



# **MPU5**

# **BASIC OPERATOR MANUAL**

**VERSION 2.5**

**03EN073**  
**Rev. G**



Copyright 2010 - 2018, Persistent Systems, LLC. All rights reserved. Wave Relay® is a registered trademark of Persistent Systems, LLC ("Persistent"). This Basic Operator Manual (the "Manual") contains information that is the sole property of Persistent Systems, LLC. Therefore, the Manual may not be excerpted, summarized, copied, distributed, or otherwise published, in whole or in part, without the prior written permission of Persistent Systems, LLC. All other product and service names, trademarks, logos, and brands are property of their respective owners. All non-Persistent company, product, and service names and all non-Persistent trademarks used in this Manual are for identification purposes only. Use of these non-Persistent names, trademarks, logos, and brands does not imply endorsement.



# **READ MANUAL BEFORE OPERATION**

**DO NOT SWAP RADIO MODULES WHILE UNIT IS POWERED ON!**

**DO NOT POWER ON UNIT WITHOUT ANTENNAS ATTACHED!**

Copyright 2010 - 2018 Persistent Systems, LLC  
Issued: July, 2018

## **PERSISTENT SYSTEMS**

Headquartered in New York City since 2007, Persistent Systems LLC is a global communications technology company which develops, manufactures and integrates a patented and secure Mobile Ad Hoc Networking (MANET) system: Wave Relay®. The company's industry-leading R&D team has designed wireless networking protocols to support their cutting edge Wave Relay® system and has designed MIMO radios to allow the Wave Relay® MANET to achieve its highest potential. Wave Relay® is capable of running real-time data, video, voice and other applications under the most difficult and unpredictable conditions. Their suite of products is field proven and utilized in Commercial, Military, Government, Industrial, Agriculture, Mining, Oil and Gas, Robotics, and Unmanned System markets.

## **THE MPU5**

The MPU5 is the Next Generation Wave Relay® platform. Leveraging multiple leading edge technologies such as MIMO and Android™, the MPU5 is a smart radio that delivers increased performance, reliability, and capability to the end user in a small, cost-efficient package. Stream multiple HD Video feeds, run commercial and custom apps, view situational awareness, and communicate with high quality audio all with a single device and a minimal number of accessories.

## **WAVE RELAY® MANET**

The Wave Relay® System is a peer-to-peer wireless MANET networking solution in which there is no master node. If any device fails, the rest of the devices continue to communicate using any remaining connectivity. By eliminating master nodes, gateways, access points, and central coordinators from the design, Wave Relay® delivers high levels of fault tolerance regardless of which nodes might fail. The system is designed to maximize the capacity of the radio frequency (RF) spectrum and to minimize the network overhead. While optimizing efficiency, Wave Relay® also implements techniques that increase multicast reliability. The advanced multicast functionality allows the system to support both multicast voice and video over IP.

Wave Relay® is designed to maintain high bandwidth connectivity among devices that are on the move. The system is scalable, enabling it to incorporate unlimited meshed devices into the wireless network, where the devices themselves form the communication infrastructure. Even in highly dynamic environments, the system is able to

maintain connectivity by rapidly re-routing data as necessary. Wave Relay® is a self-forming and self-healing network where nodes can move freely within the network. Critical information flows reliably throughout the network while individual data paths are able to adapt at sub-second intervals. This unique approach creates an ideal environment for maximizing performance across the available communications medium. Customers leverage Wave Relay®'s straight forward and effective architecture to enable a true "Plug and Play" capability. Deploying a Wave Relay® network is as simple as connecting a standard Ethernet cable; customers are immediately connected to everything on the network.

Wave Relay® is a seamless wireless networking system offering a dynamic and reliable solution for all mobile networking needs. The MPU5 offers the Wave Relay® MANET combined with other leading edge technologies in a single smart radio.

## **CONTACT PERSISTENT SYSTEMS**

### **Persistent Systems**

Tel: (212) 561-5895 | [www.persistentsystems.com](http://www.persistentsystems.com)

### **Persistent Systems Support**

Email: [support@persistentsystems.com](mailto:support@persistentsystems.com) | OS Ticket: [www.persistentsystems.com/ps-support](http://www.persistentsystems.com/ps-support)

### **Persistent Systems RMA**

Email: [rma@persistentsystems.com](mailto:rma@persistentsystems.com)

### **Persistent Systems Sales**

Email: [sales@persistentsystems.com](mailto:sales@persistentsystems.com)

### **Persistent Systems Training**

Email: [training@persistentsystems.com](mailto:training@persistentsystems.com)

<b>Introduction</b>	<b>4</b>
Persistent Systems	4
The MPU5	4
Wave Relay® MANET	4
<b>Safety</b>	<b>12</b>
<b>Suggested Hardware</b>	<b>16</b>
<b>Part I: Physical Setup</b>	<b>17</b>
<b>Section A: RF Setup</b>	<b>17</b>
Inserting the Radio Module	20
Connecting Antennas	22
<b>Section B: Power</b>	<b>26</b>
Connecting Power	28
Removing Power	30
Powering On the Unit	32
<b>Section C: Side Connector Cables</b>	<b>34</b>

Parts List	35
Connecting a Cable to a Side Connector	36
<b>Part II: Software Setup</b>	<b>40</b>
<b>Section A: Configuring the Management Computer</b>	<b>40</b>
Parts List	40
Configuring the Management Computer (Windows)	42
Configuring the Management Computer (Linux)	48
<b>Section B: Connecting the MPU5 to the Management Computer</b>	<b>49</b>
Parts List	49
<b>Section C: Accessing the Web Management Interface</b>	<b>52</b>
Parts List	52
<b>Section D: Basic Network Setup</b>	<b>60</b>
Security Key	60
Assigning IP Address and Interface Names	62
Rebooting an Individual Node	65

Network Node List	66
<b>Part III: Testing Connectivity</b>	<b>70</b>
Check Neighbor Node Status	70
Perform a Throughput Test	72
Throughput Test Logging	74
<b>Part IV: Using the Web Management Interface</b>	<b>76</b>
View Individual Node Information	76
Configuring Radio Settings for a Single Node	78
Upgrading Firmware	80
Creating a Configuration File	82
Loading Settings from a Configuration File	84
Reset Node to Factory Configuration	86
Check GPS Status	87
Network Status Tab	88
Network Visualization	90



<b>Part V: Device Operation</b>	<b>94</b>
Zeroize the Security Key	94
Connect a Camera to the MPU5	96
Configuring Video Settings	98
Video Kiosk Mode	108
Connect an EUD or Handheld Display to the MPU5	114
Connecting a Monitor or TV to the Wave Relay® MPU5	116
Connect USB Accessories to the MPU5	119
Install Android™ Apps on the MPU5	121
Using Android™ Screenshot	124
Network Configuration Tab	126
Connect a PTT Device to the MPU5	128
Configure PTT Settings	130
Enable Push-to-Talk	131
Set Earpiece Volume	131
Set Microphone Level	132

# TABLE OF CONTENTS

Set Transmit Mode	133
Set Transmit or Receive Audible Checktone	134
Enable/Disable Low Battery Audible Notification	135
Selecting Channels	136
Customize a PTT Channel	136
Using Wave Relay® Push-to-Talk	138
Using Flash Override	139
<b>Professional Installer – Compliance</b>	<b>140</b>
<b>Attachments</b>	<b>148</b>





Lire et comprendre les consignes de sécurité d'emploi et tout de l'opérateur avant d'utiliser cet équipement

## SAFETY WARNINGS

Handle Safely:



- ▶ Falling while installing or removing equipment can cause serious injury.
- ▶ If installing on a tower or any other tall locations, use proper lifting techniques and wear proper protective equipment.
- ▶ Tomber lors de l'installation ou de retirer l'équipement peut causer des blessures graves.
- ▶ Si vous installez sur une tour ou d'autres endroits de hauteur, utiliser des techniques de levage appropriées et porter un équipement de protection approprié.

### Electrical Shock and Fires:



- ▶ Understand and follow all local codes and regulations when installing electrical equipment.
- ▶ Only use approved battery and/or power supplies.
- ▶ Comprendre et respecter tous les codes et règlements locaux lors de l'installation des équipements électriques.
- ▶ Utilisez uniquement la batterie et les alimentations ou approuvée.

### RF Exposure:



- ▶ Prevent injury from exposure to high frequency fields.
- ▶ See antenna separation instructions in the Compliance section of this manual.
- ▶ Do not operate with antenna removed. This can increase RF exposure risks and/or damage the equipment.
- ▶ Prévenir les blessures d'exposition aux champs de haute fréquence.
- ▶ Voir les instructions de séparation de l'antenne dans la section de la conformité de ce manuel.
- ▶ Ne pas faire fonctionner avec antenne enlevée. Cela peut augmenter les risques d'exposition aux radiofréquences et ou endommager l'équipement.

**CAUTION**  
**DEVICE UTILIZES LITHIUM ION BATTERY**  
**RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.**  
**DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS**

---

**MISE EN GARDE**  
**Dispositif utilise la batterie Ion Lithium**  
**RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉ PAR UN TYPE INCORRECT.**  
**Jetez les piles usagées selon**  
**LES INSTRUCTIONS**

### **Lithium Batteries Handling**

- ▶ Lithium ion batteries are defined as Class 9 dangerous goods by the IATA Dangerous Goods Regulations.
- ▶ Handle with care.
- ▶ Do not use if package is damaged - it can cause fire.

### **Disposing of Used Batteries**

- ▶ Disposal should be done in accordance with applicable regulations, which vary from country to country as well as by state and local governments. In most countries, trashing of used batteries is forbidden and disposal can be done through non-profit organizations mandated by local au-

thorities or organized by professionals.

- ▶ Incineration of lithium cells and batteries by consumers is not recommended. Incineration should be done at a properly permitted facility that can handle this waste.

---

### **Manipulation des batteries lithium**

- ▶ Les batteries au lithium-ion sont définies comme Classe 9 marchandises dangereuses par le Règlement sur les marchandises dangereuses de l'IATA.
- ▶ Manipuler avec soin.
- ▶ Ne pas utiliser si l'emballage est dommage, il peut provoquer un incendie.

### **Mise au rebut des batteries usagées**

- ▶ L'élimination doit être effectuée conformément aux réglementations applicables, qui varient d'un pays à l'autre ainsi que par les gouvernements d'État et locaux. Dans la plupart des pays, le saccage des batteries usagées est interdit et l'élimination peut être faite par les organisations à but non lucratif mandatées par les autorités locales ou organisées par des professionnels.
- ▶ L'incinération des cellules et batteries au lithium par les consommateurs est déconseillée. L'incinération devrait être faite dans une installation dûment autorisée qui peut gérer ces déchets.

See Attached Battery Spec Sheet, MSDS, and compliance document for more information

### Suggested Additional Hardware

- ▶ **#1 Phillips Head Screwdriver:** Used to attach/detach radio module
- ▶ **TPI Kit:** Allows for antenna and RF cable matching
- ▶ **RF cable at various lengths (LMR-400):** Allows for flexibility in antenna setup
- ▶ **Ethernet Cables**
- ▶ **Ethernet Female-to-Female Extenders**
- ▶ **HD Screen or TV with HDMI input:** Displays Android™ computer interface and/or streaming video
- ▶ **Laptop with Administrator Access:** Used for device configuration
- ▶ **USB Thumb Drives:** Used for software configuration storage and loading



## Part I: Physical Setup

### Section A: RF Setup

#### What Will I Learn?

- ▶ How to insert radio modules into the MPU5 chassis
- ▶ How to attach antennas to the MPU5

## PHYSICAL SETUP: RF SETUP





**WARNING!:** User **MUST** refer to the **Professional Installer – Compliance** Section of this manual for approved antenna types. This warning applies only to RF-2100 with the FCC ID 2AG3J-RF-2100 and RF-5100 with the FCC ID 2AG3J-RF-5100.



## How do I tell if my antennas and radio modules are compatible?

- 1 Find the part numbers on the antennas. Antenna part numbers are on a sticker wrapped around the base of the antenna.
- 2 Find the part number on the radio module. The radio module part number is on a sticker on the back of the radio module.
- 3 Each part number will begin with ANT- (antennas) or RF- (radio modules) followed by four (4) digits. The first digit references the radio band of the part. Make sure that the first digit of the antennas and radio module match.



**WARNING!:** DO NOT use mismatched antennas and radio modules. This configuration will result in very poor performance and/or damage to the device. If you do not have matching antennas and radio modules, contact Persistent Systems.



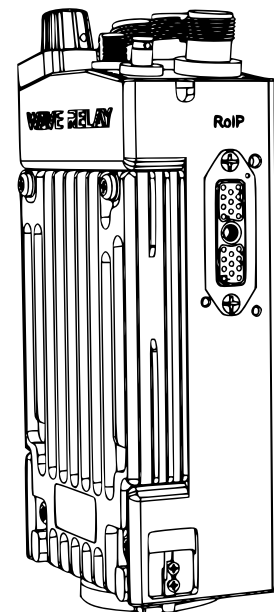
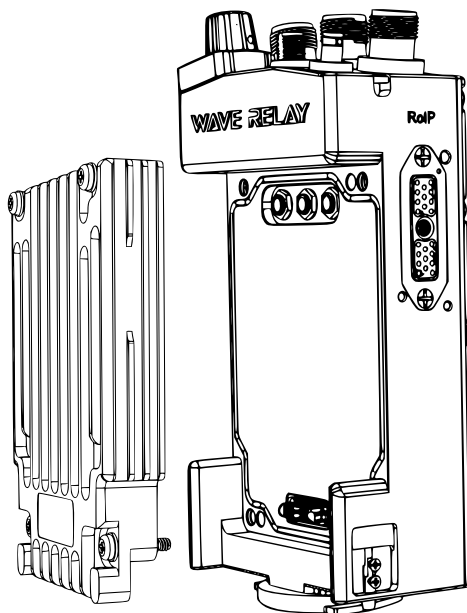
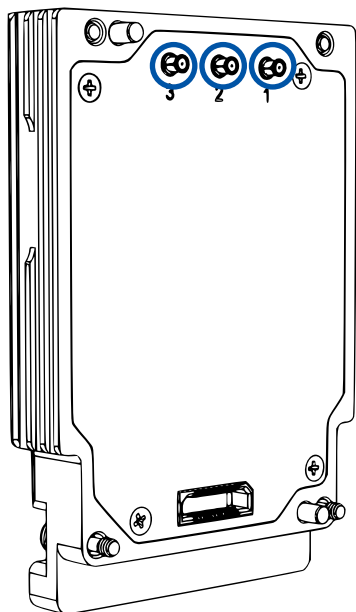
**WARNING!:** DO NOT switch radio modules while device is powered on. Power off device before changing radio modules.



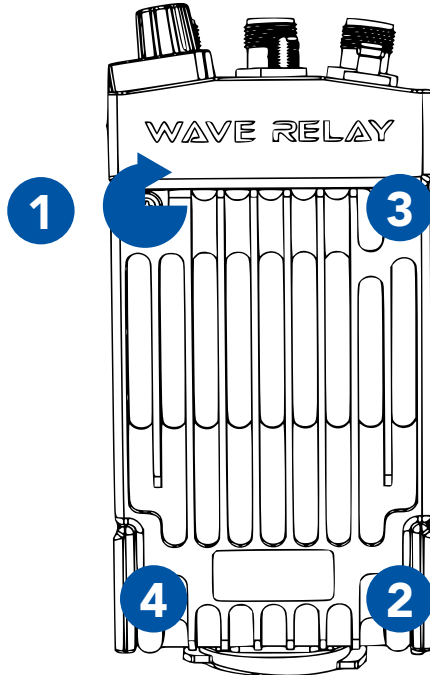
**WARNING!:** the MPU5 is not IP68 rated when the radio module is not attached. Ensure you are in a dry, dust-free environment before changing radio modules.

## Inserting the Radio Module

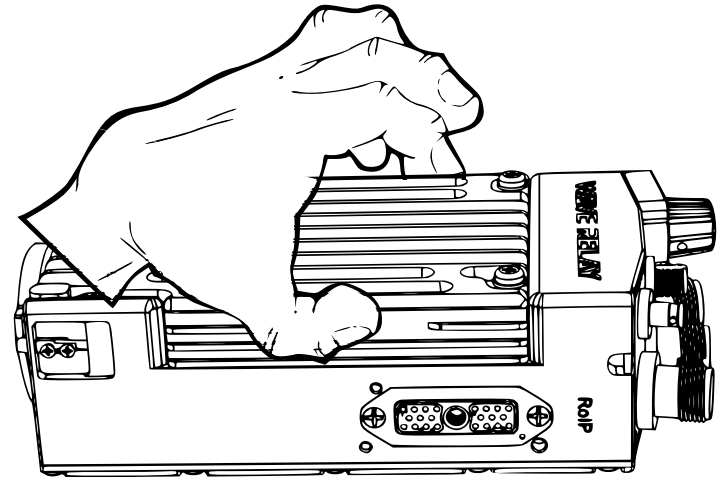
- 1** If there are **rubber caps** on the radio module contacts, **remove** them.
- 2** **Align** the radio module with the chassis.
- 3** **Apply even force** and **press** the radio module into the chassis.



- 4** Tighten screws clockwise in **diagonal** order with a #1 Phillips Head screwdriver until they stop (min. **4 in-lbs.** of torque)

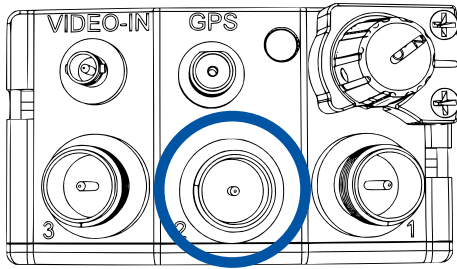


- 5** Pull on the radio module to verify that it is attached securely. Ensure there are no gaps in between the radio module and the MPU5 chassis.

