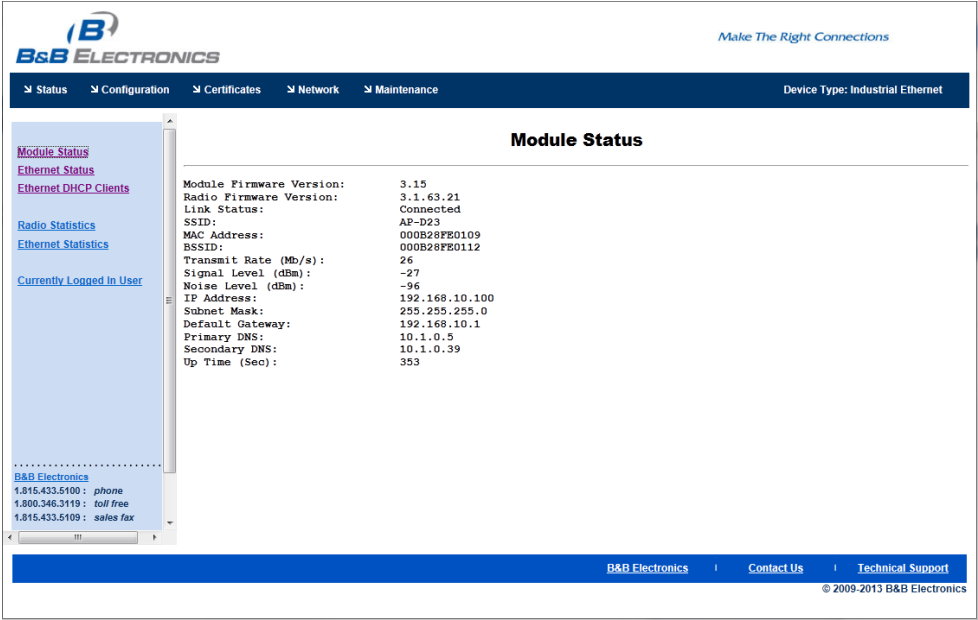
If the network is configured to not allow multiple MAC address for the same IP address, MAC address cloning should be enabled. MAC address cloning will cause the WLAN module to adopt the MAC address of the first Ethernet client that it sees traffic from. If the Ethernet client uses DHCP, the module will sniff the DHCP transactions and learn the MAC and IP that the client will use, and adopts them as its own. When in bridge mode, this makes the module look like a “cable replacement” and should be transparent to the network.

24.0 Web Page Overview

The following section highlights the contents of each web page and provides a reference to the associated CLI command. For further explanation of each of the fields please refer to the referenced command in the table (See Airborne Enterprise Command Line Reference Manual). When using CLI command, typing a command followed by a space and a '?' will display help for the command (e.g. "wl-type ?").

Module Status

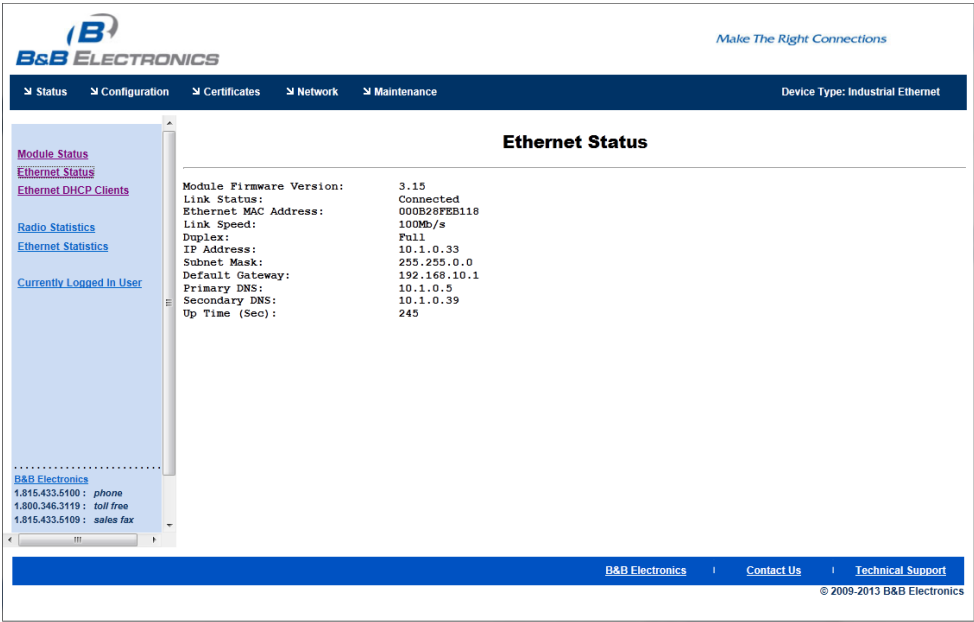
| | |
|-------------|---|
| URL | /Status/Module Status |
| Description | The home page when authenticated to the Airborne device, this page provides important information about the device’s firmware version, wireless connection status and wireless interface network configuration. |



| Field | CLI Command |
|----------------|-------------|
| Displayed Page | wl-info |

Ethernet Status

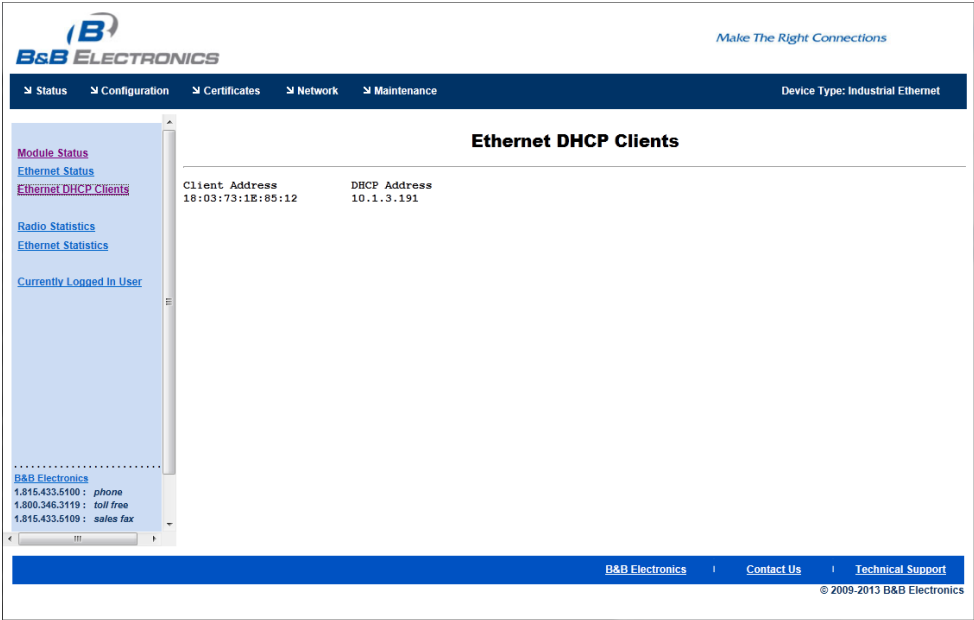
| | |
|-------------|--|
| URL | /Status/Ethernet Status |
| Description | Provides important information about the device's firmware version, Ethernet connection status and Ethernet interface network configuration. |



| Field | CLI Command |
|----------------|-------------|
| Displayed Page | eth-info |

Ethernet DHCP Clients


| | |
|-------------|--|
| URL | /Status/Ethernet DHCP Clients |
| Description | Displays the IP address issued by the DHCP server to specific MAC addresses. |



| Field | CLI Command |
|----------------|------------------|
| Displayed Page | eth-dhcp-clients |

Radio Statistics

| | |
|-------------|---|
| URL | /Status/Radio Statistics |
| Description | Provides information about the packet transmit and receive performance of the wireless interface. |



Make The Right Connections

StatusConfigurationCertificatesNetworkMaintenance

Device Type: Industrial Ethernet

Module Status

Ethernet Status

Ethernet DHCP Clients

Radio Statistics

Ethernet Statistics

Currently Logged In User

Radio Statistics

| | |
|--------------|--------|
| Rx Packets: | 816 |
| Rx Bytes: | 429879 |
| Rx Errors: | 0 |
| Rx Dropped: | 0 |
| Rx Overruns: | 0 |
| Tx Packets: | 1673 |
| Tx Bytes: | 102604 |
| Tx Errors: | 0 |
| Tx Dropped: | 0 |
| Tx Overruns: | 0 |

B&B Electronics

1.815.433.5100 : phone

1.800.346.3119 : toll free

1.815.433.5109 : sales fax

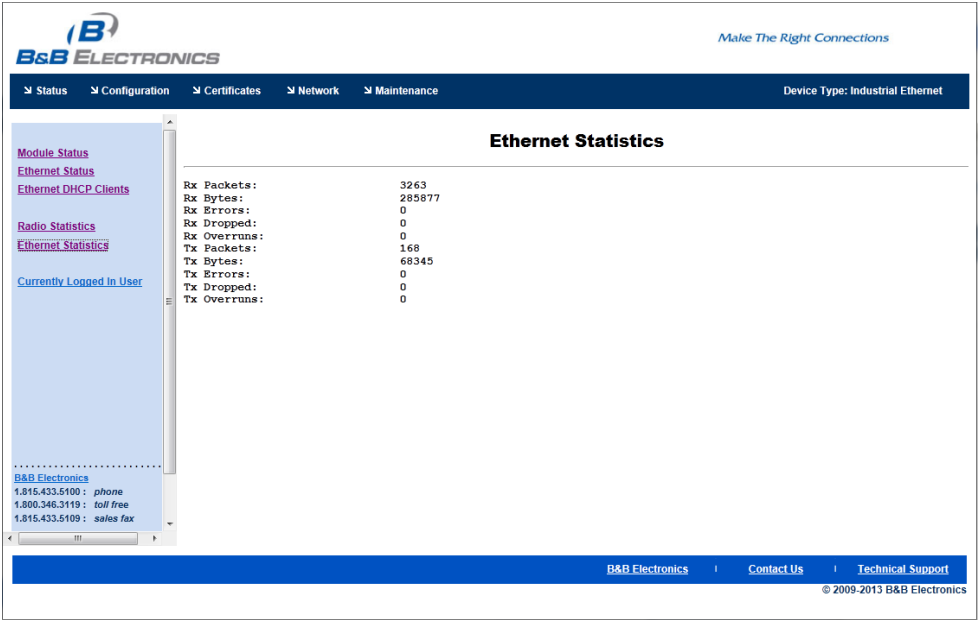
B&B Electronics | Contact Us | Technical Support

© 2009-2013 B&B Electronics

| Field | CLI Command |
|----------------|------------------------|
| Displayed Page | stats <blank> or radio |

Ethernet Statistics

| | |
|-------------|---|
| URL | /Status/Ethernet Statistics |
| Description | Provides information about the packet transmit and receive performance of the Ethernet interface. |



| Field | CLI Command |
|----------------|----------------|
| Displayed Page | stats ethernet |

Express Setup

URL /Configuration/Express Setup

Description A page that provides a simplified configuration option set in a single page. Is the default home page when configuring the device for the first time or after a factory reset has been performed.

