

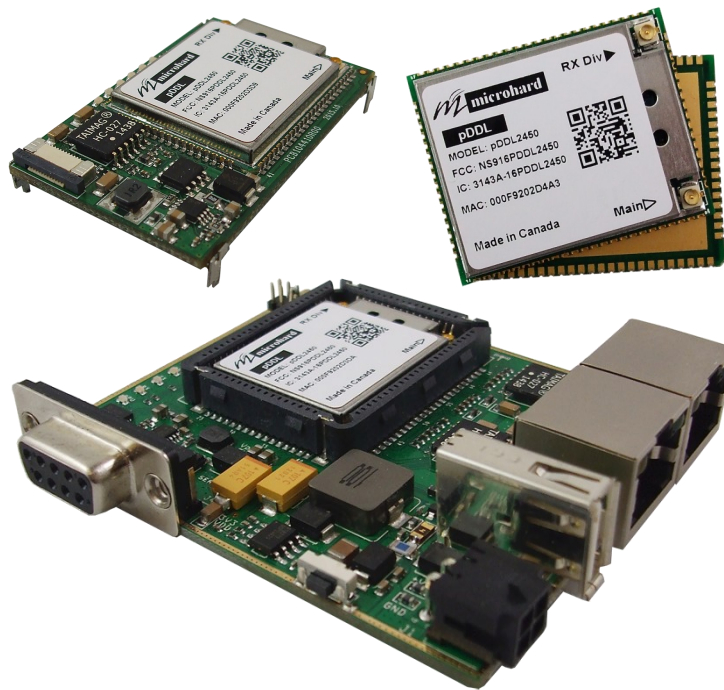
# Operating Manual

## pDDL2450

2.4 GHz 1W OEM Wireless Digital Data Link

Document: pDDL.Operating Manual.v1.2.2.pdf  
FW: v1.3.0 Build 1026

February 2017



## Important User Information

---

### Warranty

Microhard Systems Inc. warrants that each product will be free of defects in material and workmanship for a period of one (1) year for its products. The warranty commences on the date the product is shipped by Microhard Systems Inc. Microhard Systems Inc.'s sole liability and responsibility under this warranty is to repair or replace any product which is returned to it by the Buyer and which Microhard Systems Inc. determines does not conform to the warranty. Product returned to Microhard Systems Inc. for warranty service will be shipped to Microhard Systems Inc. at Buyer's expense and will be returned to Buyer at Microhard Systems Inc.'s expense. In no event shall Microhard Systems Inc. be responsible under this warranty for any defect which is caused by negligence, misuse or mistreatment of a product or for any unit which has been altered or modified in any way. The warranty of replacement shall terminate with the warranty of the product.

### Warranty Disclaims

Microhard Systems Inc. makes no warranties of any nature of kind, expressed or implied, with respect to the hardware, software, and/or products and hereby disclaims any and all such warranties, including but not limited to warranty of non-infringement, implied warranties of merchantability for a particular purpose, any interruption or loss of the hardware, software, and/or product, any delay in providing the hardware, software, and/or product or correcting any defect in the hardware, software, and/or product, or any other warranty. The Purchaser represents and warrants that Microhard Systems Inc. has not made any such warranties to the Purchaser or its agents MICROHARD SYSTEMS INC. EXPRESS WARRANTY TO BUYER CONSTITUTES MICROHARD SYSTEMS INC. SOLE LIABILITY AND THE BUYER'S SOLE REMEDIES. EXCEPT AS THUS PROVIDED, MICROHARD SYSTEMS INC. DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PROMISE.

**MICROHARD SYSTEMS INC. PRODUCTS ARE NOT DESIGNED OR INTENDED TO BE USED IN ANY LIFE SUPPORT RELATED DEVICE OR SYSTEM RELATED FUNCTIONS NOR AS PART OF ANY OTHER CRITICAL SYSTEM AND ARE GRANTED NO FUNCTIONAL WARRANTY.**

### Indemnification

The Purchaser shall indemnify Microhard Systems Inc. and its respective directors, officers, employees, successors and assigns including any subsidiaries, related corporations, or affiliates, shall be released and discharged from any and all manner of action, causes of action, liability, losses, damages, suits, dues, sums of money, expenses (including legal fees), general damages, special damages, including without limitation, claims for personal injuries, death or property damage related to the products sold hereunder, costs and demands of every and any kind and nature whatsoever at law.

IN NO EVENT WILL MICROHARD SYSTEMS INC. BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, BUSINESS INTERRUPTION, CATASTROPHIC, PUNITIVE OR OTHER DAMAGES WHICH MAY BE CLAIMED TO ARISE IN CONNECTION WITH THE HARDWARE, REGARDLESS OF THE LEGAL THEORY BEHIND SUCH CLAIMS, WHETHER IN TORT, CONTRACT OR UNDER ANY APPLICABLE STATUTORY OR REGULATORY LAWS, RULES, REGULATIONS, EXECUTIVE OR ADMINISTRATIVE ORDERS OR DECLARATIONS OR OTHERWISE, EVEN IF MICROHARD SYSTEMS INC. HAS BEEN ADVISED OR OTHERWISE HAS KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND TAKES NO ACTION TO PREVENT OR MINIMIZE SUCH DAMAGES. IN THE EVENT THAT REGARDLESS OF THE WARRANTY DISCLAIMERS AND HOLD HARMLESS PROVISIONS INCLUDED ABOVE MICROHARD SYSTEMS INC. IS SOMEHOW HELD LIABLE OR RESPONSIBLE FOR ANY DAMAGE OR INJURY, MICROHARD SYSTEMS INC.'S LIABILITY FOR ANY DAMAGES SHALL NOT EXCEED THE PROFIT REALIZED BY MICROHARD SYSTEMS INC. ON THE SALE OR PROVISION OF THE HARDWARE TO THE CUSTOMER.

### Proprietary Rights

The Buyer hereby acknowledges that Microhard Systems Inc. has a proprietary interest and intellectual property rights in the Hardware, Software and/or Products. The Purchaser shall not (i) remove any copyright, trade secret, trademark or other evidence of Microhard Systems Inc.'s ownership or proprietary interest or confidentiality other proprietary notices contained on, or in, the Hardware, Software or Products, (ii) reproduce or modify any Hardware, Software or Products or make any copies thereof, (iii) reverse assemble, reverse engineer or decompile any Software or copy thereof in whole or in part, (iv) sell, transfer or otherwise make available to others the Hardware, Software, or Products or documentation thereof or any copy thereof, except in accordance with this Agreement.

## Important User Information (continued)

---

### About This Manual

It is assumed that users of the products described herein have either system integration or design experience, as well as an understanding of the fundamentals of radio communications.

Throughout this manual you will encounter not only illustrations (that further elaborate on the accompanying text), but also several symbols which you should be attentive to:

**Caution or Warning**

Usually advises against some action which could result in undesired or detrimental consequences.

**Point to Remember**

Highlights a key feature, point, or step which is noteworthy. Keeping these in mind will simplify or enhance device usage.

**Tip**

An idea or suggestion to improve efficiency or enhance usefulness.

**Information**

Information regarding a particular technology or concept.

## Important User Information (continued)

### Regulatory Requirements / Exigences Réglementaires



#### **WARNING:**

To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 23 cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.



#### **WARNING:**

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



#### **WARNING:**

Changes or modifications not expressly approved by Microhard Systems Inc. could void the user's authority to operate the equipment. This device has been tested with UFL to Reverse Polarity SMA connectors with the antennas listed in Appendix A. When integrated in OEM products, fixed antennas require installation preventing end-users from replacing them with non-approved antennas. Antennas not listed in the tables must be tested to comply with FCC Section 15.203 (unique antenna connectors) and Section 15.247 (emissions).



#### **WARNING:**

##### **MAXIMUM EIRP**

FCC Regulations allow up to 36 dBm equivalent isotropically radiated power (EIRP). Therefore, the sum of the transmitted power (in dBm), the cabling loss and the antenna gain cannot exceed 36 dBm.



#### **WARNING:**

##### **EQUIPMENT LABELING**

The FCC and IC numbers depend on the model of the radio module. Do NOT use the Marketing Name of the product but the Model to distinguish the Certifications Numbers. This device has been modularly approved. The manufacturer, product name, and FCC and Industry Canada identifiers of this product must appear on the outside label of the end-user equipment.



#### **WARNING:**

This device complies with Industry Canada's license-exempt RSSs. 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.

### SAMPLE LABEL REQUIREMENT / EXIGENCE D'ÉTIQUETTE: pDDL

FCCID: NS916PDDL2450  
IC: 3143A-16PDDL2450

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

Please Note: These are only sample labels; different products contain different identifiers. The actual identifiers should be seen on your devices if applicable.

## Important User Information (continued)

### Regulatory Requirements / Exigences Réglementaires



#### **WARNING:**

*Pour satisfaire aux exigences de la FCC d'exposition RF pour la base et mobiles sur une distance de séparation de 23 cm ou plus doit être maintenue entre l'antenne de cet appareil et des personnes lors de fonctionnement du dispositif. Pour assurer la conformité des opérations au plus près que cette distance n'est pas recommandée. L'antenne utilisée pour ce transmetteur ne doit pas être co-localisés en conjonction avec toute autre antenne ou transmetteur.*



#### **WARNING:**

Son fonctionnement est soumis aux deux conditions suivantes : ( 1 ) ce dispositif ne doit pas causer d'interférences nuisibles et ( 2 ) cet appareil doit accepter toute interférence reçue, incluant les interférences qui peuvent provoquer un fonctionnement indésirable .



#### **WARNING:**

Les changements ou modifications non expressément approuvés par Microhard Systems Inc. pourraient annuler l'autorité de l'utilisateur à utiliser l'équipement . Ce dispositif a été testé avec MCX et connecteurs SMA à polarité inverse sur les antennes répertoriées à l'annexe A Lorsqu'il est intégré dans les produits OEM , antennes fixes nécessitent une installation empêchant les utilisateurs finaux de les remplacer par des antennes non approuvées . Antennes ne figurant pas dans les tableaux doivent être testés pour se conformer à la Section 15.203 (connecteurs d'antenne uniques ) et à la Section 15.247 ( émissions ) .



#### **WARNING:**

##### **MAXIMUM EIRP**

Règlement FCC permettent jusqu'à 36 dBm puissance isotrope rayonnée équivalente ( EIRP ) . Par conséquent, la somme de la puissance émise ( en dBm ), la perte de câblage et le gain d'antenne ne peut pas dépasser 36 dBm.



#### **WARNING:**

##### **ÉQUIPEMENT DE MARQUAGE**

Les numéros FCC et IC dépendent du modèle du module radio . Ne pas utiliser le nom marketing du produit, mais le modèle de distinguer les numéros Certifications . Ce dispositif a été approuvé de façon modulaire . Le fabricant , nom du produit, et les identificateurs de la FCC et d'Industrie Canada de ce produit doivent figurer sur l'étiquette à l'extérieur de l'équipement de l'utilisateur final .



#### **WARNING:**

Cet appareil est conforme aux CNR exempts de licence d'Industrie Canada . Son fonctionnement est soumis aux deux conditions suivantes : ( 1 ) Ce dispositif ne peut causer des interférences ; et ( 2 ) Ce dispositif doit accepter toute interférence , y compris les interférences qui peuvent causer un mauvais fonctionnement de l'appareil.

### SAMPLE LABEL REQUIREMENT / EXIGENCE D'ÉTIQUETTE: pDDL

FCCID: NS916PDDL2450  
IC: 3143A-16PDDL2450

This device complies with Part 15 of the FCC Rules.  
Operation is subject to the following two conditions:  
(1) this device may not cause harmful interference,  
and (2) this device must accept any interference  
received including interference that may cause  
undesired operation.

Please Note: S'il vous plaît noter: Ce sont des exemples d'étiquettes seulement; différents produits contiennent des identifiants différents. Les identifiants réels devrait être vu sur vos périphériques le cas échéant.

## Revision History

Revision	Description	Initials	Date
0.0	Preliminary Release. Based on Firmware v1.3.0 Build 1009-52	PEH	Feb 2016
0.1	Added current specifications.	PEH	Mar 2016
0.2	Updated Images. Added info for video applications (Wireless).	PEH	Mar 2016
0.3	Added Rx Diversity Enable (Wireless), Misc Updates. Build 1009-68	PEH	Mar 2016
0.4	Updated Wireless (RF). Firmware v1.3.0 Build 1010	PEH	Apr 2016
0.5	Updated Quick Start to include using defaults (Auto). Added Channel Selection Tool. Updated defaults. Firmware v1.3.0 Build 1011-6.	PEH	Apr 2016
0.6	Updated images, added FCC/IC numbers.	PEH	Apr 2016
1.0	Removed Channel Selection Tool. Updated to Firmware v1.3.0 Build 1012	PEH	Apr 2016
1.1.0	Added SMT temperature profile and baking instructions	PEH	May 2016
1.1.1	Added Appendix D: Serial Port Extension	PEH	May 2016
1.1.2	Updated Images	PEH	June 2016
1.2.0	Updated Logo's, Screenshots, Added USB RNDIS Support	PEH	Nov 2016
1.2.1	Updated to Firmware v1.3.0-r1024. Updated AT Commands.	PEH	Jan 2017
1.2.2	Updated to firmware v1.3.0-r1026.	PEH	Feb 2017



## Table of Contents

<b>1.0 Overview .....</b>	<b>10</b>
1.1 Performance Features .....	10
1.2 Specifications .....	11
1.3 pDDL Performance.....	13
<b>2.0 QUICK START .....</b>	<b>14</b>
2.1 Getting Started .....	14
2.2 Simple Master and Slave (Auto - Using Defaults).....	16
2.3 Simple Master and Slave (Manual).....	17
2.3.1 Configuring the Master .....	17
2.3.2 Configuring the Slave /Remote .....	19
2.3.3 Testing the Connection .....	21
<b>3.0 Hardware Features .....</b>	<b>22</b>
3.1 pDDL OEM.....	22
3.1.1 pDDL Mechanical Drawings .....	23
3.1.2 Recommended Solder Mask (Pad Landing) .....	24
3.1.3 Recommended Solder Paste Pattern.....	25
3.1.4 OEM Connectors .....	25
3.1.5 SMT Temperature Profile .....	26
3.1.6 SMT Baking Instructions (MSL).....	26
3.1.7 OEM Pin Descriptions .....	27
3.1.8 USB Device Mode .....	29
3.2 pDDL Development Board .....	30
3.2.1 Connectors & Indicators .....	31
<b>4.0 Configuration.....</b>	<b>33</b>
<b>4.0 Web User Interface.....</b>	<b>33</b>
4.0.1 Logon Window.....	34
<b>4.1 System.....</b>	<b>35</b>
4.1.1 Summary .....	35
4.1.2 Settings.....	36
Host Name.....	36
Date/Time .....	37
4.1.3 Services .....	39
SSH .....	39
Telnet.....	39
HTTP/HTTPS .....	39
4.1.4 Maintenance .....	40
Firmware Upgrade.....	40
Backup & Restore Configurations .....	41
4.1.5 Reboot.....	42
<b>4.2 Network .....</b>	<b>43</b>
4.2.1 Status .....	43
4.2.2 LAN.....	44
LAN DHCP .....	46
4.2.3 WAN .....	48
4.2.4 USB .....	50
4.2.5 DHCP (MAC Binding) .....	51
4.2.6 Routes .....	52
4.2.7 Ports .....	54
4.2.8 Device List .....	55





# Table of Contents

## 1.0 Overview

---

The pDDL is a feature rich, high power, OEM, Wireless Digital Data Link. The pDDL is designed to provide high performance wireless capabilities in a compact and rugged OEM module for system integration. The pDDL features simultaneous dual 10/100 Ethernet & Serial (RS232) Gateway capabilities for high speed wireless applications

The pDDL can be configured using a built-in WebUI interface which does not require any additional software or tools to setup or download. The unit can operate as a Master or Slave to establish long range wireless links between locations.

Providing reliable wireless Ethernet bridge functionality as well gateway service for most equipment types which employ an RS232 interface, the pDDL can be used in various types of applications such as:

- High-speed backbone
- IP video surveillance
- Voice over IP (VoIP)
- Ethernet wireless extension
- Mobile Internet
- Legacy network/device migration
- SCADA
- Display Signs
- Fleet Services
- Remote Telemetry
- Multicast Video

### 1.1 Performance Features

Key performance features of the pDDL include:

- High Power Tx (up to 1W) w/ Excellent Rx Sensitivity
- Up to 25 Mbps data rate\*
- Master, Slave/Remote operating modes
- Point to Point, Point to Multipoint, Mesh (future) topology support
- Firewall with ACL Security, Port Forwarding
- Serial Gateway (RS232)
- Dual 10/100 Ethernet Ports
- RSSI LED pins for Antenna Alignments
- Industrial grade operating temperature (-40°C to +85°C)
- Administration via local console, telnet, web browser, SNMP
- Local and remote wireless firmware upgradable

\* See [Section 1.3 Performance Specifications](#)

## 1.0 Overview

### 1.2 Specifications

For detailed specifications, please see the specification sheets available on the Microhard website @ <http://www.microhardcorp.com> for your specific model.

#### Electrical/General

<b>Frequency:</b>	2.402 - 2.482 GHz
<b>Link Rate:</b>	See <u>Section 1.3 Performance Specifications</u>
<b>TX Power:</b>	20 dBm - 30 dBm (Selectable)
<b>Channel Bandwidth:</b>	1, 2, 4, 8 MHz (Selectable)
<b>Error Detection/Control:</b>	CRC, ARQ
<b>Data Encryption*:</b> (*Requires Export Permit)	128-bit AES (Optional 256-bit)
<b>Serial Port:</b>	300bps to 921kbps - TTL Level RS232
<b>Ethernet:</b>	Dual 10/100 BaseT, Auto - MDI/X, IEEE 802.3
<b>USB:</b>	2.0
<b>Network Protocols:</b>	TCP, UDP, TCP/IP, ARP, ICMP, DHCP, HTTP, HTTPS*, SSH*, SNMP, FTP, DNS, Serial over IP (*May require an export permit)
<b>Operating Modes:</b>	Master, Slave/Remote
<b>Management:</b>	Local Serial Console, Telnet, WebUI, SNMP, FTP & Wireless Upgrade
<b>Diagnostics:</b>	Status LED's, RSSI, remote diagnostics, SNR
<b>Input Voltage:</b>	Digital Voltage: 3.3 VDC (500mA) RF Voltage: 5.0 VDC (2.5A)
<b>Current:</b>	

	Tx Power (dBm)	Vcc @ 3.3V	VRF @ 5V
Peak Avg. Transmit Current (mA)	20	360 - 400	360
	22	360 - 400	400
	24	360 - 400	450
	26	360 - 400	500
	28	360 - 400	580
	30	360 - 400	700
Instantaneous Current Draw	-	500	2500
Typical Receive Current Draw (mA)	-	360-400	-

Table 1-1: pDDL Current Consumption

## 1.0 Overview

---

### Environmental

**Operation Temperature:** -40°F(-40°C) to 185°F(85°C)

**Humidity:** 5% to 95% non-condensing

### Mechanical

**Dimensions:** 1.05" (26.5mm) X 1.3" (33mm) X 0.13" (3.5mm)

**Weight:** Approx. 5 grams

**Connectors:** Antenna: UFL x2 (Main, Diversity)  
Data: 80 Pin SMT

## 1.0 Overview

### 1.3 Performance Specifications

Modulation	Multicast IPerf Throughput (Mbps)	Throughput @ Sensitivity (dBm)	Maximum Tx Power (dBm) +/- 1dB
<b>8 MHz Channel Bandwidth</b>			
BPSK_1/2	3	-96	30dBm
QPSK_1/2	6	-94	30dBm
QPSK_3/4	9	-91	30dBm
16QAM_1/2	12	-88	29dBm
16QAM_3/4	17	-85	29dBm
64QAM_2/3	23	-80	27dBm
64QAM_3/4	25	-78	27dBm
64QAM_5/6	28	-76	27dBm
<b>4 MHz Channel Bandwidth</b>			
BPSK_1/2	1.5	-99	30dBm
QPSK_1/2	3	-98	30dBm
QPSK_3/4	4.5	-96	30dBm
16QAM_1/2	6	-92	29dBm
16QAM_3/4	9	-88	29dBm
64QAM_2/3	11.5	-83	27dBm
64QAM_3/4	12.5	-82	27dBm
64QAM_5/6	14	-80	27dBm
<b>2 MHz Channel Bandwidth</b>			
BPSK_1/2	0.78	-101	30dBm
QPSK_1/2	1.5	-100	30dBm
QPSK_3/4	2.2	-97	30dBm
16QAM_1/2	2.9	-93	29dBm
16QAM_3/4	4.3	-90	29dBm
64QAM_2/3	5.5	-86	27dBm
64QAM_3/4	6	-84	27dBm
64QAM_5/6	6.5	-82	27dBm

Table 1-2: pDDL Performance Specifications

## 2.0 Quick Start

This QUICK START guide will walk you through the setup and configuration of a few basic applications. The QUICK START will rely on the *WebUI* for configuration. This walkthrough also assumes the units used are installed in microhard interface/development boards or custom boards that allow access to the LAN port. See the appropriate section for pin-outs.

Note that the units arrive from the factory with a Radio Configuration of 'Master' and the Local Network setting configured as 'Static' (IP Address **192.168.168.1**, Subnet Mask 255.255.255.0). DHCP is enabled by default, and will assign an IP to a connected device or computer with DHCP enabled.

### 2.1 Getting Started

- ✓ Connect an appropriate Antenna to the **ANTENNA** connector of the pDDL.
- ✓ Connect and/or apply a suitable power source to the unit. Allow the unit to boot up fully, the CPU LED (Blue) should be on in a solid state
- ✓ Connect A PC to the **LAN** port (eth0) of the pDDL, using an Ethernet Cable.

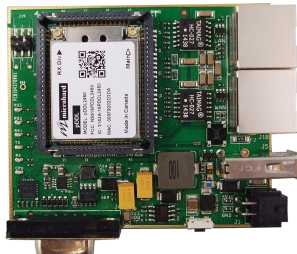


To reset to factory defaults, press and hold the CONFIG for 8 seconds with the pDDL powered up. The pDDL will reboot with factory default settings.



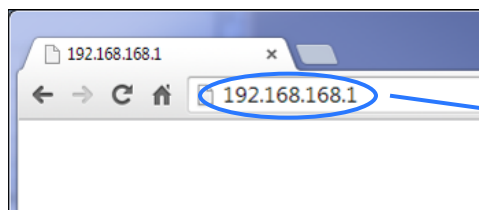
The factory default network settings:

IP: **192.168.168.1**  
Subnet: **255.255.255.0**



← LAN

- ✓ The PC must have its Network Setting (TCP/IP Properties) set to DHCP (The modem will assign a IP address to you), or STATIC with an IP Address of (e.g.) 192.168.168.10 and a Subnet Mask of 255.255.255.0.
- ✓ Open a Browser Window and enter the IP address 192.168.168.1 into the address bar.



→ 192.168.168.1

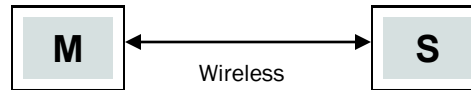




## 2.0 Quick Start

### 2.2 Simple Master and Slave - Auto (Using Defaults)

This **Quick Start** example requires (2) pDDL units, one will be configured as a Master (M), the second unit will be configured as a Slave/Remote (S). This example will use factory defaults to set up each unit so that a simple network will be established.



- ✓ Use [Section 2.1 Getting Started](#) to power up a pair of pDDL modules mounted in a Pico Ethernet Motherboard.
- ✓ **Master:** Once the pDDL is fully booted (solid blue CPU LED), press and hold the CFG button. Once the CPU LED begins to flash, continue to hold for at least **10 seconds**, then release.



Press and hold **CFG** button for at least **10 seconds** to reset to a default Master pDDL

Press and hold **CFG** button for **5 seconds** to reset to a default Slave pDDL

CPU LED (Blue)

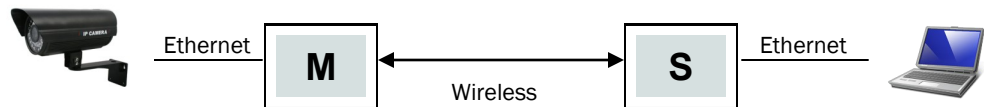
RSSI LEDs (Green)

- ✓ The pDDL will then reset all settings to default values, and set the following settings that are required to automatically create a link with a slave:
  - IP Address: **192.168.168.1**, Operating Mode: **Master**
  - Network ID: **pDDL**, Channel Bandwidth: **8 MHz**
  - Channel-Frequency: **76 - 2477 MHz**
- ✓ **Slave:** Ensure the pDDL is fully booted (solid blue CPU LED), then press and hold the CFG button. Once the CPU LED begins to flash, continue to hold for **5 seconds**, then release.
- ✓ The pDDL will then reset all settings to default values, and set the following settings that are required to automatically create a link with a slave:
  - IP Address: **192.168.168.2**, Operating Mode: **Slave**
  - Network ID: **pDDL**, Channel Bandwidth: **8 MHz**
  - Channel-Frequency: **76 - 2477 MHz**
- ✓ Once both units have finished changing settings (~60 seconds) a wireless link should automatically be established between them, this can be seen by observing the RSSI LEDs, they should be on solid, indicating a link (the more LEDs illuminated = stronger the link).

## 2.0 Quick Start

### 2.3 Simple Master and Slave — Manual Setup

This **Quick Start** example requires (2) pDDL units, one will be configured as a Master (M), the second unit will be configured as a Slave/Remote (S). This example will show the basic steps required to set up each unit so that a simple network will be established.



For the best performance it is required to connect the Master to the video source (camera) and the remote to the video receiver. The pDDL can support Point-to-Multipoint applications and multiple remotes could be used to view the video from multiple locations.

#### 2.3.1 Configuring the Master

- ✓ Use **Section 2.1 Getting Started** to connect, power up and log in to a pDDL unit.
- ✓ Give the pDDL unit a unique IP address.



To connect to an existing network, contact your Network Administrator for valid network settings.

Select **Network** from the top/main navigation.

Select **LAN** from the submenu list.  
Select Edit on the LAN interface 1.

System	Network	Wireless	Firewall
Status	LAN	WAN	Routes
	Ports	Device	
Network LAN Configuration			
LAN Interfaces Settings			
No.	Name	Static IP Address	
1	lan	192.168.168.1	

Choose **Static IP** for the **Connection Type**.

Enter the following Network Information:

**IP Address:** 192.168.168.11  
**IP Subnet Mask:** 255.255.255.0

LAN Configuration	
Spanning Tree (STP)	Off
Connection Type	Static IP
IP Address	192.168.168.11
Netmask	255.255.255.0
Default Gateway	

Click on the **Submit** button to write the changes to the pDDL. The **Cancel** button will revert back to last values saved to the unit.

Refer to **Section 5.2.2 LAN** for additional information.

**Once the IP Address is changed, you will need to type the new address into your browser to continue the configuration.**

## 2.0 Quick Start

### 2.3.1 Configuring the Master (Con't)

- ✓ Configure the pDDL as a Master

Select **Wireless** from the top/main navigation, and then **RF** from the submenu list.



RF Configuration	
Radio	<input checked="" type="radio"/> On <input type="radio"/> Off
Compatibility Mode	pDDL
Channel Bandwidth	8MHz
Channel-Frequency	76 - 2477 MHz
Tx Power	20 dbm
Wireless Distance	3000
Rx Diversity(Reboot Required)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

In the **RF Configuration** ensure the **Compatibility Mode**, **Channel Bandwidth** and **Channel-Frequency** are set the same on each module.


*If a Antenna is not physically connected to the **Rx Diversity** connector, ensure it is disabled in this menu.*

For bench or close proximity testing it is best to use a lower power setting to prevent RF saturation. Select 20dBm from the **TX Power** setting.

Select **Master** from the **Operation Mode** dropdown box.

Set a **Network ID**, which will need to be the same on each unit in the network. This example uses **TEST\_ID**.