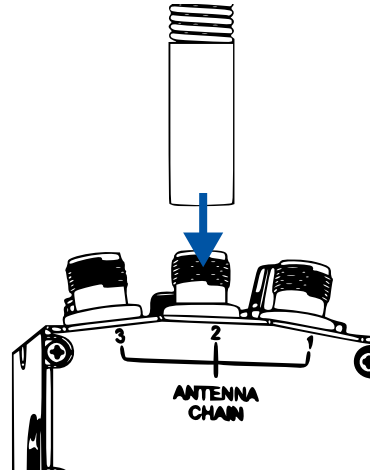


## Connecting Antennas

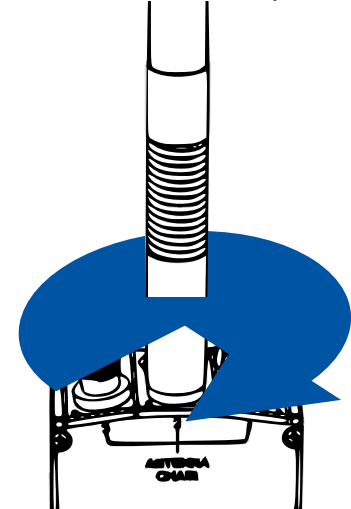
- 1 Start with the **middle** antenna port.



- 2 Align the **RF connector** on the antenna with the **RF connector** on the unit.



- 3 **Twist** the antenna clockwise until it is fully mated.

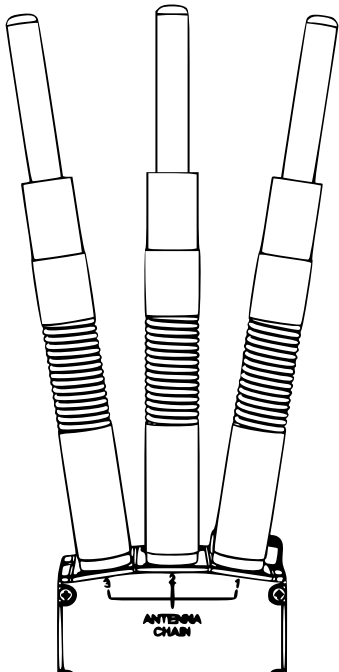


## Tips & Tricks

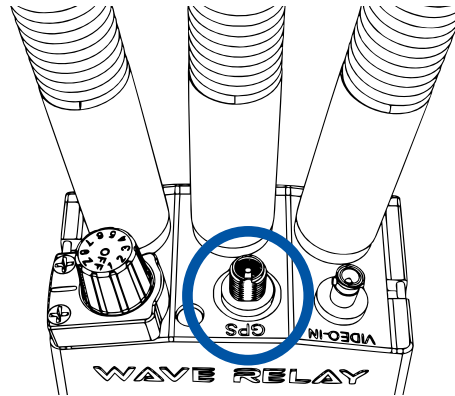
- ▶ You can use a TPI Kit and/or extra LMR-400 RF Cables to remote antennas away from the unit. This setup is particularly useful for mounted or operations center configurations.
- ▶ To operate in SISO mode, you only need to attach an antenna to the antenna port for the chain you want to use.

**!** **WARNING!:** if you want to operate in SISO mode, unused antenna chains **MUST** be turned off (See p. 78).

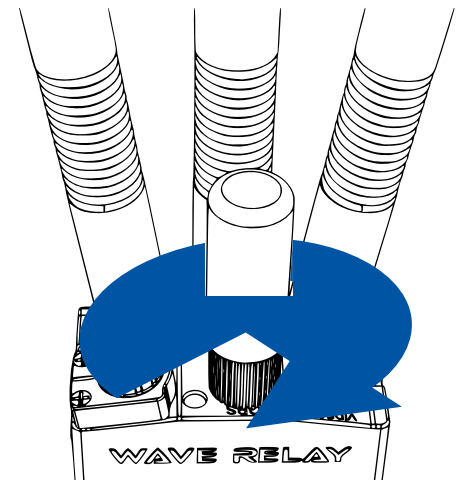
- 4** Repeat **Steps 1 - 3** for the remaining two RF antennas.



- 5** Align the **SMA connector** on the GPS antenna with the **SMA connector** on the unit.






- 6** Twist the antenna clockwise until it is fully mated.






### How do I ensure that the radio module is aligned properly?

The three RF connectors on the radio module will align with the three RF connectors on the chassis. When aligned properly, the engraved writing on the radio module will be facing the same direction as the writing on the chassis.


### What do I do if the antennas won't screw onto the RF connectors?

-  Ensure that you are using antennas with RP-TNC Male connectors or an appropriate adapter from your TPI kit.
-  Ensure that the connectors on both the unit and antennas are not damaged.
-  Ensure that there are no foreign objects in any of the connectors.

### What do I do if the radio module won't insert into the chassis?

-  Ensure that the radio module is aligned properly.
-  Ensure that the connectors on the radio module are not bent.
-  Ensure that there are no foreign objects in any of the connectors, on the bottom of the radio module, or in the chassis well.

### How do I tell if the antennas are connected properly?

-  When an antenna is mated properly, the threads on the connector will not be visible. However, there may be a small space between the antenna and the chassis.



## What Can I Do Now?

- ▶ Swap radio modules and antennas to change the RF band you are capable of operating on
- ▶ Swap out broken radio modules and antennas
- ▶ Setup hardware to receive GPS connectivity
- ▶ Remote antennas away from the unit

### Section B: Power

#### What Will I Learn?

- ▶ How to connect a power source to the MPU5
- ▶ How to power on the MPU5

 **WARNING!:** the MPU5 requires an 8 hour charge in order to retain unit settings for 30 days.

#### How can I use my old power accessories from previous Wave Relay products with my MPU5?

You can use your MPU4 twist locking battery pack or BB batteries with the MPU5. You CANNOT use old battery eliminators with the MPU5. Use only **CBL-PWR-0001** or **CBL-PWR-0002**. You CANNOT power the MPU5 via Power over Ethernet (PoE).

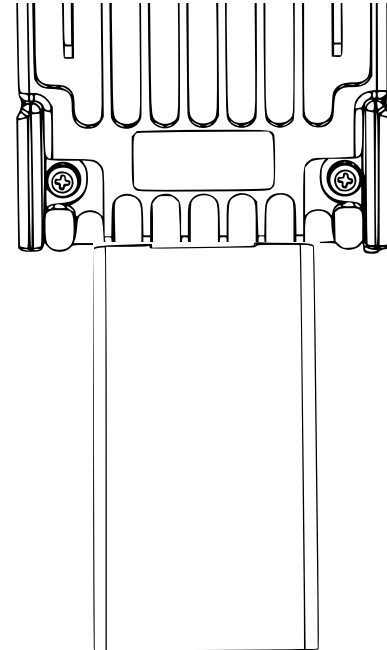
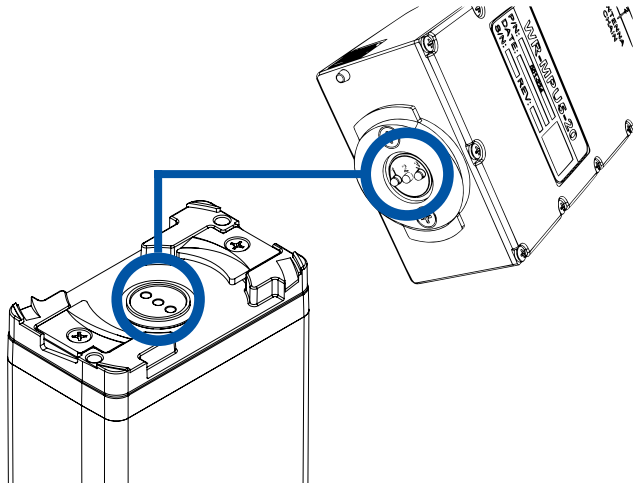
#### Will I lose all my settings if I remove power from my MPU5?

If the MPU5 has been charged for 8 hours, it will retain unit settings for 30 days.

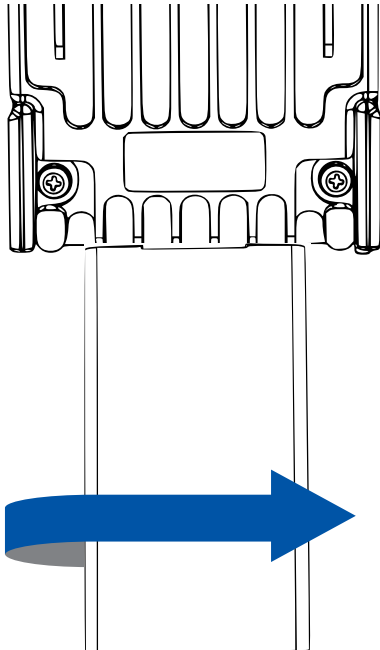


## Connecting Power

- 1** If you are using a battery, make sure that the battery is charged.
- 2** Align the **circular three pin connector** on the power source with the **circular three pin connector** on the bottom of the MPU5.
- 3** **Push** the connectors together. Make sure the connector is seated properly.



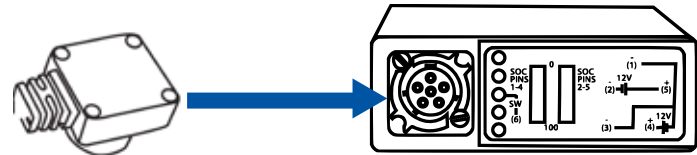
- 4** **Twist** clockwise 90°. You will hear a click when it is locked.



- 5** If you are using a Wall Battery Eliminator, plug the **standard wall plug** into a **standard wall outlet**.

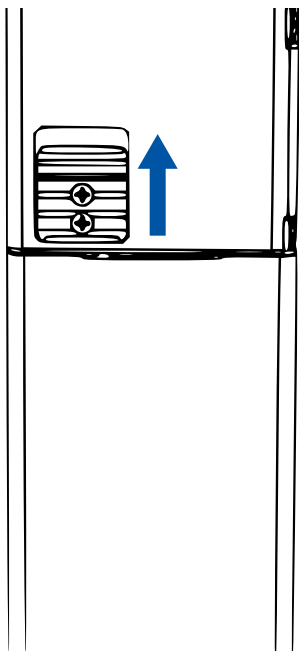


- 6** If you are using a BB Battery Eliminator, plug the **BB plug** into a **BB Battery**.

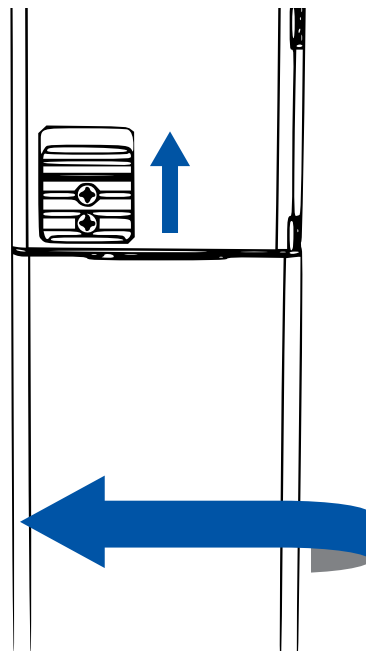


### Removing Power



- 1** Slide **up** the battery latch on the side of the MPU5.





- 2** Twist the **battery** counterclockwise until it disconnects.



### **What do I do if my power accessory will not fit the battery connector?**

-  Ensure that no parts (pins, plates, etc.) on either connector are bent or damaged.
-  Ensure that there are no foreign objects in either connector.

### **What do I do if my power accessory will not lock?**

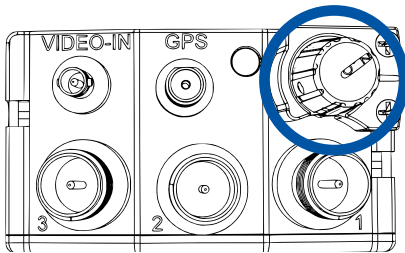
-  Ensure that the battery latch moves freely by sliding it up and down.
-  Ensure that the battery latch is not stuck in the unlocked position.

## Powering On the Unit

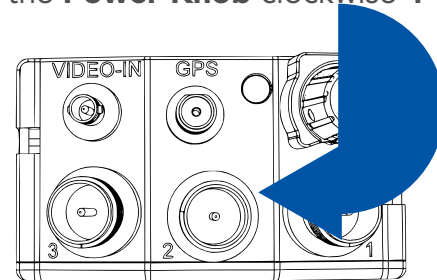
**1** Ensure that **antennas**, a **radio module**, and an appropriate **power source** are connected.

**! WARNING!:** Antennas **MUST** be installed prior to powering on the unit.

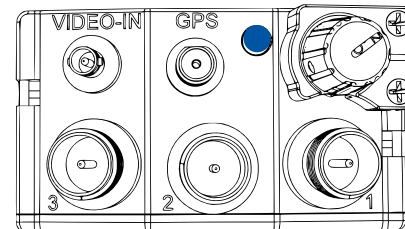
**2** **Locate** the **Power Knob** on the top of the unit.



**3** **Twist** the **Power Knob** clockwise **1 click**.



**4** If the unit is powered and has turned on, the **LED** on the top of the unit will glow a color indicating unit status.





## Quick Reference:

LED Color	Unit Status
<b>Blue</b>	Booting
<b>Yellow</b>	Running, no neighbors
<b>Green</b>	Running, neighbors
<b>Red</b>	Crypto Fail (No key or FIPS)
<b>Orange</b>	Low Battery
<b>Purple</b>	Loading Firmware

### What do I do if my Power Knob does not rotate?

- 1** Make sure that you are twisting it in the correct direction (clockwise).
- 2** Make sure that no foreign objects are blocking the rotation of the knob.
- 3** If the knob still does not rotate, it may be broken. Contact Persistent Systems Support.

### What do I do if the Power Knob does not click when I twist it?

- 1** The Power Knob may be broken. Contact Persistent Systems Support.
- 2** Ensure that the battery latch is not stuck in the unlocked position.



### What Can I Do Now?

- ▶ Provide power to an MPU5 via a battery or standard wall socket
- ▶ Power on/off the unit
- ▶ Replace dead batteries

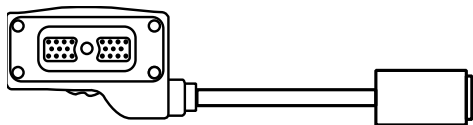
## Section C: Side Connector Cables



### What Will I Learn?

- ▶ How to connect a cable to the MPU5 side connectors

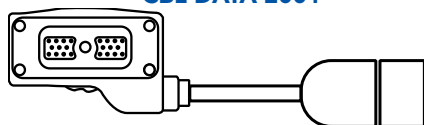
## Parts List



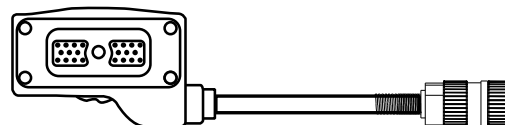
22-Pin to RJ45 Receptacle  
**CBL-DATA-2001**



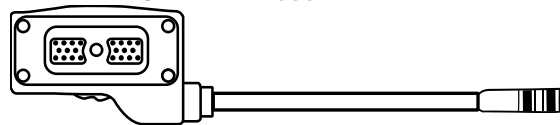
22-Pin to U94  
**CBL-AUD-0003**



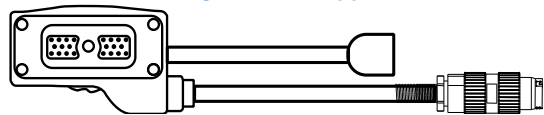
22-Pin to USB 2.0 Type A Receptacle  
**CBL-DATA-2003**



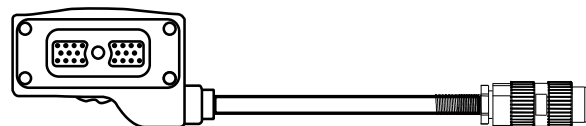
22-Pin to U-329  
**CBL-AUD-0001**



22-Pin to 6-Pin Push Pull USB Tether  
**CBL-DATA-2004**



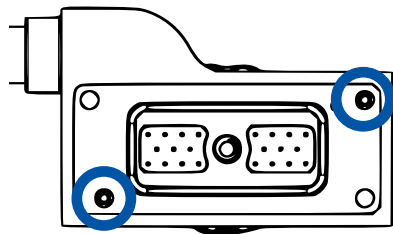
22-Pin to Audio and Video Out  
**CBL-DATA-3002**



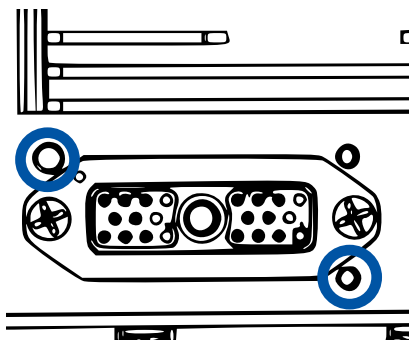
22-Pin to U-328  
**CBL-AUD-0002**

### Connecting a Cable to a Side Connector

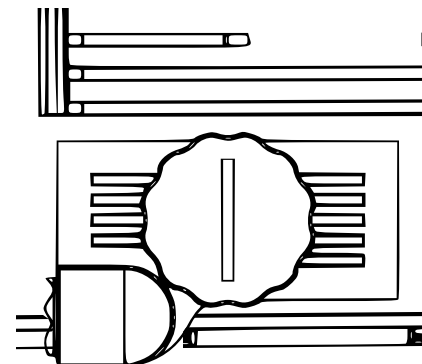
**1** The 22-Pin connector on every cable is keyed so that it will **only** attach to a compatible side connector. If a cable can attach to multiple side connectors, it is keyed (or not keyed) so that it will attach to all compatible side connectors.