B&B ELECTRONICS *Make The Right Connections*

Navigation: Status | Configuration | Certificates | Network | Maintenance | Device Type: Industrial Ethernet

Express Setup

| Express Setup | Current Values |
|----------------------------------|----------------|
| Discovery OEM Device Name: | OEM-Cfg1 |
| Radio Startup Mode: | On |
| WLAN Parameters | |
| WLAN Connection Type: | Infrastructure |
| SSID: | AP-D23 |
| WLAN Security Type: | WPA2-PSK |
| WPA / WPA2 Pre Shared Key (PSK): | |
| Ethernet Parameters | |
| Ethernet Role: | Router |
| Ethernet DHCP Server Enabled: | Enable |
| IP Address Parameters | |
| WLAN DHCP: | Enabled |
| Ethernet DHCP: | Disabled |
| Ethernet Static IP Address: | 10.1.3.190 |
| Ethernet Subnet Mask: | 255.255.0.0 |
| Ethernet Gateway Address: | 10.1.0.33 |

Buttons: Commit | Cancel | Defaults

Footer: B&B Electronics | Contact Us | Technical Support
© 2009-2013 B&B Electronics

| Field | CLI Command |
|------------------------------|---------------------|
| Discovery OEM Device Name | name-oem |
| Radio Startup Mode | radio-on, radio-off |
| Wireless LAN Connection Type | wl-type |
| SSID | wl-ssid |
| Wireless LAN Security Type | wl-security |
| WEP Key 1 | wl-key-1 |
| WPA/WPA2Pre Shared Key (PSK) | pw-wpa-psk |
| LEAP User Name | user-leap |
| LEAP Password | pw-leap |
| PEAP Identity | eap-ident |
| PEAP Password | eap-password |
| Ethernet Role | eth-role |
| Ethernet DHCP Server | eth-dhcp-server |
| WLAN DHCP | wl-dhcp |
| Ethernet DHCP | eth-dhcp |
| WLAN Static IP Address | wl-ip |
| WLAN Subnet Mask | wl-subnet |
| Ethernet Static IP Address | eth-ip |
| Ethernet Subnet Mask | eth-subnet |
| Ethernet Gateway | eth-gateway |

WLAN Settings

| | |
|-------------|---|
| URL | /Configuration/WLAN Settings |
| Description | Configures the wireless interface settings including network name and type. |

| WLAN Parameters | Current Values |
|-----------------------------|--------------------|
| Radio Startup Mode: | On |
| WLAN Connection Type: | Infrastructure |
| SSID: | AP-D23 |
| WLAN TX Power (dBm): | 15 dBm |
| Maximum Wireless Data Rate: | Auto |
| Use Fixed Data Rate: | Disabled |
| WLAN Region: | United States (US) |
| Preferred Radio Band: | Auto |
| WLAN Maximum Retries: | 13 |
| WLAN RTS Threshold: | 0 |

Commit Cancel Defaults

| Field | CLI Command |
|------------------------------|---------------------|
| Radio Startup Mode | radio-on, radio-off |
| Wireless LAN Connection Type | wl-type |
| SSID | wl-ssid |
| Wireless Transmit Power | wl-tx-power |
| Maximum Wireless Data Rate | wl-rate |
| Use Fixed Data Rate | wl-fixed-rate |
| Wireless LAN Region | wl-region |
| 802.11 Band | wl-band-pref |
| Wireless Max Retries on TX | wl-max-retries |
| Wireless RTS Threshold | wl-rts-threshold |

WLAN Security Settings

URL /Configuration/WLAN Security Settings

Description Configures the security settings for the target network.

| WLAN Security Parameters | Current Values |
|---|----------------|
| WLAN Security Type: | WEP 128 |
| Authentication Type: | Auto |
| WEP Settings | |
| Default WEP Key: | 1 |
| WEP Key 1: | |
| WEP Key 2: | |
| WEP Key 3: | |
| WEP Key 4: | |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| WLAN Security Parameters | Current Values |
|---|----------------|
| WLAN Security Type: | WPA-LEAP |
| Authentication Type: | Auto |
| WPA / WPA2 Settings | |
| WPA Protocol Version: | Auto |
| LEAP Settings | |
| LEAP User Name: | dpac |
| LEAP Password: | |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| WLAN Security Parameters | Current Values |
|---|----------------|
| WLAN Security Type: | WPA2-PSK |
| Authentication Type: | Auto |
| WPA / WPA2 Settings | |
| WPA / WPA2 Pre Shared Key (PSK): | |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| WLAN Security Parameters | Current Values |
|---|----------------|
| WLAN Security Type: | PEAP |
| Authentication Type: | Auto |
| WPA / WPA2 Settings | |
| WPA Protocol Version: | Auto |
| EAP Settings | |
| Basic/Advanced Settings: | Basic |
| EAP Identity: | |
| EAP Password: | |
| CA Certificate File Name: | |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| WLAN Security Parameters | Current Values |
|---|----------------|
| WLAN Security Type: | TLS |
| Authentication Type: | Auto |
| WPA / WPA2 Settings | |
| WPA Protocol Version: | Auto |
| EAP Settings | |
| Basic/Advanced Settings: | Basic |
| EAP Identity: | |
| CA Certificate File Name: | |
| Client Certificate File Name: | |
| Private Key File Name: | |
| Private Key File Password: | |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| WLAN Security Parameters | Current Values |
|---|----------------|
| WLAN Security Type: | TTLS |
| Authentication Type: | Auto |
| WPA / WPA2 Settings | |
| WPA Protocol Version: | Auto |
| EAP Settings | |
| Basic/Advanced Settings: | Basic |
| EAP Identity: | |
| EAP Password: | |
| EAP Anonymous Identity: | |
| EAP Phase 2 String: | |
| CA Certificate File Name: | |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| WLAN Security Parameters | Current Values |
|---|----------------|
| WLAN Security Type: | WPA-FAST |
| Authentication Type: | Auto |
| EAP Settings | |
| Basic/Advanced Settings: | Basic |
| EAP Identity: | |
| EAP Password: | |
| CA Certificate File Name: | |
| EAP-FAST Settings | |
| EAP-FAST Provisioning Type: | Authenticated |
| Maximum Number of EAP-FAST Servers: | 10 |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| Field | CLI Command |
|--------------------------------------|--|
| Wireless LAN Security Type | wl-security |
| Authentication Type | wl-auth |
| Default WEP Key | wl-def-key |
| WEP Key 1 - 4 | wl-key-1, wl-key-2, wl-key-3, wl-key-4 |
| WPA Protocol Version | wl-wpa-format |
| LEAP User Name | user-leap |
| LEAP Password | pw-leap |
| WPA/WPA2 Pre Shared Key (PSK) | pw-wpa-psk |
| EAP Identity | eap-ident |
| EAP Password | eap-password |
| EAP Anonymous Identity | eap-anon-ident |
| EAP Phase String 1 | eap-phase1 |
| EAP Phase String 2 | eap-phase2 |
| EAP Subject Match String | subject-match |
| EAP Subject Match 2 String | subject-match2 |
| EAP Alternate Subject Match String | alt-subject-match |
| EAP Alternate Subject Match 2 String | alt-subject-match2 |
| CA Certificate File Name | ca-cert-filename |
| CA Certificate 2 File Name | ca-cert2-filename |
| Client Certificate File Name | client-cert-filename |
| Client Certificate 2 File Name | client-cert2-filename |
| Private Key File Name | priv-key-filename |
| Private Key File Password | priv-key-password |
| Private Key 2 File Name | priv-key2-filename |
| Private Key File 2 Password | priv-key2-password |
| DH Parameter File Name | dh-param-filename |
| DH Parameter 2 File Name | dh-param2-filename |
| EAP-FAST Provisioning Type | eap-fast-provisioning |
| Maximum Number of EAP-FAST Servers | eap-fast-max-pac-list |

Network Settings

URL /Configuration/Network Settings

Description Configures the wireless and Ethernet interface network settings including DHCP, static IP and fall back configurations.