Operation Mode	Master
TX Rate	Auto
Extended Addressing	<input checked="" type="radio"/> On <input type="radio"/> Off
Network ID	TEST_ID
Encryption Type	AES-128
Encryption Key	1234567890
Show password	<input checked="" type="checkbox"/>

Wireless Configuration	
<b>RF Configuration</b>	
Radio	<input checked="" type="radio"/> On <input type="radio"/> Off
Compatibility Mode	pDDL
Channel Bandwidth	8MHz
Channel-Frequency	76 - 2477 MHz
Tx Power	20 dbm
Wireless Distance	3000 (m)
Rx Diversity(Reboot Required)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Channel Selection	
<b>Operation Mode</b>	
Operation Mode	Master
TX Rate	Auto (recommended)
Extended Addressing	<input checked="" type="radio"/> On <input type="radio"/> Off
Network ID	TEST_ID
Encryption Type	AES-128
Encryption Key	*****
Show password	<input type="checkbox"/>



If any additional settings need to be changed, ensure they are also changed on the Slave.

The remaining settings in the **Wireless** menu should be left as defaults for this exercise.

Refer to **Section 5.3 Wireless** for additional information.

Click on the **Submit** button to write the changes to the pDDL. The **Cancel** button will revert back to previously saved values

## 2.0 Quick Start

### 2.3.2 Configuring the Slave/Remote

The following procedure describes the steps required to set up a pDDL unit as a Slave (S). A Slave provides a single wireless connection (i.e to an Master) and provides a wired connection to a PC or other devices.

- ✓ Use [Section 2.1 Getting Started](#) to connect, power up and log in to a second pDDL unit.
- ✓ Give the pDDL unit an unique IP address.



To connect to an existing network, contact your Network Administrator for valid network settings.

Select [Network](#) from the top/main navigation.

Select [LAN](#) from the submenu list.  
Select Edit on the LAN interface 1.

System	Network	Wireless	Firewall
Status	LAN	WAN	Routes
		Ports	Device

Network LAN Configuration		
LAN Interfaces Settings		
No.	Name	Static IP Address
1	lan	192.168.168.1

LAN Configuration	
Spanning Tree (STP)	Off ▼
Connection Type	Static IP ▼
IP Address	192.168.168.12
Netmask	255.255.255.0
Default Gateway	192.168.168.11

Choose [Static IP](#) for the [Connection Type](#).

Enter the following Network Information:

**IP Address:** 192.168.168.12  
**IP Subnet Mask:** 255.255.255.0  
**Default Gateway:** 192.168.168.11

Click on the [Submit](#) button to write the changes to the pDDL. The [Cancel](#) button will revert back to last values saved to the unit.

**Once the IP Address is changed, you will need to type the new address into your browser to continue the configuration.**

Refer to [Section 5.2.2 LAN](#) for additional information.

## 2.0 Quick Start

### 2.3.3 Configuring the Slave/Remote (Con't)

- ✓ Configure the pDDL as a Slave

Select **Wireless** from the top/main navigation, and then **RF** from the submenu list.



RF Configuration	
Radio	<input checked="" type="radio"/> On <input type="radio"/> Off
Compatibility Mode	pDDL ▼
Channel Bandwidth	8MHz ▼
Channel-Frequency	76 - 2477 MHz ▼
Tx Power	20 dbm ▼
Wireless Distance	3000
Rx Diversity(Reboot Required)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

In the RF Configuration ensure the **Compatibility Mode**, **Channel Bandwidth** and **Channel-Frequency** are set the same on each module.

*If a Antenna is not physically connected to the Rx Diversity connector, ensure it is disabled in this menu.*

For bench or close proximity testing it is best to use a lower power setting to prevent RF saturation. Select 20dBm from the **TX Power** setting.


Select **Slave** from the **Operating Mode** dropdown box.

Set a **Network ID**, which will need to be the same on each unit in the network. This example uses **TEST\_ID**.

Operation Mode	Slave ▼
TX Rate	Auto (recommended) ▼
Extended Addressing	<input checked="" type="radio"/> On <input type="radio"/> Off
Network ID	TEST_ID
Encryption Type	AES-128 ▼
Encryption Key	1234567890
Show password	<input checked="" type="checkbox"/>



If any additional settings need to be changed, ensure they are also changed on the Slave.

System	Network	Wireless	Firewall	Serial	Diag	Adm
Status	RF					
Wireless Configuration						
RF Configuration						
Radio		<input checked="" type="radio"/> On <input type="radio"/> Off				
Compatibility Mode		pDDL ▼				
Channel Bandwidth		8MHz ▼				
Channel-Frequency		76 - 2477 MHz ▼				
Tx Power		20 dbm ▼				
Wireless Distance		3000 (m)				
Rx Diversity(Reboot Required)		<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
Channel Selection						
Operation Mode		Slave ▼				
TX Rate		Auto (recommended) ▼				
Extended Addressing		<input checked="" type="radio"/> On <input type="radio"/> Off				
Network ID		TEST_ID				
Encryption Type		AES-128 ▼				
Encryption Key		*****				
Show password		<input type="checkbox"/>				

The remaining settings in the **Wireless** menu should be left as defaults for this exercise.

Refer to **Section 5.3 Wireless** for additional information.

Click on the **Submit** button to write the changes to the pDDL. The **Cancel** button will revert back to previously saved values



## 2.0 Quick Start

### 2.3.3 Testing the Connection

- ✓ Visually check to see if the pDDL units are communicating.



RSSI LED's that are 'cycling' or 'scanning' indicate that the unit is searching for a signal.

The **RSSI** LED's represent signal strength, the more LED's that are illuminated, the stronger the signal. The **Wireless > Status** window also has a Connection Status section similar to that seen below:

RF Status

General Status

MAC Address	Operation Mode	Network ID	Compatibility Mode	Bandwidth	Frequency	Tx Power	Encryption Type
00:0F:92:FA:37:C5 Master		TEST_ID	pDDL	8 MHz	2.477 GHz	20 dBm	AES-128

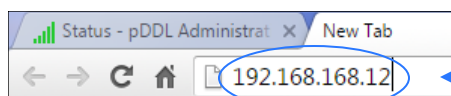
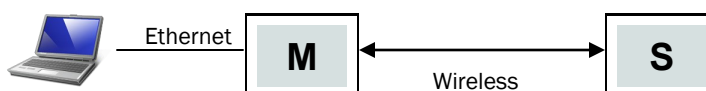
Traffic Status

Receive Bytes	Receive Packets	Transmit Bytes	Transmit Packets
104.895KB	404	77.873KB	562

Connection Info (1)

MAC Address	Tx Mod	Rx Mod	SNR (dB)	RSSI (dBm)	Signal Level	RSSI Graph
00:0F:92:FA:37:CE	64-QAM FEC 5/6	64-QAM FEC 5/6	29	-62	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div><div></div><div></div></div>

- ✓ With a PC connected to the Master (M), type in the IP address of the Slave (S) into the URL address bar of your browser. You should be able to connect, log in and view the WebUI of the Slave via the wireless connection.



Open a browser and type in the address of the slave: **192.168.168.12**

Log into the unit.

The System Summary screen should be displayed



If any additional settings need to be changed, ensure they are also changed on all radios.

Warning: This server is requesting that your user name and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

☐ Remember my password

OK

System	Network	Wireless	Firewall	Serial	Diag	Admin
Summary	Settings	Services	Maintenance	Reboot		
System Information						
System Information						
Host Name	UserDevice	Description	mypoDL			
Product Name	pDDL	System Date	2016-02-16 13:28:03			
Hardware Version	Rev A3(2MB)	System Uptime	7 min			
Software Version	v1.3.0	Build Date	2016-02-19			
Software Build	1012	Build Time	09:39:08			
LAN Status						
MAC Address	00:0F:92:02:8A:2E					
IP Address	192.168.168.12	Mode	static			
Subnet Mask	255.255.255.0	Gateway	192.168.168.1			
WAN Status						
MAC Address	00:0F:92:03:8A:2E					
IP Address	N/A	Mode	dhcp			
Subnet Mask	N/A	Gateway	N/A			

## 3.0 Hardware Features

### 3.1 pDDL OEM Module

The pDDL modems are available as OEM modules for complete integration into custom designs. The OEM module supplies all the required raw signals to allow the unit to be tightly integrated into applications to efficiently maximize space and power requirements. The Microhard development board can provide a convenient evaluation platform to test and design with the module. (Contact Microhard Systems for details)

Any pDDL module may be configured as a Master, or Slave(Remote). This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming familiar and proficient with using the module: if you are familiar with one unit, you will be familiar with all units.



Image 3-1: pDDL Top View

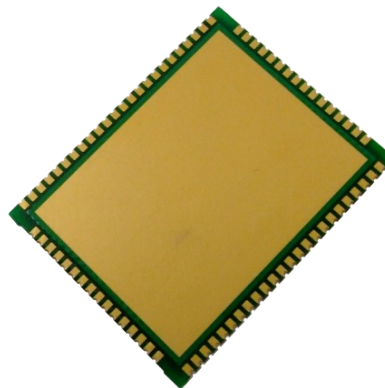
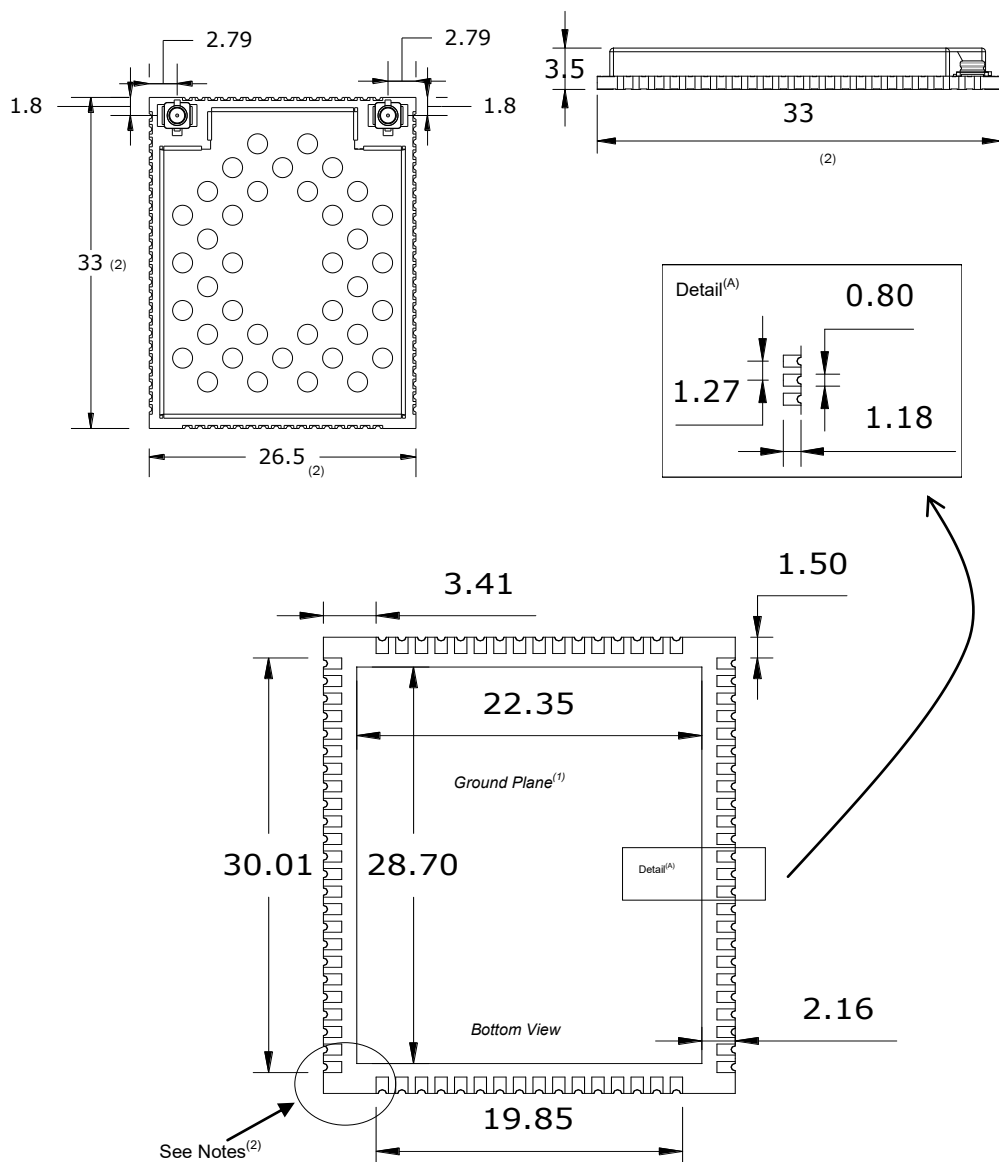


Image 3-2: pDDL Bottom View

## 3.0 Hardware Features

### 3.1.1 Mechanical Drawings

The pDDL OEM Modules have an extremely small form factor as seen *below*.



**Units: millimeters**

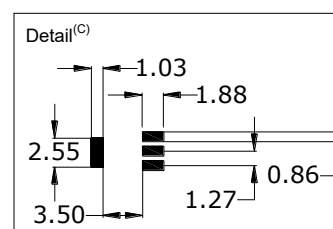
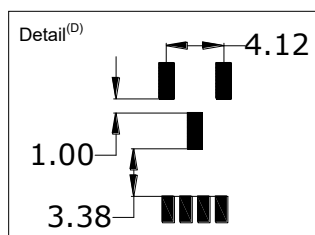
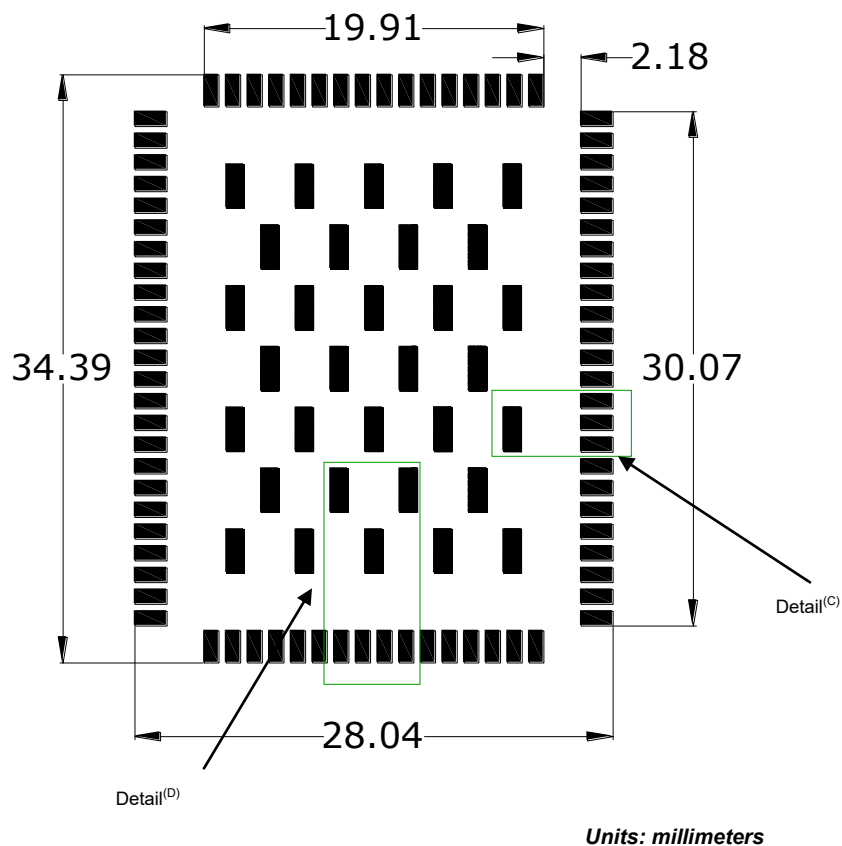
1. Ground plane must be connected to GND for required heat dissipation.
2. Due to manufacturing methods additional PCB material may be present on the corners that cannot be removed. Designs should allow for a small tolerance of this additional material,  $\pm 0.25\text{mm}$

Drawing 3-1: pDDL OEM Mechanical



### 3.0 Hardware Features

### 3.1.3 Recommended Solder Paste Pattern



*Drawing 3-3: pDDL Recommended Solder Paste*

### 3.1.4 OEM Connectors

## Antenna

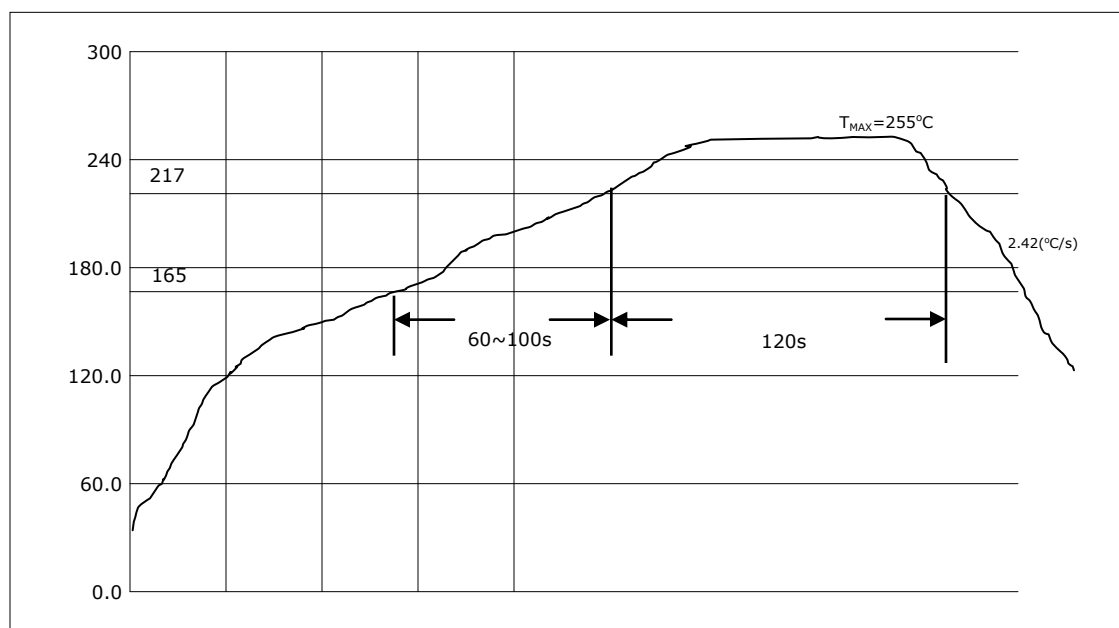
All pDDL OEM Modules use an UFL connector for the antenna connection.

## Data

The interface to the pDDL OEM module is a tight integration using 80 pad SMT connections.

## 3.0 Hardware Features

### 3.1.5 SMT Temperature Profile



Drawing 3-4: pDDL Reflow Profile

Temperature Zone	Time	Parameter
Preheat zone: (40°C - 165°C)	-	Heating rate: 0.5°C/s-2°C/s
Soak Zone: (165°C - 217°C)	60 - 100s	-
Reflow zone: (>217°C)	120s	Peak reflow: 255°C
Cooling zone	Cooling rate: 2°C/s ≤ Slope ≤ 5°C/s	

Table 3-1: pDDL Reflow Parameters

Zone	Temperature (°C)
1	120
2	140
3	160
4	180
5	215
6	255
7	255
8	255
9	250
10	130
Chain Speed: 60cm/min	

Table 3-2: pDDL Oven Temperature Profile

### 3.1.6 SMT Baking Instructions (MSL)

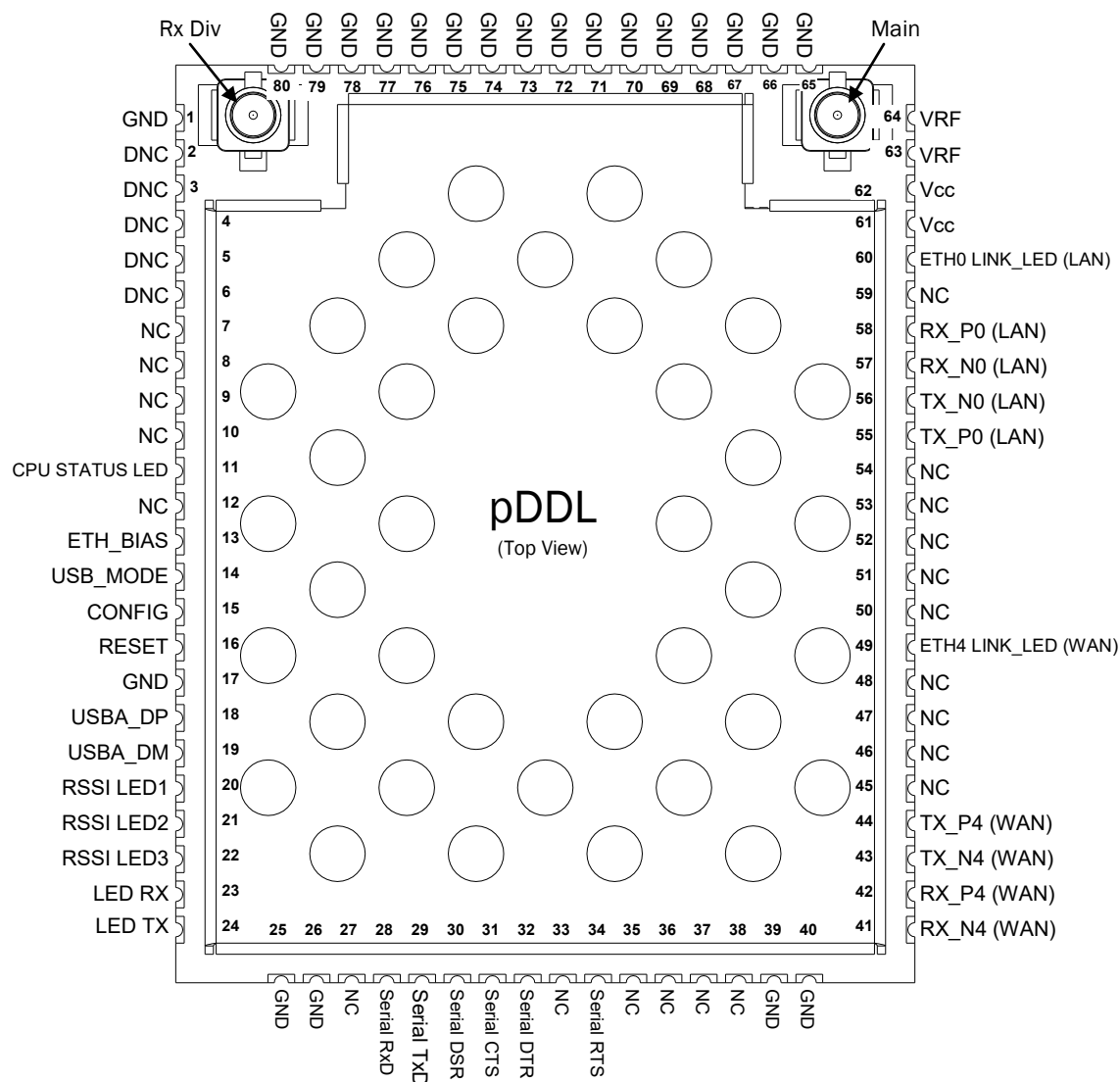
The pDDL OEM modules must be baked before mounting, the following baking instruction should be followed for the best results:

- Minimum of 8 to 12 hours at 125°C +/- 5°C for high-temperature device containers.
- Unused modules should be stored at ≤ 10% RH



## 3.0 Hardware Features

### 3.1.7 Pico OEM Pin Descriptions



Drawing 3-5: pDDL 80-pin OEM Connection Info

Inputs and outputs are 3.3V nominal (3.0V min — 3.6V max) unless otherwise specified.

The above drawing depicts a top view of the pDDL OEM Module. A full description of the connections and function of each pin is provided on the pages that follow.

## 3.0 Hardware Features



**Caution:** During power up or reset, output pins from the Pico are in an unknown state. It is advised to use pull up or pull down resistors as appropriate.

Pin Name	No.	Description	Dir
GND	1, 17, 25-26, 39-40, 65-80	Ground reference for logic, radio, and I/O pins.	
DNC	2, 3, 4, 5, 6	Reserved for factory use only.	
NC	7, 8, 9, 10, 12, 27, 33, 35, 36, 37, 38, 45, 46, 47, 48, 50, 51, 52, 53, 54, 59	<i>*Currently Not Supported. For Future Expansion*</i>	
CPU STATUS LED	11	Active high output indicates CPU/Module status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
ETH_BIAS	13	Bias Voltage to Ethernet PHY transformer	
USB_MODE	14	Indicates if the interface is in host/device mode. 0 = Device (Connected through 1K resistor to GND), 1 = Host.	I
Config	15	Active low. In normal mode, pull it low and hold for more than 8 seconds will reset the system to default settings. Pull it low upon power up will put the module into recovery mode.	I
RESET	16	Active low input will reset module	I
USBDP	18	USB D- signal; carries USB data to and from the USB 2.0 PHY	
USBDM	19	USB D+ signal; carries USB data to and from the USB 2.0 PHY	
LED_1 (RSSI1)	20	Receive Signal Strength Indicator 1. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
LED_2 (RSSI2)	21	Receive Signal Strength Indicator 2. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
LED_3 (RSSI3)	22	Receive Signal Strength Indicator 3. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
LED_RX	23	Active high output indicates receive and synchronization status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
LED_TX	24	Active high output indicates module is transmitting data over the RF channel. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
Serial RxD	28	Receive Data. Logic level input into the modem. It is recommended to wire this pin out through a zero ohm resistor to a header and jumper block for external access to the serial port for modem recovery procedures.	I
Serial TxD	29	Transmit Data. Logic level Output from the modem. It is recommended to wire this pin out through a zero ohm resistor to a header and jumper block for external access to the serial port for modem recovery procedures.	O
Serial DSR	30	Data Set Ready. Active low output. <i>The DSR line set high enables the transmitter of the RS485 driver.</i>	O
Serial CTS	31	Clear To Send. Active low output.	O
Serial DTR	32	Data Terminal Ready. Active Low output.	O
Serial RTS	34	Request To Send. Active low input.	I

Table 3-3: pDDL Pin Description

All serial communications signals are logic level (0 and 3.3V). DO NOT connect RS-232 level (+12, -12VDC) signals to these lines without shifting the signals to logic levels.

## 3.0 Hardware Features



**Caution:** During power up or reset, output pins from the Pico are in an unknown state. It is advised to use pull up or pull down resistors as appropriate.

Pin Name	No.	Description	Dir
RX_N4	41	Ethernet Port 4 (WAN) Receive Pair	
RX_P4	42		
TX_N4	43	Ethernet Port 4 (WAN) Transmit Pair	
TX_P4	44		
ETH4 LINK_LED	49	Active high output indicates Ethernet port 4 link status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
TX_P0	55	Ethernet Port 0 (LAN) Transmit Pair	
TX_N0	56		
RX_N0	57	Ethernet Port 0 (LAN) Receive Pair	
RX_P0	58		
ETH0 LINK_LED	60	Active high output indicates Ethernet port 0 link status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
Vdd	61,62	Positive voltage supply voltage for the digital section of the module (3.3V).	I
Vpa	63,64	Positive voltage supply voltage for the radio module (3.3-5V).	I

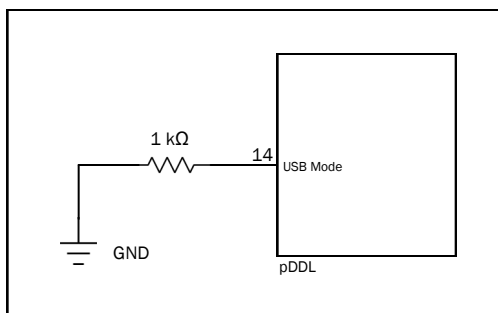
Table 3-3: pDDL Pin Description (continued)

All serial communications signals are logic level (0 and 3.3V). DO NOT connect RS-232 level (+12, -12VDC) signals to these lines without shifting the signals to logic levels.

See **Appendix D: Sample Interface Schematic** for a sample schematic that can be used to interface to the pDDL OEM module.