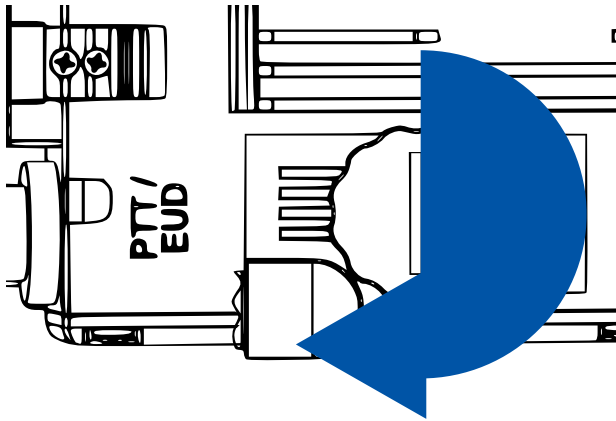
**2** To connect a cable to a side connector, **locate** the appropriate side connector.



**3** **Align** the key pins on the **22-Pin connector** with the **key holes** on the case. **Push** the key pins into the **key holes**.



- 4** **Twist** the thumbscrew **clockwise** to attach the cable to the device.



- 5** Ensure that the cable is firmly attached and the connector is sitting flush with the case.

### What do I do if the cable won't mate with the side connector?

- 1** Ensure that you are trying to connect the cable to the correct side connector.
- 2** Ensure that you are aligning the key pin properly and the cable is not upside down.
- 3** Ensure that no parts of the thumbscrew and the side connector are bent or damaged.
- 4** Ensure that there are no foreign objects in the thumbscrew or side connector.
- 5** Ensure that the cable connector is flush with the case.

## PHYSICAL SETUP: SIDE CONNECTORS

### Quick Reference:

Part Number	Description	Side Connector(s)	Uses
CBL-DATA-2001	22-Pin to RJ45 Receptacle	DATA	Connects to a standard RJ45 Ethernet cable. Use this cable to connect the unit to a computer for configuration.
CBL-DATA-2003	22-Pin to USB 2.0 Type A Female	PTT/EUD, DATA, RoIP	Connects USB accessories via a standard USB A port.
CBL-DATA-2004	22-Pin to 6-Pin Push Pull Android™ USB	PTT/EUD, DATA, RoIP	Connects an Android™ EUD or Screen
CBL-DATA-2005	22-Pin to DB9 Serial Socket	PTT/EUD, DATA, RoIP	Connects serial devices via a DB9 socket
CBL-DATA-2007	22-Pin to RJ45 Receptacle and USB 2.0 Type A Male	DATA	Connects to USB devices via a standard USB A plug and to a standard RJ45 Ethernet cable
CBL-DATA-2009	22-Pin to RJ45 Flying Leads	DATA	Flying leads for custom Ethernet integration (72")
CBL-DATA-2010	22-Pin to RJ45 Flying Leads	DATA	Flying leads for custom Ethernet integration (18")
CBL-DATA-3002	22-Pin to Audio and Video Out	PTT/EUD	Connects to a standard HDMI cable to display video on a TV or Monitor and connects to a speaker box or headset.
CBL-AUD-0001	22-Pin to U-329	RoIP	Connect the unit to a Legacy Radio via a U-329 connector.

CBL-AUD-0002	22-Pin to U-328	PTT/EUD	Connects to a headset via a U-328 connector.
CBL-AUD-0007	22-Pin to Audio and USB 2.0 Type A Female	PTT/EUD	Connects USB accessories via a standard USB A port and an audio accessory via a U-328 connector
CBL-AUD-2009	22-Pin to Audio and 6-Pin Push Pull Android™ USB	PTT/EUD	Connects an Android™ EUD or Screen and an audio accessory via a U-328 connector

Refer to the MPU5 Product Catalog for more information on MPU5 cables. If you still have questions, contact Persistent Systems.



### What Can I Do Now?

- ▶ Identify which cable you need for your configuration
- ▶ Identify which side connector your cables attach to
- ▶ Connect a cable to a side connector

## Part II: Software Setup

### Section A: Configuring the Management Computer

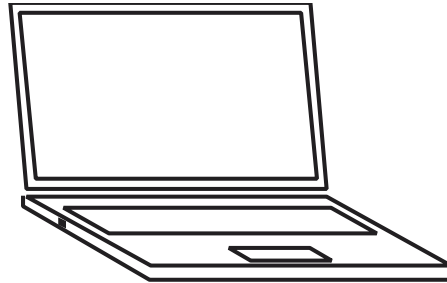


#### What Will I Learn?

- ▶ How to configure your computer to be able to communicate with an MPU5



#### Parts List



Management Computer with Administrator Access & Ethernet Port



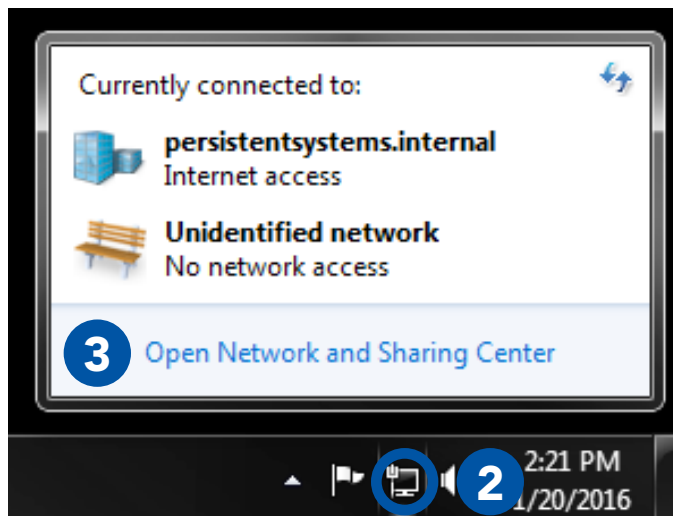


### IMPORTANT INFORMATION!:

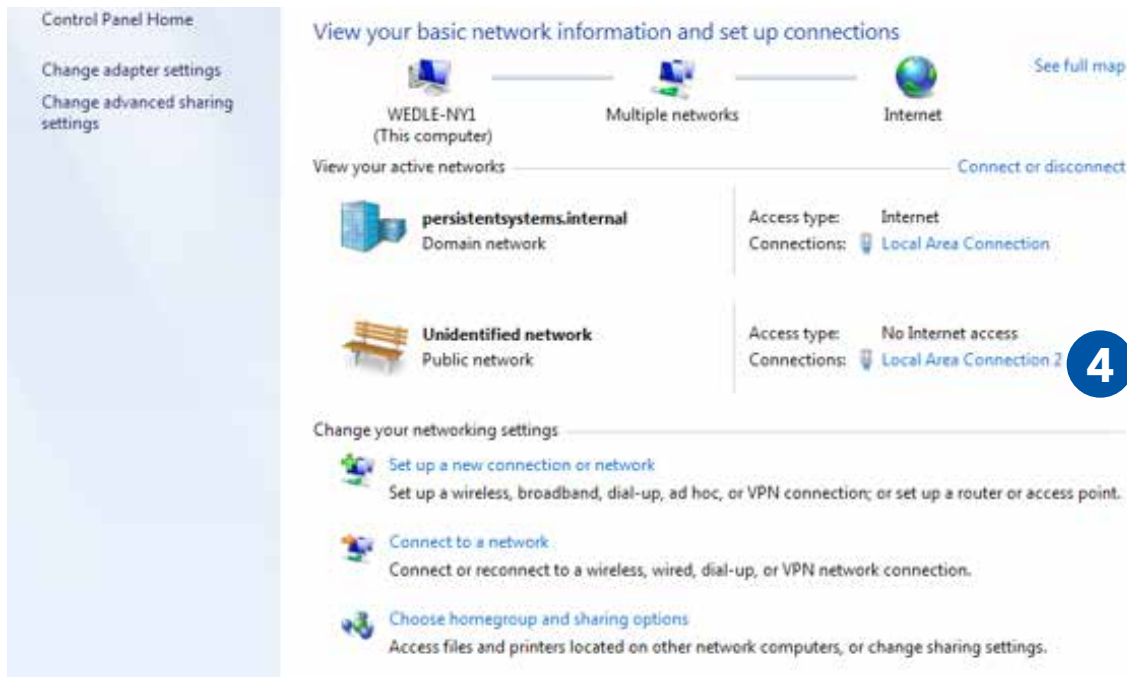
- ▶ To communicate with an MPU5, the computer must have an IP address in the same subnet mask as the MPU5's IP address.
- ▶ For example, with a subnet mask of 255.255.255.0, the computer and MPU5 will be able to communicate if they share the same first three numbers in their respective IP addresses (e.g. 10.3.1.10 and 10.3.1.254).
- ▶ If the computer and MPU5 do not share a subnet mask, the computer and MPU5 will not be able to communicate.
- ▶ If either the computer or MPU5 do not have an IP address in the same subnet mask, the computer and MPU5 device will not be able to communicate.

### Configuring the Management Computer (Windows)

- 1** Locate the **Network** icon at the bottom right of the taskbar.
- 2** Right click the **Network** icon.
- 3** Click **Open Network and Sharing Center**.



## 4 Click **Local Area Connection 2**.



The screenshot shows the Windows Network and Sharing Center. On the left, there is a sidebar with links: "Control Panel Home", "Change adapter settings", and "Change advanced sharing settings". The main area is titled "View your basic network information and set up connections" and includes a "See full map" link. Below this, a network diagram shows "WEDLE-NY1 (This computer)" connected to "Multiple networks", which is connected to "Internet".

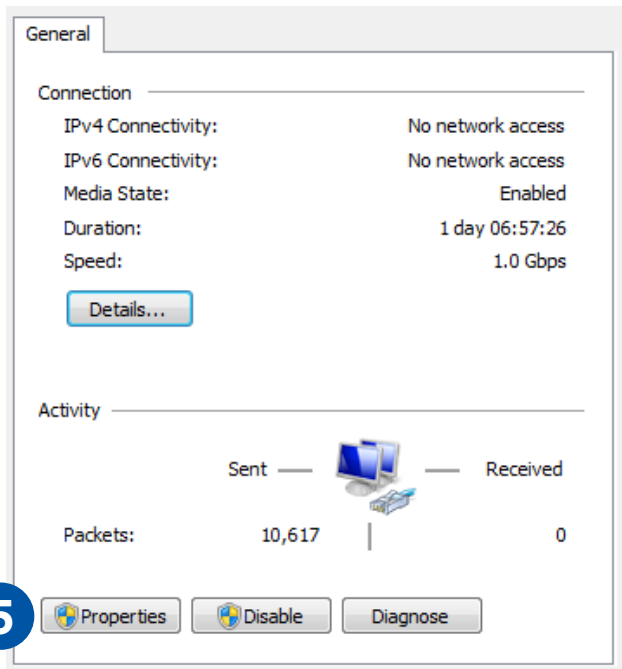
Under "View your active networks", there are two network profiles:

- persistentsystems.internal** (Domain network):
  - Access type: Internet
  - Connections: Local Area Connection
- Unidentified network** (Public network):
  - Access type: No Internet access
  - Connections: Local Area Connection 2

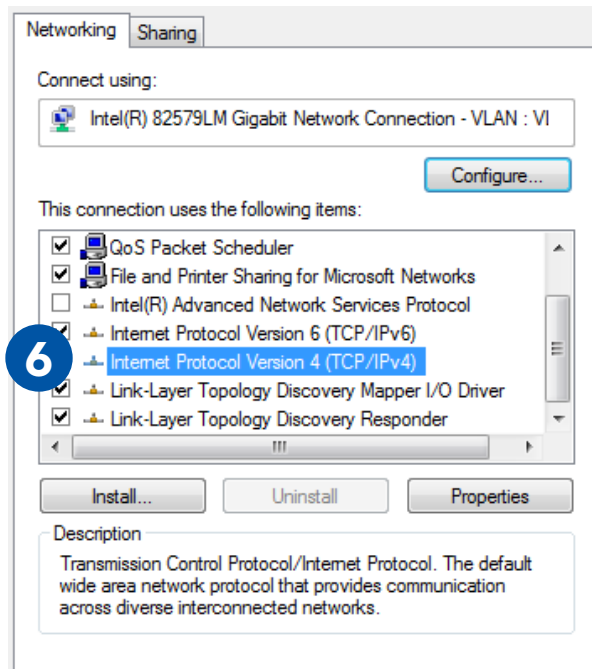
A blue circle with the number "4" is overlaid on the "Local Area Connection 2" text. Below the active networks, the "Change your networking settings" section includes three options:

- Set up a new connection or network**: Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
- Connect to a network**: Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
- Choose homegroup and sharing options**: Access files and printers located on other network computers, or change sharing settings.

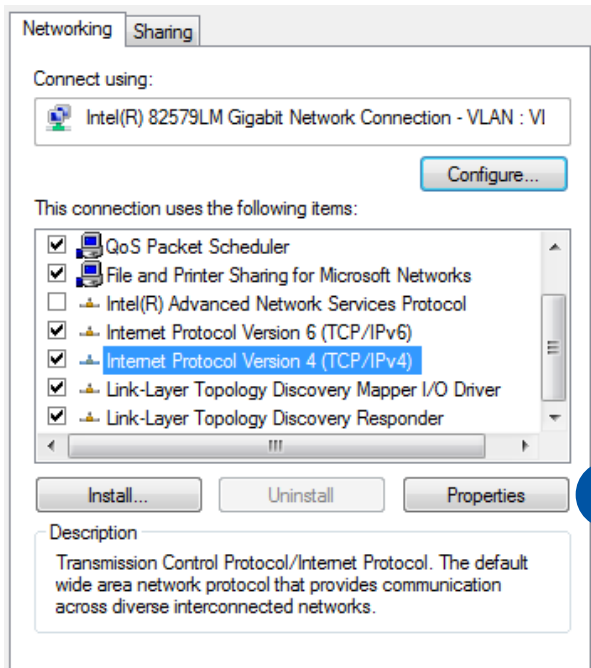
**5** Click **Properties**.



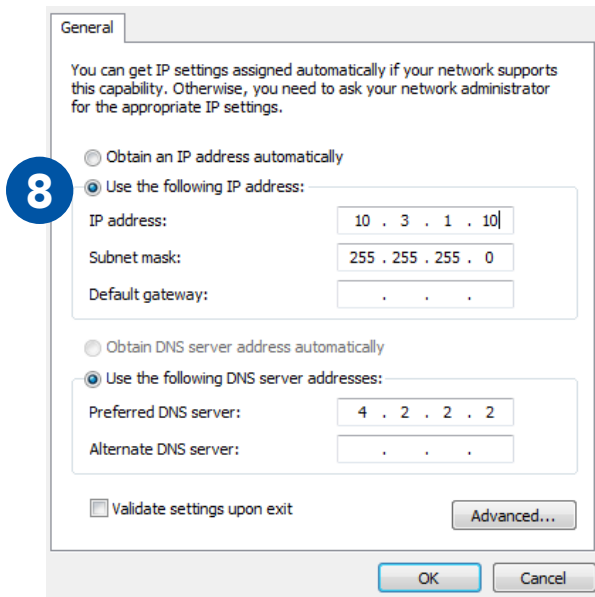
**6** Select **Internet Protocol Version 4 (TCP/IPv4)** and ensure that it is highlighted as pictured.



**7** Click **Properties**.



**8** Click **Use the following IP address**.



## SOFTWARE SETUP: MANAGEMENT COMPUTER

**9** Enter **10.3.1.10** into the **IP address** field.

**10** Enter **255.255.255.0** into the **Subnet mask** field.

**11** Click **OK**.

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

Subnet mask:

Default gateway:

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Validate settings upon exit

Advanced...

OK Cancel

**12** Your computer is now properly configured to connect to the MPU5.

## Configuring the Management Computer (Linux)

- 1** Open the **command line**.
- 2** **Type:**  

```
sudo ifconfig eth0 10.4.1.10/24
```
- 3** **Type:**  

```
sudo ip addr add 10.3.1.10/24 dev eth0
```

### What Can I Do Now?

- ▶ Configure computers to be able to communicate with Wave Relay<sup>®</sup> devices.
- ▶ Have a computer that is able to configure a Wave Relay<sup>®</sup> device.

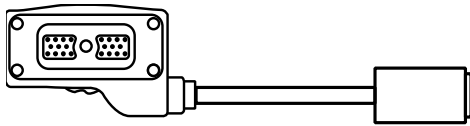


## Section B: Connecting the MPU5 to the Management Computer

### What Will I Learn?

- ▶ How to physically connect the MPU5 to the Management Computer

### Parts List



22-Pin to RJ45 Receptacle  
**CBL-DATA-2001**



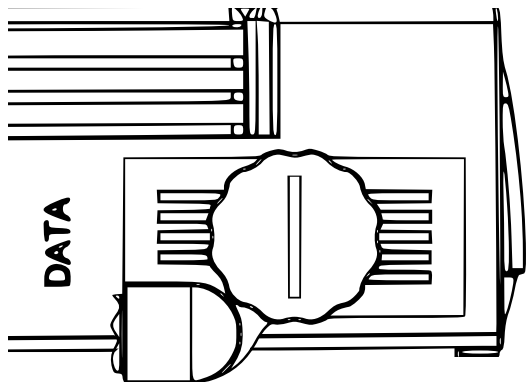
Standard RJ45 Ethernet Cable



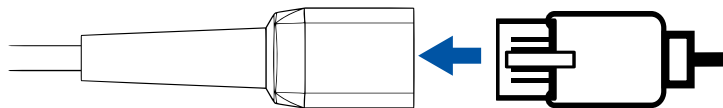
Properly Configured Management Computer with Ethernet Port

## SOFTWARE SETUP: MANAGEMENT COMPUTER

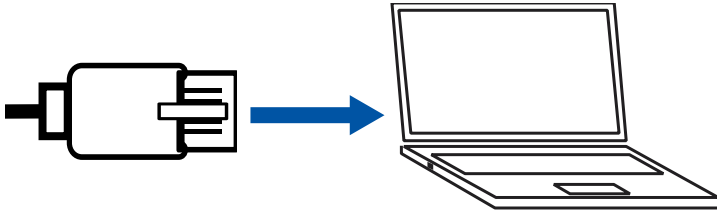
- 1** Connect **CBL-DATA-2001** to the **DATA** side connector on the MPU5.