| Network Parameters | Current Values |
|---|----------------------|
| WLAN Specific Settings | |
| WLAN DHCP: | Enabled |
| WLAN DHCP Client Name: | AirborneFE0109 |
| WLAN DHCP Acquire Limit: | 90 |
| WLAN DHCP Fallback: | Enabled |
| WLAN Fallback to Last DHCP IP Address: | Disabled |
| WLAN Fallback IP Address: | 192.168.10.1 |
| WLAN Fallback Subnet Mask: | 255.255.255.0 |
| WLAN Fallback Gateway IP Address: | 0.0.0.0 |
| Ethernet Specific Settings | |
| Ethernet DHCP: | Disabled |
| Ethernet DHCP Client Name: | AirborneFEB118 |
| Ethernet Static IP Address: | 10.1.3.190 |
| Ethernet Subnet Mask: | 255.255.0.0 |
| Ethernet Gateway IP Address: | 10.1.0.33 |
| Common Settings | |
| DNS Server1 IP Address: | 0.0.0.0 |
| DNS Server2 IP Address: | 0.0.0.0 |
| WINS Server1 IP Address: | 0.0.0.0 |
| WINS Server2 IP Address: | 0.0.0.0 |
| DHCP Request Retransmission Mode: | Exponential Interval |
| DHCP Request Retransmission Interval: | 15 |
| <input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/> | |

| Field | CLI Command |
|---|-------------------|
| WLAN DHCP | wl-dhcp |
| WLAN DHCP Client Name | wl-dhcp-client |
| WLAN Static IP Address | wl-ip |
| WLAN Subnet Mask | wl-subnet |
| WLAN Gateway IP Address | wl-gateway |
| WLAN DHCP Acquire Limit | wl-dhcp-acqlimit |
| WLAN DHCP Fallback | wl-dhcp-fb |
| WLAN Fallback to Last DHCP IP Address | wl-dhcp-fbauto |
| WLAN Fallback IP Address | wl-dhcp-fbip |
| WLAN Fallback Subnet Mask | wl-dhcp-fbsubnet |
| WLAN Fallback Gateway IP Address | wl-dhcp-fbgateway |
| Save Last WLAN DHCP IP Address as Fallback IP Addresses | wl-dhcp-fbper |
| Ethernet DHCP | eth-dhcp |
| Ethernet DHCP Client Name | eth-dhcp-client |
| Ethernet DHCP Acquire Limit | eth-dhcp-acqlimit |
| Ethernet Static IP Address | eth-ip |
| Ethernet Subnet Mask | eth-subnet |

| | |
|---|----------------------------|
| Ethernet Gateway IP Address | eth-gateway |
| Ethernet DHCP Fallback | eth-dhcp-fb |
| Ethernet Fallback to Last DHCP IP Address | eth-dhcp-fbauto |
| Ethernet Fallback IP Address | eth-dhcp-fbip |
| Ethernet Fallback Subnet Mask | eth-dhcp-fbsubnet |
| Ethernet Fallback Gateway IP Address | eth-dhcp-fbgateway |
| Save Last Ethernet DHCP IP Address as Fallback IP Addresses | eth-dhcp-fbper |
| DNS Server1/2 IP Address | dns-server1, dns-server2 |
| WINS Server1/2 IP Address | wins-server1, wins-server2 |
| WLAN DHCP Request Retransmission Mode | wl-dhcp-mode |
| WLAN DHCP Request Retransmission Interval | wl-dhcp-interval |
| Ethernet DHCP Request Retransmission Mode | eth-dhcp-mode |
| Ethernet DHCP Request Retransmission Interval | eth-dhcp-interval |

Serial Port Settings

| | |
|-------------|---|
| URL | /Configuration/Serial Port Settings |
| Description | Configures the serial port settings on the primary serial port. |

| Serial Port Parameters | Current Values |
|--------------------------|----------------|
| Serial CLI Default Mode: | CLI ⓘ |
| Serial Port Bit Rate: | 9600 ⓘ |
| Parity: | None ⓘ |
| Data Bits: | 8 ⓘ |
| Stop Bits: | 1 ⓘ |
| Flow Control: | None ⓘ |
| Input Buffer Flush Size: | 1460 ⓘ |
| Serial Escape Mode: | On ⓘ |
| Network CLI Escape Mode: | On ⓘ |
| Escape String: | 7E7E7E6473 ⓘ |
| Serial Interface Type: | RS-232 ⓘ |

Commit

Cancel

Defaults

| Field | CLI Command |
|-------------------------|-------------------------------------|
| Serial CLI Default Mode | serial-default, serial-default-p1 |
| Serial Port Bit Rate | bit-rate, parity-p1 |
| Parity | parity, parity-p1 |
| Data Bits | data-bits, data-bits-p1 |
| Stop Bits | stop-bit, stop-bit-p1 |
| Flow Control | flow, flow-p1 |
| Input Buffer Flush Size | input-size, input-size-p1 |
| Serial Escape Mode | esc-mode-serial, esc-mode-serial-p1 |
| Network CLI Escape Mode | esc-mode-lan, esc-mode-lan-p1 |
| Escape String | esc-str, esc-str-p1 |
| Serial Interface Type | intf-type |

Serial Port 2 Settings

| | |
|-------------|---|
| URL | /Configuration/Serial Port 2 Settings |
| Description | Configures the serial port settings on the secondary serial port. |

Serial Port 2 Parameters

Current Values

Serial CLI Default Mode:

CLI

Serial Port Bit Rate:

9600

Parity:

None

Data Bits:

8

Stop Bits:

1

Flow Control:

None

Input Buffer Flush Size:

1460

Serial Escape Mode:

On

Network CLI Escape Mode:

On

Escape String:

7E7E7E6473

Serial Interface Type:

RS-232

Commit

Cancel

Defaults

| Field | CLI Command |
|-------------------------|--------------------|
| Serial CLI Default Mode | serial-default-p2 |
| Serial Port Bit Rate | parity-p2 |
| Parity | parity-p2 |
| Data Bits | data-bits-p2 |
| Stop Bits | stop-bit-p2 |
| Flow Control | flow-p2 |
| Serial Assert | serial-assert-p2 |
| Input Buffer Flush Size | input-size-p2 |
| Serial Escape Mode | esc-mode-serial-p2 |
| Network CLI Escape Mode | esc-mode-lan-p2 |
| Escape String | esc-str-p2 |
| Serial Interface Type | intf-type |



Serial port 2 cannot run in RS-485 mode and will assume RS-422 mode even if it is set to RS-485 mode. Serial port 2 cannot run half duplex and must have a 4 wire connection.

Connection Settings

URL /Configuration/Connection Settings

Description Configures the data tunnel and network port settings for both serial ports. Includes management of port access and service availability.

| Connection Parameters | Current Values |
|---|----------------|
| Serial Port 1 Connection Settings | |
| Outbound Transmit Type: | Both |
| Primary TCP Target Server IP Address: | 192.168.10.102 |
| Secondary TCP Target Server IP Address: | 0.0.0.0 |
| TCP Port: | 8023 |
| TCP Timeout: | 0 |
| TCP Retry Time: | 60 |
| UDP Target Server IP Address: | 0.0.0.0 |
| UDP Port: | 8023 |
| UDP Receive Port: | 8023 |
| UDP Transmit Mode: | Disable |
| Tunnel Enabled: | Disabled |
| Serial Port 2 Connection Settings | |
| Outbound Transmit Type - Serial Port 2: | Both |
| Primary TCP Target Server IP - Serial Port 2: | 0.0.0.0 |
| Secondary TCP Target Server IP - Serial Port 2: | 0.0.0.0 |
| TCP Port - Serial Port 2: | 2571 |
| TCP Timeout - Serial Port 2: | 0 |
| TCP Retry Time - Serial Port 2: | 60 |
| UDP Target Server IP - Serial Port 2: | 0.0.0.0 |
| UDP Port - Serial Port 2: | 8024 |
| UDP Receive Port - Serial Port 2: | 8024 |
| UDP Transmit Mode - Serial Port 2: | Disable |
| Tunnel Enabled - Serial Port 2: | Disabled |
| Port Settings | |
| HTTP Port Accessible via Wireless: | Enabled |
| Web Server Port: | 80 |
| Default Web Page: | index.html |
| Telnet Port Accessible via Wireless: | Enabled |
| Telnet Port: | 23 |
| Telnet Timeout: | 0 |
| Internal FTP Server Enabled: | Enabled |
| Internal FTP Server Listen Port: | 21 |
| SSH Port Accessible via Wireless: | Enabled |
| Secure Shell Server Port: | 22 |
| Common Settings | |
| Connect LED Mode: | TCP |
| TCP Max Retries: | 5 |
| Wireless UDAP Discovery Enabled: | Enabled |
| Ethernet UDAP Discovery Enabled: | Enabled |

| Field | CLI Command |
|--|-----------------------------------|
| Outbound Transmit Type | wl-xmit-type, wl-xmit-type-p1 |
| Primary TCP Target Server IP Address | wl-tcp-ip, wl-tcp-ip-p1 |
| Secondary TCP Target Server IP Address | wl-tcp-ip2, wl-tcp-ip2-p1 |
| TCP Port | wl-tcp-port, wl-tcp-port-p1 |
| TCP Timeout | wl-tcp-timeout, wl-tcp-timeout-p1 |

| | |
|--|-----------------------------------|
| TCP Retry Time | wl-retry-time, wl-retry-time-p1 |
| Tunnel Enabled | wl-tunnel, wl-tunnel-p1 |
| Tunnel Port | wl-tunnel-port, wl-tunnel-port-p1 |
| Tunnel Mode | wl-tunnel-mode, wl-tunnel-mode-p1 |
| UDP Target Server IP Address | wl-udp-ip, wl-udp-ip-p1 |
| UDP Port | wl-udp-port, wl-udp-port-p1 |
| UDP Receive Port | wl-udp-rxport, wl-udp-rxport-p1 |
| UDP Transmit Mode | wl-udp-xmit, wl-udp-xmit-p1 |
| Outbound Transmit Type – Serial Port 2 | wl-xmit-type-p2 |
| Primary TCP Target Server IP Address – Serial Port 2 | wl-tcp-ip-p2 |
| Secondary TCP Target Server IP Address – Serial Port 2 | wl-tcp-ip2-p2 |
| TCP Port – Serial Port 2 | wl-tcp-port-p2 |
| TCP Timeout – Serial Port 2 | wl-tcp-timeout-p2 |
| TCP Retry Time – Serial Port 2 | wl-retry-time-p2 |
| UDP Target Server IP Address – Serial Port 2 | wl-udp-ip-p2 |
| UDP Port – Serial Port 2 | wl-udp-port-p2 |
| UDP Receive Port – Serial Port 2 | wl-udp-rxport-p2 |
| UDP Transmit Mode – Serial Port 2 | wl-udp-xmit-p2 |
| Tunnel Enabled – Serial Port 2 | wl-tunnel-p2 |
| Tunnel Port – Serial Port 2 | wl-tunnel-port-p2 |
| Tunnel Mode – Serial Port 2 | wl-tunnel-mode-p2 |
| HTTP Port Accessible via Wireless | http-port |
| Web Server Port | wl-http-port |
| Telnet Port Accessible via Wireless | telnet-port |
| Telnet Port | wl-telnet-port |
| Telnet Timeout | wl-telnet-timeout |
| Internal FTP Server Enabled | ftp-server |
| Internal FTP Server Listen Port | ftp-server-listen-port |
| SSH Port Accessible via Wireless | ssh-port |
| Secure Shell Server Port | wl-ssh-port |
| Connect LED Mode | wl-con-led |
| TCP Max Retries | tcp-retries |
| Wireless UDAP Discovery Enabled | wl-udap |
| Ethernet UDAP Discovery Enabled | eth-udap |