### 3.1.8 USB Device Mode

The pDDL can be set to operate as a USB Device. When set as a USB device, Microhard Composite Drivers can be installed on a USB Host to provide Ethernet and Serial functionality to the USB port on the pDDL. To enable USB Device mode, Pin 14 must be connect to GND through a 1K resistor as shown below:



Drawing 3-6: pDDL USB Device Mode

## 3.0 Hardware Features

### 3.2 pDDL Development Board

The pDDL Development board provides a platform in which to test and evaluate the operation of the pDDL without the need to design a custom interface PCB right from the start. The pDDL includes a socket to insert the pDDL and provides standard interfaces/indicators for:

- Ethernet
- RS232 Serial Port
- USB Port (Type A)
- Power (9-30 VDC)
- CPU Status LED
- Tx/Rx LED's
- RSSI (x3) LED's
- Config Button (Reset/Recovery Operations)
- Vpa (3/5V) Jumper Block



Image 3-3: pDDL Development Board

## 3.0 Hardware Features

### 3.2.1 pDDL Development Board Connectors & Indicators

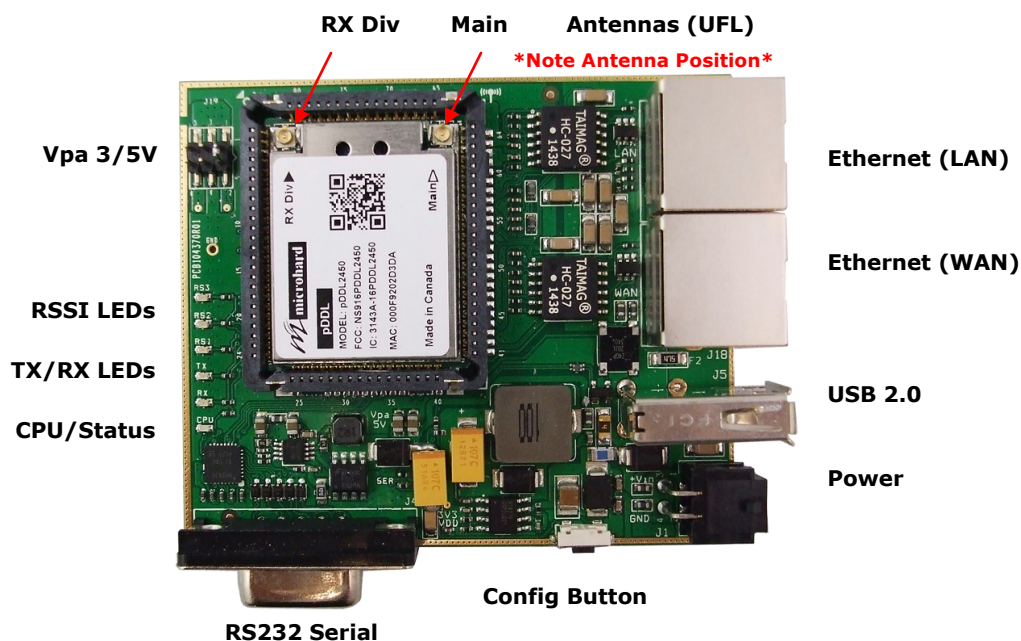


Figure 3-1: pDDL Development Board

#### Antennas:

The pDDL OEM module uses a UFL connectors, Ensure proper orientation as seen above to prevent damage to the pDDL module and to the development board. Main and Div. are marked on the module.

#### Ethernet LAN:

The Ethernet LAN port is a standard RJ45 port to connect local network devices. The default IP address for this port is 192.168.168.1.

#### Ethernet WAN:

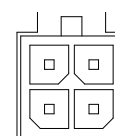
The Ethernet WAN port is a standard RJ45 Port that can be used as a separate WAN port for Router functions, or can be bridged (via software) to the LAN as a additional switch port for local devices.

The pDDL development board can be powered using **Passive PoE from 12—30 VDC Maximum** on the WAN port using a PoE injector that meets the following requirements:

Ethernet RJ45 Connector Pin Number								
Source Voltage	1	2	3	4	5	6	7	8
12 - 30 Vdc	Data	Data	Data	DC+	DC+	Data	DC-	DC-

Table 3-2: Ethernet (WAN) PoE Connections

#### Power



#### Power:

The pDDL development board can powered using an input voltage in the 9-30 VDC range.





## 3.0 Hardware Features

### Config Button:

The Config button on the pDDL can be used to either reset the modem into its factory default configuration, or it can be used to perform a firmware recovery procedure.

Factory Default Settings: While power is applied and the pDDL in an operational state, press and hold the *Config* Button for more than 10 seconds to reset to a factory default Master, alternatively hold the button for 5 seconds for a factory default Slave.

Firmware Recovery: To load the firmware on the unit it is recommended to use the normal WebUI to perform a firmware update (Maintenance). In the event that the firmware cannot be loaded using the standard WebUI (non responsive unit), pressing and holding the *Config* Button while powering-up the module will force the pDDL into a firmware recovery mode. There are 3 main modes, HTTP, TFTP and Master Reset. The table below shows the time required to hold the *Config* button while power is applied:

0 to 5 seconds	5 to 10 seconds	10 to 15 seconds	15+ seconds
HTTP Recovery	TFTP Recovery	Master Reset	No Effect

HTTP Recovery: Set an IP on a PC to 192.168.1.1. Open a web browser and Navigate to 192.168.1.39. This will open a simple webpage which will allow a firmware file to be loaded.

TFTP Recovery: Set an IP on a PC to 192.168.1.1. Use a TFTP session to push the firmware file to the modems recovery IP of 192.168.1.39. See Appendix for Firmware Recovery Procedure.

Master Reset: Runs Master Reset, file system is erased.

### RS232 Serial:

The RS232 Serial data port can be used to communicate with RS232 Serial devices or it can be configured to operate as a console port. See Table 3-3 for pin assignments.

### CPU/Status:

The CPU/Status LED indicates that power has been applied to the module. A Solid LED indicates normal operation, while flashing indicates boot or firmware upgrade status.

### TX/RX LEDs:

The TX/RX LEDs indication wireless traffic to/from the pDDL module.

### RSSI LEDs:

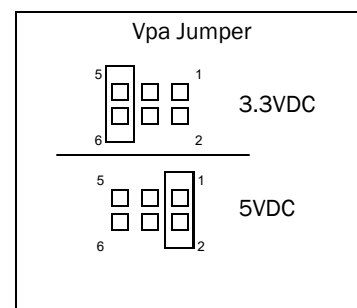
The RSSI LEDs indicate the Received Signal Strength on the Wireless Link. On a Master it will indicate an average RSSI value based on connected units. On a Slave the RSSI LEDs will represent the signal strength between the Slave and the Master it is connected to. (The more LEDs illuminated, the stronger the signal)

### Vpa 3/5V:

The Vpa jumper allows the radio inside the pDDL to be connected to 3.3 or 5VDC. For the pDDL to operate at maximum output Transmit (Tx) power of 1 Watt (30dBm), the Vpa jumper must be set to 5VDC (Pin 1+2).

Name	Data Port	Input or Output
DCD	1	O
RXD	2	O
TXD	3	I
DTR	4	I
SG	5	
DSR	6	O
RTS	7	I
CTS	8	O
RING	9	O

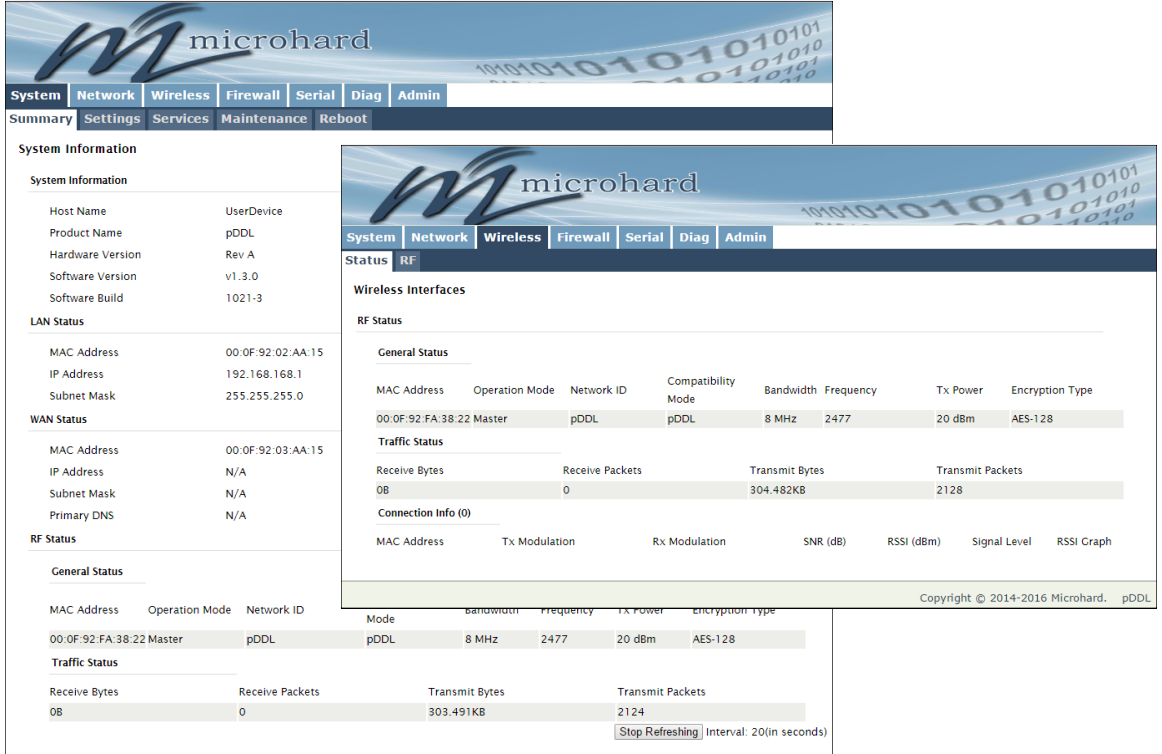
Table 3-3: Data RS232 Pin Assignment





## 4.0 Configuration

### 4.0 Web User Interface



The screenshot displays the Microhard pDDL WebUI. The top navigation bar includes tabs for System, Network, Wireless, Firewall, Serial, Diag, and Admin. Below this, a secondary bar shows Summary, Settings, Services, Maintenance, and Reboot. The main content area is divided into two columns. The left column, titled 'System Information', contains sections for System Information (Host Name: UserDevice, Product Name: pDDL, Hardware Version: Rev A, Software Version: v1.3.0, Software Build: 1021-3), LAN Status (MAC Address: 00:0F:92:02:AA:15, IP Address: 192.168.168.1, Subnet Mask: 255.255.255.0), WAN Status (MAC Address: 00:0F:92:03:AA:15, IP Address: N/A, Subnet Mask: N/A, Primary DNS: N/A), and RF Status (General Status table with MAC Address, Operation Mode, Network ID, Compatibility Mode, Bandwidth, Frequency, Tx Power, and Encryption Type; Traffic Status table with Receive Bytes, Receive Packets, Transmit Bytes, and Transmit Packets; and Connection Info (0) table with MAC Address, Tx Modulation, Rx Modulation, SNR (dB), RSSI (dBm), Signal Level, and RSSI Graph). The right column, titled 'Wireless Interfaces', shows the RF Status section with a General Status table and a Traffic Status table. A 'Stop Refreshing' button and 'Interval: 20(in seconds)' are visible at the bottom right of the RF Status section.

Image 4-0-1: WebUI



The factory default network settings:

**IP: 192.168.168.1**  
**Subnet: 255.255.255.0**

Initial configuration of an pDDL using the Web User (Browser) Interface (Web UI) method involves the following steps:

- configure a static IP Address on your PC to match the default subnet **or** if your PC is configured for DHCP, simply connect a PC to the LAN port of the pDDL and it will be assigned a IP address automatically.
- connect the pDDL LAN port to PC NIC card using an Ethernet cable
- apply power to the pDDL and wait approximately 60 seconds for the system to load
- open a web browser and enter the factory default IP address ([192.168.168.1](http://192.168.168.1)) of the unit:
- logon window appears; log on using default Username: **admin** Password: **admin**
- use the web browser based user interface to configure the pDDL as required.
- refer to **Section 2.0: Quick Start** for step by step instructions.

In this section, all aspects of the Web Browser Interface, presented menus, and available configuration options will be discussed.

## 4.0 Configuration

### 4.0.1 Logon Window

Upon successfully accessing the pDDL using a Web Browser, the Logon window will appear.



For security, do not allow the web browser to remember the User Name or Password.



It is advisable to change the login Password. Do not FORGET the new password as it cannot be recovered.

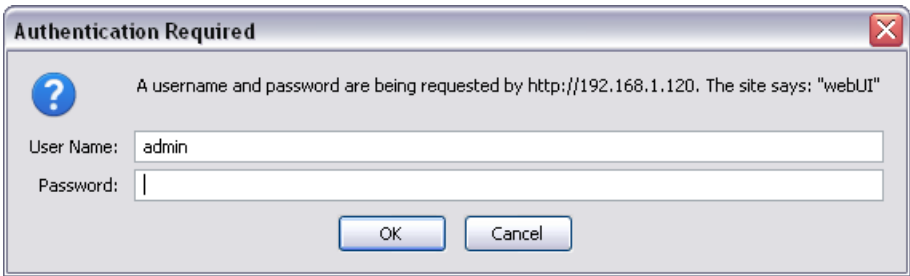


Image 4-0-2: Logon Window

The factory default User Name is: **admin**  
The default password is: **admin**

Note that the password is case sensitive. It may be changed (discussed further along in this section), but once changed, if forgotten, may not be recovered.

When entered, the password appears as 'dots' as shown in the image below. This display format prohibits others from viewing the password.

The 'Remember my password' checkbox may be selected for purposes of convenience, however it is recommended to ensure it is deselected - particularly once the unit is deployed in the field - for one primary reason: security.

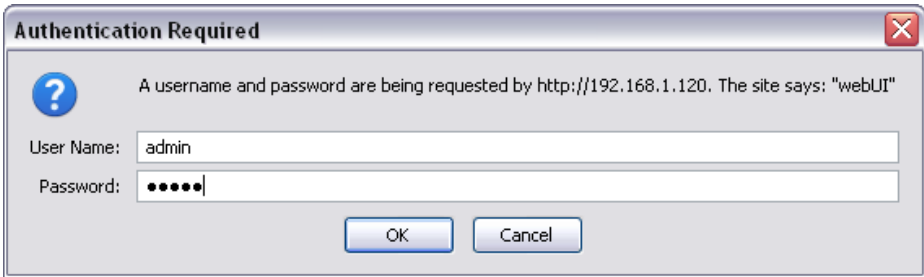


Image 4-0-3: Logon Window : Password Entry

**After successfully logging into the Pico DDL for the first time, you will be forced, and prompted to change the admin password.**

## 4.0 Configuration

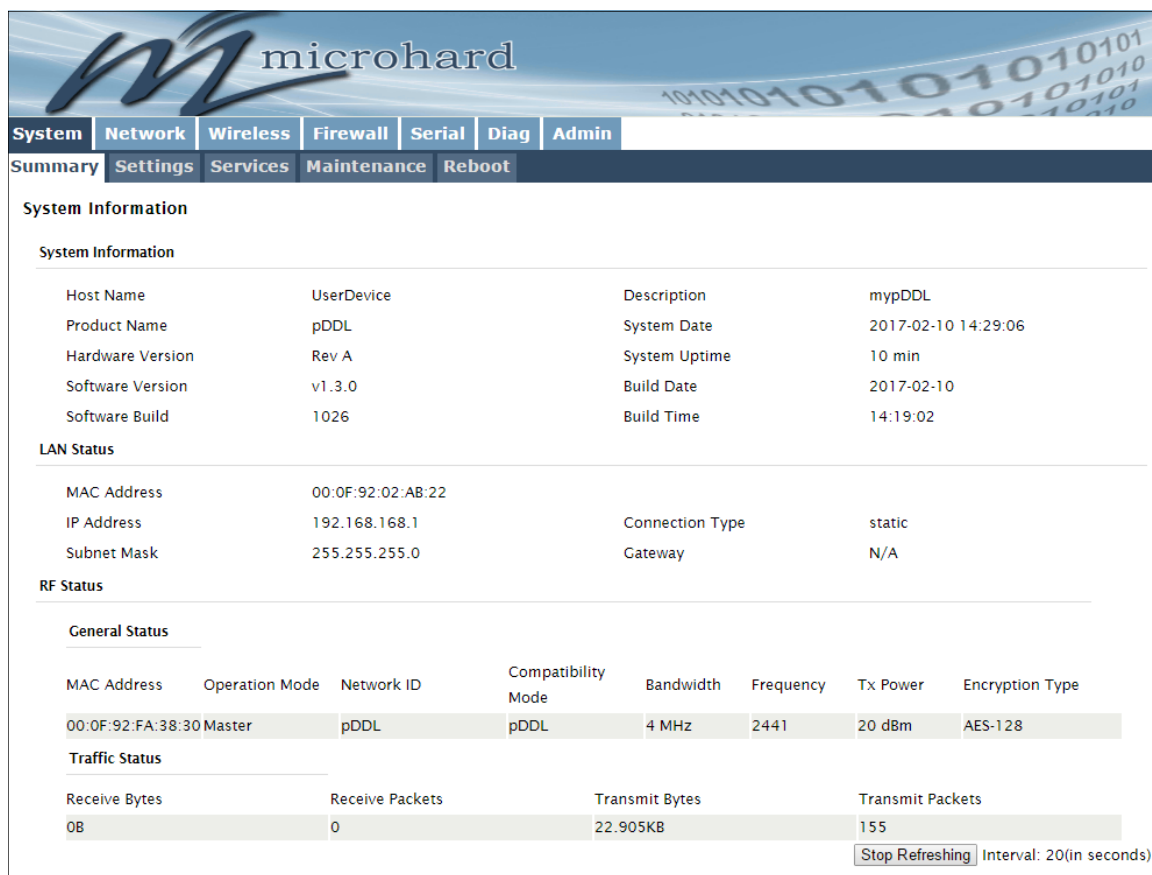
### 4.1 System

The main category tabs located at the top of the navigation bar separate the configuration of the pDDL into different groups based on function. The System Tab contains the following submenus:

- Summary - Status summary of entire radio including network settings, version information, and radio connection status.
- Settings - Host Name, System Log Settings, System Time/Date.
- Services - Enable/Disable and configure port numbers for SSH, Telnet, HTTP and HTTPS services.
- Maintenance - Remote firmware Upgrades, reset to defaults, configuration backup and restore.
- Reboot - Remotely reboot the system.

#### 4.1.1 System > Summary

The System Summary screen is displayed immediately after initial login, showing a summary and status of all the functions of the pDDL in a single display. This information includes System Status, LAN/WAN network information, version info, Radio Status etc.



The screenshot shows the pDDL System Summary window. At the top is the Microhard logo and a navigation bar with tabs: System, Network, Wireless, Firewall, Serial, Diag, Admin. Below the navigation bar is a sub-menu bar with tabs: Summary, Settings, Services, Maintenance, Reboot. The main content area is titled 'System Information' and contains several sections:

- System Information**: A table with 4 columns (Host Name, Product Name, Hardware Version, Software Version, Software Build, UserDevice, Description, System Date, System Uptime, Build Date, Build Time).
 

Host Name	UserDevice	Description	myPDDL
Product Name	pDDL	System Date	2017-02-10 14:29:06
Hardware Version	Rev A	System Uptime	10 min
Software Version	v1.3.0	Build Date	2017-02-10
Software Build	1026	Build Time	14:19:02
- LAN Status**: A table with 4 columns (MAC Address, IP Address, Subnet Mask, Connection Type, Gateway).
 

MAC Address	00:0F:92:02:AB:22	Connection Type	static
IP Address	192.168.168.1	Gateway	N/A
Subnet Mask	255.255.255.0		
- RF Status**: A section with a 'General Status' table and a 'Traffic Status' table.
 

MAC Address	Operation Mode	Network ID	Compatibility Mode	Bandwidth	Frequency	Tx Power	Encryption Type
00:0F:92:FA:38:30 Master		pDDL	pDDL	4 MHz	2441	20 dBm	AES-128

Receive Bytes	Receive Packets	Transmit Bytes	Transmit Packets
0B	0	22.905KB	155

At the bottom right of the window, there is a 'Stop Refreshing' button and an 'Interval: 20(in seconds)' label.

Image 4-1-1: System Summary Window

## 4.0 Configuration

### 4.1.2 System > Settings

#### System Settings

Options available in the System Settings menu allow for the configuration of the Host Name, Description, Console Timeout, System Log server and System Time settings.

SystemNetworkWirelessFirewallSerialDiagAdmin

SummarySettingsServicesMaintenanceReboot

System Settings

System Settings

Host Name

UserDevice

Description

mypDDL

Console Timeout (s)

120

[30 ~ 65535] 0-Disable

CFG Reset to Default Button

Enable

Disable

System Log Server IP/Name

0.0.0.0

0.0.0.0-Disable

System Log Server Port

514

Default: 514

Time Settings

Current Date(yyyy-mm-dd)

2014-01-01

Current Time(hh:mm:ss)

22:24:43

Date and Time Setting Mode

Local Time

NTP

Timezone

Mountain Time

POSIX TZ String

MST7MDT,M3.2.0,M11.1.0

NTP Server IP/Name

pool.ntp.org

NTP Server Port

123

NTP Client Interval (seconds)

0

[0 ~ 65535] 0-Disable

Image 4-1-2: System Settings > System Settings

Host Name	
The Host Name is a convenient identifier for a specific pDDL unit. This feature is most used when accessing units remotely: a convenient cross-reference for the unit's WAN IP address. This name appears when logged into a telnet session.	Values (characters)
	pDDL (varies) up to 64 characters
Description	
The description is a text field that can be used to describe the unit or system. This value can be viewed on the System > Summary screen.	Values (characters)
	pDDL (varies) up to 64 characters
Console Timeout (s)	
This value determines when a console connection (made via Console Port or Telnet) will timeout after becoming inactive.	Values (seconds)
	60 0-65535

## 4.0 Configuration

### CFG Reset to Default Button

Enabled by default, when the CFG button on the front of the pDDL is held down for 10s while the unit is powered up, the unit will reset and all settings will be reset to factory defaults. When disabled the unit will reset, but the settings will not be overwritten.

#### Values (Selection)

**Enable**  
Disable

### System Log Server IP

The pDDL can report system level events to a third party System Log server, which can be used to monitor events reported by the pDDL.

#### IP Address

0.0.0.0

### System Log Server Port

Enter the UDP listening port of the System Log Server. The default port number is generally 514, but could vary from Server to Server.

#### UDP Port

514

### Time Settings

The pDDL can be set to use a local time source, thus keeping time on its own, or it can be configured to synchronize the date and time via a NTP Server. The options and menus available will change depending on the current setting of the Date and Time Setting Mode, as seen below.

Time Settings

Current Date(yyyy-mm-dd)

2016-01-12

Current Time(hh:mm:ss)

15:03:03

Date and Time Setting Mode

☒ Local Time
 ☐ NTP

Date (yyyy-mm-dd)

2016-01-12

Time (hh:mm:ss)

15:03:03

Time Settings : Current Date(yyyy.mm.dd) 2015.11.27 Time(hh:mm:ss): 18:07:54

Date and Time Setting Mode

☐ Local Time
 ☒ NTP

Timezone

Mountain Time

POSIX TZ String

MST7MDT,M3.2.0,M11.1.0

NTP Server IP/Name

pool.ntp.org

NTP Server Port

123

NTP Client Interval (seconds)

0

[0 ~ 65535] 0-Disable



Network Time Protocol (NTP) can be used to synchronize the time and date or computer systems with a centralized, referenced server. This can help ensure all systems on a network have the same time and date.

Image 4-1-3: System Settings > Time Settings

### Date and Time Setting Mode

Select the Date and Time Setting Mode required. If set for 'Local Time' the unit will keep its own time and not attempt to synchronize with a network server. If 'NTP' is selected, a NTP server can be defined.

#### Values (selection)

**Local Time**  
NTP

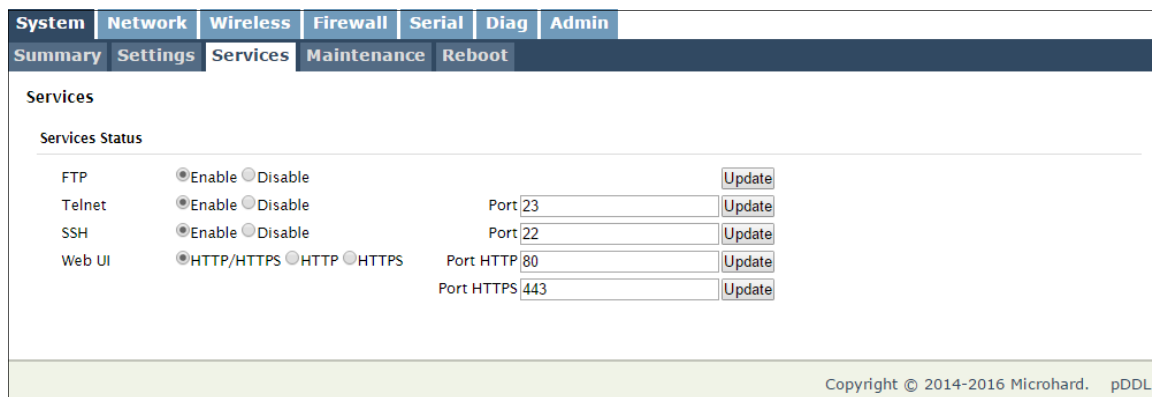
## 4.0 Configuration

Date	
The calendar date may be entered in this field. Note that the entered value is lost should the pDDL lose power for some reason.	<b>Values (yyyy-mm-dd)</b> <b>2016-01-12 (varies)</b>
Time	
The time may be entered in this field. Note that the entered value is lost should the pDDL lose power for some reason.	<b>Values (hh:mm:ss)</b> <b>11:27:28 (varies)</b>
Timezone	
If connecting to a NTP time server, specify the time zone from the dropdown list.	<b>Values (selection)</b> <b>(varies)</b>
POSIX TZ String	
This displays the POSIX TZ String used by the unit as determined by the Timezone setting.	<b>Values (read only)</b> <b>(varies)</b>
NTP Server	
Enter the IP Address or domain name of the desired NTP time server.	<b>Values (address)</b> <b>pool.ntp.org</b>
NTP Port	
Enter the IP Address or domain name of the desired NTP time server.	<b>Values (port#)</b> <b>123</b>
NTP Client Interval	
By default the modem only synchronizes the time and date during system boot up (default: 0), but it can be modified to synchronize at a regular interval. <i>This process does consume data and should be set accordingly.</i>	<b>Values (seconds)</b> <b>0</b>

## 4.0 Configuration

### 4.1.3 System > Services

Certain services in the pDDL can be disabled or enabled for either security considerations or resource/power considerations. The Enable/Disable options are applied after a reboot and will take affect after each start up.



System	Network	Wireless	Firewall	Serial	Diag	Admin
Summary	Settings	Services	Maintenance	Reboot		

**Services**

Services Status

FTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		<input type="button" value="Update"/>
Telnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Port 23	<input type="button" value="Update"/>
SSH	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Port 22	<input type="button" value="Update"/>
Web UI	<input checked="" type="radio"/> HTTP/HTTPS <input type="radio"/> HTTP <input type="radio"/> HTTPS	Port HTTP 80 Port HTTPS 443	<input type="button" value="Update"/>

Copyright © 2014-2016 Microhard. pDDL

Image 4-1-4: System > Services

#### FTP

The FTP service can be enabled/disabled using the Services Status Menu. The FTP service is used for firmware recovery operations.

**Values (port)**

**Enable / Disable**

#### Telnet

Using the Telnet Service Enable/Disable function, you can disable the Telnet service from running on the pDDL. The port used by the Telnet service can also be modified. The default is 23.

**Values (port)**

**23**

#### SSH

Using the SSH Service Enable/Disable function, you can disable the SSH service (Port 22) from running on the pDDL. The port used by the SSH service can also be modified. The default is 22.

**Values (port)**

**22**

#### Web UI

The default web server port for the web based configuration tools used in the modem is port 80 (http) and port 443 (HTTPS).

**Values (selection)**

Change as required, but keep in mind that if a non standard port is used, it must be specified in a internet browser to access the unit. (example: http://192.168.168.1:8080).

**HTTP/HTTPS**  
HTTP  
HTTPS



## 4.0 Configuration

### 4.1.4 System > Maintenance

#### Firmware Upgrade

Occasional firmware updates may be released by Microhard Systems which may include fixes and/or new features. The firmware can be updated wirelessly using the WebUI.