- 2** Plug one end of the standard RJ45 Ethernet cable into the **Ethernet receptacle** on **CBL-DATA-2001**.



- 3 Plug the other end of the standard RJ45 Ethernet cable into an **Ethernet port** on the Management Computer.



### What Can I Do Now?

- ▶ Connect an MPU5 to a computer for configuration

## Section C: Accessing the Web Management Interface

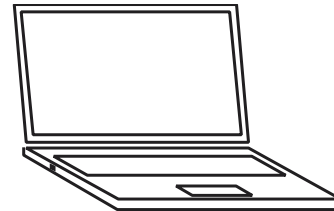
### ▶ What Will I Learn?

- ▶ How to access the Web Management Interface to configure the MPU5

### ≈ Parts List



Web Browser (Internet Explorer 7+,  
Firefox 3+, or Chrome)



Management Computer with properly configured IP ad-  
dress and subnet mask & Ethernet Port

# SOFTWARE SETUP: WEB MANAGEMENT INTERFACE

**1** Open the web browser



Microsoft Internet Explorer 7+

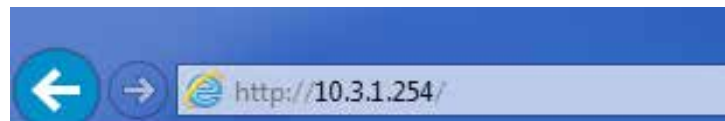


Google Chrome

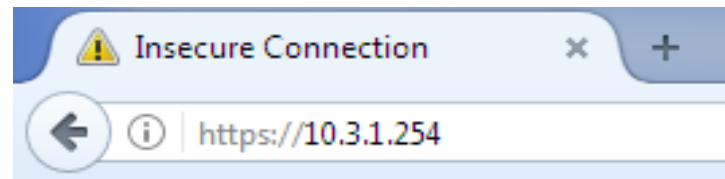


Mozilla Firefox 3+

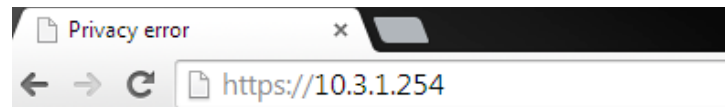
**2** In the address bar, type **https://10.3.1.254** then press the **Enter** key.



Microsoft Internet Explorer 7+



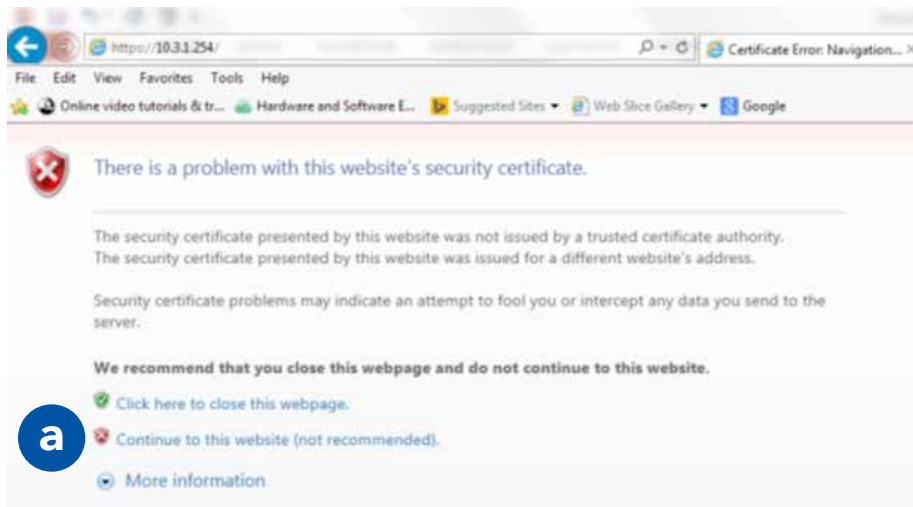
Mozilla Firefox 3+



Google Chrome

- 3** The web browser will ask you to accept a security certificate.

In Internet Explorer:



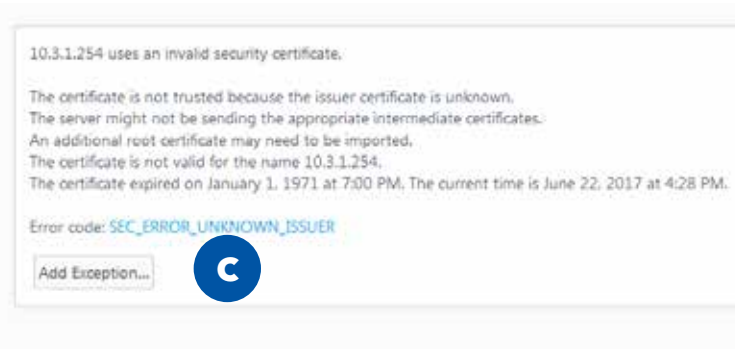
- a** Click **Continue to this website (not recommended)**

In Firefox:

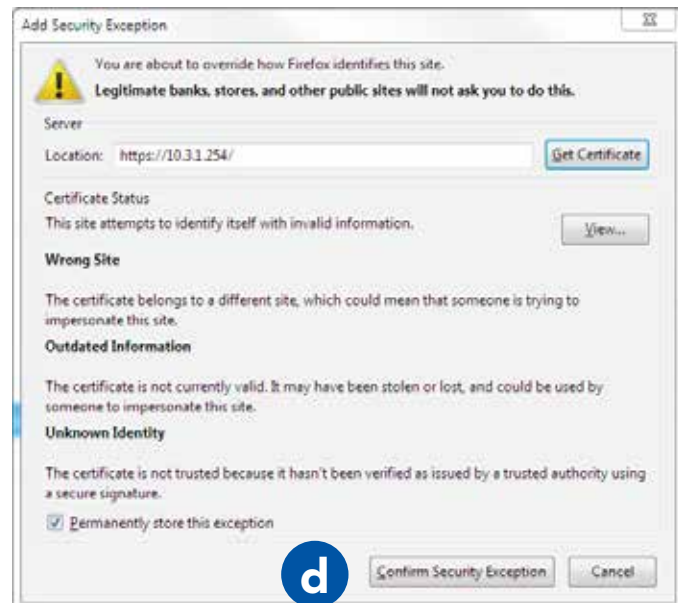


**b** Click **I Understand the Risks**

# SOFTWARE SETUP: WEB MANAGEMENT INTERFACE



**c** Click **Add Exception**



**d** Click **Confirm Security Exception**



In Chrome:



## Your connection is not private

Attackers might be trying to steal your information from **10.3.1.254** (for example, passwords, messages, or credit cards). NET::ERR\_CERT\_AUTHORITY\_INVALID

[Automatically report](#) details of possible security incidents to Google. [Privacy policy](#)

ADVANCED



Back to safety



Click **Advanced**

This server could not prove that it is **10.3.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. [Learn more](#).

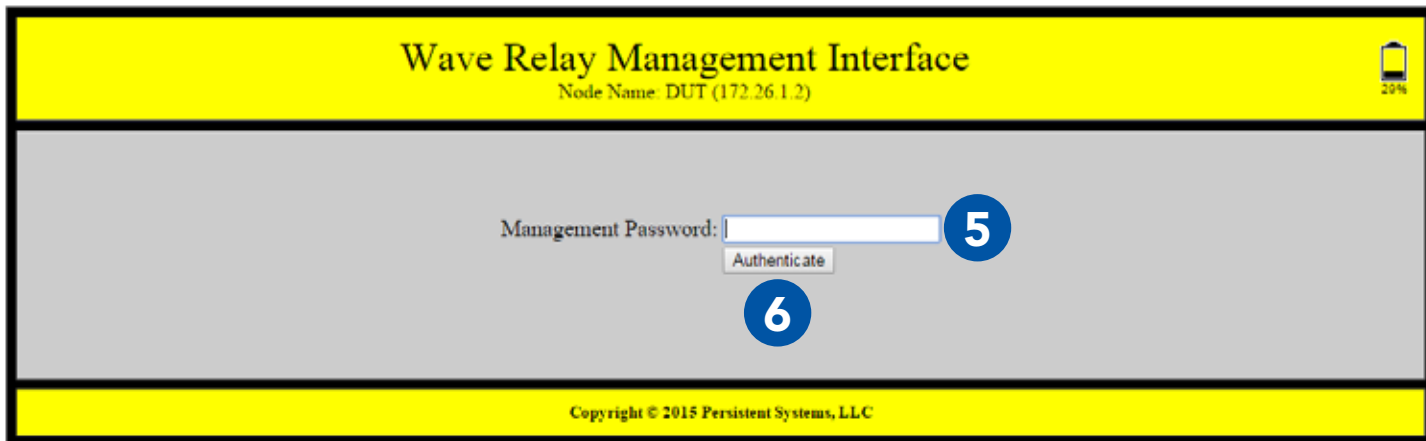
[Proceed to 10.3.1.254 \(unsafe\)](#)



Click **Proceed to 10.3.1.254 (unsafe)**

## SOFTWARE SETUP: WEB MANAGEMENT INTERFACE

- 4** Wait for the Web Management Interface page to load
- 5** In the **Management password** field, type **password**
- 6** Click **Authenticate**.



Wave Relay Management Interface  
Node Name: DUT (172.26.1.2)

Management Password:  **5**

**6** Authenticate

Copyright © 2015 Persistent Systems, LLC



## Why does the Security Exception Page or the Web Management Interface page not load?

- 1 Verify that you configured the Management Computer IP address and subnet mask properly.
- 2 Ensure that all cables are connected properly
- 3 Ensure that you are accessing the correct management IP address (10.3.1.254).
- 4 Ensure that you are using a compatible web browser.
- 5 Reboot the node.



## What Can I Do Now?

- ▶ Access the Web Management Interface for any node you connect to your computer.

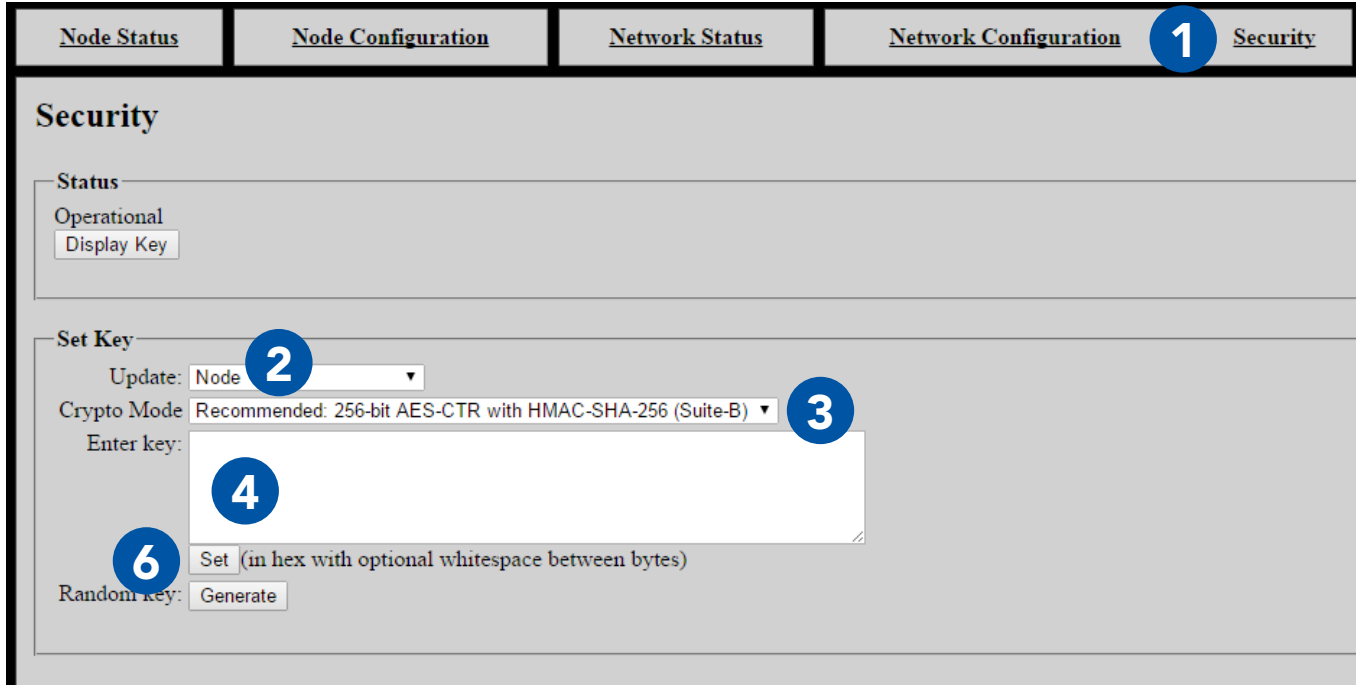
## Section D: Basic Network Setup

### Security Key

#### What Will I Learn?

- ▶ How to set the security key and crypto mode on an MPU5

- 1** Click the **Security** tab.
- 2** In the **Set Key** section, locate the **Update** drop down menu. Select **Node**.
- 3** In the **Crypto Mode** drop down menu, select the desired **Crypto Mode**.  
**Note:** All nodes must have the same Crypto Mode in order to communicate.
- 4** In the **Enter key** field, type the desired security key or click the **Generate** button to generate a random key.
- 5** **Copy** and **paste** the security key to a text file in a secure place on the Management Computer.
- 6** Click the **Set** button to set the key for the node.



The screenshot shows a web interface with a top navigation bar containing five tabs: Node Status, Node Configuration, Network Status, Network Configuration, and **1 Security**. The **Security** tab is active and highlighted with a blue circle containing the number 1. Below the navigation bar, the page title is **Security**. The main content area is divided into two sections: **Status** and **Set Key**. In the **Status** section, the text "Operational" is displayed above a "Display Key" button. In the **Set Key** section, there are several elements: an "Update:" label followed by a dropdown menu showing "Node" (with a blue circle containing the number 2); a "Crypto Mode" label followed by a dropdown menu showing "Recommended: 256-bit AES-CTR with HMAC-SHA-256 (Suite-B)" (with a blue circle containing the number 3); an "Enter key:" label followed by a large text input field (with a blue circle containing the number 4); a "Set (in hex with optional whitespace between bytes)" button (with a blue circle containing the number 6); and a "Random key:" label followed by a "Generate" button.

### What Can I Do Now?

- ▶ Set or change the security key and crypto mode for a single node
- ▶ Generate a random security key
- ▶ Save a security key in a text file to copy to other nodes

## Assigning IP Address and Interface Names

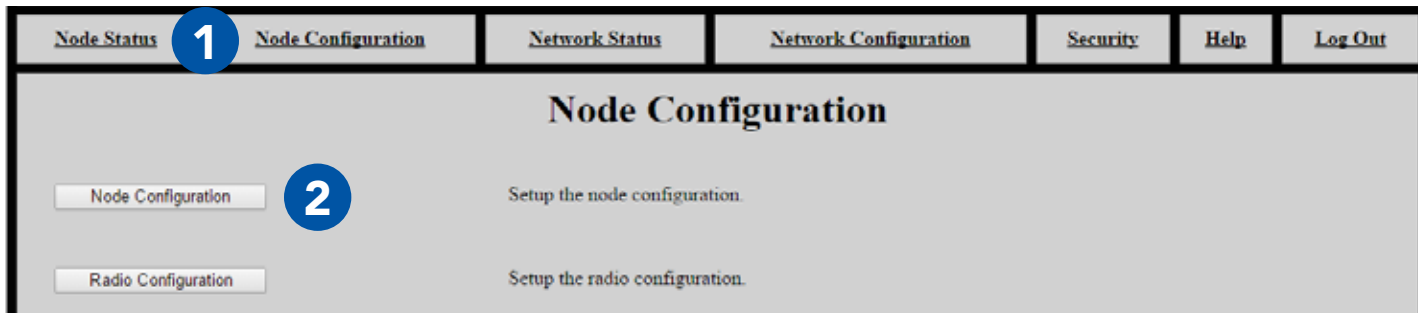
### What Will I Learn?

- ▶ How to set and change the Node Name and IP Address of a node

# SOFTWARE SETUP: ASSIGNING IP ADDRESS AND INTERFACE NAMES

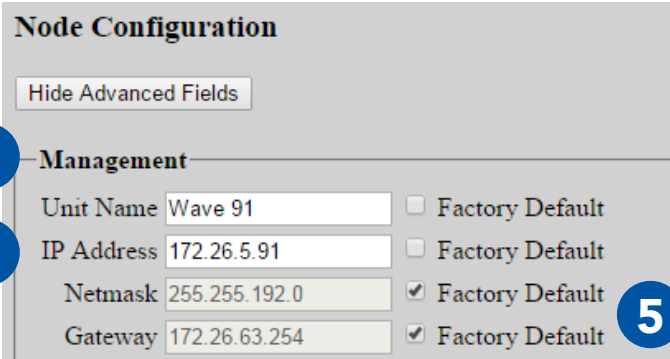
**1** Click the **Node Configuration** tab.

**2** Click the **Node Configuration** button.



## SOFTWARE SETUP: ASSIGNING IP ADDRESS AND INTERFACE NAMES

- 3** In the **Management** section, find the **Node Name** field and enter the desired Node Name.
- 4** In the **IP Address** field, enter the desired IP Address.
- 5** Enter a **Netmask** and **Gateway**, if required. Otherwise, **check** the **Factory Default** box.
- 6** Scroll to the bottom of the page and click the **Save & Reconfigure Unit** button.
- 7** Wait for the page to reload.