Ethernet Settings

| | |
|-------------|---|
| URL | /Configuration/Ethernet Settings |
| Description | Configures the Ethernet interface for AirborneDirect™ Ethernet devices. |

| Ethernet Parameters | Current Values |
|-----------------------------|-----------------|
| Ethernet Role: | Router ⓘ |
| DHCP Server Enabled: | Enable ⓘ |
| MAC Cloning: | Disable ⓘ |
| Ethernet Port Speed/Duplex: | Autonegotiate ⓘ |

CommitCancelDefaults

| Field | CLI Command |
|----------------------------|-----------------|
| Ethernet Role | eth-role |
| DHCP Server Enabled | eth-dhcp-server |
| MAC Cloning | wl-mac-clone |
| Ethernet Port Speed/Duplex | eth-mode |

Wireless Routing Settings

URL /Configuration/Wireless Routing Settings

Description Configures the port forwarding routing rules for the wireless interface.

| Wireless Routing Parameters | Current Values | | | | |
|---|---|------------|-----------------|-------------------------|----------|
| Wireless Routing Default: | FORWARD  | | | | |
| Wireless Routing Rule: | Protocol: TCP | Port: 8080 | Action: FORWARD | Dest IP: 192.168.10.100 | Port: 80 |
| Remove:  | | | | | |
| <input type="button" value="Add rule"/> <input type="button" value="Commit"/> <input type="button" value="Cancel"/> | | | | | |

| Field | CLI Command |
|--------------------------|------------------|
| Wireless Routing Default | wl-route-default |
| Add rule [Button] | wl-route |

Additional details on using the wl-route command:

Usage: wl-route [tcp|udp|icmp|bcast|all] [port xxx] forward|drop|relay [xxx.xxx.xxx.xxx:xxx]

Sets up a specific rule for incoming wireless traffic.

The tcp|udp|icmp|bcast|all option selects the protocol for this rule.

The port option defines the port number for this rule. You cannot set the port option if the protocol is icmp or all.



The drop option will cause traffic matching the protocol and port specifications to be dropped. In this case, any parameters following the drop option will be ignored. The forward option will cause traffic to be forwarded to the ethernet interface, and requires another parameter to define the destination IP address and port. The other parameter is formatted as xxx.xxx.xxx.xxx:port.

The relay option can only be used if the protocol is bcast and will cause UDP traffic with destination address 255.255.255.255 received on the specified port to be relayed to the ethernet interface.

For example, the command wl-route tcp port 80 forward 192.168.2.101:8080 will cause all tcp port 80 traffic received on the wireless interface to be forwarded to IP address 192.168.2.101, port 8080 on the Ethernet interface.

wl-route with no parameters will display the current set of wireless routing rules in the order that they will be applied to incoming traffic.

Ethernet Routing Settings


| | |
|-------------|--|
| URL | /Configuration/Ethernet Routing Settings |
| Description | Configures the firewall routing rules for the Ethernet interface.. |

Ethernet Routing Parameters

Current Values

Ethernet Routing Default:

ACCEPT



Ethernet Routing Rule: Protocol:

TCP

 IP:

192.168.1.100

 Port:

2020

 Action:

ACCEPT

 Remove: ☐

Add rule

Commit

Cancel

| Field | CLI Command |
|--------------------------|-------------------|
| Ethernet Routing Default | eth-route-default |
| Add rule [Button] | eth-route |

Advanced Settings

URL /Configuration/Advanced Settings

Description Configures the advanced configuration settings for the unit, including authentication usernames and passwords, configuration of SSH, power save setup, GPIO, indicator LED and FTP settings.

| Advanced Parameters | Current Values |
|--|---------------------------|
| Version / User Management | |
| OEM Defined Version String: | oemverstr |
| Discovery Manufacturer Device Name: | DPAC-Airborne-IndustrialE |
| Discovery OEM Device Name: | OEM-Cfg1 |
| Discovery Device Name: | Device |
| Administrator Password: | |
| Manufacturing User Name: | dpac |
| Manufacturing Password: | |
| OEM User Name: | oem |
| OEM Password: | |
| CFG User Name: | cfg |
| CFG Password: | |
| Regular User Name: | user |
| Regular User Password: | |
| Encrypt Wireless Keys: | Disabled |
| Protect the OEM Configuration: | Disabled |
| Authorization Level Settings | |
| Minimum Authorization Level for Reset To Factory Defaults: | CFG Level User |
| Minimum Authorization Level for Radio Off: | CFG Level User |
| Minimum Authorization Level for Radio On: | CFG Level User |
| SSH Settings | |
| SSH Default User Name: | |
| SSH Default Password: | |
| SSH Keysize (evenly divisible by 8): | 1024 |
| Power Save Settings | |
| Module Power Save Mode: | Active |
| Serial Port 1 Inactivity Timer: | 0 |
| Serial Port 2 Inactivity Timer: | 0 |
| Radio Startup Mode: | On |
| FTP Settings | |
| FTP Server IP Address or Name: | |
| FTP User Name: | |
| FTP Password: | |
| FTP Server Path: | |
| FTP File Name: | |
| System Time Settings | |
| Timezone Name: | EST |
| Timezone Offset: | -5:00 |
| Daylight Saving Time Adjustment: | Enabled |
| Daylight Saving Time Name: | EDT |
| Daylight Saving Time Offset: | -4:00 |
| Daylight Saving Time Starting Week: | Second |
| Daylight Saving Time Starting Day: | Sunday |
| Daylight Saving Time Starting Month: | March |
| Daylight Saving Time Ending Week: | First |
| Daylight Saving Time Ending Day: | Sunday |
| Daylight Saving Time Ending Month: | November |
| NTP Server IP Address or Name: | pool.ntp.org |
| NTP Sync at Startup: | Disabled |
| NTP Refresh Interval: | 0 |

cont.

| WLAN Specific Settings | |
|---------------------------------------|----------------------|
| Antenna Mode: | Antenna 2 Only |
| Speedlink Roaming: | Enabled |
| Beacons Missed Before Roaming: | 6 |
| Association Retry Count: | 3 |
| Association Backoff Time (msec): | 10000 |
| ARP Staleout Time: | 120 |
| ARP Reachable Time: | 120 |
| Use Directed Probes: | Disabled |
| Lost Association Link Timeout: | 1 |
| Startup Options | |
| Startup Message Mode: | Disabled |
| Startup Message Text: | Ready |
| DHCP Vendor Class ID Strings | |
| WLAN DHCP Vendor Class ID String: | <input type="text"/> |
| Ethernet DHCP Vendor Class ID String: | <input type="text"/> |
| LED / GPIO Settings | |
| I/O Port F Bit Direction: | 0xFF |
| I/O Port F Internal Pullup Resistor: | 0xFF |
| I/O Port G Bit Direction: | 0xFF |
| I/O Port G Internal Pullup Resistor: | 0xFF |
| Enable LED Signal Strength Meter: | Disabled |
| Enable POST LED: | Enabled |
| Enable RF_LINK LED: | Enabled |
| Enable WLN_CFG LED: | Enabled |
| Enable CONN LED: | Enabled |
| Other Advanced Settings | |
| Enable Echo for Telnet Sessions: | Enabled |
| UDP Server Ping: | Disabled |

| Field | CLI Command |
|---|----------------------|
| OEM Defined Version String | |
| Discovery Manufacturer Device Name | name-manuf |
| Discovery OEM Device Name | name-oem |
| Discovery Device Name | name-device |
| Administrator Password | pw-root |
| Manufacturing User Name | user-manuf |
| Manufacturing Password | pw-manuf |
| OEM User Name | user-oem |
| OEM Password | pw-oem |
| CFG User Name | user-cfg |
| CFG Password | pw-cfg |
| Regular User Name | user |
| Regular User Password | pw |
| Encrypt Wireless Keys | cfg-encrypt |
| OEM Configuration Protect | cfg-oem-protect |
| Minimum Authorization Level for Reset | auth-level reset |
| Minimum Authorization Level for Radio off | auth-level radio-off |
| Minimum Authorization Level for Radio on | auth-level radio-on |
| SSH Default User | ssh-default-user |
| SSH Default Password | ssh-default-password |
| SSH Keysize (evenly divisible by 8) | ssh-keysize |
| Module Power Save Mode | pm-mode |