SystemNetworkWirelessFirewallSerialDiagAdmin

SummarySettingsServicesMaintenanceReboot

System Maintenance

Version Information

Product Name	Hardware Type	Build Version	Build Date	Build Time
pDDL	1.0	v1.3.0 build 1026	2017-02-10	14:19:02

Firmware Upgrade

Erase Current Configurations

Keep All Configurations

Firmware Image

Choose fileNo file chosen

Upgrade

Upgrade Firmware

Reset to Default Configurations

Reset to Default Configurations

Reset to Default

☐ Wipeout data and logs

Image 4-1-5: Maintenance > Firmware Upgrade

#### Erase Current Configuration

Choose to keep or erase the current configuration. Erasing the configuration of the pDDL unit during the upgrade process will upgrade, and return the unit to factory defaults, including the default IP Address and password.

##### Values (check box)

**Keep ALL Configuration**  
Erase Configuration

#### Firmware Image

Use the Browse button to find the firmware file supplied by Microhard Systems. Select “Upgrade Firmware” to start the upgrade process. This can take several minutes.

##### Values (file)

(no default)

#### Reset to Default Configurations

The pDDL may be set back to factory defaults by using the Reset to Default option under System > Maintenance > Reset to Default. **\*Caution\* - All configuration settings will be lost!!!**

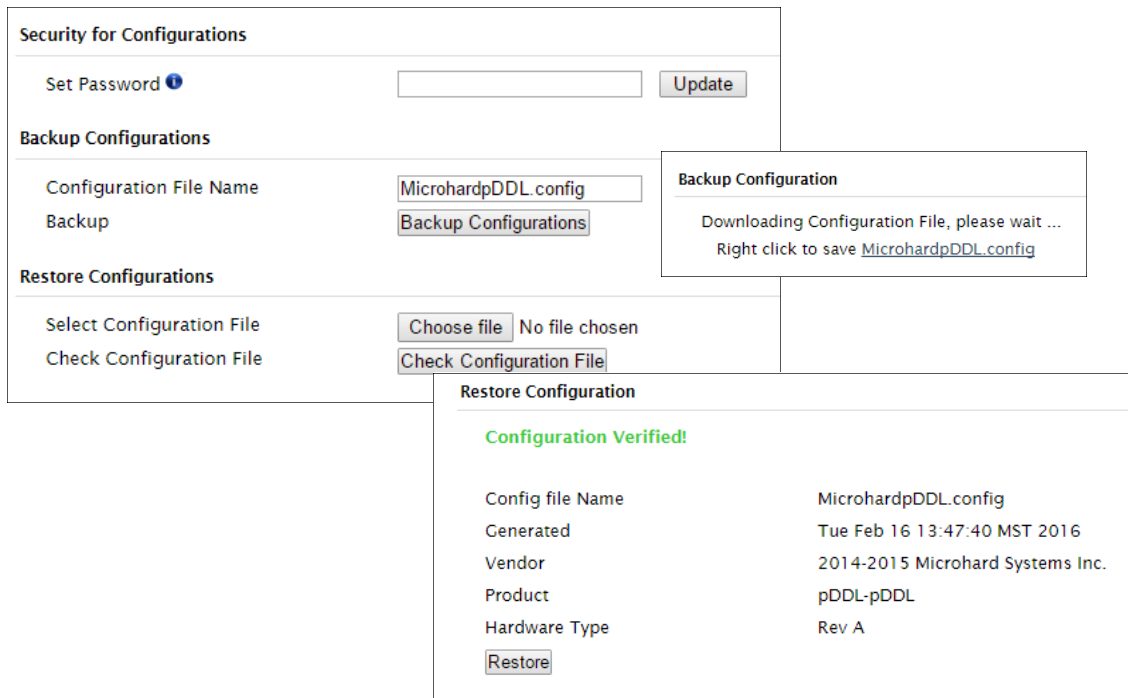
Additionally you can select the “Wipeout data and logs” check box to delete all data including historical logs and any other data from the device. **\*Caution\* - All configuration settings & data/logs will be lost!!!**

## 4.0 Configuration

### Security for Configurations / Backup & Restore Configuration

The configuration of the pDDL can be backed up to a file at any time using the Backup Configuration feature. The file can then be restored using the Restore Configuration feature. It is always a good idea to backup any configurations in case of unit replacement.

The configuration files cannot be edited offline, they are used strictly to backup and restore units. A password can be added to the Backup and Restore files. If the password is lost, files that have been backed up with a password can not be restored.



The screenshot displays the 'Security for Configurations' and 'Backup & Restore Configuration' interface. It includes fields for setting a password, a backup configuration section with a file name field (MicrohardpDDL.config) and a backup button, and a restore configuration section with a file selection button (Choose file), a check configuration button, and a restore button. A modal window shows the backup configuration details, including the file name, generation time, vendor, product, hardware type, and a restore button.

Image 4-1-6: Maintenance > Reset to Default / Backup & Restore Configuration

### Configuration File Name / Backup

Use this field to name the configuration file. The .config extension will automatically be added to the configuration file.

### Select Configuration file / Check Configuration File / Restore

Use the 'Browse' button to find the backup file that needs to be restored to the unit. Use the 'Check Restore File' button to verify that the file is valid, and then the option to restore the configuration is displayed, as seen above.

If the selected file is password protected the password must be set before restoring the file using the "Set Password" field under "Security for Configurations".

## 4.0 Configuration

### 4.1.5 System > Reboot

The pDDL can be remotely rebooted using the System > Reboot menu. As seen below a button 'Reboot Now' is provided. Once pressed, the unit immediately reboots and starts its boot up procedure. An automatic Scheduled Reboot (up to 3) can also be configured to force the pDDL to reboot daily, weekly or monthly.

SystemNetworkWirelessFirewallSerialDiagAdmin

SummarySettingsServicesMaintenanceReboot

Reboot Now

Config Scheduled Reboot

Schedule No.1

Status

Enable

Type

Reboot Daily

Time

01

:

01

Schedule No.2

Status

Enable

Type

Reboot Weekly

Days

1,

(Example: 1,2,3...)

Time

01

:

01

Schedule No.3

Status

Enable

Type

Reboot Monthly

Days

6,

(Example: 1,2,3...)

Time

01

:

01

Image 4-1-7: System > Reboot

Status	
Enable or disable the Scheduled Reboot.	Values (selection) Enable / <b>Disable</b>
Type	
Set the reboot schedule to reboot the modem once a day, week or month at a time and date specified below.	Values (selection) <b>Reboot Daily</b> Reboot Weekly Reboot Monthly
Days / Time	
When set to Weekly, set the day (1 is Sunday, 7 is Saturday) in which to reboot the modem. In a monthly configuration it is simply the date of the month (1 to 31). Once the day or date has been selected, specify the time (24hr clock) in which to initiate the scheduled reboot.	Values (varies)

## 4.0 Configuration

### 4.2 Network

#### 4.2.1 Network > Status

The Network Summary display gives a overview of the currently configured network interfaces including the Connection Type (Static/DHCP), IP Address, Net Mask, Default Gateway, DNS, and IPv4 Routing Table.



The screenshot shows the 'Network Status' page in the pDDL interface. The page has a navigation bar with tabs for System, Network, Wireless, Firewall, Serial, Diag, and Admin. Under the Network tab, there are sub-tabs for Status, LAN, WAN, USB, DHCP, Routes, Ports, and Device List. The 'Status' sub-tab is selected, showing the 'Network Status' section.

**LAN Port Status**

General Status			
IP Address	Connection Type	Subnet Mask	MAC Address
192.168.168.1	static	255.255.255.0	00:0F:92:02:AA:15

Traffic Status			
Receive bytes	Receive packets	Transmit bytes	Transmit packets
355.176KB	3849	857.981KB	3322

**WAN Port Status**

General Status			
IP Address	Connection Type	Subnet Mask	MAC Address
N/A	dhcp	N/A	00:0F:92:03:AA:15

Traffic Status			
Receive bytes	Receive packets	Transmit bytes	Transmit packets
0B	0	0B	0

**Default Gateway**

Gateway
192.168.168.1

**DNS**

DNS Server(s)
None

**IPv4 Routing Table**

Destination	Gateway	Subnet Mask	Flags	Metric	Ref	Use	Interface
0.0.0.0	192.168.168.1	0.0.0.0	UG	0	0	0	(br-lan)
192.168.168.0	0.0.0.0	255.255.255.0	U	0	0	0	(br-lan)

Stop Refreshing Interval: 20 (in seconds)

Copyright © 2014-2016 Microhard. pDDL

Image 4-2-1: Network > Network Status

## 4.0 Configuration

### 4.2.2 Network > LAN

## LAN Port Configuration

The LAN Ethernet port(s) on the pDDL are for connection of devices on a local network. By default, this port has a static IP Address. It also, by default is running a DHCP server to provide IP Addresses to devices that are connected to the physical LAN port (directly or via a switch).


microhard

System
Network
Wireless
Firewall
Serial
Diag
Admin

Status
LAN
WAN
USB
DHCP
Routes
Ports
Device List

### Network LAN Configuration

#### LAN Interfaces Settings

No.	Name	Static IP Address	Connection Type	DHCP Server	Config
1	LAN	192.168.168.1	static	On	<a href="#">Edit</a>
2	usb	N/A	static	Off	<a href="#">Remove</a> <a href="#">Edit</a>

Add

Image 4-2-2: Network > Network LAN Configuration

## LAN Add/Edit Interface

By selecting the Add or Edit buttons the LAN network interface can be configured, or additional LAN interfaces can be created.

System	Network	Wireless	Firewall	Serial	Diag	Admin
Status	LAN	WAN	USB	DHCP	Routes	Ports

### Network LAN Configuration

LAN Configuration

Spanning Tree (STP)	Off ▼
IGMP Snooping	On ▼
Connection Type	Static IP ▼
IP Address	192.168.168.1
Netmask	255.255.255.0
Default Gateway	192.168.168.1
Default Route	Yes ▼
DNS Mode	Manual ▼
Primary DNS	
Secondary DNS	

Image 4-2-3: Network > LAN Port Configuration

## Spanning Tree (STP)

## Values (selection)

Off  
On

**DHCP:** Dynamic Host Configuration Protocol may be used by networked devices (Clients) to obtain unique network addresses from a DHCP server.

**Advantage:**  
Ensures unique IP addresses are assigned, from a central point (DHCP server) within a network.

**Disadvantage:**  
The address of a particular device is not 'known' and is also subject to change.

STATIC addresses must be tracked (to avoid duplicate use), yet they may be permanently assigned to a device.



Within any IP network, each device must have its own unique IP address.

This option allows the pDDL to participate in the Spanning Tree protocol with other devices to prevent local loops. By default this is disabled.

## 4.0 Configuration



The factory default network settings:

**IP: 192.168.168.1**  
**Subnet: 255.255.255.0**  
**Gateway: 192.168.168.1**



A SUBNET MASK is a bit mask that separates the network and host (device) portions of an IP address.

The 'unmasked' portion leaves available the information required to identify the various devices on the subnet.



A GATEWAY is a point within a network that acts as an entrance to another network.

In typical networks, a router acts as a gateway.



Within any IP network, each device must have its own unique IP address.

### IGMP Snooping

Enable or disable IGMP snooping on the pDDL. **IGMP snooping** is the process of listening to Internet Group Management Protocol traffic. This allows the pDDL to listen in on the **IGMP** conversations between network devices. The pDDL then maintains a map of which links need which IP multicast streams.

#### Values (selection)

On  
Off

### Connection Type

This selection determines if the pDDL will obtain an IP address from a DHCP server on the attached network, or if a static IP address will be entered. If a Static IP Address is chosen, the fields that follow must also be populated.

#### Values (selection)

DHCP  
Static

### IP Address

If 'Static' Connection Type is selected, a valid IPv4 Address for the network being used must be entered in the field. If 'DHCP' is chosen this field will not appear and it will be populated automatically from the DHCP server.

#### Values (IP Address)

192.168.168.1

### Netmask

If 'Static' Connection Type is selected, the Network Mask must be entered for the Network. If 'DHCP' is chosen this field will not appear and it will be populated automatically from the DHCP server.

#### Values (IP Address)

255.255.255.0

### Default Gateway

If the pDDL is integrated into a network which has a defined gateway, then, as with other hosts on the network, this gateway's IP address will be entered into this field. If there is a DHCP server on the network, and the Connection Type (see previous page) is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

#### Values (IP Address)

(no default)

A simple way of looking at what the gateway value should be is: If a device has a packet of data it does not know where to send, send it to the gateway. If necessary - and applicable - the gateway can forward the packet onwards to another network.

### DNS

Set the DNS (Domain Name Server) for use by devices on the LAN port, if required.

#### Values (IP Address)

(no default)





## 4.0 Configuration



DNS: Domain Name Service is an Internet service that translates easily-remembered domain names into their not-so-easily-remembered IP addresses.

Being that the Internet is based on IP addresses, without DNS, if one entered the domain name `www.microhardcorp.com` (for example) into the URL line of a web browser, the website 'could not be found'.

<b>Preferred DNS Server</b>	
Specify a preferred DNS server address to be assigned to DHCP devices.	<b>Values (IP Address)</b> (IP Address)
<b>Alternate DNS Server</b>	
Specify the alternate DNS server address to be assigned to DHCP devices.	<b>Values (IP Address)</b> (IP Address)
<b>Domain Name</b>	
Enter the Domain Name for the DHCP devices.	<b>Values (string)</b> (IP Address)
<b>WINS/NBNS Servers</b>	
Enter the address of the WINS/NBNS (NetBIOS) Server. The WINS server will translate computers names into their IP addresses, similar to how a DNS server translates domain names to IP addresses.	<b>Values (IP/Domain)</b> (no default)
<b>WINS/NBT Node Type</b>	
Select the method used to resolve computer names to IP addresses. Four name resolution methods are available: B-node: broadcast P-node: point-to-point M-node: mixed/modified H-node: hybrid	<b>Values (selection)</b>  none b-node p-node m-node h-node



## 4.0 Configuration

### Default Gateway

If the pDDL is integrated into a network which has a defined gateway, then, as with other hosts on the network, this gateway's IP address will be entered into this field. If there is a DHCP server on the network, and the Connection Type (see previous page) is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

#### Values (IP Address)

(no default)

### Default Route

The Default Route parameter allows you to set this interface as the default route in the routing table. This is result in all data being sent to the WAN interface if there the destination network is not directly connected (LAN, Wireless etc), and no other route has been specified. In cases where the WAN is the primary connection this would be set to **Yes**.

#### Values (selection)

**No** / Yes

### DNS Servers

The following section will allow a user to specify DNS Server(s) to be used by the WAN interface of the pDDL.

### Mode

Select between Manual or Auto for DNS server(s) for the WAN interface. If set to Auto the pDDL will try to automatically detect the DNS servers to use, which is normally the case when the WAN is DHCP. Manual required the DNS addresses to be known and entered below.

#### Values (selection)

Manual / **Auto**

### Primary DNS

DNS (Domain Name Service) Servers are used to resolve domain names into IP addresses. If set to auto and the Connection Type is set for DHCP the DHCP server will populate this field and the value set can be viewed on the Network > Status page. To add additional static servers, enter them here.

#### Values (IP Address)

(no default)

### Secondary DNS

DNS (Domain Name Service) Servers are used to resolve domain names into IP addresses. If set to auto and the Connection Type is set for DHCP the DHCP server will populate this field and the value set can be viewed on the Network > Status page. To add additional static servers, enter them here.

#### Values (IP Address)

(no default)

# 4.0 Configuration

## 4.2.4 Network > USB

### USB Port Configuration

Normally, the pDDL module is bootstrapped to USB host mode that allows select generic devices to be used to extend Ethernet and serial functions (USB to Ethernet Adapters, USB to Serial Converters).

Alternatively, the pDDL can be set to Device mode by pulling PIN 14 (on OEM module) low through an 1k resistor to switch the USB mode. Older development boards will not support this and will either need to be modified or new boards will need to be acquired. In USB device mode, there are two functions supported, RNDIS/CDC Ethernet and CDC Serial port, when connected a host machine (PC etc).

RDNIS Ethernet and CDC Serial composite drivers are available from Microhard Systems.

SystemNetworkWirelessFirewallSerialDiagAdmin

StatusLANWANUSB DHCPRoutesPortsDevice List

USB Port Configuration

Configuration

Working ModeIndependent LAN

LAN Configuration

Connection TypeStatic IP

IP Address

Netmask

Default Gateway

Default RouteNo

DNS ModeManual

Primary DNS

Secondary DNS

DHCP Server

ModeDisable

Image 4-2-7: Network > USB

Working Mode

The RNDIS Ethernet USB port can be configured to operate as an additional LEN Ethernet Port with the current LAN (Bridged) or it can be configured to operate as a independent LAN (Subnet).

Values (selection)

Independent LAN  
Bridge with LAN Port

### LAN Configuration

When bridged with LAN the network parameters are set from the Network > LAN menu. When set to Independent the port can be configured as Statis or DHCP. Again refere to the LAN configuration for help with the displayed fields and definitions.

### DHCP Server

When in Independent mode the pDDL can run a DHCP service on the USB port to assign IP addresses and lease information. Refer to Network > LAN > DHCP for help with parameters and definitions.

## 4.0 Configuration

### 4.2.5 Network > DHCP

#### Static IP Addresses (for DHCP Server)

In many applications it is required to know the IP address of connected devices in order to implement security and firewall rules as well as for Port Forwarding rules. The Static IP Address (for DHCP Server) features MAC binding to allow connected devices to automatically obtain a specific IP address.

For configuration of the LAN DHCP Service see Network > LAN > (Edit) > LAN DHCP.

SystemNetworkWirelessFirewallSerialDiagAdmin

StatusLANWANUSB**DHCP**RoutesPortsDeviceList

DHCP Configuration

Static IP addresses (for DHCP Server)

Name

MAC Address

IP Address

Add static IP

Static Addresses

MAC Address	IP Address	Name	NetStatus
-------------	------------	------	-----------

Active DHCP Leases

MAC Address	IP Address	Name	Expires in
A6:12:20:F4:9A:0D	192.168.168.132	DMKT0002-2	9hr 59min 30sec

Release All

Refresh

Image 4-2-8: Network > DHCP

#### Static Addresses

Displays the MAC Binding table that is configured in the pDDL device.

#### Active DHCP Leases

Displays the active DHCP leases for any IP Addresses that have been assigned. This includes the IP address, the MAC, Device Name as well as the lease expiry.



## 4.0 Configuration

#### 4.2.6 Network > Routes

## Static Routes Configuration

It may be desirable to have devices on different subnets to be able to talk to one another. This can be accomplished by specifying a static route, telling the pDDL where to send data.



System

Network

Wireless

Firewall

Serial

Diag

Admin

Status

LAN

WAN

USB

DHCP

Routes

Ports

Device List

### Static Routes Configuration

Add Static Route

Name	<input type="text" value="route1"/>
Destination Subnet <sup>i</sup>	<input type="text" value="192.168.168.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.168.1"/>
Metric	<input type="text" value="0"/>
Interface	<input type="text" value="LAN"/>

#### Static Route Summary

Name	Destination	Netmask	Gateway	Metric	Interface
------	-------------	---------	---------	--------	-----------

Image 4-2-9: Network > Routes

Name	
Routes can be names for easy reference, or to describe the route being added.	<div>Values (characters)</div> <div>(no default)</div>
Destination	
Enter the network IP address for the destination.	<div>Values (IP Address)</div> <div>(192.168.168.0)</div>
Gateway	
Specify the Gateway used to reach the network specified above.	<div>Values (IP Address)</div> <div>192.168.168.1</div>
Netmask	
Enter the Netmask for the destination network.	<div>Values (IP Address)</div> <div>255.255.255.0</div>

## 4.0 Configuration

Metric	
In some cases there may be multiple routes to reach a destination. The Metric can be set to give certain routes priority, the lower the metric is, the better the route. The more hops it takes to get to a destination, the higher the metric.	<div>Values (Integer)</div> <div>0</div>
Interface	
Define the exit interface. Is the destination a device on the LAN, LAN1 (If physical WAN port is bridged as an independent LAN), or the WAN?	<div>Values (Selection)</div> <div>LAN / LAN1 / WAN / USB / None</div>

## 4.0 Configuration

### 4.2.7 Network > Ports

The Network > Ports menu can be used to determine the characteristics of the physical Ethernet interfaces on the pDDL. As seen below the Mode (Auto/Manual), Auto-Negotiation, Speed (10/100Mbit/s) and the Duplex (Full/Half) can all be configured on the pDDL.

System	Network	Wireless	Firewall	Serial	Diag	Admin
Status	LAN	WAN	USB	DHCP	Routes	Ports
Device List						
Ethernet Port Configuration						
Port	Mode	Auto-Negotiation	Speed	Duplex		
WAN	<input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="radio"/> On <input type="radio"/> Off	<input checked="" type="radio"/> 100Mbit/s <input type="radio"/> 10Mbit/s	<input checked="" type="radio"/> Full <input type="radio"/> Half		
LAN	<input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="radio"/> On <input type="radio"/> Off	<input checked="" type="radio"/> 100Mbit/s <input type="radio"/> 10Mbit/s	<input checked="" type="radio"/> Full <input type="radio"/> Half		
Ethernet Port Status						
Port	Linked	Auto-Negotiation	Speed	Duplex		
WAN	no	on	10Mb/s	Half		
LAN	no	on	10Mb/s	Half		

Image 4-2-10: Network > Ports

#### Mode

If set to Auto, the pDDL will negotiate and determine the best connection speed and mode.

Values (selection)

Auto / Manual

#### Auto-Negotiation

Enable or disable auto-negotiation.

Values (selection)

On / Off

#### Speed

If the mode and auto negotiation are set you manual the connection speed can be specified.

Values (selection)

100Mbit/s / 10 Mbit/s

#### Duplex

Selection between full or half duplex for the direction of data.

Values (selection)

Full / Half

## 4.0 Configuration

### 4.2.8 Network > Device List

The Network > Device List shows the current ARP table for the local network adapter. The MAC address and IP address are shown, however not only DHCP assigned devices are listed in the device list, any devices, even those statically assigned, that are connected through the local network interface (s) are displayed, including those connected through a hub or switch.

Devices can also be filtered by the network that they are attached to. Devices with a MAC and no IP and vice versa can also be filtered.



Image 4-2-11: Network > Device List

## 4.0 Configuration

### 4.3 Wireless

#### 4.3.1 Wireless > Status

The Status window gives a summary of all radio or wireless related settings and connections.

The **General Status** section shows the MAC address of the current radio, the Operating Mode (Master, Slave etc), the Network ID being used, the Compatibility Mode, Channel Bandwidth and frequency information and the type of security used.

**Traffic Status** shows statistics about the transmitted and received data.

The pDDL shows information about all Wireless connections in the **Connection Info** section. The MAC address, TX & RX Modulation, Signal to Noise ratio (SNR), Signal Strength (RSSI), and a graphical representation of the signal level or quality, as well as a RSSI Graph Link.

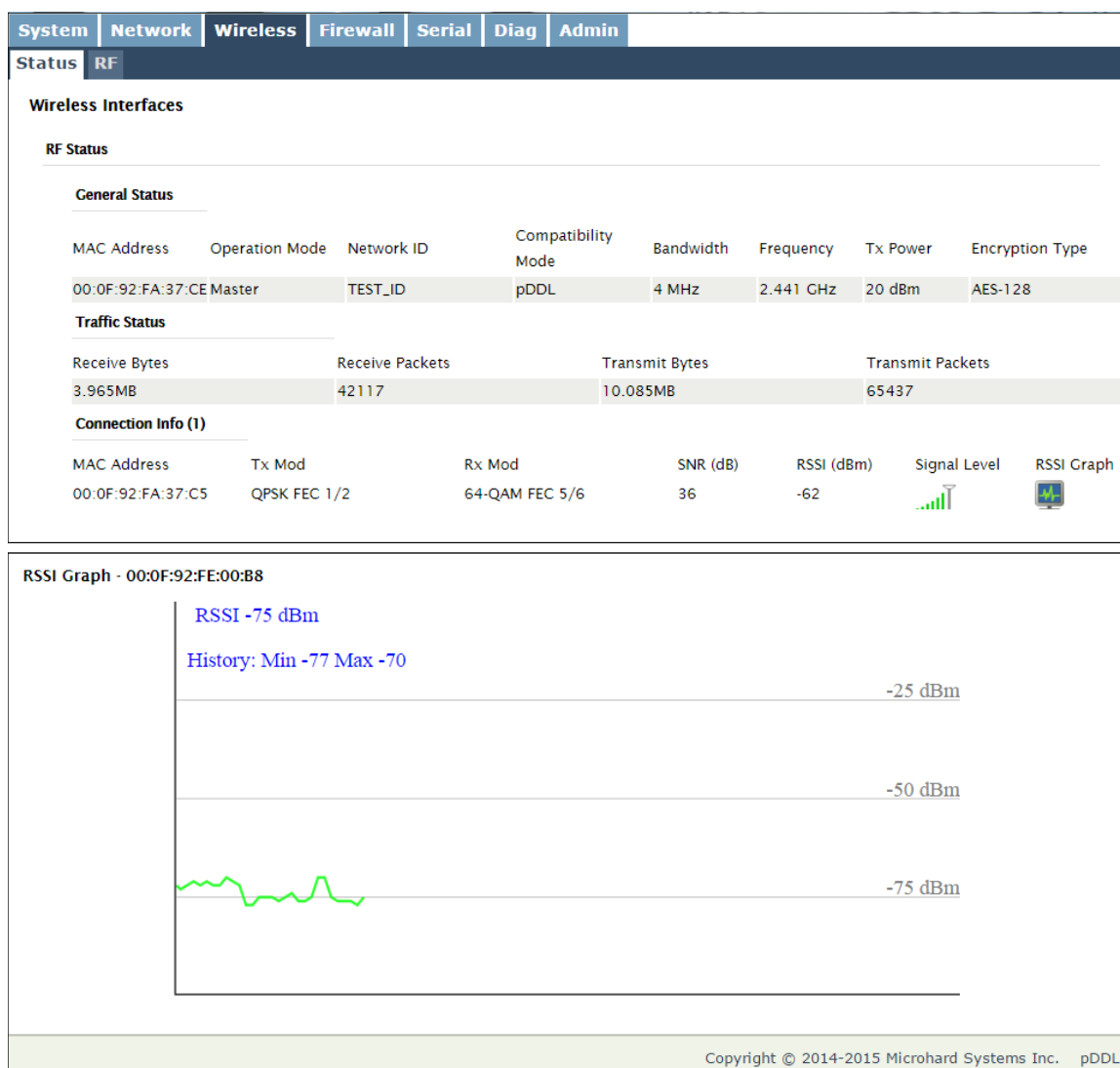


Image 4-3-1: Wireless > Status (RSSI Graph Shown Below)

## 4.0 Configuration

### 4.3.2 Wireless > RF

#### RF Configuration

The RF Configuration allows for the configuration of the radio module. You can turn the radio on or off, adjust the TX power, select the channel bandwidth and frequency, as well as the operating mode of the radio as seen below.

System	Network	Wireless	Firewall	Serial	Diag	Admin
<div> <div>Status</div> <div>RF</div> </div>						
<b>Wireless Configuration</b>						
<b>RF Configuration</b>						
<div> <div>Radio</div> <div> <input checked="" type="radio"/> On           <input type="radio"/> Off         </div> </div>						
<div> <div>Compatibility Mode</div> <div>pDDL ▾</div> </div>						
<div> <div>Channel Bandwidth</div> <div>8MHz ▾</div> </div>						
<div> <div>Channel-Frequency</div> <div>76 - 2477 MHz ▾</div> </div>						
<div> <div>Tx Power</div> <div>20 dbm ▾</div> </div>						
<div> <div>Wireless Distance</div> <div>3000 (m)</div> </div>						
<div> <div>Rx Diversity(Reboot Required)</div> <div> <input checked="" type="radio"/> Disable           <input type="radio"/> Enable         </div> </div>						
<div> <div>Operation Mode</div> <div>Master ▾</div> </div>						
<div> <div>TX Rate</div> <div>Auto (recommended) ▾</div> </div>						
<div> <div>Extended Addressing</div> <div> <input checked="" type="radio"/> On           <input type="radio"/> Off         </div> </div>						
<div> <div>Network ID</div> <div>pDDL</div> </div>						
<div> <div>Encryption Type</div> <div>AES-128 ▾</div> </div>						
<div> <div>Encryption Key</div> <div>*****</div> </div>						
<div> <div>Show password</div> <div><input type="checkbox"/></div> </div>						
<b>RF Comport Configuration</b>						
<div> <div>Comport1 TX Rate</div> <div>Normal Rate ▾</div> </div>						
<div> <div>Comport2 TX Rate</div> <div> <input checked="" type="radio"/> Data Mode Disabled         </div> </div>						

Image 4-3-2: Wireless > RF Configuration

#### Radio

This option is used to turn the radio module on or off. If turned off Wireless connections can not be made. The default is On.