**Node Configuration**

Hide Advanced Fields

**3** **Management**

Unit Name	<input type="text" value="Wave 91"/>	<input type="checkbox"/> Factory Default
IP Address	<input type="text" value="172.26.5.91"/>	<input type="checkbox"/> Factory Default
Netmask	<input type="text" value="255.255.192.0"/>	<input checked="" type="checkbox"/> Factory Default
Gateway	<input type="text" value="172.26.63.254"/>	<input checked="" type="checkbox"/> Factory Default

**5**

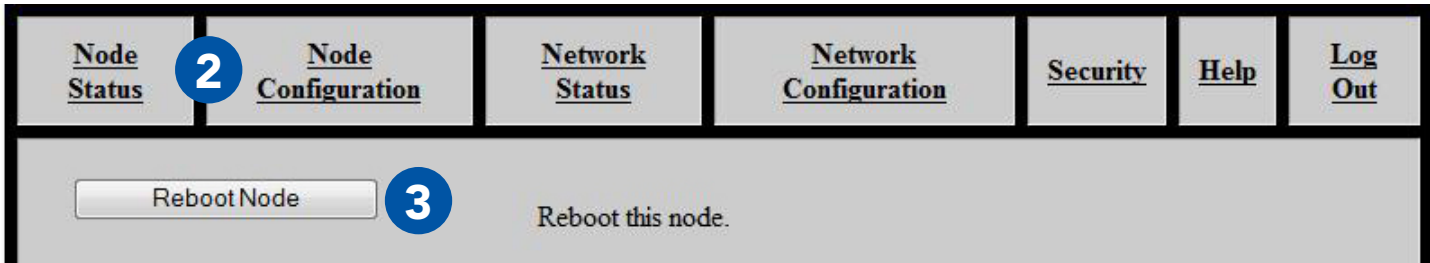


## What Can I Do Now?

- ▶ Access the Node Configuration page for an individual node
- ▶ Set the Node Name and IP Address of a node to fit the node into your IP scheme and identify the node in status functions

## Rebooting an Individual Node

- 1** Log into the node.
- 2** Click the **Node Configuration** tab.
- 3** Scroll down and click the **Reboot Node** button.



The screenshot shows a navigation bar with several tabs: Node Status, Node Configuration, Network Status, Network Configuration, Security, Help, and Log Out. The Node Configuration tab is highlighted with a blue circle containing the number 2. Below the navigation bar, there is a button labeled "Reboot Node" with a blue circle containing the number 3 next to it, and the text "Reboot this node." to its right.

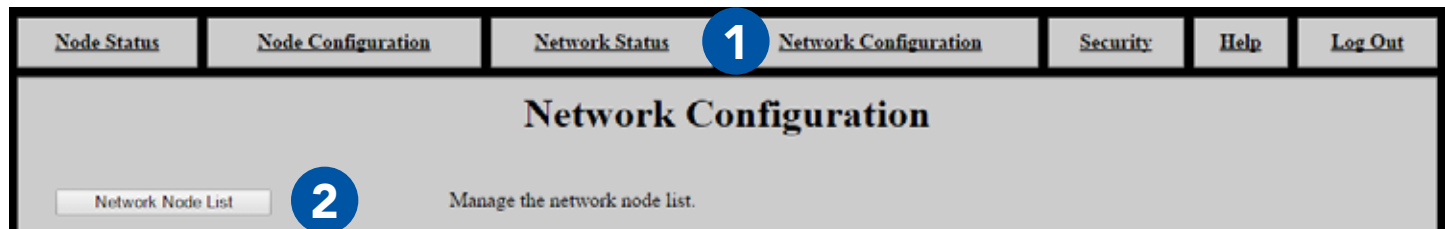
## Network Node List

### ▶ What Will I Learn?

- ▶ How to add and remove nodes from the Management Node List
- ▶ How to push the Management Node List to all nodes in your network

**1** Click the **Network Configuration** tab.

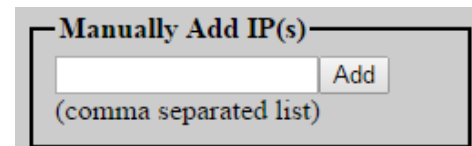
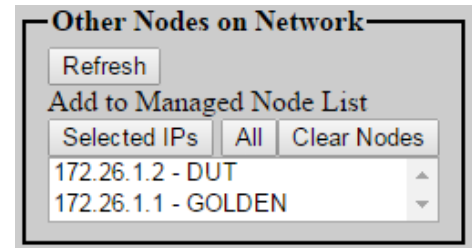
**2** Click **Network Node List**.



The **Network Node List** creates a list of nodes for **Network Status** and **Network Configuration** functions. Those functions will **ONLY** operate on nodes that are in the Network Node List.

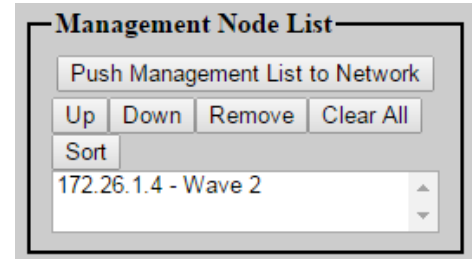
## Adding Nodes to the Network Node List

- 1** Ensure that all your nodes are powered on and that you have configured their IP addresses and node names. These will appear in the **Other Nodes on Network** box.
- 2** Click **Refresh** if all nodes do not appear.
- 3** Click **All** to add all nodes in the box to the Network Node List. Alternatively, select one or more nodes and click **Selected IPs** to add those nodes to the Network Node List. Hold the **shift** key or **ctrl** key while clicking to select multiple nodes.
- 4** Nodes can be added manually as well. Enter a comma separated list of all IP addresses to add in the **Manually Add IP(s)** box, then click **Add**.



### Managing the Network Node List

- 1 After you add nodes to the Network Node List, they will appear in the box on the left of the page.
- 2 Use the **Up**, **Down**, **Remove**, **Clear All**, and **Sort** buttons to reorder or delete nodes from the Network Node List.
- 3 Click **Push Management List to Network** to copy the Network Node List to all the nodes in the Network Node List. This will ensure that Network Status and Network Configuration functions will work properly on all nodes in the network.



**Note:** ensure that all nodes are turned on and have the same radio settings (i.e. they are able to be contacted). If nodes are not able to be contacted, they will not receive the Network Node List.

**Note:** remember to add new nodes to the Network Node List when you are expanding your network.



### What Can I Do Now?

- ▶ Add new nodes to the Network Node List
- ▶ Remove nodes from the Network Node List
- ▶ Synchronize the Network Node List between all nodes on your network

## Part III: Testing Connectivity

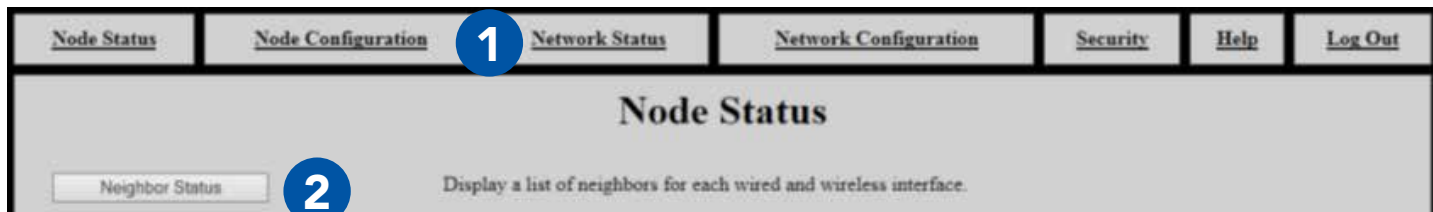
### ▶ What Will I Learn?

- ▶ How to tell if nodes are connected
- ▶ How to see the connection strength between Neighbor Nodes
  - ▶ Neighbor Nodes are nodes connected without hops through other nodes
- ▶ How to test bandwidth between nodes

### Check Neighbor Node Status

**1** Click the **Network Status** tab.

**2** Click the **Neighbor Status** button.



## 3 Verify that all nodes are communicating with the network.

**Neighbor SNR**

Interface	Neighbor	Receive SNR
Radio 3	13-A window (172.26.6.50) - Radio 3	6.79
Radio 3	2-B lunchroom window (172.26.6.40) - Radio 4	24.87
Radio 3	2-B mainroom window (172.26.6.70) - Radio 3	46.27
Radio 3	2-D DH desk (Reciever) (172.26.0.121) - Radio 1	30.83
Radio 3	2-E JH_EL desk (172.26.0.145) - Radio 1	45.53

Return to Menu    MANET Monitor

### Notes:

- ▶ This table only displays Neighbor Nodes (nodes directly connected without hops through other nodes. If you spread nodes apart, they may disappear from the Neighbor Nodes Status page when they become connected via a hop.
  - ▶ The Neighbor Nodes status page displays:
    - ▶ Node Names
    - ▶ IP Addresses
    - ▶ Receive Signal-to-Noise Ratio (SNR) between nodes

### Perform a Throughput Test

- 1** Click the **Node Status** tab.
  - 2** Click the **Bandwidth Test** button.
  - 3** Select a **destination node** for the throughput test from the **Destination** drop-down menu. This menu is populated from the Node List.
  - 4** Enter the desired **test duration (in seconds)** in the **Test Duration** field.  
**Note:** Persistent Systems recommends the test duration to be set to a minimum of 5 seconds.
  - 5** **Check** or **uncheck** the **Upload only test** box. If this box is checked, only upload speed to the destination node will be tested.
- ! WARNING!:** During long duration tests, data will continue to be sent for the full specified duration even if a different data flow is started or the web browser is exited.
- 6** Click **Run Test** and wait for the test to complete.
  - 7** The page will display the upload speed to and download speed from the destination node.



1 [Node Status](#) [Node Configuration](#) [Network Status](#) [Network Configuration](#) [Security](#) [Help](#) [Log Out](#)

[Bandwidth Test](#) 2 Test TCP throughput from this device to other devices in the network.

## Network TCP Throughput Testing

Destination:  Upload 5  
only test

172.26.1.18 - STREET 1 ▾ 3

Test Duration:  
30 4 Seconds

TCP Throughput test to 172.26.1.18 for 30 seconds =  
Upload 35.2 Mbps 7 Download 45.2 Mbps

[Run Test](#) 6 [Enable Logging](#)

## Throughput Test Logging

- 1 Click the **Enable Logging** button.
- 2 When the throughput test is run, data will be collected in a table at the bottom of the page.

**Position Status**

Source: Internal GPS  
 Position: Unknown  
 Satellites Used: 0  
 Satellites Visible: 0  
 Satellite ID/PRN: 6 31 32 133 135 138  
 Satellite SNR: 28 25 26 0 0 0 00

Clear Download CSV Download KML

Time	Lcl Iface	SNR(dB)	Chain1(dB)	Chain2(dB)	Chain3(dB)	Tx Rate	Dist(m)	Rem Name	Lcl Name	Rx(%)	Tx(%)	Cs(%)	Tl(%)	Bw Tx(Mbps)	Bw Rx(Mbps)	Interval(s)
Fri Jul 22 14:02:48 2016									W36					53.7		0.0-1.0
Fri Jul 22 14:02:49 2016	Radio 1	45	39	40	42	MIMO 4:3		W20	W36	2	25	0	29	70.7		1.0-2.0
Fri Jul 22 14:02:50 2016	Radio 1	45	39	40	42	MIMO 4:3		W20	W36	2	25	0	29	70.7		2.0-3.0
Fri Jul 22 14:02:51 2016	Radio 1	45	39	40	42	MIMO 4:3		W20	W36	2	77	1	81	70.7		3.0-4.0
Fri Jul 22 14:02:52 2016	Radio 1	45	39	40	42	MIMO 4:3		W20	W36	2	77	1	81	77.8		4.0-5.0
Fri Jul 22 14:02:52 2016	Radio 1	45	39	40	42	MIMO 4:3		W20	W36	2	77	1	81	68.9		0.0-5.0
Fri Jul 22 14:02:55 2016	Radio 1	46	40	40	42	MIMO 4:3		W20	W36	2	82	1	86		34.5	0.0-1.0
Fri Jul 22 14:02:56 2016	Radio 1	44	37	37	41	MIMO 4:3		W20	W36	21	0	0	23		41.5	1.0-2.0
Fri Jul 22 14:02:57 2016	Radio 1	44	37	37	41	MIMO 4:3		W20	W36	21	0	0	23		40.9	2.0-3.0
Fri Jul 22 14:02:58 2016	Radio 1	45	39	40	43	MIMO 4:3		W20	W36	69	1	1	72		45.1	3.0-4.0
Fri Jul 22 14:02:59 2016	Radio 1	45	39	40	43	MIMO 4:3		W20	W36	69	1	1	72		50.3	4.0-5.0
Fri Jul 22 14:02:59 2016	Radio 1	45	39	40	43	MIMO 4:3		W20	W36	69	1	1	72		42.6	0.0-5.0

**Position Status:** displays GPS status information for the current node. See the Check GPS Status section for an explanation of these fields.

**Clear:** clears all data from the table

**Note:** If Clear is not pressed before beginning a test, the new throughput test data will be appended sequentially to the existing table of data.

**Download CSV:** downloads all throughput test data in the table as a CSV file

**Download KML:** downloads all throughput test data in the table as a KML file

**Time:** date and time for each line of test data

**Interface:** interface used to communicate during the test

**SNR (dB):** Signal-to-Noise Ratio at which the destination node is heard

**Chain 1/2/3 (dB):** Signal-to-Noise Ratio for each chain on the source node

**Tx Rate:** MIMO or SISO rate used to communicate between nodes in the format

**MIMO|SISO [Rate]:[Number of streams].**

**Dist (m):** distance between nodes, in meters, if available

**Rem Name:** Node Name of the destination node

**Lcl Name:** Node Name of the source node

**Rx(%):** percentage of the channel used to receive

**Tx(%):** percentage of the channel used to transmit

**Cs(%):** percentage of the channel occupied by noise

**TI(%):** total percentage of channel used

**Bw Tx (Mbps):** Upload Bandwidth, in Mbps

**Bw Rx (Mbps):** Download Bandwidth, in Mbps

**Interval (s):** time interval of the throughput test for each line of throughput test data

## Part IV: Using the Web Management Interface

### View Individual Node Information

**1** Click the **Node Status** tab.

**2** Click the **Unit Info** button.

The screenshot displays a web management interface with a navigation bar at the top. The navigation bar contains seven tabs: **Node Status**, **Node Configuration**, **Network Status**, **Network Configuration**, **Security**, **Help**, and **Log Out**. The **Node Status** tab is highlighted with a blue circle containing the number 1. Below the navigation bar, the main content area is titled **Node Status**. In the lower-left corner of this area, there is a button labeled **Unit Info**, which is highlighted with a blue circle containing the number 2. To the right of the button, the text reads: "Display a suite of information related to this device."

## 3 The page will display:

**Firmware Version:** Wave Relay® firmware version loaded on the node

**Wave Relay Model:** Device model

**Serial No.:** Serial number of the node

**Uptime:** Operating time since the node was last powered on or rebooted

**Temperature:** Temperature of the power board, main board CPU, and all three RF chains

**Input Power Voltage:** Voltage supplied to node

**Battery Status:** Battery percentage remaining

**Battery Temperature:** Appx. temperature of battery

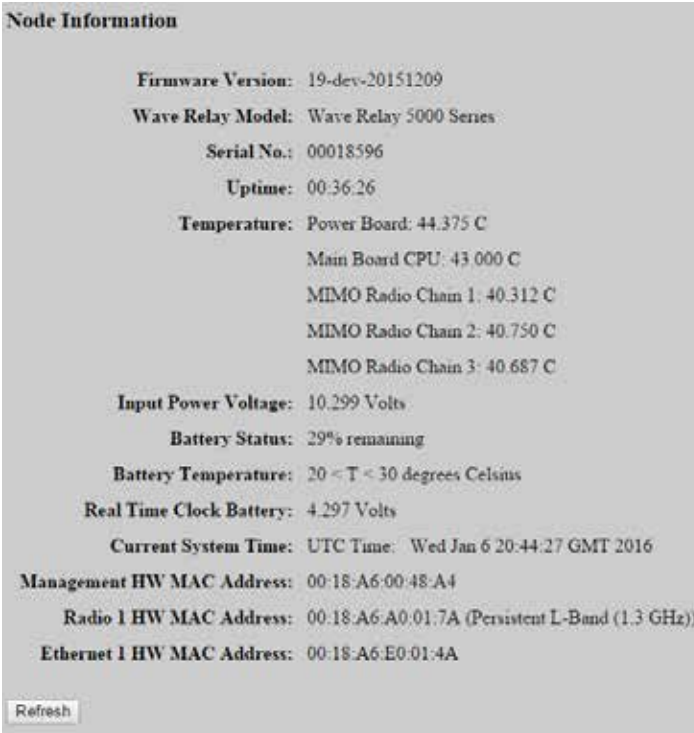
**Real Time Clock Battery:** Voltage of real-time-clock keep-alive battery (on units with RTC)

**Current System Time:** Current system time of the node (in both UTC and current time zone if not UTC)

**Management HW MAC Address:** MAC Address for the management hardware of the node

**Radio 1 HW MAC Address:** MAC Address and frequency band for the radio installed in the node

**Ethernet 1 HW MAC Address:** MAC Address for the Ethernet port in the node



**Node Information**

<b>Firmware Version:</b>	19-dev-20151209
<b>Wave Relay Model:</b>	Wave Relay 5000 Series
<b>Serial No.:</b>	00018596
<b>Uptime:</b>	00:36:26
<b>Temperature:</b>	Power Board: 44.375 C Main Board CPU: 43.000 C MIMO Radio Chain 1: 40.312 C MIMO Radio Chain 2: 40.750 C MIMO Radio Chain 3: 40.687 C
<b>Input Power Voltage:</b>	10.299 Volts
<b>Battery Status:</b>	29% remaining
<b>Battery Temperature:</b>	20 < T < 30 degrees Celsius
<b>Real Time Clock Battery:</b>	4.297 Volts
<b>Current System Time:</b>	UTC Time: Wed Jan 6 20:44:27 GMT 2016
<b>Management HW MAC Address:</b>	00:18:A6:00:48:A4
<b>Radio 1 HW MAC Address:</b>	00:18:A6:A0:01:7A (Persistent L-Band (1.3 GHz))
<b>Ethernet 1 HW MAC Address:</b>	00:18:A6:E0:01:4A

## Configuring Radio Settings for a Single Node

- 1 Click the **Node Configuration** tab.
- 2 Click the **Radio Configuration** button.
- 3 Scroll to the **Radio Configuration** section

**Radio 1**

Radio Name	<input type="text" value="Radio 1"/>	<input checked="" type="checkbox"/> Factory Default
Frequency	<input type="text" value="1.362 GHz"/>	
Bandwidth	<input type="text" value="10MHz"/>	
Max Link Distance	<input type="text" value="0.5 mi - 0.8 km"/>	
Channel Density	<input type="text" value="Low: 2-3 Nodes"/>	
Radio Preference	<input type="text" value="Factory Default (None)"/>	
Max Transmit Power/Chain	<input type="text" value="33.0 dBm - 2W"/>	---> Total Power: 37.8dBm - 6W
Transmit Chain Select	<input type="text" value="Three Chains"/>	
Receive Chain Select	<input type="text" value="Three Chains"/>	

## USING THE WEB MANAGEMENT INTERFACE: INDIVIDUAL NODE INFO

4

Configure settings if needed.