| | |
|--------------------------------------|-----------------------------------|
| Serial Port 1 Inactivity Timer | wl-sleep-timer, wl-sleep-timer-p1 |
| Serial Port 2 Inactivity Timer | wl-sleep-timer-p2 |
| Radio Startup Mode | radio-startup |
| FTP Server IP Address or Name | ftp-server-address |
| FTP User Name | ftp-user |
| FTP Password | ftp-password |
| FTP Server Path | ftp-server-path |
| FTP Filename | ftp-filename |
| Timezone Name | timezone-name |
| Timezone Offset | timezone-offset |
| Daylight Saving Time Adjustment | daylight-saving-time |
| Daylight Saving Time Name | daylight-saving-name |
| Daylight Saving Time Offset | daylight-saving-offset |
| Daylight Saving Time Starting Week | daylight-saving-startweek |
| Daylight Saving Time Starting Day | daylight-saving-startday |
| Daylight Saving Time Starting Month | daylight-saving-startmonth |
| Daylight Saving Time Ending Week | daylight-saving-stopweek |
| Daylight Saving Time Ending Day | daylight-saving-stopday |
| Daylight Saving Time Ending Month | daylight-saving-stopmonth |
| NTP Server IP Address or Name | ntp-server-address |
| NTP Sync at Startup | ntp-startup-sync |
| NTP Refresh Interval | ntp-refresh-interval |
| Antenna Mode | wl-ant |
| Speedlink Roaming | speedlink |
| Beacons Missed Before Roaming | wl-beacons-missed |
| Association Retry Count | wl-assoc-retries |
| Association Backoff Time (msec) | wl-assoc-backoff |
| ARP Staleout Time | arp-staleout-time |
| ARP Reachable Time | arp-reachable-time |
| Use Directed Probes | wl-specific-scan |
| Lost Association Link Timeout | wl-link-timeout |
| Startup Message Mode | startup-msg |
| Startup Message Text | startup-text |
| WLAN DHCP Vendor Class ID String | wl-dhcp-vendorid |
| Ethernet DHCP Vendor Class ID String | eth-dhcp-vendorid |
| I/O Port F Bit Direction | io-dir-f |
| I/O Port F Internal Pullup Resistor | io-pullup-f |
| I/O Port G Direction | io-dir-g |
| I/O Port G Internal Pullup Resistor | io-pullup-g |
| Enable LED Signal Strength Meter | led-mode |
| Enable POST LED | post-led |
| Enable RF_LINK LED | rf-link-led |
| Enable WLN_CFG LED | wln-cfg-led |
| Enable CONN LED | conn-led |
| Enable Echo for Telnet Sessions | telnet-echo |
| UDP Server Ping | wl-udp-ping |

Upload Configuration File

| | |
|-------------|---|
| URL | /Configuration/Upload Configuration File |
| Description | Allows user, OEM or encrypted configuration files to be uploaded to the device. |

Upload a Configuration File to the Module

Select a Configuration File to upload and save on the module:

Browse...

Select the destination filename:

☒ User Configuration

☐ Encrypted Configuration

☐ OEM Configuration

Upload Configuration

Cancel

| Field | CLI Command |
|-------------------------------|-----------------------------|
| Upload Configuration [button] | put-cfg |
| User Config | put-cfg user_config.txt |
| Encrypted Configuration | put-cfg user_enc_config.uue |
| OEM Configuration | put-cfg oem_config.txt |

List Configuration File

| | |
|-------------|---|
| URL | /Configuration/List Configuration File |
| Description | Displays a list of the configuration files saved to the device. |

Configuration File Listing

[timezone.sh](#) 42 bytes
[user_config.txt](#) 523 bytes
2 Files 565 bytes
131072 bytes free

| Field | CLI Command |
|----------------|-------------|
| Displayed Page | list-cfg |

Delete Configuration File

| | |
|-------------|---|
| URL | /Configuration/Delete Configuration File |
| Description | Allows configuration files saved to the device to be deleted. |

Delete a Configuration File From Flash

Choose a Configuration File to Delete:

Choose a Configuration File...

Choose a Configuration File...

timezone.sh

user_config.txt

Delete File

| Field | CLI Command |
|----------------------|-------------|
| Delete File [Button] | del-cfg |

Active Configuration

| | |
|-------------|---|
| URL | /Configuration/Active Configuration |
| Description | Displays the current configuration settings being used by the device. |

Active Configuration

```
#!bin/gtsh
# /var/tmp/active_config.txt
#
ver-fw 1.40E
ver-oemverstr
user-leap dpac
name-manuf DPAC-Airborne-IndustrialE
name-oem OEM-Cfg1
name-device Device
pm-mode active
esc-str 7E7E7E6473
esc-mode serial on
esc-mode-lan on
serial-default cli
intf-type rs232
bit-rate 9600
data-bits 8
parity n
flow n
input-size 0x05B4
serial-assert xon
stop-bit 1
io-dir-f 0xFF
io-dir-g 0xFF
io-pullup-f 0xFF
io-pullup-g 0xFF
wl-http-port 0x0050
wl-telnet-port 0x0017
wl-telnet-timeout 0x00000000
wl-http-def-index host
```

| Field | CLI Command |
|----------------|-----------------|
| Displayed Page | cfg-dump active |

User Configuration

| | |
|-------------|--|
| URL | /Configuration/User Configuration |
| Description | Displays the contents of the user_config.txt configuration file. |

User Configuration

```
#!/bin/qsh
# /var/etc/config/user_config.txt
#
name-oem Quatech_DP501
```

| Field | CLI Command |
|----------------|---------------|
| Displayed Page | cfg-dump user |

OEM Configuration

URL /Configuration/OEM Configuration

Description Displays the contents of the oem_config.txt configuration file.

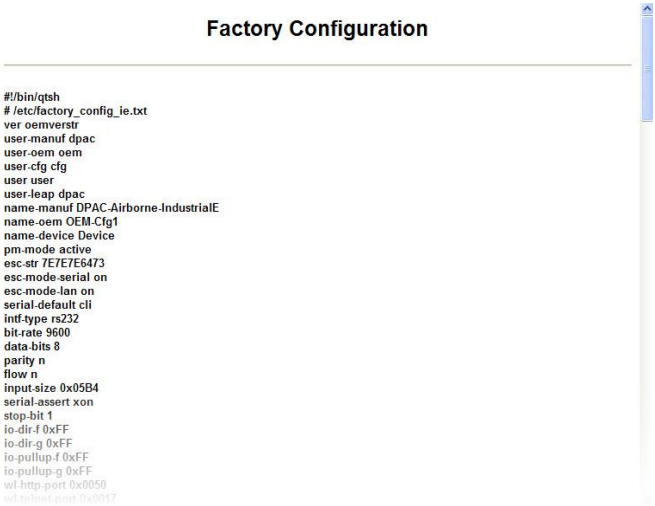
OEM Configuration

```
#!/bin/gtsh
# /var/etc/config/user_config.txt
#
wl-ssid Cisco1100WPA
wl-security wpa-psk
wl-route-default forward
eth-route-default accept
```

| Field | CLI Command |
|----------------|--------------|
| Displayed Page | cfg-dump oem |

Factory Configuration

| | |
|-------------|---|
| URL | /Configuration/Factory Configuration |
| Description | Displays the factory configuration settings. These are the default settings delivered from the B&B Electronics factory. |



| Field | CLI Command |
|----------------|------------------|
| Displayed Page | cfg-dump factory |

WPA Configuration

| | |
|-------------|--|
| URL | /Configuration/WPA Configuration |
| Description | Displays the current security configuration settings being used by the device. |

WPA Configuration

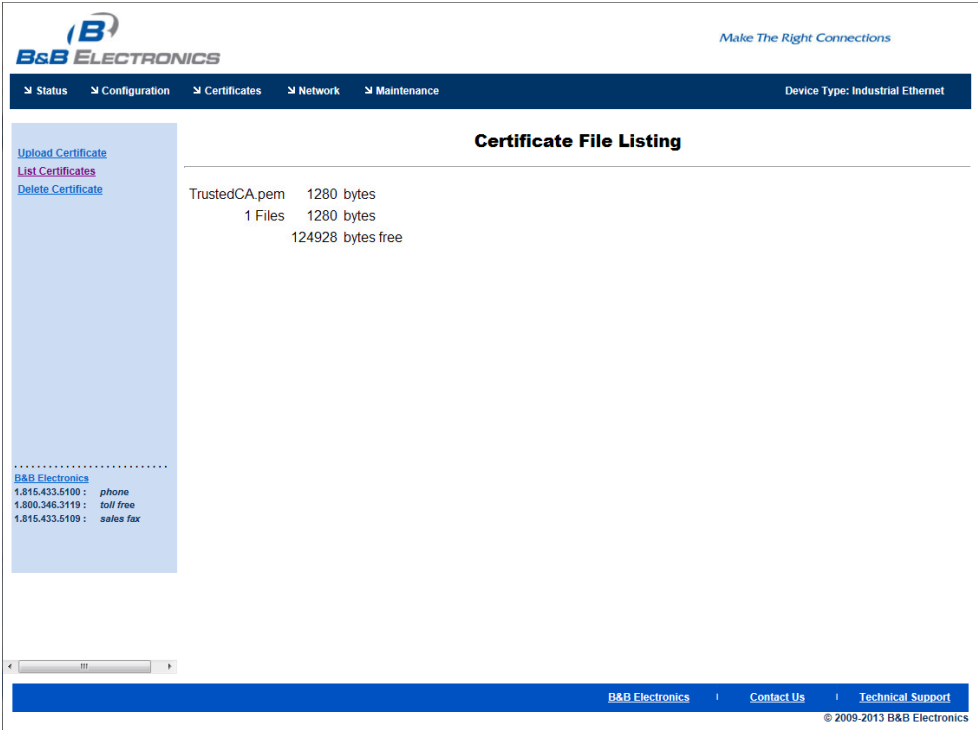
```
#
# /var/tmp/wpa_supplicant.conf
#

ctrl_interface=/var/run/wpa_supplicant
eapol_version=1
ap_scan=1
fast_reauth=1
assoc_retries=3
assoc_backoff=10
network={
ssid="Cisco1100WPA"
scan_ssid=1
mode=0
key_mgmt=WPA-PSK
proto=WPA
pairwise=TKIP
group=TKIP
}
```

| Field | CLI Command |
|----------------|--------------|
| Displayed Page | cfg-dump wpa |

List Certificates


| | |
|-------------|---|
| URL | /Certificates/List Certificates |
| Description | Displays a list of the certificates saved to the device. This is the home page for the Certificates link. |



| Field | CLI Command |
|----------------|-------------|
| Displayed Page | list-cert |

Upload Certificate

| | |
|-------------|---|
| URL | /Certificates/Upload Certificate |
| Description | Enables certificates and private keys to be uploaded to the device. |



Make The Right Connections

StatusConfigurationCertificatesNetworkMaintenance

Device Type: Industrial Ethernet

[Upload Certificate](#)[List Certificates](#)[Delete Certificate](#)

.....