#### Values (selection)

On / Off

#### Compatibility Mode

Future option for setting different compatibility modes.

#### Values (selection)

pDDL



## 4.0 Configuration



Refer to FCC (or as otherwise applicable) regulations to ascertain, and not operate beyond, the maximum allowable transmitter output power and effective isotropic radiated power (EIRP).

### Channel Bandwidth

Select the channel bandwidth from the list. Refer to the specifications to see the relationship and performance between channel bandwidth, throughput and sensitivity.

Generally a larger channel has greater throughput, at the cost of sensitivity, while a smaller channel tends to be more robust, but at the cost of throughput.

#### Values (selection)

8 / 4 / 2 MHz

### Channel-Frequency

Set the Channel-Frequency. This must be the same on each unit in a network. The frequency shown is the center frequency and is available in 1 MHz increments, values shown will vary with the Channel Bandwidth selected above.

***The noise floor of the specified channel will dramatically affect the quality of the link, it is essential to select the cleanest channel for superior performance.***

#### Values (selection (MHz))

2402 - 2482 (2MHz BW, CH 1-81)  
2405 - 2479 (4MHz BW, CH 4-78)  
2407 - 2477 (8MHz BW, CH 6-76)

### TX Power

This setting establishes the transmit power level which will be presented to the antenna connector of the pDDL.

Unless required, the Tx Power should be set not for maximum, but rather for the minimum value required to maintain an adequate system fade margin.

#### Values (selection)

20 dBm	25 dBm
21 dBm	26 dBm
22 dBm	27 dBm
23 dBm	28 dBm
24 dBm	29 dBm
	30 dBm

### Wireless Distance

The Wireless Distance parameter allows a user to set the expected distance the wireless signal needs to travel. The pDDL sets various internal timeouts to account for this travel time. Longer distances will require a higher setting, and shorter distances may perform better if the setting is reduced.

#### Values (meters)

3000

### Rx Diversity

When enabled Rx Diversity can provide enhanced sensitivity potentially allowing greater throughput. When enabled, **an Antenna must be connected** to the Rx Diversity port or system performance will be degraded. If an antenna is not connected Rx Diversity must be disabled. The unit must be rebooted.

#### Values (selection)

Disable / Enable

## 4.0 Configuration

		Mode
<b>Master</b>	- A Master may provide a wireless data connection to many slaves/remotes.	<b>Values (selection)</b>
<b>Slave/Remote</b>	- A Slave may sustain one wireless connection, i.e. to an Master.	Master <b>Slave</b>

For video applications it is required to connect the video source (camera) to the radio designated as the Master. Video receivers would then be connected to the Slave radios, this would allow for multiple viewing stations. See the diagram below for an example.

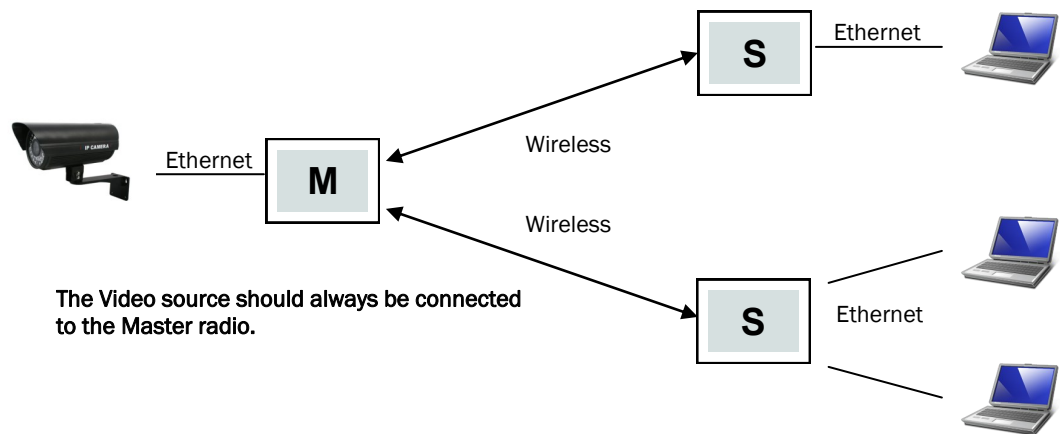


Diagram 4-3-1: Operating Modes

		TX Rate
This setting determines the modulation type and in turn the rate at which the data is to be wirelessly transferred.		<b>Values (selection)</b>
<b>The default and recommended setting for both Master and Slave units is 'Auto'.</b> When in 'Auto' the unit will transfer data at the highest possible rate in consideration of the receive signal strength (RSSI).		<b>Auto (recommended)</b> 64-QAM 5/6 FEC 64-QAM 3/4 FEC 64-QAM 2/3 FEC 16-QAM 3/4 FEC 16-QAM 1/2 FEC QPSK FEC 3/4 QPSK FEC 1/2
Refer to <a href="#">Section 1.3 Performance Specifications</a> for a table breakdown of performance at selected rates. If setting a fixed TX Rate It is recommended to retain a fade margin of at least 10 dBm for optimum performance. For example, for a link (8MHz channel) with a signal strength of at least -75dBm, a TX rate of 16-QAM 3/4 FEC is recommended. Setting to the highest rate with a poor link may result in reduced performance.		

## 4.0 Configuration



Change the default value for the Network ID to something unique for your network. Do this for an added measure of security and to differentiate your network from others which may be operating nearby.

Extended Addressing	
Enable or disable extended addressing.	<b>Values (selection)</b> On / Off
Network ID	
Each network of pDDL modules must an a unique Network ID. This Network ID must be set in each unit on the network.	<b>Values</b> pDDL
Encryption Type	
The encryption types defines the type of security used for the Wireless Interface, to join a network a device must know the correct Encryption Key. Security options are dependent on the version type. Export versions may not have all optional available to meet regulatory requirements set government policies.	<b>Values (selection)</b> Disabled AES-128
Encryption Key	
This is the password, or preshared key that is required by any device to connect to the wireless interface of the pDDL. It is <b><u>strongly recommended</u></b> to always have a password defined, and changed from the factory default.	<b>Values (string)</b> 1234567890
Show Password	
Check this box to show the currently configured password for the encryption passphrase.	<b>Values (selection)</b> unchecked
Comport Tx Rate	
When using Ethernet and Serial data. If the volume of serial data is high, leave at the default (Normal Rate), if the volume of Ethernet data is high set com data to High Rate (Compressed).	<b>Values (selection)</b> Normal / High

## 4.0 Configuration

### 4.4 Firewall

#### 4.4.1 Firewall > Summary

The Firewall Summary allows a user to see detailed information about how the firewall is operating. The All, Filter, Nat, Raw, and Mangle options can be used to view different aspects of the firewall.

System	Network	Wireless	Firewall	Serial	Diag	Admin
Summary	General	Port Forwarding	MAC-IP List	Rules	Firewall Default	
<b>Firewall Status</b>						
Status and Rules <span>All</span> <span>Check</span>						
Target Filter						
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)						
num	pkts	bytes	target	prot	opt	in out source destination options
1	76204	7440K	delegate_input	all	--	* * 0.0.0.0/0 0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)						
num	pkts	bytes	target	prot	opt	in out source destination options
1	0	0	delegate_forward	all	--	* * 0.0.0.0/0 0.0.0.0/0
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)						
num	pkts	bytes	target	prot	opt	in out source destination options
1	70807	10M	delegate_output	all	--	* * 0.0.0.0/0 0.0.0.0/0
Chain delegate_forward (1 references)						
num	pkts	bytes	target	prot	opt	in out source destination options
1	0	0	forwarding_rule	all	--	* * 0.0.0.0/0 0.0.0.0/0 / <sup>k</sup> user chain for forwarding <sup>k</sup> /
2	0	0	ACCEPT	all	--	* * 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED
3	0	0	zone_lan_forward	all	--	br-lan * 0.0.0.0/0 0.0.0.0/0
4	0	0	reject	all	--	* * 0.0.0.0/0 0.0.0.0/0
Chain delegate_input (1 references)						
num	pkts	bytes	target	prot	opt	in out source destination options
1	0	0	ACCEPT	all	--	lo * 0.0.0.0/0 0.0.0.0/0
2	76204	7440K	input_rule	all	--	* * 0.0.0.0/0 0.0.0.0/0 / <sup>k</sup> user chain for input <sup>k</sup> /
3	65396	6648K	ACCEPT	all	--	* * 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED
4	2873	149K	syn_flood	tcp	--	* * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x17/0x02
5	10808	793K	zone_lan_input	all	--	br-lan * 0.0.0.0/0 0.0.0.0/0
Chain delegate_output (1 references)						
num	pkts	bytes	target	prot	opt	in out source destination options
1	0	0	ACCEPT	all	--	* * 0.0.0.0/0 0.0.0.0/0
2	70807	10M	output_rule	all	--	* * 0.0.0.0/0 0.0.0.0/0 / <sup>k</sup> user chain for output <sup>k</sup> /
3	70807	10M	ACCEPT	all	--	* * 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED
4	0	0	zone_lan_output	all	--	* * 0.0.0.0/0 0.0.0.0/0
Chain forwarding_lan_rule (1 references)						
num	pkts	bytes	target	prot	opt	in out source destination options

Image 4-4-1: Firewall > Status

## 4.0 Configuration

### 4.4.2 Firewall > General

The General Firewall settings allow users to enable or disable the firewall, and to decide which areas of the modem to protect. The Firewall can also be reset to factory defaults from this area of the WebUI.

System	Network	Wireless	Firewall	Serial	Diag	Admin
Summary	General	Port Forwarding	MAC-IP List	Rules	Firewall Default	

**Firewall General**

**Firewall General Configuration**

WAN Remote Management ⓘ

☒ Enable
☐ Disable

WAN Request ⓘ

☒ Block
☐ Allow

LAN to WAN Access Control ⓘ

☐ Block
☒ Allow

Anti-Spoof ⓘ

☐ Enable
☒ Disable

Packet Normalization ⓘ

☐ Enable
☒ Disable

Image 4-4-2: Firewall > General

#### WAN Remote Management

Allow remote management of the pDDL on the WAN side using the WebUI on port 80(HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN.

##### Values

Enable / Disable

#### WAN Request

When Blocked the pDDL will block all requests from devices on the WAN unless specified otherwise in the Access Rules, MAC List, IP List configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the **WAN Remote Management** option.

##### Values

Block / Allow

#### LAN to WAN Access Control

Allows or Blocks traffic from the LAN accessing the WAN unless specified otherwise using the Access Rules, MAC, and IP List configuration.

##### Values

Block / Allow

#### Anti-Spoof

The Anti-Spoof protection is to create some firewall rules assigned to the external interface (WAN) of the firewall that examines the source address of all packets crossing that interface coming from outside. If the address belongs to the internal network or the firewall itself, the packet is dropped.

##### Values

Enable / Disable

#### Packet Normalization

Packet Normalization is the normalization of packets so there are no ambiguities in interpretation by the ultimate destination of the packet. The scrub directive also reassembled fragmented packets, protecting some operating systems from some forms of attack, and drops TCP packets that have invalid flag combinations.

##### Values

Enable / Disable

## 4.0 Configuration

### 4.4.3 Firewall > Port Forwarding

The pDDL can be used to provide remote access to connected devices. To access these devices a user must define how incoming traffic is handled by the pDDL. If all incoming traffic is intended for a specific connected device, DMZ could be used to simplify the process, as all incoming traffic can be directed towards a specific IP address.

In the case where there is multiple devices, or only specific ports need to be passed, Port forwarding is used to forward traffic coming in from the WAN to specific IP Addresses and Ports on the LAN. Port forwarding can be used in combination with other firewall features, but the Firewall must be enabled for Port forwarding to be in effect. If the WAN Request is blocked on the General Tab, additional rules and/or IP Lists must be set up to allow the port forwarding traffic to pass through the firewall.

System

Network

Wireless

Firewall

Serial

Diag

Admin

Summary

General

Port Forwarding

MAC-IP List

Rules

Firewall Default

Firewall Port Forwarding

Notice

Port Forwarding Rules are taken into consideration after the General firewall settings are applied. If the WAN and/or cellular traffic is blocked, additional rules must be created:  
1. Add rules in the Rules configuration to open ports or allow IP addresses.  
2. Create a firewall rule in the Firewall->Rules page to allow desired connections.

Firewall DMZ Configuration

DMZ Source: WAN

DMZ Mode

Disable

DMZ Server IP

192.168.200.100

Exception Port

0

Firewall Port Forwarding Configuration

Name

forward1

Source

Internal Server IP

192.168.2.1

Internal Port

3000

Protocol

TCP

External Port

2000

Add Port Forwarding

Firewall Port Forwarding Summary

Name	Source	Internal IP	Internal Port	Protocol	External Port
------	--------	-------------	---------------	----------	---------------

If DMZ is enabled and an exception port for the WebUI is not specified, remote management will not be possible. The default port for remote management is TCP 80.

Image 4-4-3: Firewall > Port Forwarding

DMZ Mode	
Enable or disable DMZ Mode. DMZ can be used to forward all traffic to the DMZ Server IP listed below.	Values (selection) Disable / Enable
DMZ Server IP	
Enter the IP address of the device on the LAN side of the pDDL where all the traffic will be forwarded to.	Values (IP Address) 192.168.100.100

© Microhard Systems Inc.

63



## 4.0 Configuration



If the firewall is set to block incoming traffic on the WAN interface, additional rules or IP/MAC lists must be configured to allow desired traffic access.

Exception Port	
Enter a exception port number that will NOT be forwarded to the DMZ server IP. Usually a configuration or remote management port that is excluded to retain external control of the pDDL.	<b>Values (Port #)</b> 0
<b>Firewall Port Forwarding Configuration</b>	
Name	
This is simply a field where a convenient reference or description is added to the rule. Each Forward must have a unique rule name and can use up to 10 characters.	<b>Values (10 chars)</b> Forward
Source	
Select the source for the traffic, if applicable.	<b>Values (selection)</b> (none)
Internal Server IP	
Enter the IP address of the intended internal (i.e. on LAN side of the pDDL) server. This is the IP address of the device you are forwarding traffic to.	<b>Values (IP Address)</b> 192.168.2.1
Internal Port	
Target port number of the internal server on the LAN IP entered above.	<b>Values (Port #)</b> 3000
Protocol	
Select the type of transport protocol used. For example Telnet uses TCP, SNMP uses UDP, etc.	<b>Values (selection)</b> TCP / UDP / Both
External Port	
Port number of the incoming request (from WAN-side).	<b>Values (Port #)</b> 2000

## 4.0 Configuration

#### 4.4.4 Firewall > MAC-IP List

MAC List configuration can be used to control which physical LAN devices can access the ports on the pDDL, by restricting or allowing connections based on the MAC address. IP List configuration can be used to define who or what can access the pDDL, by restricting or allowing connections based on the IP Address/Subnet.

MAC-IP List can be used alone or in combination with LAN to WAN Access Control to provide secure access to the physical ports of the pDDL.

System	Network	Wireless	Firewall	Serial	Diag	Admin
Summary	General	Port Forwarding	MAC-IP List	Rules	Firewall Default	

### Firewall MAC/IP List

#### Firewall MAC List Configuration

Name	<input type="text" value="mac1"/>
Action	<input type="text" value="Accept"/>
Mac Address	<input type="text" value="00:00:00:00:00:00"/>
<input type="button" value="Add Mac List"/>	

#### Firewall IP List Configuration

Name	<input type="text" value="ip1"/>
Action	<input type="text" value="Accept"/>
Source	<input type="text" value="LAN"/>
Source IP / Prefix	<input type="text" value="0.0.0.0"/> / <input type="text" value=""/>
<input type="button" value="Add IP List"/>	

#### Firewall MAC List Summary

Name	Action	Source	Mac Address
------	--------	--------	-------------

#### Firewall IP List Summary

Name	Action	Src	Src IP	Prefix
------	--------	-----	--------	--------

Image 4-4-4: Firewall > MAC-IP List

## Firewall MAC List Configuration

Rule Name	
The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.	<div>Values (10 chars)</div> <div>MAC_List</div>
MAC Address	
Specify the MAC Address to be added to the list. Must be entered in the correct format as seen above. Not case sensitive.	<div>Values (MAC Address)</div> <div>00:00:00:00:00:00</div>

## 4.0 Configuration

### Firewall MAC List Configuration (Continued)

Action
<p>The Action is used to define how the rule handles the connection request.</p> <p>ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.</p>
<b>Values (selection)</b> ACCEPT DROP REJECT

### Firewall IP List Configuration

Rule Name
<p>The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.</p>
<b>Values (10 chars)</b> IP_List

Action
<p>The Action is used to define how the rule handles the connection request. ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.</p>
<b>Values (selection)</b> ACCEPT / DROP / REJECT

Source
<p>Enter the specific zone that the IP List will apply to, LAN, WAN or None (both).</p>
<b>Values (Selection)</b> LAN/LAN1/WAN/USB NONE

Source IP Address
<p>Match incoming traffic from the specified source IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)</p>
<b>Values (IP Address)</b> 192.168.0.0

Destination Address
<p>Match incoming traffic from the specified destination IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)</p>
<b>Values (IP Address)</b> 192.168.0.0

## 4.0 Configuration

### 4.4.5 Firewall > Rules

The Rules configuration can be used to define specific rules on how local and remote devices access different ports and services. MAC List and IP List are used for general access, and are applied before rules are processed.

It is highly recommended to block as much traffic as possible from the modem, especially when using a public IP address. The best security would be to allow traffic only from trusted IP addresses, and only the specific ports being used, and block everything else. Not configuring the firewall and the firewall rules correctly could result in unpredictable data charges from your provider.

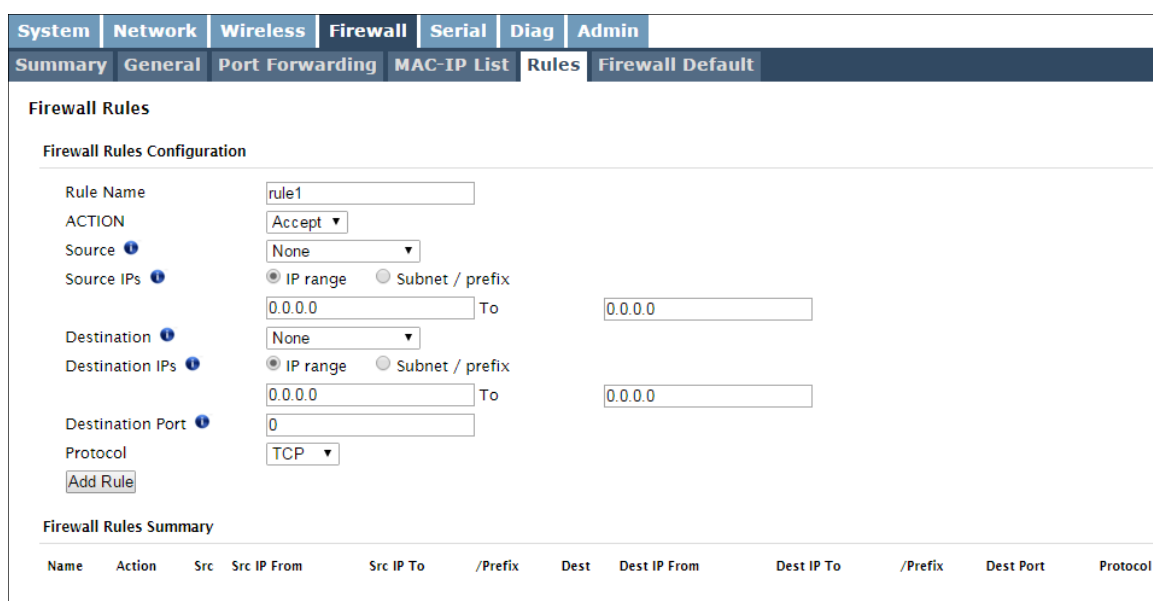


Image 4-4-5: Firewall > Rules

#### Rule Name

The rule name is used to identify the created rule. Each rule must have a unique name and up to 10 characters can be used.

Values (10 Chars)

characters

#### Action

The Action is used to define how the rule handles the connection request.

Values (selection)

ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.

ACCEPT  
DROP  
REJECT

This is configured based on how the **WAN Request** and **LAN to WAN Access Control** are configured in the previous menus.

#### Source

Select the zone which is to be the source of the data traffic. The LAN/WAN refers to local connections on the pDDL.

Values

LAN/WAN/Independent  
LAN/None

## 4.0 Configuration

Source IPs	
Match incoming traffic from the specified source IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)	<b>Values (IP Address)</b>  <b>192.168.0.0 to 192.168.0.0</b>
Destination	
Select the zone which is the intended destination of the data traffic. The selections shown will reflect any network interfaces configured.	<b>Values (selection)</b>  LAN/WAN/None <i>(varies)</i>
Destination IPs	
Match incoming traffic from the specified destination IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)	<b>Values (IP Address)</b>  <b>192.168.0.0 to 192.168.0.0</b>
Destination Port	
Match incoming traffic directed at the given destination port or port range.  (To specify a port range use a From:To (100:200) format)	<b>Values (port)</b>  <b>0</b>
Protocol	
The protocol field defines the transport protocol type controlled by the rule.	<b>Values</b>  <b>TCP</b> <b>UDP</b> <b>Both</b> <b>ICMP</b>

## 4.0 Configuration

#### 4.4.6 Firewall > Default

The firewall can be returned to default setting without requiring the entire modem to be reset to defaults. It is recommended to restart the modem once changes to the firewall or a reset is performed.

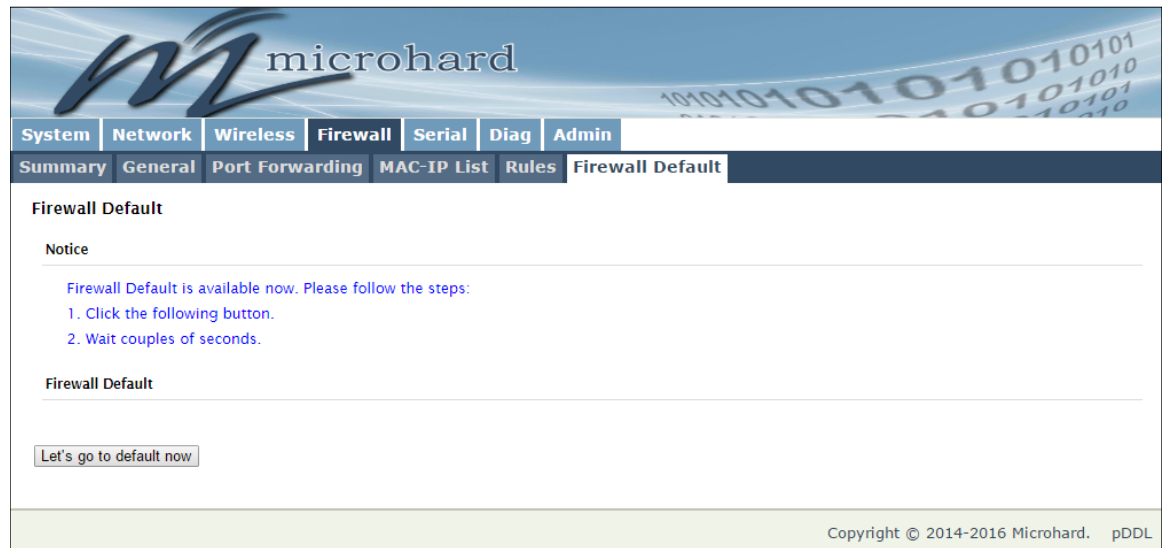


Image 4-4-6: Firewall > Default

## 4.0 Configuration

### 4.5 Serial

#### 4.5.1 Serial > Summary

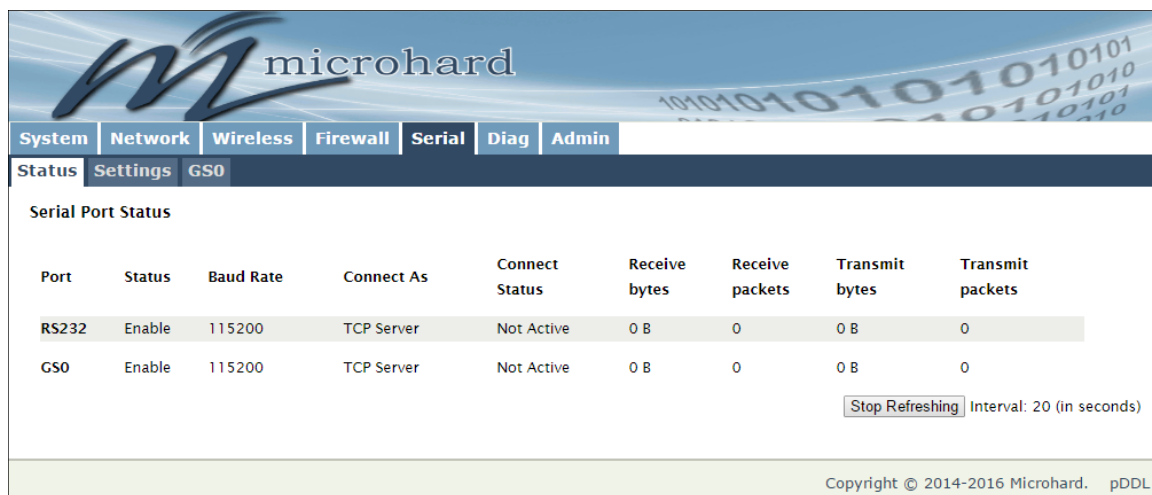
The Serial > Summary window gives a summary of the on board serial data port. A second serial port can be added to the pDDL OEM by interfacing a FTDI USB to Basic UART IC as shown in **Appendix D: Serial Port Extension**.

**GS0** - If the pDDL has been set to USB Device mode (Pin 14 connected to GND through a 1K resistor), the GS0 tab will appear and the USB port can be used to connect to a USB host that has the Microhard Composite Drivers installed. The USB port will appear as a serial device on the host system.

The Summary window shows a number of status items that aid in viewing the operation, statistics, and troubleshooting of the RS232 & USB Serial Ports.

#### General Status

- Port Status - Shows if the RS232 has been enabled in the configuration.
- Baud Rate - The current baud rate used to interface with the connected device.
- Connect As - The type of IP Protocol Config is displayed here (TCP, UDP, SMTP, PPP, etc)
- Connect Status - Shows if there are any current connections / if the port is active.



Port	Status	Baud Rate	Connect As	Connect Status	Receive bytes	Receive packets	Transmit bytes	Transmit packets
RS232	Enable	115200	TCP Server	Not Active	0 B	0	0 B	0
GS0	Enable	115200	TCP Server	Not Active	0 B	0	0 B	0

Stop Refreshing Interval: 20 (in seconds)

Copyright © 2014-2016 Microhard. pDDL

Image 4-5-1: Serial > Summary



## 4.0 Configuration

### 4.6.2 Serial > Settings

This menu option is used to configure the serial device server for the serial communications port. Serial device data may be brought into the IP network through TCP, UDP, or multicast; it may also exit the pDDL network on another pDDL serial port. The fully-featured RS232 interface supports hardware handshaking.



The screenshot shows the 'Serial Port Configuration' web interface. At the top, there is a navigation bar with tabs for System, Network, Wireless, Firewall, Serial (selected), Diag, and Admin. Below this is a sub-navigation bar with Status, Settings (selected), and GS0. The main content area is titled 'Serial Port Configuration' and is divided into two sections: 'Port Configuration' and 'TCP Configuration'.

**Port Configuration**

Port status	Data ▼
Escape Sequence	Disabled ▼
Data Baud Rate	115200 ▼
Data Format	8N1 ▼
Data Mode ⓘ	<input type="radio"/> Seamless <input checked="" type="radio"/> Transparent
Character Timeout	24
Maximum Packet Size	256
No-Connection Data ⓘ	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
MODBUS TCP Status	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IP Protocol Config	TCP Server ▼

**TCP Configuration**

Server Mode	<input checked="" type="radio"/> Monitor <input type="radio"/> Polling
Polling Timeout (seconds)	10
Local Listening port	20002
Incoming Connection Timeout(seconds)	300
Fast Recovery ⓘ	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Image 4-5-2: Serial > Settings Configuration

## 4.0 Configuration

### Port Status

Select operational status of the Serial Port. The port is in console mode by default.