**Note:** changing these settings may cause poor performance or loss of connectivity.

**Radio Name:** Assign a name to the radio - check the **Factory Default** box to use the factory default name.

**Frequency:** Assign a frequency to operate on. Radios must be operating on the same frequency to communicate. Ensure that the frequency is set to match the radio module installed in the unit.



**WARNING!:** User **MUST** refer to the **Professional Installer – Compliance** Section of this manual for approved power levels and approved channels. This warning applies only to RF-2100 with the FCC ID 2AG3J-RF-2100 and RF-5100 with the FCC ID 2AG3J-RF-5100.

**Bandwidth:** Assign a bandwidth to operate on. Nodes must be set to the same bandwidth to communicate. Bandwidth should be increased for shorter distances and decreased for longer distances.

**Max Link Distance:** Set Max Link Distance to the maximum distance any individual link between nodes in the network may need to be. All nodes on the network must be set to the same Max Link Distance.

**Channel Density:** Select the menu item that corresponds to the number of nodes in the network.

**Radio Preference:** Increasing radio preference will make the routing protocol more likely to choose this radio when routing traffic in the network.

**Max Transmit Power/Chain:** Adjust transmit power of the radio - this setting is per chain. The total power is shown to the right of the drop down menu.



**WARNING!:** User **MUST** refer to the **Professional Installer – Compliance** Section of this manual for approved power levels and approved channels. This warning applies only to RF-2100 with the FCC ID 2AG3J-RF-2100 and RF-5100 with the FCC ID 2AG3J-RF-5100.

**Transmit Chain Select:** Choose which RF chains to use to transmit - you may select one, two, or three chains. The Auto setting will instruct the MPU5 to select Transmit Chains on its own.


**Receive Chain Select:** Choose which RF chains to use to receive - you may select one, two, or three chains. The Auto setting will instruct the MPU5 to select Receive Chains on its own.


5

Scroll to the bottom of the page and click **Save & Reconfigure Unit**.

## Upgrading Firmware

- 1 Click the **Node Configuration** tab.
- 2 Click the **Firmware Upgrade** button.
- 3 Click **Choose File**, then navigate to and select the firmware file you wish to load.
- 4 Click **Upload**.

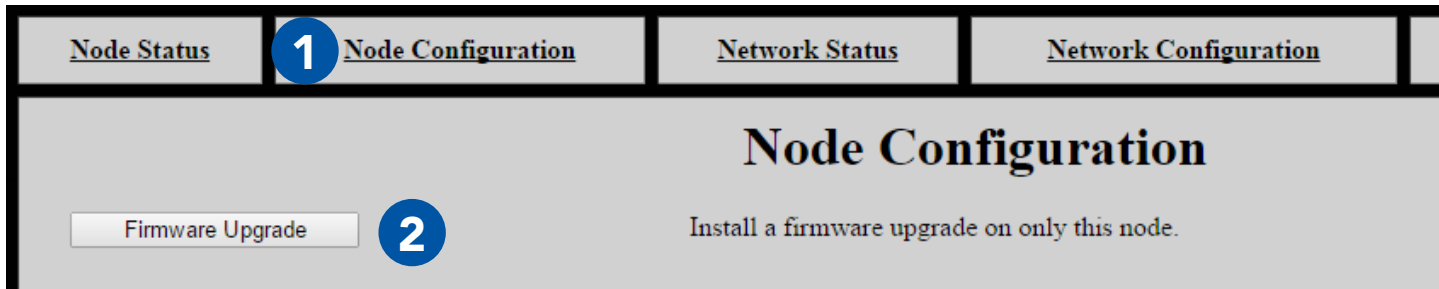
 **WARNING!:** A firmware upgrade will cause the node to be reconfigured, an operation that causes a period of downtime. Do not perform a firmware upgrade during mission critical operations that cannot tolerate such disruptions. Perform firmware upgrades only during scheduled maintenance or other appropriate times.

 **WARNING!:** when upgrading or downgrading a node's firmware, the LED will turn purple. Do not unnecessarily disturb devices during an upgrade. Loss of power during the upgrade can permanently damage the device.

**Note:** when new firmware is available for the MPU5, you will receive an email with the new firmware file to upgrade your units.

**Note:** MPU5 firmware will NOT load on legacy Wave Relay<sup>®</sup> devices (MPU4, MPU3, QUAD).





Node Status **1** Node Configuration Network Status Network Configuration

## Node Configuration

**2** Firmware Upgrade

Install a firmware upgrade on only this node.

## Node Firmware Upgrade

Upgrade this device:

**3**

Upgrade file to install:  No file chosen

**4**

There will be a 20 to 90 second delay when Upload button is pressed.

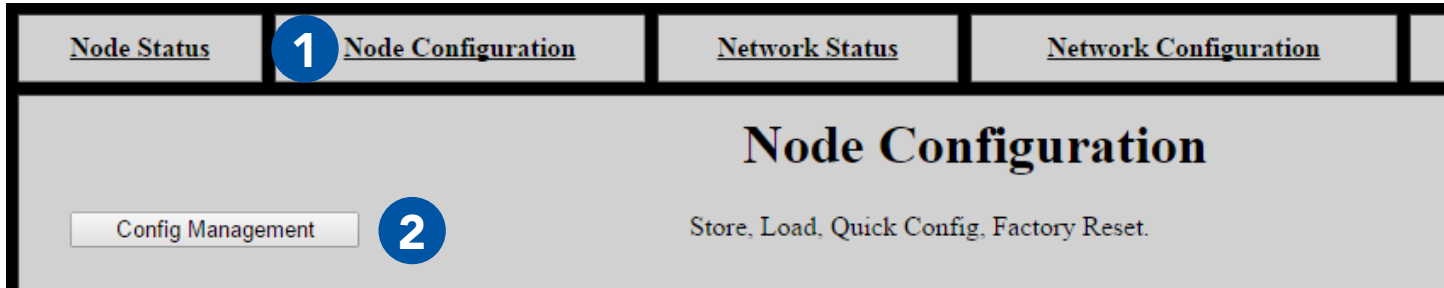
Current Firmware Version: 19-dev-20151209

### Creating a Configuration File

- 1** Click the **Node Configuration** tab.
- 2** Click the **Config Management** button.
- 3** Click **Store File**.
- 4** Click **Store**.
- 5** A prompt will appear to choose where to save the configuration file.

**Note:** this file contains settings (both Network Configuration and Node Configuration settings) for the current node only.

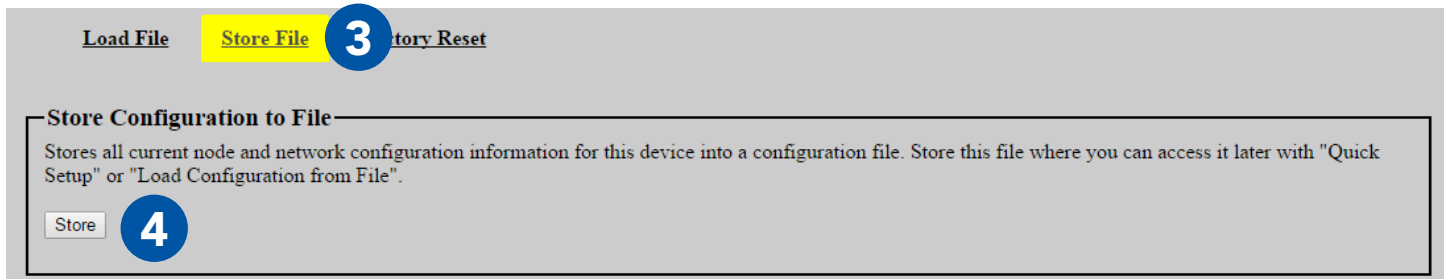
**Note:** do not save configuration files from nodes without a radio module installed.



Node Status **1** Node Configuration Network Status Network Configuration

## Node Configuration

**2** Config Management Store, Load, Quick Config, Factory Reset.



Load File **3** Store File Factory Reset

### Store Configuration to File

Stores all current node and network configuration information for this device into a configuration file. Store this file where you can access it later with "Quick Setup" or "Load Configuration from File".

**4** Store

### Loading Settings from a Configuration File

- 1** Click the **Node Configuration** tab.
- 2** Click the **Config Management** button.
- 3** Click **Load File**.
- 4** Configure **Node Name and Management IP configuration (IP, Netmask, Gateway) source**.  
**Keep Current Settings:** Node Name, Management IP, Netmask, and Gateway will not change after the configuration file is loaded.  
**Pull from Config File:** Node Name, Management IP, Netmask, and Gateway will be set to the values in the Config File you are loading.  
**Quick Setup:** A box will appear that will allow you to enter a Node Name and Management IP Address to be set when the Config File is loaded.
- 5** Configure Push to Managed Node List.  
**No:** The configuration file will be loaded on this node only.  
**Yes, Require All:** The configuration file will be loaded on every node in the Managed Node List if and only if all nodes in the Managed Node List are able to be contacted. If at least one node in the Managed Node List is not able to be contacted, the configuration file will not be loaded onto any nodes.  
**Yes, Any Available:** The configuration file will be loaded onto any node in the Managed Node List that is able to be contacted. The configuration file will not be loaded on any nodes in the Node List that are not able to be contacted.

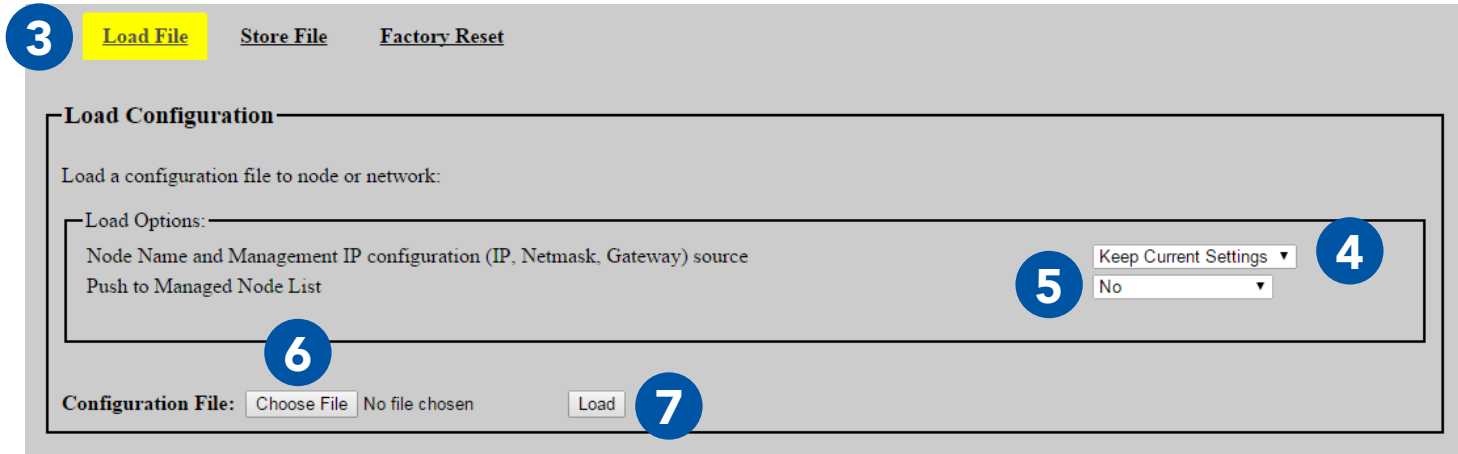
# USING THE WEB MANAGEMENT INTERFACE: CONFIGURATION FILES

**6** Click **Choose File**. Navigate to the desired configuration file to load.

**7** Click **Load**.

**Note:** the configuration file should be from a device with the same firmware version and radio hardware configuration as the device being configured.

**Note:** do not load configuration files that have been saved from nodes with no radio module installed.



**3** **Load File** Store File Factory Reset

**Load Configuration**

Load a configuration file to node or network:

Load Options:

Node Name and Management IP configuration (IP, Netmask, Gateway) source **5** **4**

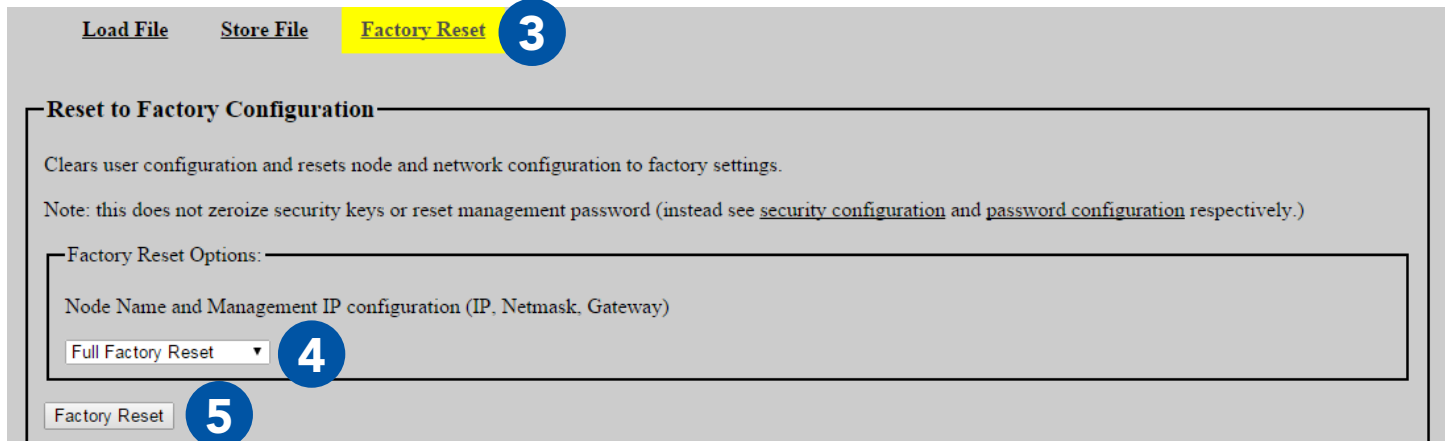
Push to Managed Node List

**6**

**Configuration File:**  No file chosen  **7**

## Reset Node to Factory Configuration

- 1 Click the **Node Configuration** tab.
- 2 Click **Config Management**.
- 3 Click **Factory Reset**.
- 4 Configure **Node Name and Management IP configuration (IP, Netmask, Gateway)**.  
**Keep Current Settings:** Node Name, Management IP, Netmask, and Gateway will not change after the node is reset to factory configuration.  
**Full Factory Reset:** All settings will be reset to factory configuration.
- 5 When you are ready to remove all custom configuration and restore the node to factory settings, click the **Factory Reset** button.



Load File Store File **Factory Reset** 3

**Reset to Factory Configuration**

Clears user configuration and resets node and network configuration to factory settings.

Note: this does not zeroize security keys or reset management password (instead see [security configuration](#) and [password configuration](#) respectively.)

Factory Reset Options:

Node Name and Management IP configuration (IP, Netmask, Gateway)

Full Factory Reset 4

Factory Reset 5

## Check GPS Status

- 1 Click the **Node Status** tab.
- 2 Click the **GPS Status** button.
- 3 The page will display:
  - Source:** GPS information source
  - Latitude:** Current latitude of the node
  - Longitude:** Current longitude of the node
  - Altitude:** Current altitude of the node as MSL (above sea level) and HAE (above ellipsoid)

### Position Update Status

```
Source:          gps
Latitude:        0.0000
Longitude:       0.0000
Altitude MSL:    0 (feet)
Altitude HAE:    18 (feet)
```

### Internal GPS Status

```
Fix Mode:        No Fix
Latitude:        unknown
Longitude:       unknown
Altitude:        unknown
Speed:           unknown
Track:           unknown
Fix Time:        unknown
Satellites Used: 0
Satellites in View: 0
ID/PRN: None
Signal: None
```

[Return to Menu](#)

### Network Status Tab

The **Network Status** tab allows you to view information about every node in the network at the same time. Besides MANET Monitor, Network Visualization, and Channel Plan, each page displays the same information as its counterpart on the Node Status page, but for every node in the network.