[B&B Electronics](#)
1.816.433.5100 : phone
1.800.346.3119 : toll free
1.816.433.5109 : sales fax

Upload a Certificate to the Module

Select a Certificate File to upload and save on the module:

Browse...

Upload Certificate

Cancel

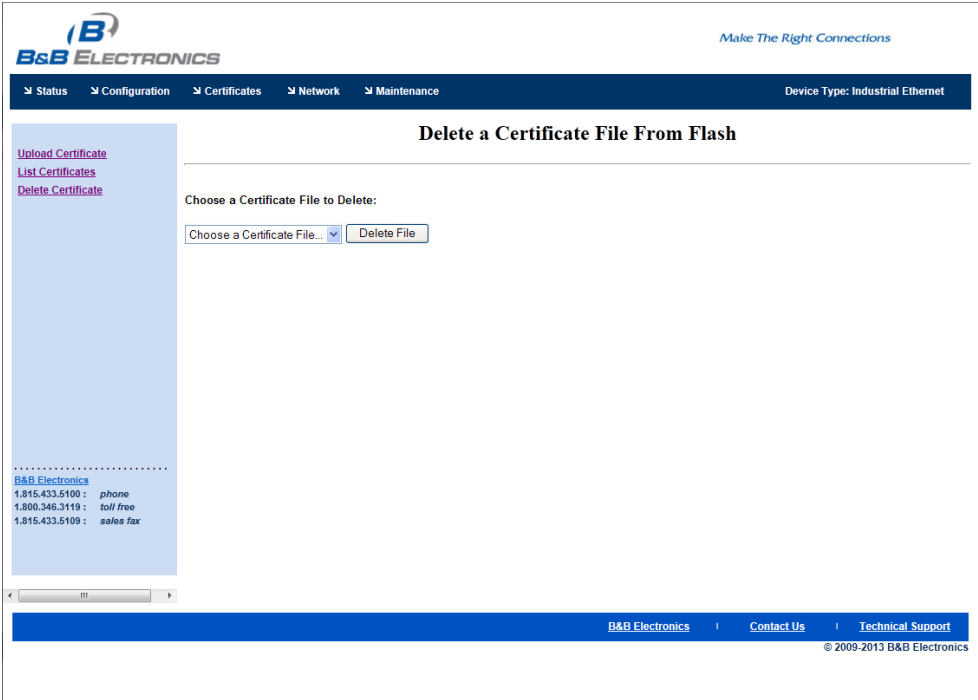
B&B Electronics | Contact Us | Technical Support

© 2009-2013 B&B Electronics

| Field | CLI Command |
|-----------------------------|-------------|
| Upload Certificate [Button] | put-cert |

Delete Certificate

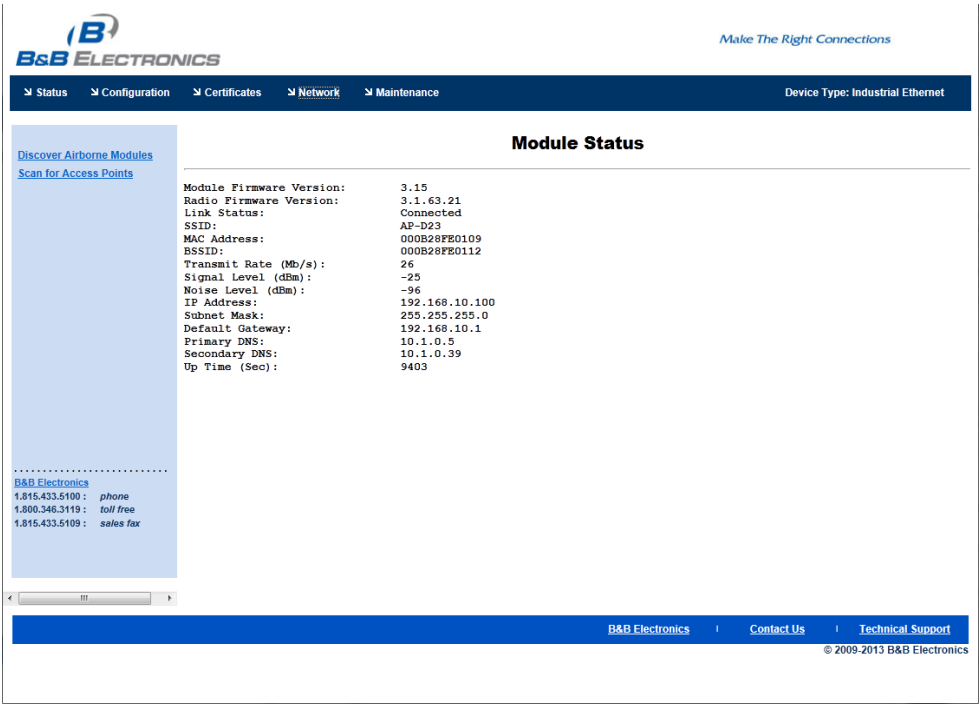
| | |
|-------------|---|
| URL | /Certificates/Delete Certificate |
| Description | Allows certificates stored on the device to be deleted. |



| Field | CLI Command |
|-----------------------------|-------------|
| Delete Certificate [Button] | del-cert |

Network (Home Page)


| | |
|-------------|--|
| URL | /Network |
| Description | Home page for the network related pages. |



| Field | CLI Command |
|----------------|-------------|
| Displayed Page | wl-info |

Discover Airborne Modules

| | |
|-------------|---|
| URL | /Network/Discover Airborne Modules |
| Description | Displays a list of Airborne devices, with IP address, device type and Wireless or Ethernet MAC address, visible to the device on the current network. |



Make The Right Connections

Status

Configuration

Certificates

Network

Maintenance

Device Type: Industrial Ethernet

Discover Airborne Modules

Scan for Access Points

| Device Name | IP Address | MAC Address | Device Type | FW Ver |
|-------------|--------------|--------------|----------------|--------|
| OEM-Crg1 | 192.168.10.1 | 000B28FE0112 | INDUSTR-SERIAL | 3.15 |
| OEM-Crg1 | 10.1.5.141 | 000B28FE0121 | INDUSTR-SERIAL | 3.15 |

B&B Electronics

1.815.433.5100 : phone

1.800.346.3119 : toll free

1.815.433.5109 : sales fax

B&B Electronics

Contact Us

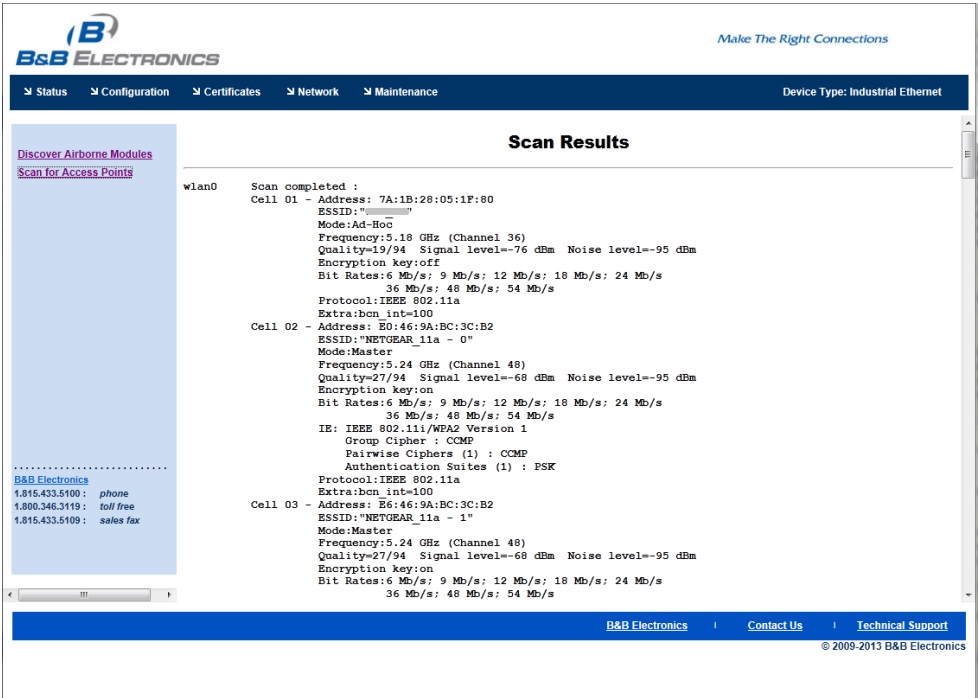
Technical Support

© 2009-2013 B&B Electronics

| Field | CLI Command |
|----------------|-------------|
| Displayed Page | discover |

Scan for Access Points


| | |
|-------------|---|
| URL | /Network/Scan for Access Points |
| Description | Displays a list of wireless networks within range of the device |



| Field | CLI Command |
|----------------|-------------|
| Displayed Page | wl-scan |

Maintenance (Home Page)

| | |
|-------------|--|
| URL | /Maintenance |
| Description | Home page for the maintenance related pages. |



Make The Right Connections

[Status](#) [Configuration](#) [Certificates](#) [Network](#) [Maintenance](#)

Device Type: Industrial Ethernet

[Update Module Firmware](#)
[Reset to Factory Defaults](#)
[Restart Module](#)

[Set System Time](#)

[Blink the POST LED](#)
[Stop Blinking the POST LED](#)

[Upload Script File](#)
[List Script Files](#)
[Display Script File](#)
[Delete Script File](#)
[Run Script File](#)

.....