Values (selection)

Data / **Console**

### Escape Sequence

Enabling the escape sequence allows users to temporarily exit data mode and enter console mode for the serial port.

Values (selection)

Enabled / **Disabled**

### Escape Guard Interval

Appears only when the Escape Sequence is enabled. Enter the time interval in which the escape sequence must be entered fully.

Values (seconds)

**1**

### Escape Sequence String

Only shown when the escape sequence is enabled. Enter the characters to be used for the escape sequence.

Values (characters)

**+++**

### Data Baud Rate

The serial baud rate is the rate at which the modem is to communicate with the attached local asynchronous device.

Values (bps)

921600	<b>9600</b>
460800	7200
230400	4800
115200	3600
57600	2400
38400	1200
28800	600
19200	300
14400	

### Data Format

This setting determines the format of the data on the serial port. The default is 8 data bits, No parity, and 1 Stop bit.

Values (selection)

**8N1**  
8E1  
8O1



Note: Most PCs do not readily support serial communications greater than 115200bps.

## Data Mode

## Values (selection)

## Seamless / Transparent

## Character Timeout

**Values (characters)**

24

## Maximum Packet Size

Values (bytes)

256

## No-Connection Data

### Values (selection)

**Disable** / Enable

## MODBUS TCP Status

## Values (selection)

**Disable** / Enable

## 4.0 Configuration

### IP Protocol Config

This setting determines which protocol the serial server will use to transmit serial port data over the pDDL network.

The protocol selected in the IP Protocol Config field will determine which configuration options appear in the remainder of the RS232 Configuration Menu.

#### Values (selection)

TCP Client  
TCP Server  
TCP Client/Server  
UDP Point-to-Point  
PPP (Not supported on USB)

**TCP Client:** When TCP Client is selected and data is received on its serial port, the pDDL takes the initiative to find and connect to a remote TCP server. The TCP session is terminated by this same unit when the data exchange session is completed and the connection timeout has expired. If a TCP connection cannot be established, the serial port data is discarded.



UDP: User Datagram Protocol does not provide sequencing information for the packets sent nor does it establish a 'connection' ('handshaking') and is therefore most suited to communicating small packets of data.

- **Remote Server Address**  
IP address of a TCP server which is ready to accept serial port data through a TCP connection. For example, this server may reside on a LAN network server.  
Default: **0.0.0.0**
- **Remote Server Port**  
A TCP port which the remote server listens to, awaiting a session connection request from the TCP Client. Once the session is established, the serial port data is communicated from the Client to the Server.  
Default: **20001**
- **Outgoing Connection Timeout**  
This parameter determines when the pDDL will terminate the TCP connection if the connection is in an idle state (i.e. no data traffic on the serial port).  
Default: **60** (seconds)
- **Fast Recovery**  
Sets the TCP session parameters and buffers to be set such that TCP sessions recover faster in environments where the wireless link is weak/unstable. This is ideal for critical, near real time applications such as flight control data. Data is not buffered during outages.  
Default: **Disable**



TCP: Transmission Control Protocol in contrast to UDP does provide sequencing information and is connection-oriented; a more reliable protocol, particularly when large amounts of data are being communicated.

Requires more bandwidth than UDP.

**TCP Server:** In this mode, the pDDL Series will not INITIATE a session, rather, it will wait for a Client to request a session of it (it's being the Server—it 'serves' a Client). The unit will 'listen' on a specific TCP port. If a session is established, data will flow from the Client to the Server, and, if present, from the Server to the Client. If a session is not established, both Client-side serial data, and Server-side serial data, if present, will be discarded.

- **Local Listening Port**  
The TCP port which the Server listens to. It allows a TCP connection to be created by a TCP Client to carry serial port data.  
Default: **20001**
- **Incoming Connection Timeout**  
Established when the TCP Server will terminate the TCP connection is the connection is in an idle state.  
Default: **300** (seconds)
- **Fast Recovery**  
Sets the TCP session parameters and buffers to be set such that TCP sessions recover faster in environments where the wireless link is weak/unstable. This is ideal for critical, near real time applications such as flight control data. Data is not buffered during outages.  
Default: **Disable**

## 4.0 Configuration



A UDP or TCP port is an application end-point. The IP address identifies the device and, as an extension of the IP address, the port essentially 'fine tunes' where the data is to go 'within the device'.

Be careful to select a port number that is not predetermined to be associated with another application type, e.g. HTTP uses port 80.

### IP Protocol Config (Continued...)

**TCP Client/Server:** In this mode, the pDDL will be a combined TCP Client and Server, meaning that it can both initiate and serve TCP connection (session) requests. Refer to the TCP Client and TCP Server descriptions and settings described previously as all information, combined, is applicable to this mode.

**UDP Point-to-Point:** In this configuration the pDDL will send serial data to a specifically-defined point, using UDP packets. This same pDDL will accept UDP packets from that same point.

- **Remote IP Address**  
IP address of distant device to which UDP packets are sent when data received at serial port.  
Default: **0.0.0.0**
- **Remote Port**  
UDP port of distant device mentioned above.  
Default: **20001**
- **Listening Port**  
UDP port which the IP Series listens to (monitors). UDP packets received on this port are forwarded to the unit's serial port.  
Default: **20001**
- **UDP Timeout(s)**  
UDP Timeout in seconds.  
Default: **10**

## 4.0 Configuration

### IP Protocol Config (Continued...)

**PPP:** The serial port can be configured as a PPP server for a serial connection with a PC or other device. The attached PC could then use a dedicated serial (WindowsXP - dialup/modem) type PPP connection to access the network resources of the pDDL.

- **PPP Mode**  
Can be set for Active or Passive. If set for Active, the PPP server will initiate the PPP connection with a PPP client. The server will periodically send out link requests following PPP protocol. If set to Passive, the PPP server will not initiate the PPP connection with PPP client. The server will wait passively for the client to initiate connection.  
Default: **Passive**
- **Expected String**  
When a client (PC or device) initiates a PPP session with the modem, this is the handshaking string that is expected in order to allow a connection. Generally this does not need to be changed.  
Default: **CLIENT**
- **Response String**  
This is the handshaking string that will be sent by the modem once the expected string is received. Generally this does not need to be changed.  
Default: **CLIENTSERVER**
- **PPP LCP Echo Failure Number**  
The PPP server will presume the peer to be dead if the LCP echo-requests are sent without receiving a valid LCP echo-reply. If this happens, PPP server will terminate the connection. Use of this option requires a non-zero value for the LCP Echo Interval parameter. This option can be used to enable PPP server to terminate after the physical connection has been broken (e.g., the modem has hung up).  
Default: **0**
- **PPP LCP Echo Interval**  
The PPP server will send an LCP echo-request frame to the peer every 'n' seconds. Normally the peer should respond to the echo-request by sending an echo-reply. This option can be used with the LCP-echo-failure option to detect that the peer is no longer connected.  
Default: **0**
- **PPP Local IP**  
Enter the local PPP IP Address, the IP Address of the pDDL COM Port.  
Default: **192.168.0.1**
- **PPP Host IP**  
Enter the PPP Host IP here. This is the IP of the PC or attached device.  
Default: **192.168.0.99**
- **PPP Idle Timeout(s)**  
It is the timeout for tearing down the ppp connection when there is no data traffic within the time interval. When there is data coming, new ppp connection will be created.  
Default: **30**

## 4.0 Configuration

### 4.6.3 Serial > GS0

This tab only appears if the pDDL has been set to operate as a USB Device (Pin 14 connected to GND through a 1k resistor). Microhard USB Serial Composite Drivers are available which allow the pDDL to appear as a serial device to a USB Host (PC etc.)

The USB port can be set to “Idle” or to operate as a Data port as seen below:

System

Network

Wireless

Firewall

Serial

Diag

Admin

Status

Settings

GS0

GS0 Serial Port Configuration

Port Configuration

Port status

Data ▾

Data Baud Rate

115200 ▾

Data Format

8N1 ▾

Flow Control

none ▾

Data Mode ⓘ

☒ Seamless ☐ Transparent

Character Timeout

24

Maximum Packet Size

256

No-Connection Data ⓘ

☐ Disable ☒ Enable

MODBUS TCP Status

☒ Disable ☐ Enable

IP Protocol Config

TCP Server ▾

TCP Configuration

Server Mode

☒ Monitor ☐ Polling

Polling Timeout (seconds)

10

Local Listening port

20003

Incoming Connection Timeout(seconds)

300

Fast Recovery ⓘ

☒ Disable ☐ Enable

Image 4-5-2: Serial > Settings Configuration

## GS0 Serial Port Configuration

The USB port configuration is identical to the Serial Port > Settings parameters. For help or definitions of each field, refer to the previous section of this manual which describes the available settings.



#### 4.6.1 Diag > Ping

System

Network

Wireless

Firewall

Serial

Diag

Admin

Ping

Traceroute

Iperf

Network Tools

Ping

Ping Host Name

192.168.168.250

Ping Count

4

(0 = continuous)

Ping Size

56

Start

Stop

Clear

Please wait for output of "ping -c 4 -s 56 192.168.168.250"...

PING 192.168.168.250 (192.168.168.250): 56 data bytes  
03:39:24.160097 -- sending icmp request  
64 bytes from 192.168.168.250: seq=0 ttl=128 time=5.763 ms  
03:39:25.160753 -- sending icmp request  
64 bytes from 192.168.168.250: seq=1 ttl=128 time=0.788 ms  
03:39:26.161321 -- sending icmp request  
64 bytes from 192.168.168.250: seq=2 ttl=128 time=0.851 ms  
03:39:27.161816 -- sending icmp request  
64 bytes from 192.168.168.250: seq=3 ttl=128 time=0.788 ms

Image 4-6-1: Diagnostics > Ping

The **Traceroute** command can be used to provide connectivity data by providing information about the number of hops, routers and the path taken to reach a particular destination.

System

Network

Wireless

Firewall

Serial

Diag

Admin

Ping

Traceroute

Iperf

### Network Tools

Traceroute

Traceroute Host Name

192.168.168.250

Start

Stop

Clear

Begin traceroute test at ...

1 \* \* \*

2 \* \* \*

3 \* \* \*

4 \* \* \*

5 \* \* \*

6 \* \* \*

7 \* \* \*

8 \* \* \*

9 \* \* \*

10 \* \* \*

11 \* \* \*

12 \* \* \*

Image 4-6-2: Diagnostics > Trace Route

## 4.0 Configuration

### 4.6.3 Diag > Iperf

The pDDL features an integrated lperf server/client to use to measure and analyze throughput of TCP/UDP packets to and/or from the pDDL. lperf is a 3rd party utility that can be loaded on any PC to measure network performance. For additional information about lperf, please visit the [lperf website](#).

The pDDL can be configured to operate as a Server, listening for an incoming connection from another device (with lperf), or PC running an lperf client. If set to lperf client, the pDDL will connect to or send packets to a specified lperf server.

System

Network

Wireless

Firewall

Serial

Diag

Admin

Ping

Traceroute

Iperf

Throughput Testing

Iperf Configuration

Iperf Mode

Server

Server Status

Enable

Disable

Protocol

TCP

TCP Window Size

128K

(0 for default 85.3KByte)

TCP Maximum Segment Size

0

(0 for default)

Save Server Settings

Iperf Configuration

Iperf Mode

Client

Protocol

TCP

Remote Server IP Address

192.168.168.100

Duration(seconds)

5

TCP Window Size

128K

(0 for default 85.3KByte)

TCP Maximum Segment Size

0

(0 for default)

Report Format

Mbits

Save & Run Test

Image 4-6-3: *Diag > lperf*

## Iperf Mode

Select between an Iperf Server (listens for incoming connections) and client (initiates a connection with a server)

## Values (selection)

**Server / Client**

## Server Status

If the lperf mode is set to Server, this Server Status allows a user to Enable or Disable the server.

## Values (selection)

**Enable / Disable**

## Protocol

Select the type of packets to be sent to test the throughput. TCP packets are connection oriented and require additional overhead for the handshaking that occurs, while UDP is a connectionless, best effort oriented protocol.

## Values (selection)

**TCP / UDP**

## 4.0 Configuration

### 4.7 Admin

#### 4.7.1 Admin > Users

##### Password Change

The Password Change menu allows the password of the user 'admin' to be changed. The 'admin' username cannot be deleted, but additional users can be defined and deleted as required as seen in the Users menu below. After the modem has been reset to factory defaults, it is mandatory to change the default password for admin, the modem will prompt a user to do so upon the first login.

SystemNetworkWirelessFirewallSerialDiagAdmin

UsersSNMPDiscoveryLogout

Access Control

New password will take effect immediately after pressing "Change Password" button.

Account Name

admin

Change Password ⓘ

(5-64 characters, no space)

Confirm Password

Change Password

Add User (It will take effect immediately after pressing "Add User" button)

Username

(5-32 characters)

Password ⓘ

(5-64 characters, no space)

Confirm Password

System

Hide Submenu ▾

Network

Hide Submenu ▾

Wireless

Hide Submenu ▾

Firewall

Hide Submenu ▾

Serial

Hide Submenu ▾

Diag

Hide Submenu ▾

Admin

Hide Submenu ▾

Add User

Add User

Users Summary

No users defined.

Image 4-7-1: Users > Password Change

New Password

Enter a new password for the 'admin' user. It must be at least 5 characters in length. **The default password for 'admin' is 'admin'.**

Values (characters)

admin

Confirm Password

The exact password must be entered to confirm the password change, if there is a mistake all changes will be discarded.

Values (characters)

admin

## 4.0 Configuration

### Add Users

Different users can be set up with customized access to the WebUI. Each menu or tab of the WebUI can be disabled on a per user basis as seen below.

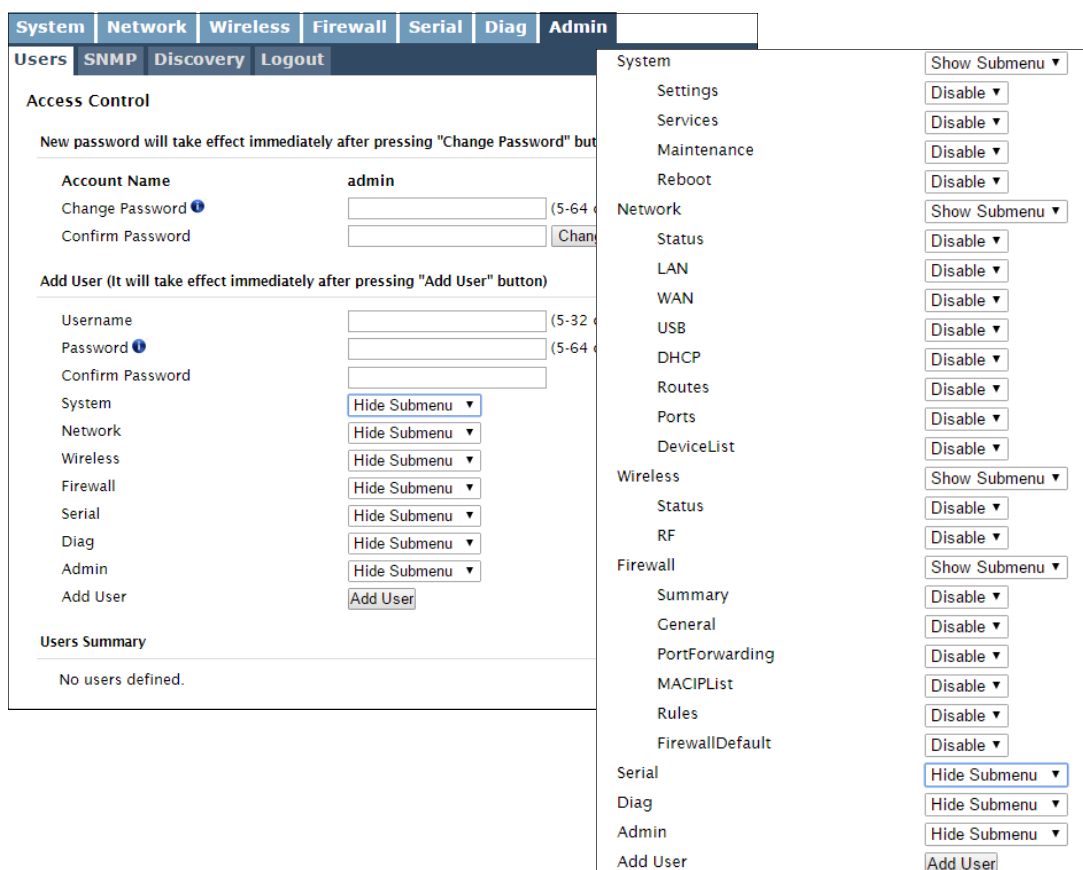


Image 4-7-2: Access Control > Users

#### Username

Enter the desired username. Minimum of 5 character and maximum of 32 character. Changes will not take effect until the system has been restarted.

#### Values (characters)

(no default)  
Min 5 characters  
Max 32 characters

#### Password / Confirm Password

Passwords must be a minimum of 5 characters. The Password must be re-entered exactly in the Confirm Password box as well.

#### Values (characters)

(no default)  
min 5 characters

## 4.0 Configuration

### 4.7.2 Admin > SNMP

The pDDL may be configured to operate as a Simple Network Management Protocol (SNMP) agent. Network management is most important in larger networks, so as to be able to manage resources and measure performance. SNMP may be used in several ways:



SNMP: Simple Network Management Protocol provides a method of managing network devices from a single PC running network management software.

Managed networked devices are referred to as SNMP agents.

- configure remote devices
- monitor network performance
- detect faults
- audit network usage
- detect authentication failures

A SNMP management system (a PC running SNMP management software) is required for this service to operate. This system must have full access to the pDDL. Communications is in the form of queries (information requested by the management system) or traps (information initiated at, and provided by, the SNMP agent in response to predefined events).

Objects specific to the pDDL are hosted under private enterprise number **21703**.

An object is a variable in the device and is defined by a Management Information Database (MIB). Both the management system and the device have a copy of the MIB. The MIB in the management system provides for identification and processing of the information sent by a device (either responses to queries or device-sourced traps). The MIB in the device relates subroutine addresses to objects in order to read data from, or write data to, variables in the device.

An SNMPv1 agent accepts commands to retrieve an object, retrieve the next object, set an object to a specified value, send a value in response to a received command, and send a value in response to an event (trap).

SNMPv2c adds to the above the ability to retrieve a large number of objects in response to a single request.

SNMPv3 adds strong security features including encryption; a shared password key is utilized. Secure device monitoring over the Internet is possible. In addition to the commands noted as supported above, there is a command to synchronize with a remote management station.

The pages that follow describe the different fields required to set up SNMP on the pDDL. MIBs may be requested from Microhard Systems Inc.

The MIB file can be downloaded directly from the unit using the **'Get MIB File'** button on the Network > SNMP menu.

Download MIB File

Get MIB File

## 4.0 Configuration

### SNMP Settings

SystemNetworkWirelessFirewallSerialDiagAdmin

UsersSNMPDiscoveryLogout

SNMP Settings

SNMP Settings

SNMP Agent Status

Enable

Read Only Community Name

public

Read Write Community Name

private

Listening Port

161

SNMP Version

Version 3

V3 User Name

userV3

V3 User Read Write Limit

Read Only

V3 User Authentication Level

AuthPriv

V3 Authentication Protocol

MD5

V3 Authentication Password

\*\*\*\*\*

Show Secret

V3 Privacy Protocol

DES

V3 Privacy Password

\*\*\*\*\*

Show Secret

SNMP Trap Settings

SNMP Trap Status

Disable

Download MIB File

Get MIB File

Image 4-7-3: Admin > SNMP

#### SNMP Agent Status

If disabled, an SNMP service is not provided from the device. Enabled, the device - now an SNMP agent - can support SNMPv1, v2, & v3.

Values (selection)

Disable / Enable

#### Read Only Community Name

Effectively a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ priority.

Values (string)

public

#### Read Write Community Name

Also a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ/WRITE priority.

Values (string)

private

#### Listening Port

Enter the UDP port on which the pDDL listens for incoming SNMP get/set messages. The default is port 161.

Values (UDP Port)

161

## 4.0 Configuration

SNMP Version	
Select the SNMP version used. Only SNMP version 1 & 2 support SNMP traps (See MIB).	<b>Values (selection)</b> Version 1 / <b>Version 2</b> / Version 3
SNMP V3 User Name	
Defines the user name for SNMPv3.	<b>Values (string)</b> <b>V3user</b>
V3 User Read Write Limit	
Defines accessibility of SNMPv3; If Read Only is selected, the SNMPv3 user may only read information; if Read Write is selected, the SNMPv3 user may read and write (set) variables.	<b>Values (selection)</b> <b>Read Only</b> / Read Write
V3 User Authentication Level	
Defines SNMPv3 user's authentication level: NoAuthNoPriv: No authentication, no encryption. AuthNoPriv: Authentication, no encryption. AuthPriv: Authentication, encryption.	<b>Values (selection)</b> <b>NoAuthNoPriv</b> AuthNoPriv AuthPriv
V3 User Authentication Password	
SNMPv3 user's authentication password. Only valid when V3 User Authentication Level set to AuthNoPriv or AuthPriv.	<b>Values (string)</b> <b>00000000</b>
V3 User Privacy Password	
SNMPv3 user's encryption password. Only valid when V3 User Authentication Level set to AuthPriv (see above).	<b>Values (string)</b> <b>00000000</b>
Auth Failure Traps	
If enabled, an authentication failure trap will be generated upon authentication failure. (SNMP v1 & v2 only).	<b>Values (selection)</b> <b>Disable</b> / Enable
Trap Community Name	
The community name which may receive traps. (SNMP v1 & v2 only).	<b>Values (string)</b> <b>TrapUser</b>
Trap Manage Host IP	
Defines a host IP address where traps will be sent to (e.g. SNMP management system PC IP address). (SNMP v1 & v2 only).	<b>Values (IP Address)</b> <b>0.0.0.0</b>



## 4.0 Configuration

### SNMP Trap Settings

SNMP Trap Settings

SNMP Trap Status

Enable ▾

Trap Community Name

TrapUser

Trap Manage Host IP

0.0.0.0

0.0.0.0-Disable

Auth Failure Traps

Disable ▾

Trap Selection:

RSSI

☐ Disable
☒ Enable

RSSI Threshold

90

[30 - 120] (- dBm)

Resend Interval (seconds)

90

[0 - 65535] 0-Disable

WAN IP

☐ Disable
☒ Enable

Image 4-7-4: Admin > SNMP Trap Settings

#### SNMP Trap Status

Enable or disable autonomous SNMP traps from the device.

Values (selection)

Disable / Enable

#### Trap Community Name

Effectively a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMP traps.

Values (string)

TrapUser

#### Trap Manage Host IP

Enter the IP address of the SNMP host to which SNMP traps are sent from the device.

Values (IP Address)

0.0.0.0

#### Auth Failure Traps

Enable or Disable authentication requirements for outgoing configured SNMP event traps.

Values (selection)

Disable / Enable

#### RSSI

Enable or Disable RSSI traps. The threshold in which that traps are triggered can also be configured, as well as the frequency at which the traps are sent when the threshold has been crossed.

Values (selection)

Disable / Enable

90 (30-120) in -dBm

90 (0 - 65535 seconds, 0=disabled.)





## 4.0 Configuration

#### 4.7.4 Admin > Logout

The logout function allows a user to end the current configuration session and prompt for a login screen.

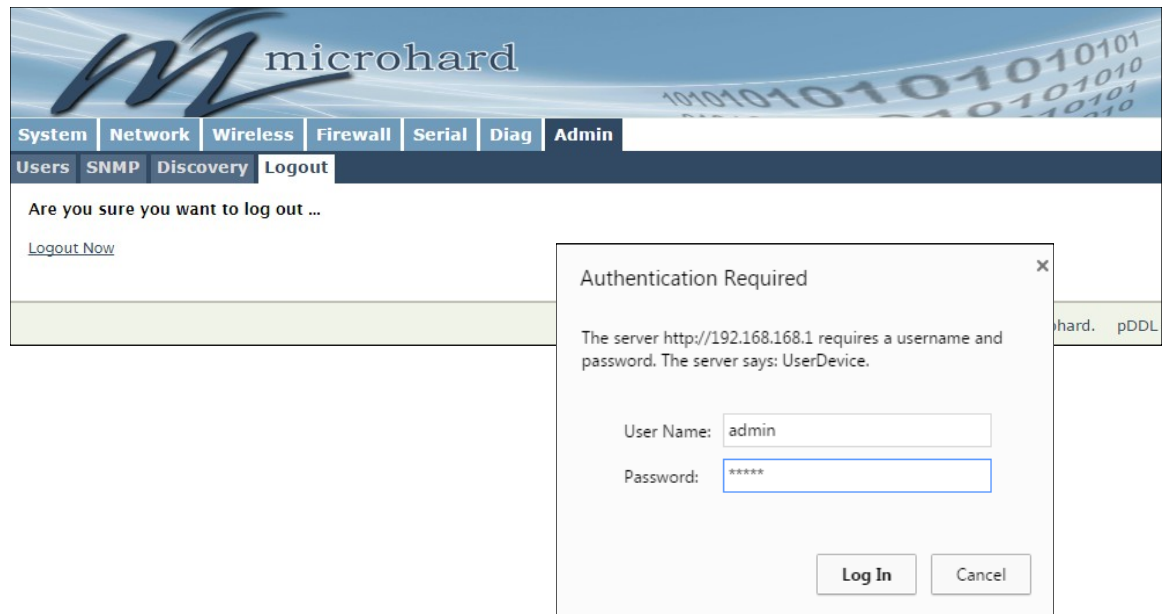


Image 4-7-6: Admin > logout

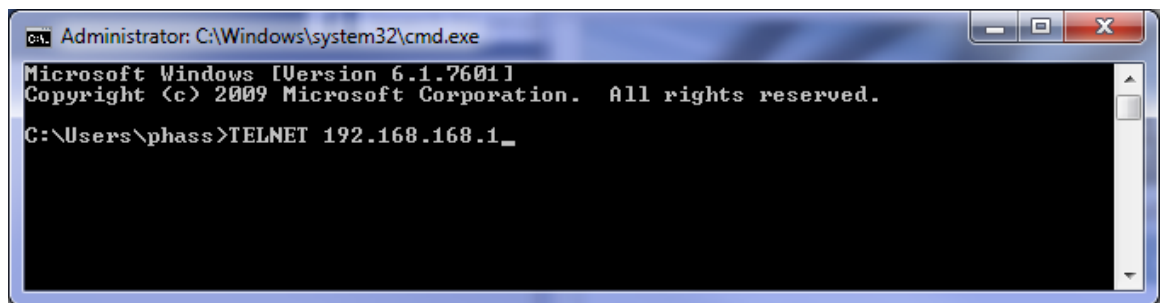
## 5.0 AT Command Line Interface

## 5.1 AT Command Overview

AT Commands can be issued to configure and manage the pDDL, via TCP/IP (telnet).

### 5.1.1 Telnet (TCP/IP)

Telnet can be used to access the AT Command interface of the pDDL. The default port is TCP Port 23. A telnet session can be made to the unit using any Telnet application (Windows Telnet, Tera Term, ProComm etc). Once communication is established, a login is required to continue.