**Unit Info:** general node information for every node in the network

**Neighbor Status:** neighbors and SNR for every node in the network

**MANET Monitor:** number of nodes in the network, serial number, node name, IP address, velocity and direction, altitude, neighbors, battery percentage remaining, SNR for every node in the network

**GPS Status:** GPS information for every node in the network

**Network Traffic Load:** traffic load information for every node in the network

**Network Visualization:** view the network in Google Earth

**Channel Plan:** channel setting for each radio

**IP Flow List:** IP flows on the network

**IP Multicast Status:** IP Multicast information



<a href="#">Node Status</a>	<a href="#">Node Configuration</a>	<a href="#">Network Status</a>	<a href="#">Network Configuration</a>	<a href="#">Security</a>	<a href="#">Help</a>	<a href="#">Log Out</a>
-----------------------------	------------------------------------	--------------------------------	---------------------------------------	--------------------------	----------------------	-------------------------

## Network Status

Every node in the node list will be contacted and the combined results will be displayed on one page.

<a href="#">Unit Info</a>	The operational time since last power on or reboot, firmware version, system temperature, voltages, and date.
<a href="#">Neighbor Status</a>	Display a list of neighbors on all managed nodes for each wired and wireless interface.
<a href="#">MANET Monitor</a>	Monitors active nodes heard on the MANET.
<a href="#">GPS Status</a>	The current GPS position.
<a href="#">Network Traffic Load</a>	Monitor and analyze wireless medium and bridged interface traffic loads.
<a href="#">Network Visualization</a>	Display Network Visualization in Google Earth Refresh every: <input type="text" value="2"/> seconds ▼

## Configuring Visualization Settings

- 1 Click the **Node Configuration** tab.
- 2 Click **Node Configuration**.
- 3 Scroll to the **Wave Relay SA** box.
- 4 Configure Wave Relay Situational Awareness settings:

**Enable/Disable WRSA Packets:** select Enabled to enable Wave Relay SA

**WRSA Multicast Address:** defines the multicast address for sending and receiving Wave Relay SA packets - uncheck the Factory Default box to modify this field.

**SA Neighbor Info:** enables or disabled SA Neighbor info - if disabled, Google Earth will not display SNR lines, and SNR will not appear in the MANET monitor. Disable this setting to reduce network overhead and improve scalability and performance of high density networks.

**Visualization Icon:** select an icon to represent the node in Google Earth.

**1** Node Configuration      Network Status      Network Configuration

## Node Configuration

Node Configuration      **2**      Setup the node configuration.

**3** Wave Relay SA

Enable/Disable WRSA packets

WRSA Multicast Address   Factory Default

SA Neighbor Info

Visualization Icon

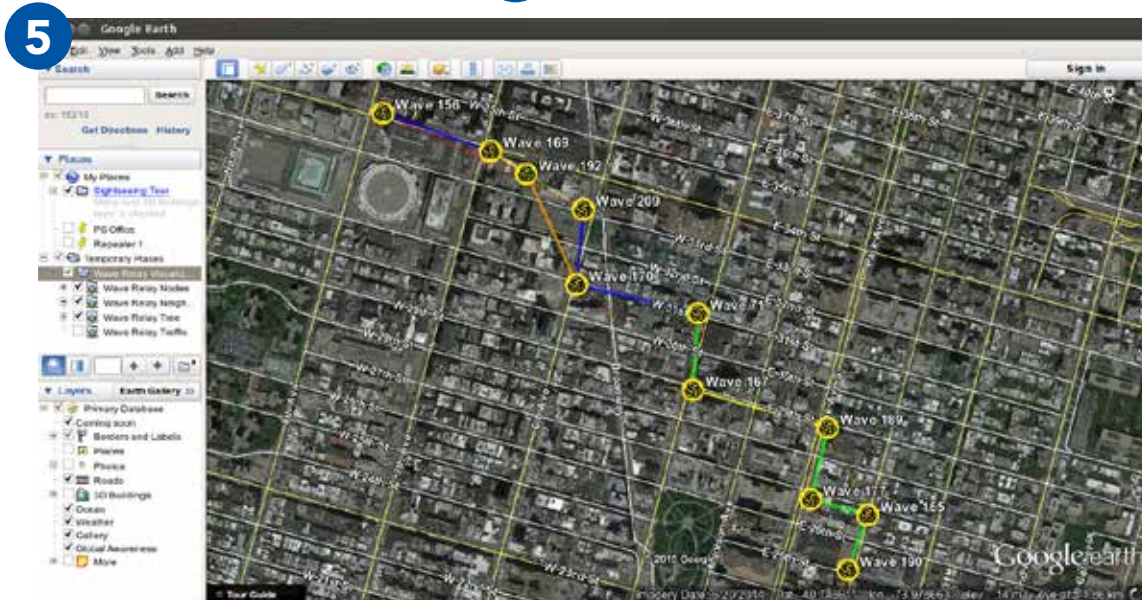


## Viewing Network Visualization

- 1** Click the **Network Status** tab.
- 2** Scroll to **Network Visualization**.
- 3** Select a refresh rate from the drop-down menu. Faster refresh rates will use more bandwidth.
- 4** Click Network Visualization. A file named node-monitor.kml will download.
- 5** Open this file in Google Earth to view network visualization.

# USING THE WEB MANAGEMENT INTERFACE: NETWORK VISUALIZATION

<a href="#">Node Status</a>	<a href="#">Node Configuration</a>	<b>1</b> <a href="#">Network Status</a>	<a href="#">Network Configuration</a>	<a href="#">Security</a>	<a href="#">Help</a>	<a href="#">Log Out</a>
<b>4</b> <a href="#">Network Visualization</a> Display Network Visualization in Google Earth Refresh every: 2 seconds <span style="border: 1px solid black; padding: 2px;">▼</span>						



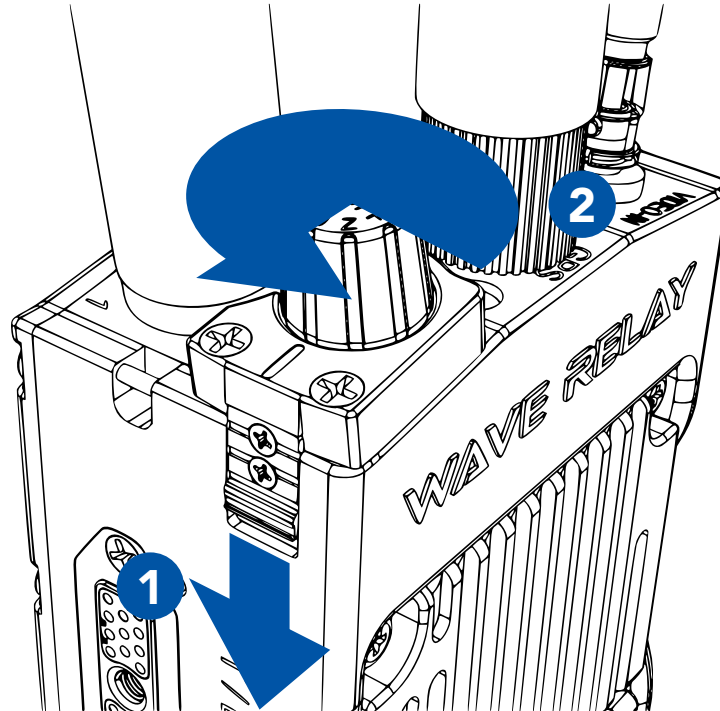
## Part V: Device Operation

### Zeroize the Security Key

- 1** Pull down the **zeroize latch** on the top of the unit.
- 2** With the zeroize latch held down, **twist** the **Power Knob** counterclockwise from the **OFF** position to the **Z** position.

**Note:** the status indicator LED will blink **red** once when the key is zeroized.

# DEVICE OPERATION: ZEROIZE THE SECURITY KEY



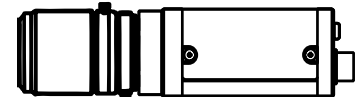
## Connect a Camera to the MPU5

### 🌀 Parts List

For HD-SDI Connection:



HD-BNC to BNC Cable  
**CBL-VID-2001**



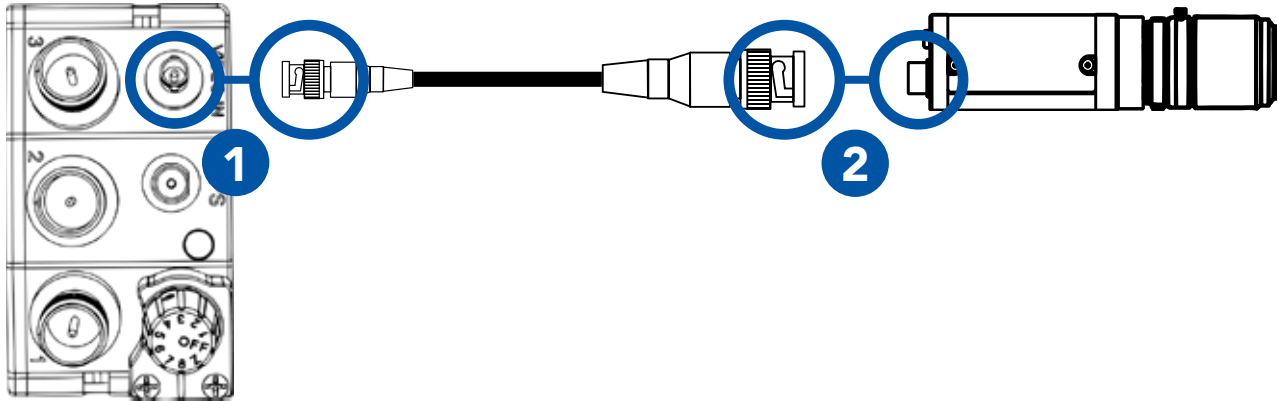
Camera with BNC output



## DEVICE OPERATION: CONNECTING A CAMERA

**1** Connect the **HD-BNC** end of **CBL-VID-2001** to the **HD-BNC** connector on the top of the MPU5.

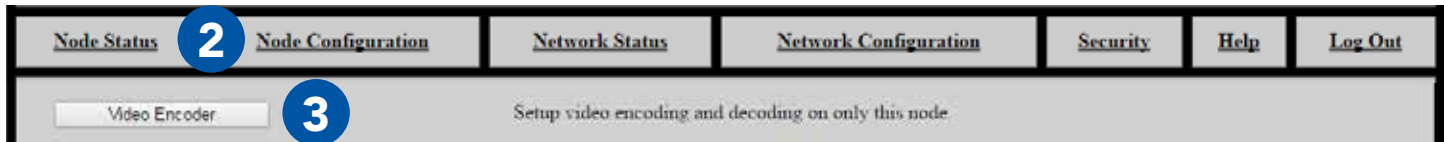
**2** Connect the **BNC** end of **CBL-VID-2001** to the **BNC** connector on the camera.



**Note:** the Video In connector does not supply power to the camera. Ensure that your camera is properly powered via another source.

## Configuring Video Settings

- 1 Connect the MPU5 to the Management Computer and log into the Web Management Interface.
- 2 Click the **Node Configuration** tab.
- 3 Click the **Video Configuration** button.



## Check Camera Input Status

**1** The left column displays status information for the camera connected to the MPU5. Use this status information to verify that the connected camera is configured and working properly.

**Overall Input Status:** displays Yes if a camera is connected; displays No otherwise.

**Scan Mode:** scan mode setting of the connected camera, if available

**Video Data Format:** output format setting of the connected camera, if available

**Input Resolution:** resolution setting of the connected camera, if available

**Input Frames/Sec:** frame rate setting of the connected camera, if available

**Audio Present:** audio status from the connected camera, if available

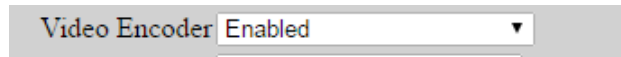
Input Status	
Overall Input Status:	Yes
Scan Mode:	--
Video Data Format:	NTSC
Input Resolution:	NTSC
Input Frames/Sec:	30
Audio Present:	None

## Encoder Configuration

The center column displays configuration settings for the MPU5's onboard video encoder.

### Enable/Disable Video Encoding

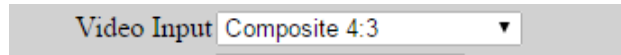
**1** In the **Enable/Disable** drop-down menu, select **Enabled**.



**2** To disable Video, select **Disabled**.

### Select Video Input

**1** Select the video source that corresponds to your camera from the **Video Input** drop-down menu.



**3G-SDI:** 3G-SDI input via the **Video In** connector on the top of the MPU5

**Composite 4:3:** Composite input with a 4:3 aspect ratio via the **Video In** connector on the top of the MPU5

**Composite 16:9:** Composite input with a 16:9 aspect ratio via the **Video In** connector on the top of the MPU5

**Note:** you **MUST** manually configure the correct input source. If the correct input source is not selected, input status will show no camera detected.

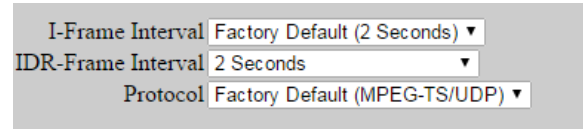
## Configure Video Output IP Address and Port

Video Output IP	239.23.212.200	<input checked="" type="checkbox"/> Factory Default
Video Output Port	9722	<input checked="" type="checkbox"/> Factory Default

- 1** Enter an IP address for the video in the **Video Output IP** field. Pick a unique IP address. Uncheck the **Factory Default** box to make changes to this field. Check the **Factory Default** box to use the Factory Default Video Output IP.
- 2** Enter a port for the video stream in the **Video Output Port** field. Uncheck the **Factory Default** box to make changes to this field. Check the **Factory Default** box to use the Factory Default Video Output Port.

### Advanced Video Configuration Options

**1** Click **Show/Hide Advanced Settings**. This will show or hide drop-down menus for **I-Frame Interval**, **IDR-Frame Interval**, and **Protocol**.



A screenshot of a configuration panel with three dropdown menus. The first menu is labeled 'I-Frame Interval' and is set to 'Factory Default (2 Seconds)'. The second menu is labeled 'IDR-Frame Interval' and is set to '2 Seconds'. The third menu is labeled 'Protocol' and is set to 'Factory Default (MPEG-TS/UDP)'.

**I-Frame Interval (Advanced):** Sets the time between I-Frames (in seconds). The shorter amount of time between I-Frames, the better video quality will be, but the video stream will use more bandwidth. It is not recommended for non-advanced users to change this setting.

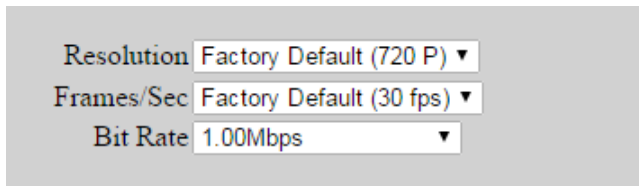
**IDR-Frame Interval (Advanced):** Sets the time between IDR-Frames (in seconds). Increasing IDR-Frame interval will decrease the bandwidth used by the stream, but it may reduce video quality. It is not recommended for non-advanced users to change this setting.

**Note:** Available IDR-Frame Interval options change based on the selected I-Frame interval. If you change I-Frame Interval and the selected IDR-Frame Interval setting is available for that I-Frame Interval, the IDR-Frame Interval will not change. If you change I-Frame Interval and the selected IDR-Frame Interval setting is not available for that I-Frame Interval, IDR-Frame Interval will be set to the factory default setting for that I-Frame Interval.

**Protocol (Advanced):** Selects the streaming protocol for the video stream. Options are: **MPEG-TS/UDP** or **RTP/UDP**.

## Select Video Encoding Settings

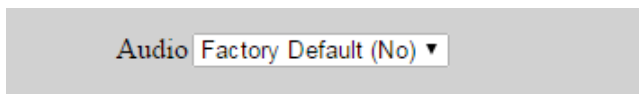
- 1 Select a resolution from the Resolution drop-down menu. This setting selects the resolution at which video will be encoded. Options are:
- 2 Select a frame rate from the Frame Rate drop-down menu. This setting selects the frame rate at which video will be encoded.
- 3 Select a bit rate from the Bit Rate drop-down menu. This setting selects the bit rate at which video will be encoded.



Resolution Factory Default (720 P) ▼  
Frames/Sec Factory Default (30 fps) ▼  
Bit Rate 1.00Mbps ▼

**Note:** Available frame rate and bit rate options change based on the selected resolution. If you change resolution and the selected frame rate and bit rate settings are available for that resolution, they will not change. If you change resolution and the selected frame rate or bit rates settings are not available for that resolution, frame rate and bit rate will be set to the factory default setting for that resolution.

- 4 If you wish to encode audio with the video stream, select **Yes** from the **Audio** drop-down menu. Otherwise, select **No**.



Audio Factory Default (No) ▼

## DEVICE OPERATION: CONFIGURING VIDEO SETTINGS

**6** When you are finished configuring settings, click **Save & Reconfigure Unit**.

**7** Use the **Camera Motion & Estimated Video Quality** table on the bottom left of the page to check if the bit rate you have selected will be sufficient for good-quality video based on how much your camera will be moving. If it is not, adjust the bit rate setting accordingly.

Camera Motion	Estimated Video Quality
VeryLow/None:	Good
Low:	Good
Medium:	Good
High:	Good
Very High:	Sub-optimal



## Video Viewer URLs

```
Video Viewer URLs
For VLC:      udp://@239.23.212.200:9722
Other Viewers: udp://239.23.212.200:9722
```

The **Video View URLs** page will display two URLs below the Video Configuration settings. To pull video from this node, enter the **For VLC** URL into VLC or the **Other Viewers** URL in another video player.

**Note:** if you change **Video Output IP** or **Video Output Port** on the **Video Configuration** page, these URLs will change as well.

## Video Encoding Status

The center column displays configuration settings for the MPU5's onboard video encoder.