[B&B Electronics](#)
1.816.433.5100 : phone
1.800.346.3119 : toll free
1.816.433.5109 : sales fax

System Information

Firmware Version: 3.15
Radio Firmware Version: 3.1.63.21
Uboot Version: 1.3.2
Kernel Version: 2.6.32.28
Total RAMDisk Space: 224256
RAMDisk Space Used: 94208
Percent RAMDisk Space Used: 42%
RAMDisk Space Free: 130048
FW Partition Total Disk Space: 0
FW Partition Disk Space Used: 0
FW Partition Percent Disk Space Used: 0%
FW Partition Disk Space Free: 0
Total Memory: 30785536
Memory Used: 14639104
Percent Memory Used: 47%
Memory Free: 16146432
Up Time (Sec): 9962

B&B Electronics | Contact Us | Technical Support

© 2009-2013 B&B Electronics

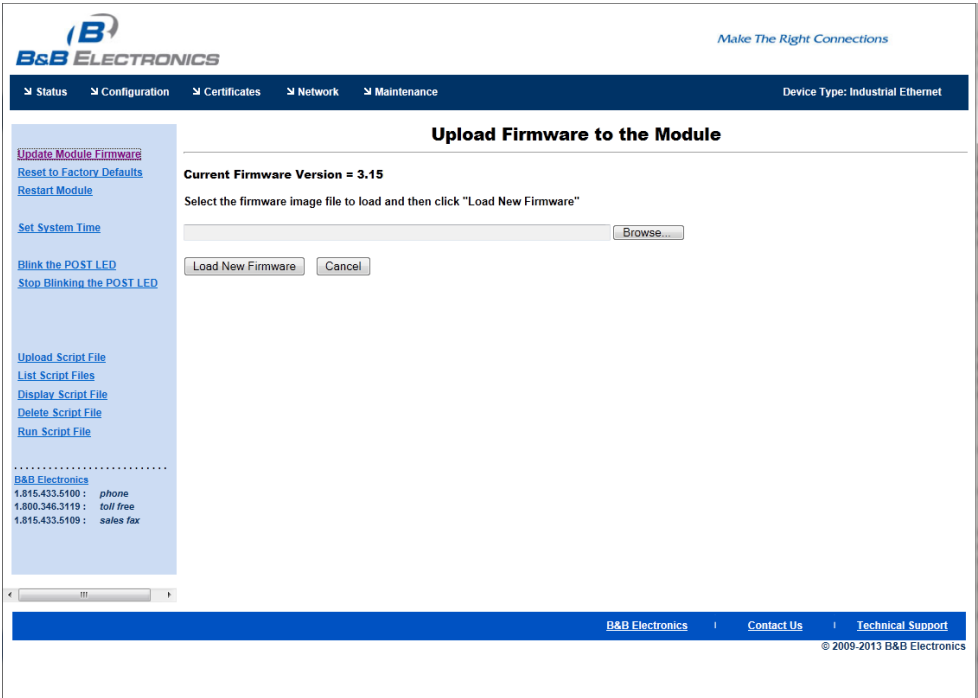
| Field | CLI Command |
|----------------|-------------|
| Displayed Page | sys-info |

123

Update Module Firmware

URL /Maintenance/Update Module Firmware

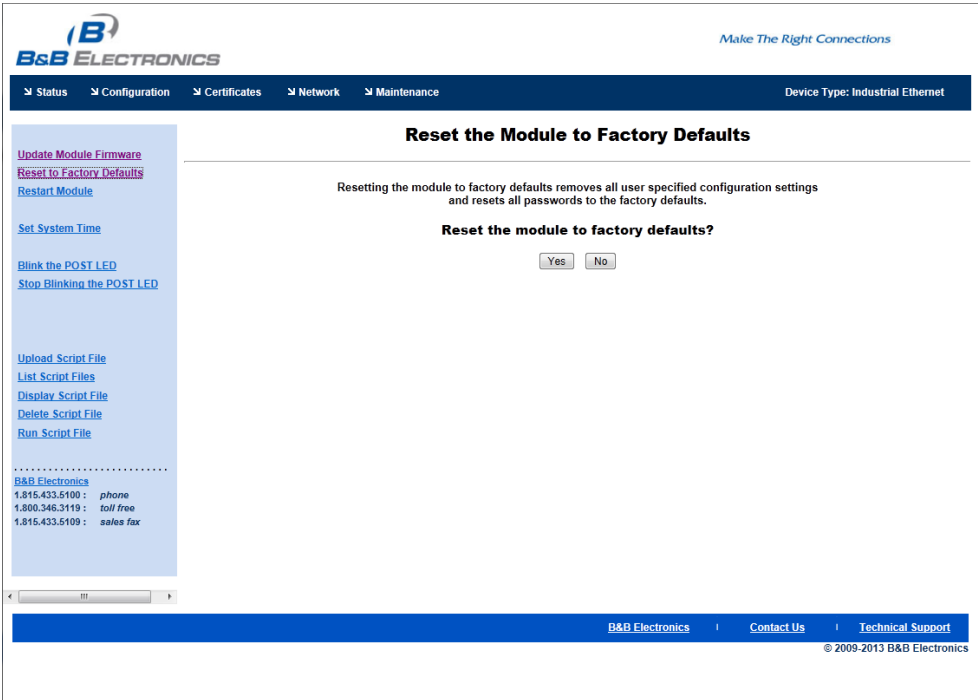
Description Enables module firmware to be updated.



| Field | CLI Command |
|----------------------------|-------------|
| Load New Firmware [Button] | update |

Reset Factory Defaults

| | |
|-------------|--|
| URL | /Maintenance/Reset Factory Defaults |
| Description | Returns device to factory defaults. If oem_config.txt is present this will take precedence over the factory configuration. |

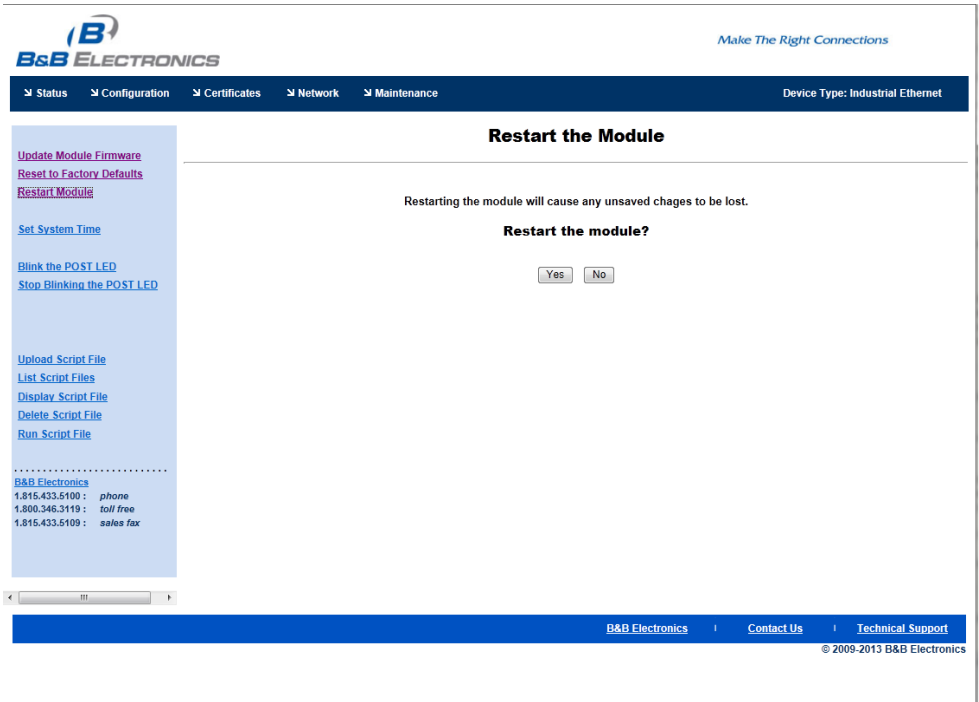


| Field | CLI Command |
|--------------|-------------|
| Yes [Button] | reset |

Restart Module

URL /Maintenance/Restart Module

Description Restarts device.

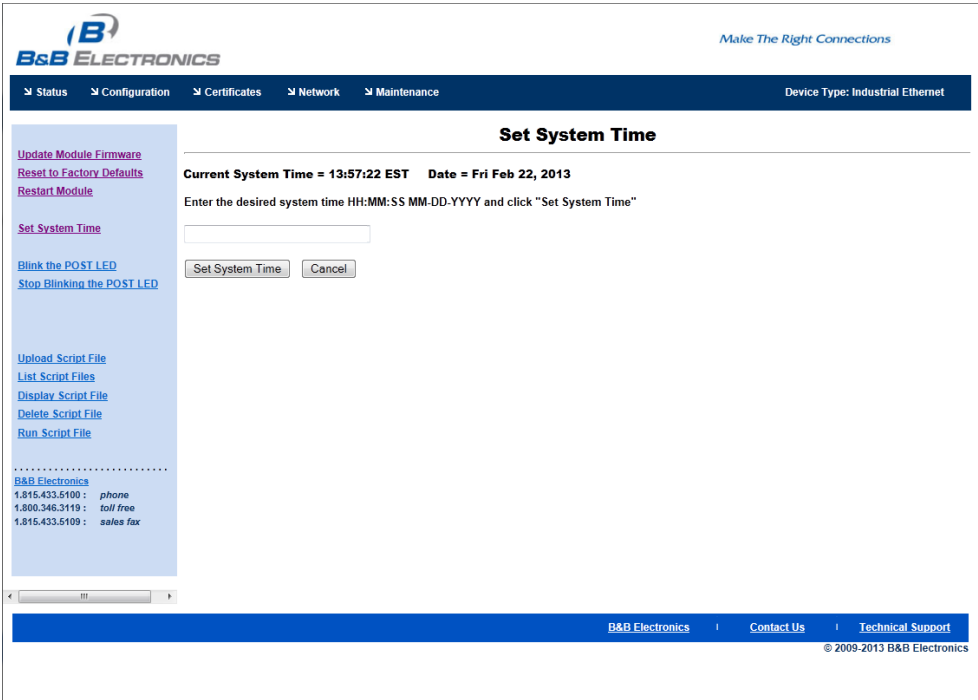


| Field | CLI Command |
|--------------|-------------|
| Yes [Button] | restart |