*Image 5-1: Establishing a Telnet Session*

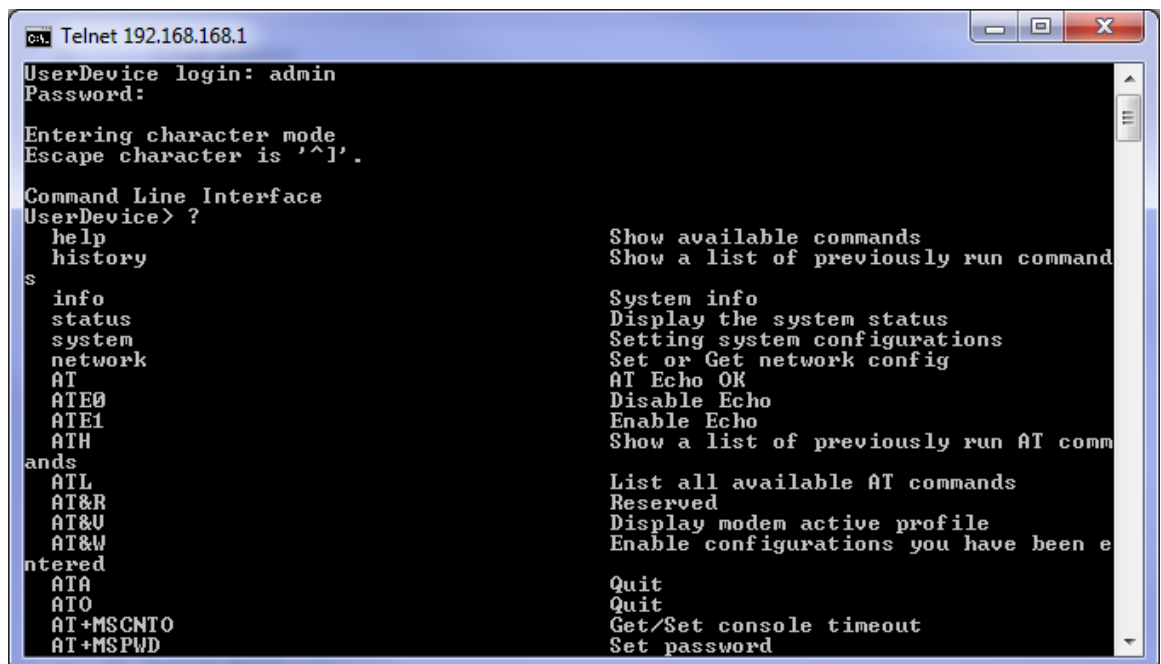
A session can be made to the WAN IP Address (if allowed in the firewall settings) for remote configuration, or to the local RJ45 interface.



The factory default network settings:

**IP: 192.168.168.1**  
**Subnet: 255.255.255.0**  
**Gateway: 192.168.168.1**

Once a session is established a login is required to continue. As seen in the Serial port setup, the default login is **admin**, and the password is **admin**. Once verified, the AT Command Line Interface menu is shown and AT Commands can now be issued. (Type "?" or Help to list the commands).



*Image 5-2: Telnet AT Command Session*

## 5.0 AT Command Line Interface

### 5.2 AT Command Syntax

The follow syntax is used when issuing AT Commands on the pDDL

- All commands start with the AT characters and end with the <Enter> key
- Microhard Specific Commands start with +M
- Help will list top level commands (ATL will list ALL available AT Commands)
- To query syntax of a command: AT+<command\_name>=?
- Syntax for commands that are used only to query a setting:  
AT<command\_name>
- Syntax for commands that can be used to query *and* set values:  
AT<command\_name>=parameter1,parameter2,... (Sets Values)  
AT<command\_name>? (Queries the setting)

#### Query Syntax:

AT+MSCNTO=? <Enter>

+MSCNTO:

Command Syntax: AT+MSCNTO=<Timeout\_s>

Parameter:

<Timeout\_s> 30 to 65535 in seconds, 0-Disable

OK

#### Setting a value:

AT+MSCNTO=300 <Enter>

OK

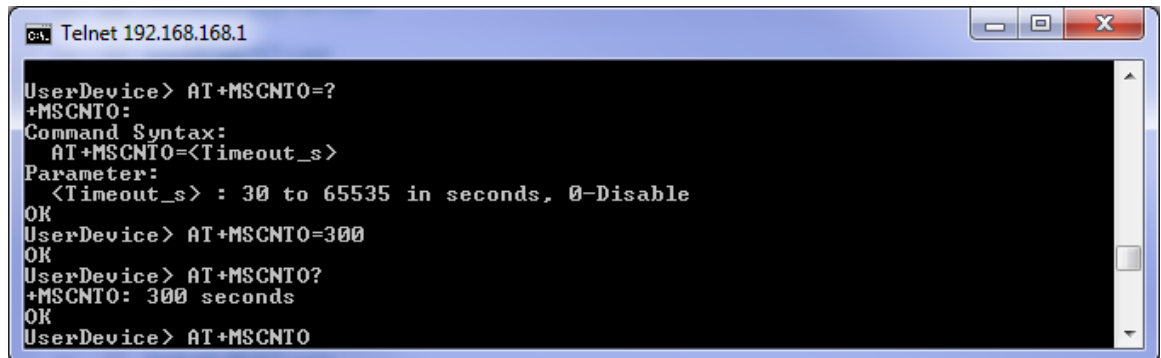
#### Query a setting:

AT+MSCNTO? <Enter>

+MSCNTO: 300 seconds

OK

A screen capture of the above commands entered into a unit is shown below:



```

C:\> Telnet 192.168.168.1

UserDevice> AT+MSCNTO=?
+MSCNTO:
Command Syntax:
  AT+MSCNTO=<Timeout_s>
Parameter:
  <Timeout_s> : 30 to 65535 in seconds, 0-Disable
OK
UserDevice> AT+MSCNTO=300
OK
UserDevice> AT+MSCNTO?
+MSCNTO: 300 seconds
OK
UserDevice> AT+MSCNTO
  
```

Image 5-3: Telnet AT Command Syntax

Once AT commands are entered, they must be saved into the file system to enable the changes.

AT&W

Saves changes.

ATO or ATA

Exits the AT Command Line Interface, if used before AT&W, changes are discarded.

## 5.0 AT Command Line Interface

### 5.3 Supported AT Commands

Basic AT Commands			
AT Command	Description	Syntax	Effect
AT	AT echo OK	AT <enter>	Immediate
ATE0	Disable echo	ATE0 <enter>	Immediate
ATE1	Enabled local echo	ATE1 <enter>	Immediate
ATH	Show a list of previously run commands	ATH <enter>	Immediate
ATL	Show a list of all available AT Commands	ATL <enter>	Immediate
AT&R	Read modem profile to editable profile. (Reserved)	AT&R <enter>	Immediate
AT&V	Read modem active profile	AT&V <enter>	Immediate
AT&W	Enable configuration changes that have been entered	AT&W <enter>	Immediate
ATA	Quit. Exits AT command session and returns to login prompt	ATA <enter>	Immediate
ATO	Quit. Exits AT command session and returns to login prompt	ATO <enter>	Immediate
Administrative AT Commands			
AT Command	Description	Syntax	Effect
AT+MADISS	Get/Set discovery service used by the modem	<b>AT+MADISS[=&lt;Mode&gt;[,&lt;Port&gt;]]</b> Mode: 0 - Disable 1 - Discoverable Port: 1 to 65535. Default is 20097	AT&W
AT+MASNMP	Get/Set SNMP service	<b>AT+MASNMP[=&lt;Mode&gt;[,&lt;ROCommunity&gt;,&lt;RWCommunity&gt;,&lt;Port&gt;,&lt;Version&gt;]]</b> <Mode>: 0 - Disable 1 - Enable <ROCommunity>: Read Only Community Name 1 to 32 characters <RWCommunity>: Read Write Community Name 1 to 32 characters <Port>: Listening Port 0 to 65535. Default is 161 <Version>: SNMP version 1 - Version 1 2 - Version 2 3 - Version 3 (Use AT+MASNMPV3 to set Authentication and Privacy parameters)	AT&W
AT+MASNMPV3	Get/Set SNMP Version 3	<b>AT+MASNMPV3=&lt;UserName&gt;,&lt;RWLimit&gt;,&lt;AuthLevel&gt;[,&lt;Auth&gt;,&lt;AuthPassword&gt;[,&lt;Privacy&gt;,&lt;PrivacyPassword&gt;]]</b> <UserName> : V3 User Name 1 to 32 characters <RWLimit> : V3 User Read Write Limit 0 - Read Only 1 - Read Write <AuthLevel> : V3 User Authentication Level 0 - NoAuthNoPriv 1 - AuthNoPriv 2 - AuthPriv <Auth> : V3 Authentication Protocol 0 - MD5 1 - SHA <AuthPassword> : V3 Authentication Password 5 to 64 characters <Privacy> : V3 Privacy Protocol 0 - DES 1 - AES <PrivacyPassword>: V3 Privacy Password 5 to 64 characters Usage: NoAuthNoPriv : AT+MASNMPV3=<UserName>,<RWLimit>,0 AuthNoPriv : AT+MASNMPV3=<UserName>,<RWLimit>,1,<Auth>,<AuthPassword> AuthPriv : AT+MASNMPV3=<UserName>,<RWLimit>,<Auth>,<AuthPassword>,<Privacy>,<PrivacyPassword>	AT&W



## 5.0 AT Command Line Interface

Administrative AT Commands (Continued)			
AT Command	Description	Syntax	Effect
AT+MASNMPTRAP	Get/Set SNMP Trap	<b>AT+MASNMPTRAP[=&lt;Mode&gt;[,&lt;Name&gt;,&lt;IP&gt;[,&lt;AuthFailureTraps&gt;]]]</b> <Mode>: 0 - Disable 1 - Enable <Name>: Trap Community Name. 1 to 32 characters <IP>: Trap Manage Host IP. Default 0.0.0.0 (Disable) <AuthFailureTraps>: 0 - Disable 1 - Enable Usage: AT+MASNMPTRAP AT+MASNMPTRAP=0 AT+MASNMPTRAP=1[,<Name>,<IP>[,<AuthFailureTraps>]]	AT&W
Serial Port AT Commands			
AT Command	Description	Syntax	Effect
AT+MCPS2	Get/Set Serial port	<b>AT+MCPS2=&lt;Mode&gt;</b> Parameters: COM2 Mode: 0 - Console 1 - Data	AT&W
AT+MCBR2	Get/Set Serial port baud rate	<b>AT+MCBR2=&lt;Baud Rate Type&gt;</b> Parameters: COM2 Baud Rate Type: 0 - 300 1 - 600 2 - 1200 3 - 2400 4 - 3600 5 - 4800 6 - 7200 7 - 9600 8 - 14400 9 - 19200 10 - 28800 11 - 38400 12 - 57600 13 - 115200 14 - 230400 15 - 460800 16 - 921600	AT&W
AT+MCDF2	Get/Set Serial port data format	<b>AT+MCDF2=&lt;Data Formate Type&gt;</b> Parameters: COM2 Data Formate Option: 0 - 8N1 2 - 8E1 3 - 8O1	AT&W
AT+MCDM2	Get/Set Serial port data mode	<b>AT+MCDM2=&lt;Data Mode Type&gt;</b> Parameters: COM2 Data Mode Option: 0 - Seamless 1 - Transparent	AT&W
AT+MCCT2	Get/Set Serial port character timeout	<b>AT+MCCT2=&lt;timeout&gt;</b> Parameters: COM2 timeout: 1 to 65535 in seconds	AT&W
AT+MCMP2	Get/Set Serial port maximum packet size	<b>AT+MCMP2=&lt;size&gt;</b> Parameters: COM2 maximum packet size: 1 to 2048	AT&W
AT+MCNCDI2	Get/Set Serial port no-connection data intake	<b>AT+MCNCDI2=&lt;Mode&gt;</b> Parameters: COM2 Mode Option: 0 - Disable 1 - Enable	AT&W
AT+MCMT2	Get/Set Serial port Modbus tcp configuration	<b>AT+MCMT2=&lt;Status&gt;</b> Parameters: COM2 Modbus Status: 0 - Disable 1 - Enable	AT&W

## 5.0 AT Command Line Interface

Serial Port AT Commands (Continued)			
AT Command	Description	Syntax	Effect
AT+MCIPM2	Get/Set Serial port IP protocol mode	<b>AT+MCIPM2=&lt;IP Protocol Config&gt;</b> Parameters: COM2 IP Protocol Config: 0 - TCP Client 1 - TCP Server 2 - TCP Client/Server 3 - UDP Point to Point 4 - UDP Point to Multipoint(P) 5 - UDP Point to Multipoint(MP) 8 - PPP	AT&W
AT+MCCT2	Get/Set Serial port tcp client configuration when IP protocol mode is TCP Client	<b>AT+MCTC2=&lt;Remote Server IP&gt;,&lt;Remote Server Port&gt;,&lt;Outgoing timeout&gt;</b> Parameters: COM2: Remote Server IP : valid IP address Remote Server Port : 1 to 65535 Outgoing timeout : 1 to 65535 in seconds	AT&W
AT+MCTS2	Get/Set Serial port tcp server configuration when IP protocol mode is TCP Server	<b>AT+MCTS2=&lt;Server Mode&gt;,&lt;Polling Timeout&gt;,&lt;Local Listening Port&gt;,&lt;Connection timeout&gt;</b> Parameters: Server Mode : 0 - Monitor; 1 - Polling Polling timeout : 1 to 65535 in seconds Local Listening Port : 1 to 65535 Connection timeout : 1 to 65535 in seconds	AT&W
AT+MCTCS2	Get/Set Serial port tcp client/server configuration when IP protocol mode is TCP Client/Server	<b>AT+MCTCS2[=&lt;Remote Server IP&gt;,&lt;Remote Server Port&gt;,&lt;Outgoing timeout&gt;,&lt;Server Mode&gt;,&lt;Polling Timeout&gt;,&lt;Local Listener Port&gt;,&lt;Incoming timeout&gt;]</b> Parameters: Remote Server IP : valid IP address Remote Server Port : 1 to 65535 Outgoing timeout : 1 to 65535 in seconds Server Mode : 0 - Monitor; 1 - Polling Polling timeout : 1 to 65535 in seconds Local Listening Port : 1 to 65535 Incoming timeout : 1 to 65535 in seconds	AT&W
AT+MCUPP2	Get/Set Serial port UDP point to point configuration when IP protocol mode is UDP point to point	<b>AT+MCUPP2[=&lt;Remote IP&gt;,&lt;Remote Port&gt;,&lt;Listening Port&gt;,&lt;UDP Timeout&gt;]</b> Parameters: Remote IP : valid IP address Remote Port : 1 to 65535 Listening Port : 1 to 65535 UDP Timeout : 1 to 65535 in seconds	AT&W
AT+MCPPP2	Get/Set Serial port PPP configuration when IP protocol mode is PPP	<b>AT+MCPPP2[=&lt;Mode&gt;,&lt;CCP negotiation&gt;,&lt;LCP Echo Failure Number&gt;,&lt;LCP Echo Interval&gt;,&lt;Local IP&gt;,&lt;Host IP&gt;,&lt;Idle Timeout&gt;,&lt;Expected String&gt;,&lt;Response String&gt;]</b> Parameters: COM2: Mode : 0 - Active; 1 - Passive CCP negotiation : 0 - Disable; 1 - Enable LCP Echo Failure Number : [0 .. 65535] LCP Echo Interval : [0 .. 65535] Local IP : Valid IP address Host IP : Valid IP address Idle Timeout : 1 to 65535 in seconds Expected String : (Optional) 0 - 63 characters Response String : (Optional) 0 - 63 characters	AT&W
AT+MCUPMP2	Get/Set Serial port UDP point to multipoint as point configuration when IP protocol mode is set to UDP point to multipoint (P)	<b>AT+MCUPMP2[=&lt;Multicast IP&gt;,&lt;Multicast Port&gt;,&lt;Listening Port&gt;,&lt;Time To Live&gt;,&lt;Multicast Interface&gt;]</b> Parameters: COM2: Multicast IP : valid IP address Multicast Port : 1 to 65535 Listening Port : 1 to 65535 Time To Live : 1 to 255 in seconds Multicast Interface : 0 - default 1 - LAN	AT&W
AT+MCUPMM2	Get/Set Serial port UDP point to multipoint as MP configuration when IP protocol mode be set to UDP point to multipoint (MP)	<b>AT+MCUPMM2[=&lt;Remote IP&gt;,&lt;Remote Port&gt;,&lt;Multicast IP&gt;,&lt;Multicast Port&gt;,&lt;Multicast Interface&gt;]</b> Parameters: COM2: Remote IP : valid IP address Remote Port : 1 to 65535 Multicast IP : valid IP address Multicast Port : 1 to 65535 Multicast Interface : 0 - default 1 - LAN	AT&W
AT+MCESCP2	Get/Set Serial support escape sequence configuration	<b>AT+MCESCP2[=&lt;Escape Mode&gt;,&lt;Escape Guard Interval&gt;,&lt;Escape Sequence String&gt;]</b> Parameters: COM2: Escape Mode : 0 - Disabled; 1 - Enabled Escape Guard Interval : 1 to 10 seconds Escape Sequence String : 3 to 7 characters	AT&W

## 5.0 AT Command Line Interface

Firewall AT Commands			
AT Command	Description	Syntax	Effect
AT+MFGEN	Get/Set firewall general configuration	<b>AT+MFGEN[=&lt;Config&gt;[,&lt;Mode&gt;]]</b> Parameters Config : 0 - WAN Remote Management 1 - WAN Request 2 - LAN to WAN Access Control 3 - Anti-Spoof 4 - Packet Normalization Mode : 0 - Disable (Block) 1 - Enable (Allow)	AT&W
AT+MFDMZ	Get/Set firewall DMZ configuration	<b>AT+MFDMZ[=&lt;DMZ Source&gt;[,&lt;DMZ Mode&gt;[,&lt;DMZ Server IP&gt;,&lt;Exception Port&gt;]]]</b> Parameters: DMZ Source : 0 - WAN DMZ Mode : 0 - Disable 1 - Enable DMZ Server IP : Valid IP address Exception Port : 0 - 65535	AT&W
AT+MFPORTFWD	Get/Set firewall Port Forwarding rule	<b>AT+MFPORTFWD[=&lt;Name&gt;[,&lt;Operation&gt;[,&lt;Source&gt;,&lt;Internal IP&gt;,&lt;Internal Port&gt;,&lt;Protocol&gt;,&lt;External Port&gt;,&lt;SNAT&gt;]]]</b> Parameters: Name : Name of Port Forwarding rule, 1 - 64 characters Operation : ADD - Add a rule EDIT - Edit a rule DEL - Delete a rule Source : 0 - WAN 1 - USB Internal IP : Valid IP address Internal Port : Valid port number, 1 - 65535 Protocol : 0 - TCP 1 - UDP 2 - TCPUDP External Port : Valid port number, 1 - 65535 Source NAT : 0 - No; 1 - Yes Usage: AT+MFPORTFWD AT+MFPORTFWD=<Name> AT+MFPORTFWD=<Name>,DEL AT+MFPORTFWD=<Name>,ADD,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port>,<SNAT> AT+MFPORTFWD=<Name>,EDIT,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port>,<SNAT>	AT&W
AT+MFMAC	Get/Set firewall MAC list	<b>AT+MFMAC[=&lt;Name&gt;[,&lt;Operation&gt;[,&lt;Action&gt;,&lt;Mac Address&gt;]]]</b> Parameters: Name : Name of firewall MAC list name, 1 - 64 characters Operation : ADD - Add a firewall MAC list EDIT - Edit a firewall MAC list DEL - Delete a firewall MAC list Action : 0 - Accept 1 - Drop 2 - Reject MAC Address : Valid MAC address Usage: AT+MFMAC AT+MFMAC=<Name> AT+MFMAC=<Name>,DEL AT+MFMAC=<Name>,ADD,<Action>,<Mac Address> AT+MFMAC=<Name>,EDIT,<Action>,<Mac Address>	AT&W
AT+MFIP	Get/SET firewall IP list	<b>AT+MFIP[=&lt;Name&gt;[,&lt;Operation&gt;[,&lt;Action&gt;,&lt;Source&gt;,&lt;IP Address&gt;[,&lt;Prefix&gt;]]]]]</b> Parameters: Name : Name of firewall IP list name, 1 - 64 characters Operation : ADD - Add a firewall IP list EDIT - Edit a firewall IP list DEL - Delete a firewall IP list Action : 0 - Accept 1 - Drop 2 - Reject Source : 0 - LAN 1 - Independent LAN 2 - WAN 3 - USB Source IP : Valid IP address Prefix : 0 ~ 32. 32 (default) - single IP address Usage: AT+MFIP AT+MFIP=<Name> AT+MFIP=<Name>,DEL AT+MFIP=<Name>,ADD,<Action>,<Source>,<IP Address>[,<Prefix>] AT+MFIP=<Name>,EDIT,<Action>,<Source>,<IP Address>[,<Prefix>]	AT&W

## 5.0 AT Command Line Interface

Firewall AT Commands (Continued)			
AT Command	Description	Syntax	Effect
AT+MFRULE	Get/Set firewall rule	<b>AT+MFRULE=[&lt;Name&gt;[,&lt;Operation&gt;[,&lt;Action&gt;,&lt;Source&gt;,&lt;Src IP Format&gt;,&lt;Src IP From/Subnet&gt;,&lt;Src IP To/Prefix&gt;,&lt;Destination&gt;,&lt;Dest IP Format&gt;,&lt;Dest IP From/Subnet&gt;,&lt;Dest IP To/Prefix&gt;,&lt;Dest Port&gt;,&lt;Protocol&gt;]]]</b> Parameters: Name : Name of firewall rule name, 1 - 64 characters Operation : ADD - Add a firewall rule EDIT - Edit a firewall rule DEL - Delete a firewall rule Action : 0 - Accept 1 - Drop 2 - Reject Source : 0 - LAN 1 - Independent LAN 2 - WAN 3 - USB 4 - None IP Format : 0 - IP Range 1 - Subnet / Prefix IP From/Subnet: Valid IP address. 0 - Set to blank IP To/Prefix : Valid IP address. 0 - Set to blank; or 0 ~ 32 for Prefix Destination : 0 - LAN 1 - Independent LAN 2 - WAN 3 - USB 4 - None IP Format : 0 - IP Range 1 - Subnet / Prefix IP From/Subnet: Valid IP address. 0 - Set to blank IP To/Prefix : Valid IP address. 0 - Set to blank; or 0 ~ 32 for Prefix Port/Range : Port 0 ~ 65535 or Port range specified as 100:200 format Protocol : 0 - TCP 1 - UDP 2 - TCPUDP 3 - ICMP	AT&W
AT+MFRST	Reset to default firewall	<b>AT+MFRST &lt;enter&gt;</b>	Immediate
Network AT Commands			
AT Command	Description	Syntax	Effect
AT+MNLAN	Show/Add/Edit/Delete the network LAN interface	<b>AT+MNLAN</b> <b>AT+MNLAN=&lt;LAN Name&gt;</b> <b>AT+MNLAN=&lt;LAN Name&gt;,DEL</b> <b>AT+MNLAN=&lt;LAN Name&gt;,ADD/EDIT,&lt;Protocol&gt;[,&lt;IP&gt;,&lt;Netmask&gt;[,&lt;Gateway&gt;]]</b> Where <Protocol>=0 <b>AT+MNLAN=&lt;LAN Name&gt;,ADD/EDIT,&lt;Protocol&gt;</b> Where <Protocol>=1 or 3 <b>AT+MNLAN=&lt;LAN Name&gt;,EDIT,&lt;Protocol&gt;[,&lt;IP&gt;,&lt;Netmask&gt;]</b> Where <Protocol>=2 and <LAN Name>="lan" Parameters: LAN Name : Name of Network LAN interface. System built-in one is "lan" Operation : ADD - Add a new LAN interface EDIT - Edit an existing LAN interface DEL - Delete an existing LAN interface Protocol : 0 - Static IP 1 - DHCP with LAN alias disabled 2 - DHCP with LAN alias enabled, only for "lan" 3 - None. Not for "lan" IP Address : Valid IP address Netmask : Valid netmask Gateway : Valid IP address. 0 - Reset	AT&W
AT+MNLANDHCP	Get/Set LAN DHCP server on LAN interface	<b>AT+MNLANDHCP=&lt;LAN Name&gt;[,&lt;Mode&gt;[,&lt;Start IP&gt;,&lt;Limit&gt;,&lt;Lease Time&gt;[,&lt;Alt. Gateway&gt;,&lt;Pre. DNS&gt;,&lt;Alt. DNS&gt;,&lt;WINS/NBNS Servers&gt;,&lt;WINS/NBT Node&gt;]]]</b> Parameters: LAN Name : Name of Network LAN interface Mode : 0 - Disable DHCP Server 1 - Enable DHCP Server Start IP : The starting address DHCP assignable IP Addresses Limit : The maximum number of IP addresses. min=1 max=16777214 Lease Time : The DHCP lease time in minutes. 2~2147483647 minutes. 0 means'infinity' Alt. Gateway : Alternate Gateway for DHCP assigned devices if the default gateway is not to be used Pre. DNS : Preferred DNS server address to be assigned to DHCP devices Alt. DNS : Alternate DNS server address to be assigned to DHCP devices WINS/NBNS Server : WINS/NBNS Servers WINS/NBT Node : WINS/NBT Node Type 0 - none 1 - b-node 2 - p-node 3 - m-node 4 - h-node	AT&W

## 5.0 AT Command Line Interface

Network AT Commands (Continued)			
AT Command	Description	Syntax	Effect
AT+MNLANSTP	Get/Set the network LAN interface: Spanning Tree (STP)	<b>AT+MNLANSTP=&lt;LAN Name&gt;[,&lt;STP&gt;]</b> Parameters: LAN Name : Name of Network LAN interface Spanning Tree : 0 - Off 1 - On	AT&W
AT+MNLANIGMP	Get/Set the network LAN interface: IGMP Snooping	<b>AT+MNLANIGMP=&lt;LAN Name&gt;[,&lt;IGMP Snooping&gt;]</b> Parameters: LAN Name : Name of Network LAN interface IGMP Snooping : 0 - Off 1 - On	AT&W
AT+MNLANDR	Get/Set the network LAN interface: Default Route	<b>AT+MNLANDR=&lt;LAN Name&gt;[,&lt;Default Route&gt;]</b> Parameters: LAN Name : Name of Network LAN interface Default Route : 0 - No 1 - Yes	AT&W
AT+MNLANDNS	Get/Set the network LAN interface: DNS	<b>AT+MNLANDNS=&lt;LAN Name&gt;[,&lt;Mode&gt;[,&lt;Primary DNS&gt;,&lt;Secondary DNS&gt;]]</b> Usage: AT+MNLANDNS=<LAN Name> AT+MNLANDNS=<LAN Name>,<Mode> Where <Mode>=0 AT+MNLANDNS=<LAN Name>,<Mode>[,<Primary DNS>,<Secondary DNS>] Where <Mode>=1 Parameters: LAN Name : Name of Network LAN interface Mode : 0 - Auto 1 - Manual Primary DNS : Valid IP Address or 0 (Reset) Secondary DNS : Valid IP address or 0 (Reset)	AT&W
AT+MNWAN	Get/Set the network WAN interface	<b>AT+MNWAN[=&lt;Mode&gt;[,&lt;Protocol&gt;[,&lt;IP&gt;,&lt;Netmask&gt;[,&lt;Gateway&gt;]]]]</b> Usage: AT+MNWAN AT+MNWAN=<Mode>,<Protocol>,<IP>,<Netmask>,<Gateway> Where <Mode>=0 and <Protocol>=0 AT+MNWAN=<Mode>,<Protocol>,<IP>,<Netmask> Where <Mode>=2 and <Protocol>=0 AT+MNWAN=<Mode>,<Protocol> Where <Mode>=0/2 and <Protocol>=1 AT+MNWAN=<Mode>,<Protocol> Where <Mode>=2 and <Protocol>=2 AT+MNWAN=<Mode> Where <Mode>=1 Parameters: Mode : 0 - Independent WAN 1 - Bridge with LAN Port 2 - Independent LAN Protocol: 0 - Static IP 1 - DHCP 2 - None IP : Valid IP address Netmask : Valid netmask Gateway : Valid IP address. 0 - Reset	AT&W
AT+MNWANDR	Get/Set the network WAN interface: Default Route	<b>AT+MNWANDR[=&lt;Default Route&gt;]</b> Parameters: Default Route : 0 - No 1 - Yes	AT&W
AT+MNWANDNS	Get/Set DNS Server when WAN port works as Independent WAN	<b>AT+MNWANDNS[=&lt;Mode&gt;[,&lt;Primary DNS&gt;,&lt;Secondary DNS&gt;]]</b> Usage: AT+MNWANDNS AT+MNWANDNS=<Mode> Where <Mode>=0 AT+MNWANDNS=<Mode>[,<Primary DNS>,<Secondary DNS>] Where <Mode>=1 Parameters: Mode : 0 - Auto 1 - Manual Primary DNS : Valid IP Address or 0 (Reset) Secondary DNS : Valid IP address or 0 (Reset)	AT&W
AT+MNWANLANDHCP	Get/Set LAN DHCP server when the WAN port is set as Independent LAN	<b>AT+MNWANLANDHCP[=&lt;Mode&gt;[,&lt;Start IP&gt;,&lt;Limit&gt;,&lt;Lease Time&gt;[,&lt;Alt.Gateway&gt;,&lt;Pre.DNS&gt;,&lt;Alt.DNS&gt;]]]</b> Usage: AT+MNWANLANDHCP AT+MNWANLANDHCP=<Mode> Where <Mode>=0 AT+MNWANLANDHCP=<Mode>,<Start IP>,<Limit>,<Lease Time>[,<Alt.Gateway>,<Pre.DNS>,<Alt.DNS>] Where <Mode>=1 Parameters: Mode : 0 - Disable DHCP Server 1 - Enable DHCP Server Start IP : The starting address DHCP assignable IP Addresses Limit : The maximum number of IP addresses. min=1 max=16777214 Lease Time : The DHCP lease time in minutes. 2~2147483647 minutes. 0 means 'infinity' Alt. Gateway : Alternate Gateway for DHCP assigned devices if the default gateway is not to be used Pre. DNS : Preferred DNS server address to be assigned to DHCP devices Alt. DNS : Alternate DNS server address to be assigned to DHCP devices	AT&W