Set System Time

URL /Maintenance/Set System Time

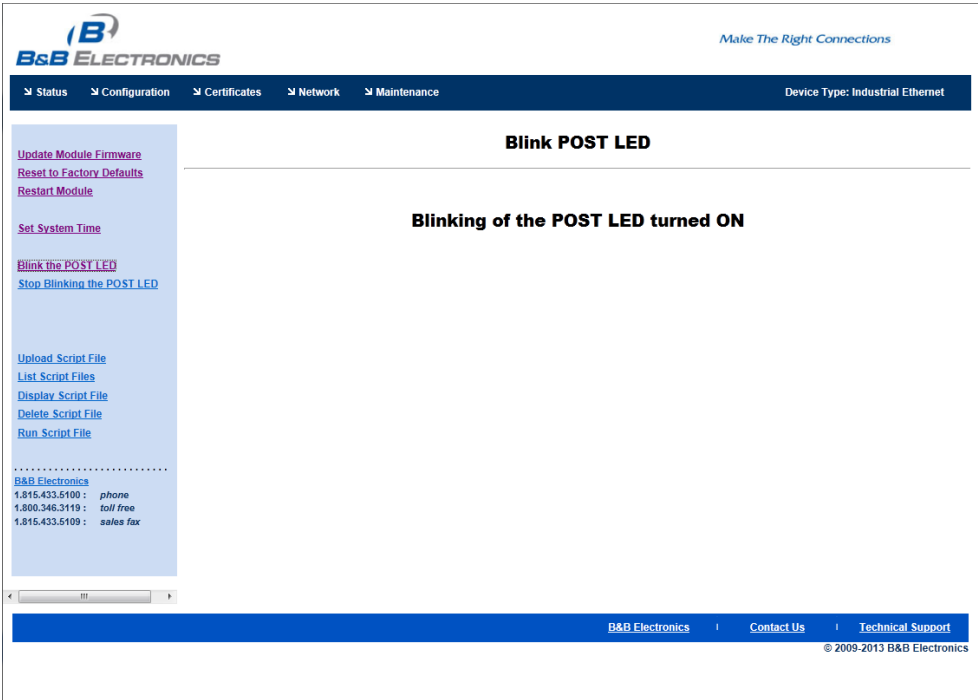
Description Sets the current system time.



| Field | CLI Command |
|--------------------------|-------------|
| Set System Time [Button] | sys-time |

Blink the POST LED

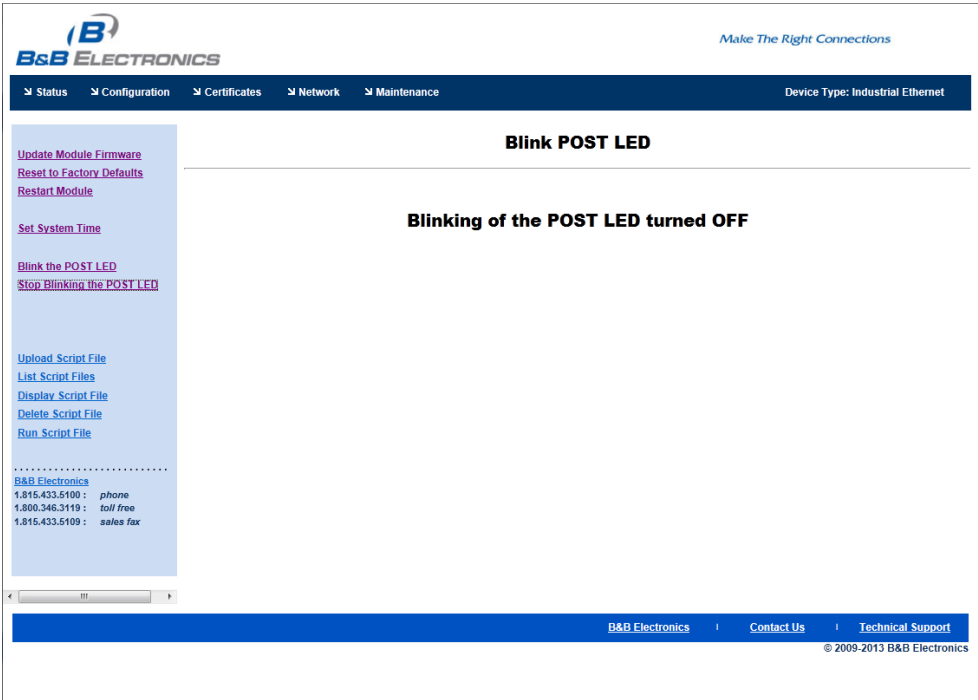
| | |
|-------------|--|
| URL | /Maintenance/Blink the POST LED |
| Description | Starts the POST LED blinking. This identifies the specific device being communicated with. |



| Field | CLI Command |
|----------------|-------------------|
| Displayed Page | blink-post-led on |

Stop Blinking the POST LED

| | |
|-------------|---|
| URL | /Maintenance/Stop Blinking the POST LED |
| Description | Stops the POST LED blinking. |



| Field | CLI Command |
|----------------|--------------------|
| Displayed Page | blink-post-led off |

25.0 Certification & Regulatory Approvals

The unit complies with the following agency approvals:

Table 48 - Regulatory Approvals

| Country | Standard | Status |
|--------------------------------|--|----------|
| North America (US & Canada) | FCC Part 15 Sec. 15.107, 15.109, 15.207, 15.209, 15.247 Modular Approval | Complete |
| Europe | CISPR 16-1 :1993 ETSI EN 300 328 Part 1 V1.2.2 (2000-07) ETSI EN 300 328 Part 2 V1.1.1 (2000-07) | Complete |
| Japan | ARIB STD-T71 v1.0, 14 (Dec 2000) ARIB RCR STD-T33 (June 19, 1997) ARIB STD-T66 v2.0 (March 28, 2002) | Pending |

25.1 FCC Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for assistance.

25.2 FCC RF Exposure Statement

To satisfy RF exposure requirements, this device and its antenna must operate with a separation distance of a least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

25.3 Information for Canadian Users (IC Notice)

This device has been designed to operate with an antenna having a maximum gain of 5dBi for 802.11b/g and 802.11a bands. An antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than required for successful communication.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

25.4 FCC/IC Modular Approval

This document describes the Airborne WLN FCC modular approval and the guidelines for use as outlined in FCC Public Notice (DA-00-1407A1).

The ABDx-XX-DP501 is covered by the following modular grants:

Table 49 - Modular Approval Grant Numbers

| Country | Standard | Grant |
|--------------------|--|---------------|
| North America (US) | FCC Part 15 Sec. 15.107, 15.109, 15.207, 15.209, 15.247 Modular Approval | F4AWLNN551 |
| Canada | RSS 210 Modular Approval | 3913A-WLNN551 |

By providing FCC modular approval on the Airborne WLN modules, the customers are relieved of any need to perform FCC part15 subpart C Intentional Radiator testing and certification, except where they wish to use an antenna that is not already certified.

B&B Electronics supports a group of pre-approved antenna; use of one of these antennas eliminates the need to do any further subpart C testing or certification. If an antenna is not on the list, it is a simple process to add it to the pre-approved list without having to complete a full set of emissions testing. Please contact B&B Electronics Technical support for details of our qualification processes.

Please note that as part of the FCC requirements for the use of the modular approval, the installation of any antenna must require a professional installer. This is to prevent any non-authorized antenna being used with the radio. There are ways to support this requirement but the most popular is to utilize a non-standard antenna connector, this designation includes the reverse polarity versions of the most popular RF antenna types (SMA, TNC, etc.). For more details please contact B&B Electronics.

The following documents are associated with this applications note:

- FCC Part 15 – Radio Frequency Devices
- FCC Public Notice – DA-00-1407A1 (June 26th, 2000)

B&B Electronics recommends that during the integration of the radio, into the customers system, that any design guidelines be followed. Please contact B&B Electronics Technical Support if you have any concerns regarding the hardware integration.

Contact B&B Electronics Technical support for a copy of the FCC and IC grant certificates, the test reports and updated approved antenna list.

25.5 Regulatory Test Mode Support

The Airborne Device Server includes support for all FCC, IC and ETSI test modes required to perform regulatory compliance testing on the module, please contact B&B Electronics Technical Support for details on enabling and using these modes.

26.0 Physical & Environmental Approvals

The device has passed the following primary physical and environmental tests. The test methods referenced are defined in SAE J1455 Aug1994.

Table 50 - Mechanical Approvals

| Test | Reference | Conditions |
|-------------------------------------|-------------------|--|
| Temperature Range (Operational) | Table 1B, Type 2b | -40°C to +85°C |
| Temperature Range (Non-Operational) | | -50°C to +125°C |
| Humidity | Sect 4.2.3 | 0-95%RH @ 38°C condensing Fig 4a – 8 hours active humidity cycle |
| Altitude | Sect 4.8 | Operational: 0-12,000ft (62 KPa absolute pressure) Non-operational: 0-40,000ft (18.6 KPa absolute pressure) |
| Vibration | Sect 4.9 | Operational: 2.4 Grms, 10-1K Hz, 1hr per axis Non-operational: 5.2 Grms, 10-1K Hz, 1hr per axis |
| Shock | Sect 4.10 | Operational: 20Gs MAX, 11ms half-sine pulse |
| Product Drop | Sect 4.10.3.1 | 1m onto concrete, any face or corner, 1 drop |
| Packaging Drop | Sect 4.10.2.1 | 32 inches onto concrete on each face and corner. Packaged in 'for transit' configuration. |

Test reports are available from B&B Electronics Technical Support, please contact directly for the latest documentation.

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

B&B Electronics:

[ABDN-SE-IN5420](#) [APXN-Q5428](#) [ABDN-ER-DP553](#) [ABDN-ER-IN5018](#) [ABDN-SE-IN5410](#) [ABDN-ER-DP551](#) [ABDN-ER-IN5010](#)