## 5.0 AT Command Line Interface

Network AT Commands (Continued)			
AT Command	Description	Syntax	Effect
AT+MNIPMAC	Show/Add/Delete/Release/ReleaseAll the MAC-IP address binding	<b>AT+MNIPMAC[=&lt;Operation&gt;[,&lt;Name&gt;[,&lt;IP Address&gt;,&lt;MAC Address&gt;]]]</b> Usage: AT+MNIPMAC AT+MNIPMAC=SHOW,<Name> AT+MNIPMAC=ADD,<Name>,<IP Address>,<MAC Address> AT+MNIPMAC=DEL,<NAME> AT+MNIPMAC=RELEASE,<NAME> AT+MNIPMAC=RELEASEALL Parameters: Operation : SHOW - Show the details of the MAC-IP address binding ADD - Add a new MAC-IP address binding DEL - Delete an existing MAC-IP address binding RELEASE - Release the active DHCP lease RELEASEALL - Release all active DHCP leases Name : Name of the MAC-IP binding, 1-64 characters IP Address : Valid IP address MAC Address: The physical MAC address of the device or interface	AT&W
AT+MNEMAC	Get the MAC address of the local Ethernet interface	<b>AT+MNEMAC &lt;enter&gt;</b>  Sample Output: +MNEMAC: "00:0F:92:02:F9:0F" OK	Immediate
AT+MNPORT	Get/Set the Ethernet port configuration	<b>AT+MNPORT[=&lt;Ethernet Port&gt;[,&lt;Mode&gt;[,&lt;Auto Negotiation&gt;,&lt;Speed&gt;,&lt;Duplex&gt;]]]</b> Parameters: Ethernet Port : 0 - WAN 1 - LAN Mode : 0 - Auto 1 - Manual Auto-Negotiation : 0 - Off 1 - On Speed : 0 - 10 Mbit/s 1 - 100 Mbit/s Duplex : 0 - Full 1 - Half	AT&W
AT+MNSTATUS	Get the network status	<b>AT+MNSTATUS &lt;enter&gt;</b>  Sample Output: LAN Port Status General Status IP Address : 192.168.168.1 Connection Type : static Subnet Mask : 255.255.255.0 MAC Address : 00:0F:92:02:F9:0F Traffic Status Receive bytes : 262.633KB Receive packets : 3345 Transmit bytes : 168.370KB Transmit packets : 2229 WAN Port Status General Status IP Address : N/A Connection Type : dhcp Subnet Mask : N/A MAC Address : 00:0F:92:03:F9:0F Traffic Status Receive bytes : 0B Receive packets : 0 Transmit bytes : 0B Transmit packets : 0 Default Gateway : 192.168.168.1 DNS Server(s) : None  Kernel IP routing table Destination Gateway Subnet Mask Flags Metric Ref Use Iface 0.0.0.0 192.168.168.1 0.0.0.0 UG 0 0 0 br-lan 192.168.168.0 0.0.0.0 255.255.255.0 U 0 0 0 br-lan	Immediate



## 5.0 AT Command Line Interface

System AT Commands			
AT Command	Description	Syntax	Effect
AT+MSCNTO	Get/Set the console timeout	<b>AT+MSCNTO=&lt;Timeout_s&gt;</b> Parameter: <Timeout_s> : 30 to 65535 in seconds, 0-Disable	AT&W
AT+MSPWD	Set password	<b>AT+MSPWD=&lt;New Password&gt;,&lt;Confirm Password&gt;</b> Parameters: <New Password> : 5-64 characters except space <Confirm Password> : Same as <New Password>	AT&W
AT+MSGMI	Get manufacturers identification	<b>AT+MSGMI &lt;enter&gt;</b> Sample Output: +MSGMI: 2014-2016 Microhard. OK	Immediate
AT+MSSYSI	Get system summary information	<b>AT+MSSYSI &lt;enter&gt;</b> Sample Output: +MSSYSI: Ethernet Port: MAC : 00:0F:92:02:AB:22 IP : 192.168.168.1 MASK : 255.255.255.0 System: Device : UserDevice Product : pDDL Image : PWii Hardware : Rev A Software : v1.3.0 build 1024 Copyright : 2014-2016 Microhard. System Time : Tue Nov 29 14:14:32 2016 OK	Immediate
AT+MSGMR	Get modem Record information	<b>AT+MSGMR &lt;enter&gt;</b> Sample Output: +MSGMR: Hardware Version : Rev A Software Version : v1.3.0 build 1024 Copyright : 2014-2016 Microhard. System Time : Tue Nov 29 14:15:02 2016 OK	Immediate
AT+MSMNAME	Get/Set modem Name setting	<b>AT+MSMNAME=&lt;Modem_Name&gt;</b> Parameter: <Modem_Name> : 1 - 64 characters. Must be alphanumeric or dots(.), or dashes(-) or underscores(_)	AT&W
AT+MSRTF	Reset the modem to the factory default settings from non-volatile (NV) memory	<b>AT+MSRTF=&lt;Action&gt;</b> Parameter: <Action>: 0 - Pre-set action 1 - Confirm action	AT&W
AT+MSREB	Reboot the modem	<b>AT+MSREB &lt;enter&gt;</b> Sample Output: Rebooting... OK	Immediate
AT+MSNTP	Get/Set NTP server	<b>AT+MSNTP[=&lt;Mode&gt;,&lt;Server&gt;,&lt;Port&gt;,&lt;Client Interval&gt;]]</b> Parameters: <Mode> : 0 - Local Time; 1 - NTP <Server> : Valid IP Address or Name <Port> : 1 to 65535. Default is 123 <Client Interval> : 15 to 65535 in seconds, 0-Disable	AT&W
AT+MSSYSLOG	Get/Set Syslog server settings	<b>AT+MSSYSLOG[=&lt;Server&gt;,&lt;Port&gt;]]</b> Parameters: <Server> : Valid IP Address or Name. 0.0.0.0 - Disable. 1 to 256 characters <Port> : 1 to 65535. Default is 514	AT&W
AT+MSSERVICE	Get/Set service status and port	<b>AT+MSSERVICE[=&lt;Service&gt;,&lt;Mode&gt;,&lt;Port&gt;]]]</b> Parameters: <Service> : 0 - FTP 1 - Telnet 2 - SSH <Mode> : 0 - Disable 1 - Enable <Port> : 0 to 65535. For Telnet (23 by default) and SSH (22 by default) only	AT&W
AT+MSWEBUI	Get/Set Web UI protocol and port	<b>AT+MSWEBUI[=&lt;Mode&gt;,&lt;HTTP Port&gt;,&lt;HTTPS Port&gt;]]]</b> Parameters: <Mode> : 0 - HTTP/HTTPS 1 - HTTP 2 - HTTPS 3 - Disable <HTTP Port> : 2 to 65534. 80 by default <HTTPS Port> : 2 to 65534. 443 by default	AT&W



## 5.0 AT Command Line Interface

Wireless (Radio) AT Commands			
AT Command	Description	Syntax	Effect
AT+MWRADIO	Get/Set radio status, On or Off	<b>AT+MWRADIO[=&lt;Radio&gt;]</b> <Radio> 0 - Off 1 - On	AT&W
AT+MWMODE	Get/Set Radio Mode	<b>AT+MWMODE[=&lt;Mode&gt;]</b> <Mode> 0 - pDDL	AT&W
AT+MWDISTANCE	Get/Set radio Wireless Distance	<b>AT+MWDISTANCE[=&lt;Distance&gt;]</b> <Distance> 1 - 200000 in meter	AT&W
AT+MWTXPOWER	Get/Set radio Tx power	<b>AT+MWTXPOWER[=&lt;Tx Power&gt;]</b> <Tx Power> 7 - 7 dbm 8 - 8 dbm 9 - 9 dbm 10 - 10 dbm 11 - 11 dbm 12 - 12 dbm 13 - 13 dbm 14 - 14 dbm 15 - 15 dbm 16 - 16 dbm 17 - 17 dbm 18 - 18 dbm 19 - 19 dbm 20 - 20 dbm 21 - 21 dbm 22 - 22 dbm 23 - 23 dbm 24 - 24 dbm 25 - 25 dbm 26 - 26 dbm 27 - 27 dbm 28 - 28 dbm 29 - 29 dbm 30 - 30 dbm	AT&W
AT+MWBAND	Get/Set radio channel bandwidth	<b>AT+MWBAND[=&lt;Channel Bandwidth&gt;,&lt;Symbol Rate&gt;]</b> Available radio channel bandwidth for pDDL mode 0 - 8 MHz 1 - 4 MHz 2 - 2 MHz Symbol Rate: (Only need to set for 2MHz and 1MHz bandwidth) 0 - Normal 1 - Fast	AT&W
AT+MWFREQ	Get/Set radio channel-frequency (Options vary by channel bandwidth)	<b>AT+MWFREQ2400[=&lt;MHz Channel Frequency&gt;]</b> <Channel Frequency> : 4 - 2405 MHz 78- 2479 MHz	AT&W
AT+MWRXDIV	Get/Set radio diversity (reboot required)	<b>AT+MWRXDIV[=&lt;Rx Diversity&gt;]</b> <Rx Diversity> 0 - Off 1 - On	AT&W
AT+MWMCASTR	Get/Set radio Multicast Rate	<b>AT+MWMCASTR[=&lt;Multicast Rate&gt;]</b> <Multicast Rate> : 0 - QPSK FEC 1/2 1 - QPSK FEC 3/4 2 - 16-QAM FEC 1/2 3 - 16-QAM FEC 3/4 4 - 64-QAM FEC 2/3	AT&W
AT+MWVMODE	Get/Set radio mode	<b>AT+MWVMODE[=&lt;Virtual Interface Mode&gt;]</b> <Virtual Interface Mode> : 0 - Master 1 - Slave	AT&W
AT+MWVRATE	Get/Set radio TX Rate	<b>AT+MWVRATE[=&lt;Virtual Interface TX Rate&gt;]</b> <Virtual Interface TX Rate> : 0 - auto (Recommended) 1 - 64-QAM 5/6 FEC 2 - 64-QAM 3/4 FEC 3 - 64-QAM 2/3 FEC 4 - 16-QAM 3/4 FEC 5 - 16-QAM 1/2 FEC 6 - QPSK FEC 3/4 7 - QPSK FEC 1/2	AT&W

## 5.0 AT Command Line Interface

Wireless (Radio) AT Commands (Continued)			
AT Command	Description	Syntax	Effect
AT+MWEXTADDR	Get/Set radio extended addressing	<b>AT+MWEXTADDR[=&lt;Extended Addressing&gt;]</b> <Extended Addressing> : 0 - Off 1 - On	AT&W
AT+MWNETWORKID	Get/Set radio Network ID	<b>AT+MWNETWORKID[=&lt;Network ID&gt;]</b> <Network ID> Radio Virtual Interface Network ID: 1-64 characters	AT&W
AT+MWVENCRIPT	Get/Set radio Encryption Type & Key	<b>AT+MWVENCRIPT[=&lt;Encryption Type&gt;[,&lt;Key&gt;]]</b> <Encryption Type> Radio Virtual Interface Encryption Type: 0 - Disabled 1 - AES-128 <Key>: Min 8 characters, Max 64 characters	AT&W
AT+MWRESYNC	RF Re-Sync from the slave side	<b>AT+MWRESYNC &lt;enter&gt;</b>	Immediate
AT+MWINTFSCAN	Generate radio channel interference information in 10 to 30 seconds	<b>AT+MWINTFSCAN[=&lt;Sorting&gt;]</b> The spectral scan action takes about 10 to 30 seconds. <Sorting> : 0 - Not sorting the scan result (default) 1 - Sorting the scan result	Immediate
AT+MWSTATUS	Get the status of RF	<b>AT+MWSTATUS &lt;enter&gt;</b> Sample Output: General Status MAC Address : 00:0F:92:FA:38:30 Operation Mode : Master Network ID : pDDL Compatibility Mode : pDDL Bandwidth : 4 MHz Frequency : 2441 Tx Power : 20 dBm Encryption Type : AES-128 Traffic Status Receive Bytes : 0B Receive Packets : 0 Transmit Bytes : 89.076KB Transmit Packets : 550 OK Connection Info MAC Address : 00:0F:92:FA:59:F9 Tx Mod : 64-QAM FEC 5/6 Rx Mod : 64-QAM FEC 2/3 SNR (dB) : 75 RSSI (dBm) : -24	Immediate
AT+MWSNR	Get the value of SNR (Slave)	<b>AT+MWSNR &lt;enter&gt;</b> Sample Output: 43 OK	Immediate
AT+MWNOISEFLOOR	Get the value of Noise Floor (Slave)	<b>AT+MWNOISEFLOOR &lt;enter&gt;</b> Sample Output: -99 OK	Immediate
AT+MWSQTHRESH	Get/Set Squelch threshold	<b>AT+MWSQTHRESH[=&lt;Squelch Threshold&gt;]</b> Squelch Threshold : -1 to -128 (-1 = Turn off the threshold)	AT&W
AT+MWRFTST	RF Test (power cycle the device after the tests)	<b>AT+MWRFTST=&lt;Operation&gt;</b> <Operation> : 0 - Start Transmit 1 - Start Receive 2 - Stop 3 - Poll the result Note : !!! Power cycle the device after the tests for the RF link to work properly!!!	AT&W
AT+MWRSSI	Get radio RSSI	<b>AT+MWRSSI &lt;enter&gt;</b> Sample Output: 00:0F:92:FA:59:F9 -74 dBm	Immediate

## 6.0 Installation



The installation, removal, or maintenance of any antenna system components must be undertaken only by qualified and experienced personnel.

There are a number of factors to consider when preparing to deploy a radio network, several of which have been touched-upon or detailed elsewhere within this manual. Following is a listing of a number of factors, in no particular order:

### Network Topology

The pDDL currently supports Master, Slave and Mesh modes which can create either Point to Multipoint or Point to Point, or Mesh network topologies.

### Throughput

The pDDL is capable of up to 25 Mbps throughput. The network topology has an effect on how this available throughput is 'shared' between all nodes on the network.

### Distance

The physical distance between the modems dictates such things as required antenna performance and heights. When contemplating antenna types, keep in mind the directivity (omnidirectional or directional) of the antennas being used.

### Terrain

Along with distance, the terrain is a very important consideration with respect to antenna height requirements. The term 'line-of-sight' (LOS) refers to being able to 'see' one location from another - a minimum requirement for a radio signal path. In addition to LOS, adequate clearance must also be provided to satisfy 'Fresnel Zone' requirements - an obstruction-free area much greater than the physical LOS, i.e. LOS is not enough to completely satisfy RF path requirements for a robust communications link.

### Transmit Power

Having read thus far through the factors to be considered, it should be clear that they are all interrelated. Transmit power should be set for the minimum required to establish a reliable communications path with adequate fade margin. Required transmit power is dictated primarily by distance, antenna type (specifically the 'gain' of the antennas being used), and the receive sensitivity of the distant modem. Cable and connector losses (the physical path from the modem's 'antenna connector' to the antenna's connector) must also be taken into account.

### Receive Sensitivity

The Pico Series has exceptional receive sensitivity, which can produce a number of benefits, such as: added fade margin for a given link, being able to use less expensive coaxial cable or antenna types, being able to operate at greater distances for a given distant transmitter power (perhaps negating the requirement for a Repeater site!). Distance, antenna gain, transmit power, and receive sensitivity are critical 'numbers' for radio path calculations. Fortunately, the Pico Series features the maximum available transmit power combined with exceptional receive sensitivity - two 'numbers' which will produce the most favorable path calculation results.

## 6.0 Installation

---

### **Fade Margin**

When all radio path numbers are being considered and hardware assumptions are being made, another factor to consider is the 'fade margin' of the overall system. The fade margin is the difference between the anticipated receive signal level and the minimum acceptable receive level (receive sensitivity). Being that the Pico Series performs to exacting specifications, the overall deployment should be such that the modems may be utilized to their full potential to provide a reliable and robust communications link. A typical desired fade margin is in the order of 20dB, however oftentimes a 10dB fade margin is acceptable.

### **Frequency**

The 2.4 GHz frequency range is not effected by rain to any significant degree, and is also able to penetrate through foliage and 'around obstacles' to a certain degree. This being the case, some may choose to scrimp on the physical deployment, particularly when it comes to antenna (tower) heights. Path calculations provide results which specify 'required' antenna heights. For cost savings and in taking advantage of the characteristics of the frequency range, sometimes the height requirements are not adhered to: this may result in unreliable communications.

### **Power Requirements**

The Pico Series may be integrated into a system (Development Board, or custom) which accepts a range of DC input voltages (supply current requirements must also be met). In some deployments, power consumption is critical. A number of features related to minimizing power consumption are available with the pDDL such the ability to operate at lower transmit power given the receive sensitivity of the distant modem.

### **Interference**

The channel selection of the pDDL often allows it to work well in an environment within which there may be sources of in-band interference. Cavity filters are also available if required: contact Microhard Systems Inc. for further information.

## 6.0 Installation

### 6.1 Path Calculation



FCC regulations allow for up to 36dBi effective isotropic radiated power (EIRP). The sum (in dBm) of the transmitted power, the cabling loss, and the antenna gain cannot exceed 36dBi.

Assuming adequate antenna heights, a basic formula to determine if an adequate radio signal path exists (i.e. there is a reasonable fade margin to ensure reliability) is:

$$\text{Fade Margin} = \text{System Gain} - \text{Path Loss}$$

*where all values are expressed in dB.*

As discussed on the previous page, a desired fade margin is 20dB.

System gain is calculated as follows:

$$\text{System Gain} = \text{Transmitter Power} + (\text{Transmitter Antenna Gain} - \text{Transmitter Cable and Connector Losses}) + (\text{Receiver Antenna Gain} - \text{Receiver Cable and Connector Losses}) + |\text{Receiver Sensitivity}|$$

*where all values are expressed in dB, dBi, or dBm, as applicable.*

Assuming a path loss of 113dB for this example, the fade margin = 143-113 = 30dB.

30dB exceeds the desired fade margin of 20dB, therefore this radio communications link would be very reliable and robust.

On the following page are examples of actual path loss measurements taken in an open rural environment; the path loss numbers do not apply to urban or non-LOS environments.

#### Example:

Tx power = 30dBm  
Tx antenna gain = 6dBi  
Tx cable/connector loss = 2dB  
Rx antenna gain = 3dBi  
Rx cable/connector loss = 2dB  
Rx sensitivity = -108dBm

$$\begin{aligned} \text{System Gain} &= [30 + (6 - 2) + (3 - 2) + 108] \text{dB} \\ &= [30 + 4 + 1 + 108] \text{dB} \\ &= 143 \text{dB} \end{aligned}$$

## 6.0 Installation



To satisfy FCC radio frequency (RF) exposure requirements for mobile transmitting devices, a separation distance of 23cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operation at less than this distance is not recommended. The antenna used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.



Never work on an antenna system when there is lightning in the area.

Distance (km)	Master Height (m)	Remote Height (m)	Path Loss (dB)
5	15	2.5	116.5
5	30	2.5	110.9
8	15	2.5	124.1
8	15	5	117.7
8	15	10	105
16	15	2.5	135.3
16	15	5	128.9
16	15	10	116.2
16	30	10	109.6
16	30	5	122.4
16	30	2.5	128.8

Table 6-1: Path Loss

### 6.2 Installation of Antenna System Components

The installation, removal, or maintenance of any antenna system components must be undertaken only by qualified and experienced personnel.

#### 6.2.1 Antennas

The two most common types of antenna are the omnidirectional ('omni') and directional (Yagi).

An **omni** typically has 3-6dBi gain and spreads its energy in all directions (hence the name 'omnidirectional'). The 'pattern' of the energy field is in the shape of a donut, with the antenna mounted vertically at the centre. This vertical-mounted antenna produces a signal which is vertically 'polarized'.

A **Yagi** has a more focused antenna pattern, which results in greater gain: commonly, 6-12dBi. The pattern of a Yagi is in the shape of a large raindrop in the direction in which the antenna is pointed. If the elements of the Yagi are perpendicular to the ground (most common orientation) the radiated signal will be vertically polarized; if parallel to the ground, the polarization is horizontal.

The network topology, application, and path calculation are all taken into consideration when selecting the various antenna types to be used in a radio network deployment.

## 6.0 Installation



Direct human contact with the antenna is potentially unhealthy when a pDDL is generating RF energy.

Always ensure that the pDDL equipment is powered down (off) during installation.



To comply with FCC regulations, the maximum EIRP must not exceed 36dBm.



All installation, maintenance, and removal work must be done in accordance with applicable codes.

### 6.2.2 Coaxial Cable

The following types of coaxial cable are recommended and suitable for most applications (followed by loss at 2.4GHz, in dB, per 100 feet):

- LMR 195 (10.7)
- LMR 400 (3.9)
- LMR 600 (2.5)

For a typical application, LMR 400 may be suitable. Where a long cable run is required - and in particular within networks where there is not a lot of margin available - a cable with lower loss should be considered.

When installing cable, care must be taken to not physically damage it (be particularly careful with respect to not kinking it at any time) and to secure it properly. Care must also be taken to affix the connectors properly - using the proper crimping tools - and to weatherproof them.

### 6.2.3 Surge Arrestors

The most effective protection against lightning-induced damage is to install two lightning surge arrestors: one at the antenna, the other at the interface with the equipment. The surge arrestor grounding system should be fully interconnected with the transmission tower and power grounding systems to form a single, fully integrated ground circuit. Typically, both ports on surge arrestors are N-type female.

### 6.2.4 External Filter

Although the Pico Series is capable of filtering-out RF noise in most environments, there are circumstances that require external filtering. Paging towers and cellular base stations in close proximity to the pDDL's antenna can desensitize the receiver. Microhard Systems Inc.'s external cavity filter eliminates this problem. The filter has two N-female connectors and should be connected inline at the interface to the RF equipment.



## Appendix A: Serial Interface

Module (DCE)	Signal	Host (e.g. PC) (DTE)	
1	DCD →	IN	Arrows denote the direction that signals are asserted (e.g., DCD originates at the DCE, informing the DTE that a carrier is present).
2	RX →	IN	The interface conforms to standard RS-232 signals, so direct connection to a host PC (for example) is accommodated.
3	← TX	OUT	
4	← DTR	OUT	
5	SG		
6	DSR →	IN	
7	← RTS	OUT	The signals in the asynchronous serial interface are described below:
8	CTS →	IN	

**DCD** *Data Carrier Detect* - Output from Module - When asserted (TTL low), DCD informs the DTE that a communications link has been established with another device.

**RX** *Receive Data* - Output from Module - Signals transferred from the pDDL are received by the DTE via RX.

**TX** *Transmit Data* - Input to Module - Signals are transmitted from the DTE via TX to the pDDL.

**DTR** *Data Terminal Ready* - Input to Module - Asserted (TTL low) by the DTE to inform the module that it is alive and ready for communications.

**SG** *Signal Ground* - Provides a ground reference for all signals transmitted by both DTE and DCE.

**DSR** *Data Set Ready* - Output from Module - Asserted (TTL low) by the DCE to inform the DTE that it is alive and ready for communications. DSR is the module's equivalent of the DTR signal.

**RTS** *Request to Send* - Input to Module - A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.

**CTS** *Clear to Send* - Output from Module - A "handshaking" signal which is asserted by the DCE (TTL low) when it has enabled communications and transmission from the DTE can commence. When hardware handshaking is used, the CTS signal indicates to the host that the DCE can receive data.

Notes: It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the module (DCE); the module transmits data on the RX line, and receives on TX.

"DCE" and "module" are often synonymous since a module is typically a DCE device.

"DTE" is, in most applications, a device such as a host PC.

## Appendix B: Firmware Recovery Procedure

In event that your unit becomes unresponsive it may be required to perform a firmware recovery procedure outlined below:

1. Download and save firmware file in a local folder, for example C:\;

2. Separate the PC from the network and set IP to static:

```
192.168.1.1
255.255.255.0
```

3. Connect PC Ethernet port to the Ethernet port of the modem to be recovered

4. Start a ping on the PC

```
C:\>ping 192.168.1.39 -t
Pinging 192.168.1.39 with 32 bytes of data:
Request timed out.
Request timed out.
```

5. Power cycle modem while pressing and holding CFG (Config) button;

6. Release the CFG button when ping responded:

```
C:\>ping 192.168.1.39 -t
Pinging 192.168.1.39 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
```

Note, If ping responds as shown above, then you can probably recover the unit, please proceed. Otherwise, send the unit back for RMA.

7. Now use TFTP to push firmware file into the corrupted unit:

*For example, on Windows XP using following command line:*

```
tftp -i 192.168.1.39 put pDDL-v1_1_0-r1003.bin (use the filename saved).
```

8. Wait until above command to successfully transferred the image, similar message should show

*Transfer successful: xxxxxx bytes in 5 seconds, nnnnnn bytes/s, note the number might change for different firmware file*

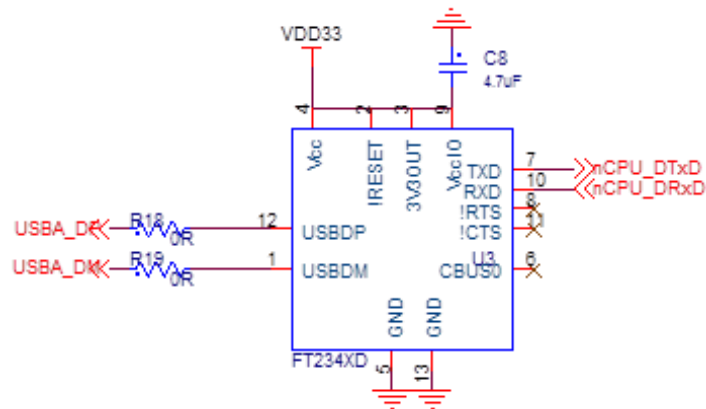
Note, if you see message above, the unit will re-flash itself and reboot, otherwise call for help or send back for RMA.

9. Wait for the unit to recover and reboot.



## Appendix D: Serial Port Extension

The pDDL can support a second serial port by utilizing a FT234XD USB to serial UART interfaced to the USB lines of the pDDL. The sample circuit below shows how this is done.



Drawing App-D: FTDI USB to Basic UART

## Appendix E: Troubleshooting

---

Below is a number of the common support questions that are asked about the pDDL. The purpose of the section is to provide answers and/or direction on how to solve common problems with the pDDL.

---

**Question:** *What is the default IP Address of the pDDL?*

**Answer:** The default IP address for the LAN is 192.168.168.1.

---

**Question:** *What is the default login for the pDDL?*

**Answer:** The default username is **admin**, the default password is **admin**. You will be prompted to change the password as soon as you login using the default.

---

**Question:** *How do I reset my modem to factory default settings?*

**Answer:** If you are logged into the pDDL navigate to the System > Maintenance Tab. If you cannot log in, power on the pDDL and wait until the modem complete the boot up process. Press and hold the Config button for 8 seconds to reset to a factory default Master.

---

**Question:** *I connected a device to the serial port of the pDDL and nothing happens?*

**Answer:** In addition to the basic serial port settings, the IP Protocol Config has to be configured. Refer to the COM0/1 Configuration pages for a description of the different options.

---

Additional topics will be added in future releases.



150 Country Hills Landing NW  
Calgary, Alberta  
Canada T3K 5P3

Phone: (403) 248-0028  
Toll Free: 1-855-353-0028  
[www.microhardcorp.com](http://www.microhardcorp.com)