**Overall Encoder Status:** displays whether this node is encoding video or not.

**Subscribers:** displays whether there are users on the network subscribing to the video from this node.

**Note:** if no one is subscribed to the video from this node, the node will not encode video.

**Output Resolution:** displays the resolution of the encoded video being output

**Output Frames/Sec:** displays frame rate of the encoded video being output

**Output Bit Rate:** displays the bit rate of the encoded video being output

**Audio Encoded:** displays whether audio is being encoded with the video stream or not

Encoder Output Status	
Overall Encoder Status:	Encoding Video
Subscribers	Subscribers Present
Output Resolution:	1280x720
Output Frames/Sec:	30.00
Output Bit Rate:	1.00 Mbps
Audio Encoded:	Not Present



## What do I do if video is not being encoded?

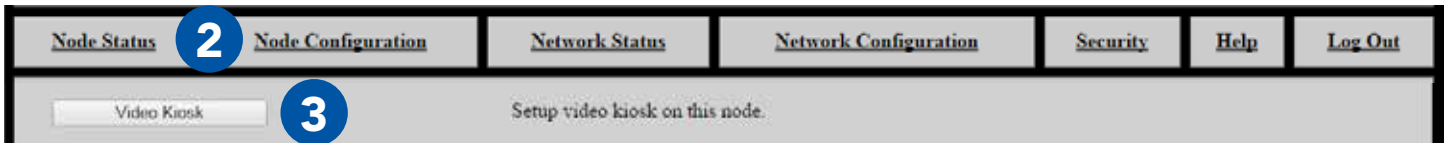
- 1 Ensure that the camera is powered and all cables are connected securely to the correct connectors.
- 2 Ensure Video Encoding is enabled on the node. You must click the Save & Reconfigure Unit button for settings to take effect.
- 3 Ensure that the correct video input is selected on the Video Encoding Configuration page.
- 4 If there are no subscribers to the video, video will not be encoded. Check if video is being encoded when a subscriber is present.
- 5 Ensure the correct Video Viewer URL is entered into your video viewer.

## Video Kiosk Mode

Video Kiosk Mode allows you set up the MPU5 as a kiosk video player. When Kiosk Mode is enabled, up to four video feeds may be configured. The MPU5 will automatically display one of these video feeds, and the standard MPU5 Android interface is disabled. The video being viewed can be changed from within the Web Management Interface or toggled by using the keypad.

## Configuring Video Kiosk Mode

- 1 Connect the MPU5 to the Management Computer and log into the Web Management Interface.
- 2 Click the **Node Configuration** tab.
- 3 Click the **Video Configuration** button.

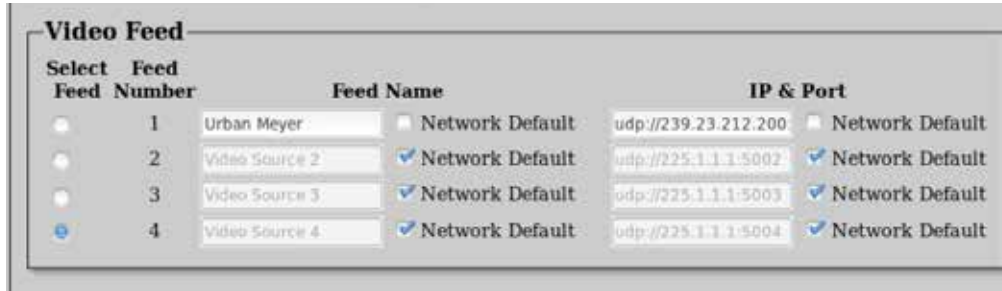


## Enable Video Kiosk Mode

- 1** In the **Enable/Disable** drop-down menu, select **Enabled**.
- 2** To disable Video, select **Disabled**.



## Configure Video Feed Settings



Video Feed					
Select	Feed	Feed Name		IP & Port	
Feed Number					
<input type="radio"/>	1	Urban Meyer	<input type="checkbox"/> Network Default	udp://239.23.212.200	<input type="checkbox"/> Network Default
<input type="radio"/>	2	Video Source 2	<input checked="" type="checkbox"/> Network Default	udp://225.1.1.1:5002	<input checked="" type="checkbox"/> Network Default
<input type="radio"/>	3	Video Source 3	<input checked="" type="checkbox"/> Network Default	udp://225.1.1.1:5003	<input checked="" type="checkbox"/> Network Default
<input checked="" type="radio"/>	4	Video Source 4	<input checked="" type="checkbox"/> Network Default	udp://225.1.1.1:5004	<input checked="" type="checkbox"/> Network Default

The **Video Feed** box configures settings for each of the 4 feeds to be viewed in Video Kiosk Mode.

**Select Feed:** this column controls which video feed will be displayed by default in Video Kiosk Mode. Click the circle for the video feed you wish to be the default.

**Feed Number:** displays the number of each of the four video feeds. When in Video Kiosk Mode, you may select a feed to be displayed using the corresponding keypad number or the left and right arrow keys.

**Feed Name:** assigns a custom name to each video feed. Uncheck the Network Default box to edit this field.

**IP & Port:** sets the IP address and Port for the video feed to be accessed in the format **<IP Address>:<Port>**. Uncheck the Network Default box to edit this field.

## Video Kiosk Mode Status

**Status**

Enabled:

Currently  
Playing

Feed:

Feed Number	Feed Name	Feed IP & Port
1	Urban Meyer	udp://239.23.212.200:9722
2	Video Source 2	udp://225.1.1.1:5002
3	Video Source 3	udp://225.1.1.1:5003
4	Video Source 4	udp://225.1.1.1:5004

The **Status** box displays Video Kiosk Mode status information.

**Enabled:** displays **Yes** if Video Kiosk Mode is enabled and displays **No** if Video Kiosk Mode is disabled

**Currently Playing Feed:** displays the number of the video feed that is currently being viewed in Video Kiosk Mode

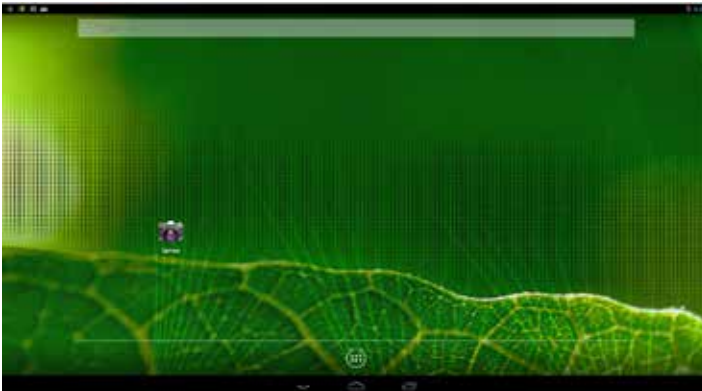
**Feed Number:** displays the number of each of the four video feeds

**Feed Name:** displays the name for each video feed

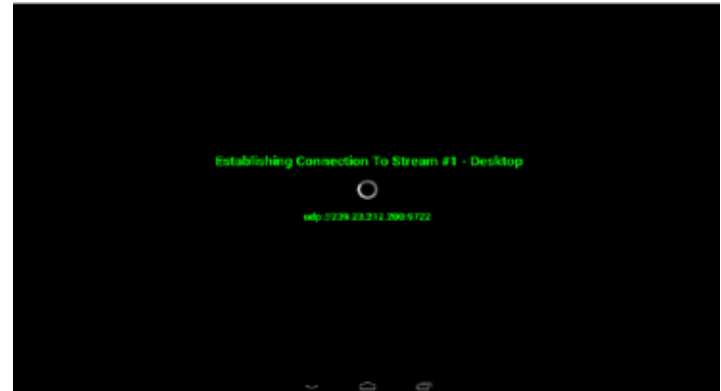
**Feed IP & Port:** displays the IP address and port for each video feed

### Video Kiosk Mode Operation

- ▶ The video kiosk app will automatically restart if video encoding settings change or a problem occurs.
- ▶ The only way to exit the video kiosk player is to disable Video Kiosk Mode from the Web Management Interface.



Video Kiosk Mode Disabled



Video Kiosk Mode Enabled



## DEVICE OPERATION: VIDEO KIOSK MODE OPERATION

- ▶ The video feed being viewed can be changed from the Web Management Interface or from the app:
  - ▶ With num lock disabled, use the left and right arrow keys
  - ▶ With num lock enabled, use the keypad to select the corresponding video feed



Num Lock Disabled



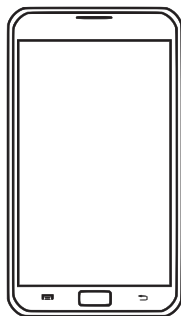
Num Lock Enabled

## Connect an EUD or Handheld Display to the MPU5

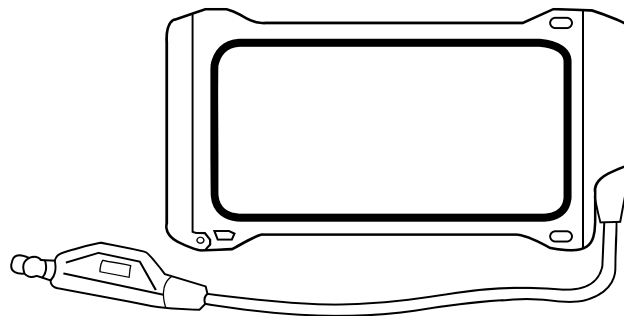
### 🌀 Parts List



22-Pin to 6-Pin USB Push Pull Android™ Tether Cable  
**CBL-DATA-2004**



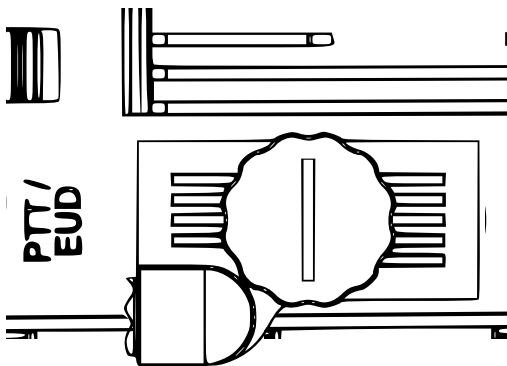
Android™ EUD  
**ACC-EUD-0001**



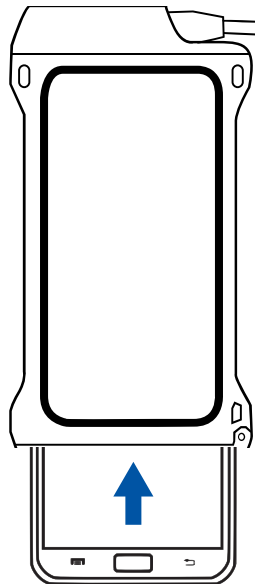
EUD IP67 Enclosure  
**MOLLE-IP67-N3**

## DEVICE OPERATION: CONNECTING AN EUD OR HANDHELD DISPLAY

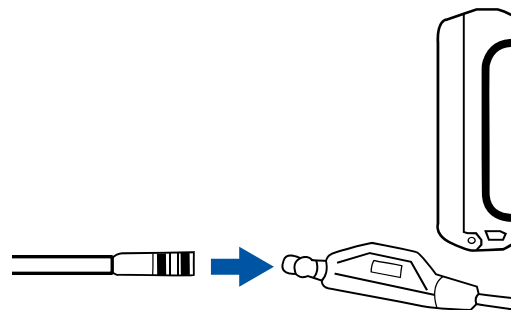
- 1** Connect **CBL-DATA-2004** to the **PTT/EUD** side connector on the MPU5.



- 2** Insert the Android™ EUD into the Juggernaut Case.



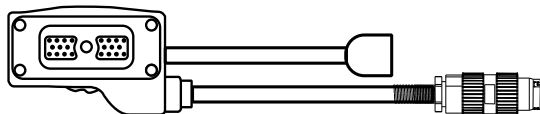
- 3** Connect the **6-Pin Push Pull connector** on the Juggernaut Case to the **6-Pin Push Pull connector** on **CBL-DATA-2004**.



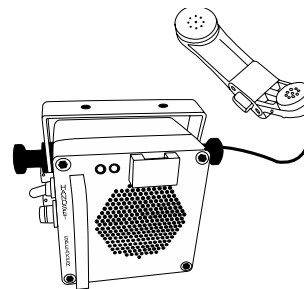
- 4** The MPU5 Android™ OS will be displayed on the EUD or Display.

## Connect a Monitor or TV to the MPU5

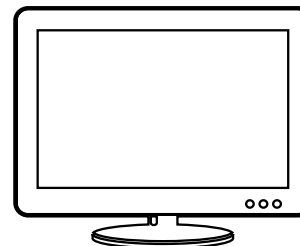
### 🌀 Parts List



22-Pin to Audio and Video Out  
**CBL-DATA-3002**



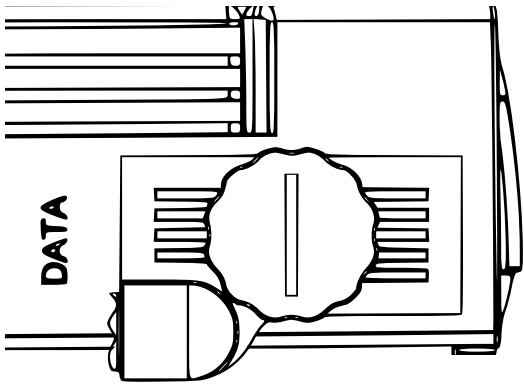
Speaker Box or Headset with U-328 Connector



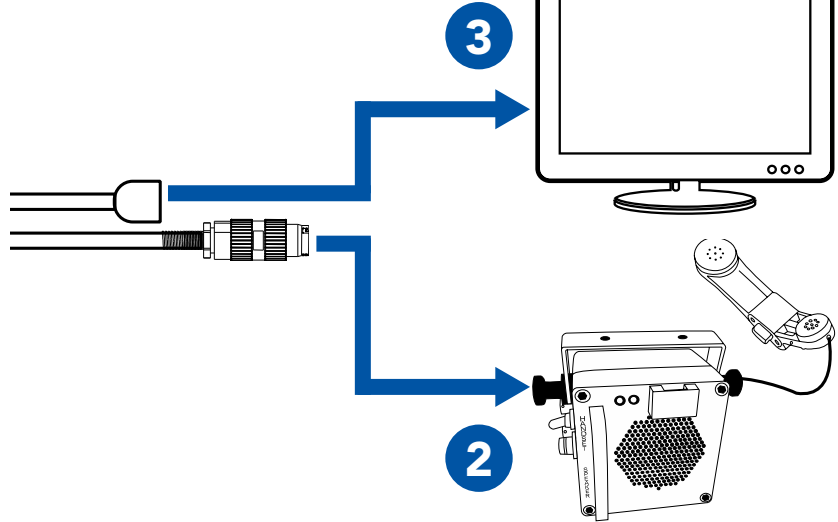
Monitor or TV with HDMI Input

## DEVICE OPERATION: CONNECTING A MONITOR OR TV

**1** Connect **CBL-DATA-3002** to the **DATA** side connector on the MPU5.







**2** Connect the speaker box or headset to the **U-328 audio connector** on **CBL-DATA-3002**.



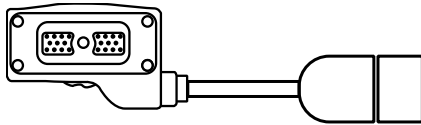
**3** Connect the **HDMI** end of **CBL-DATA-3002** to the **HDMI Input** on the monitor or TV.

### Why can't I see video on my Monitor or TV?

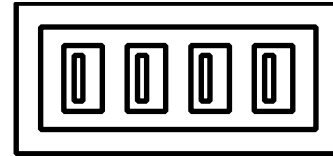
-  1 Ensure that the Monitor or TV is powered on.
-  2 Ensure that all cables are connected properly.
-  3 Ensure that the Monitor or TV is set to the correct HDMI input.
-  4 Reboot the node.

## Connect USB Accessories to the MPU5

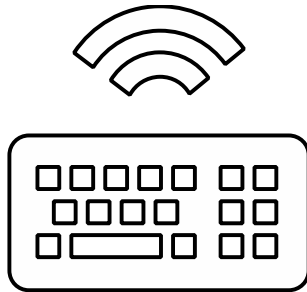
### Parts List



22-Pin to Type A Female USB 2.0 Receptacle  
**CBL-DATA-2003**



USB Hub  
(Optional)



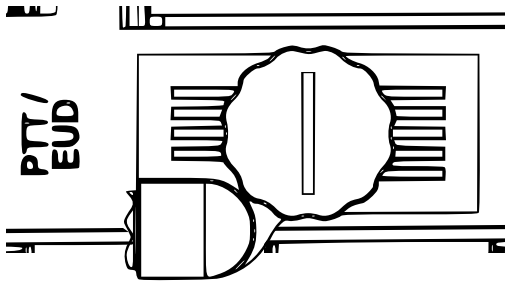
USB Keyboard  
(Optional)



USB Mouse  
(Optional)

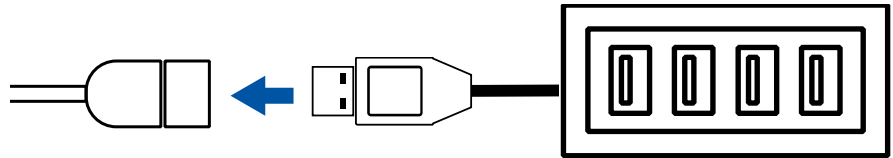
## 🌀 DEVICE OPERATION: USB ACCESSORIES

**1** Connect **CBL-DATA-2003** to an unused side connector on the MPU5.



**2** Connect the USB Hub or one USB accessory to the **USB receptacle** on the end of CBL-DATA-2003.

**3** If you are using a USB Hub, connect USB accessories to the USB receptacles in the USB Hub.



### ? Why don't my USB accessories work?

**1** Ensure all cables are connected properly.

**2** Ensure that all wireless accessories (keyboards/mice/etc.) are powered (i.e. batteries are not dead)

**3** If you are using a USB Hub, connect the USB accessory directly to CBL-DATA-2003. If the accessory works, replace the USB hub.

**4** If available, test a different CBL-DATA-2003. If the accessory works, the original CBL-DATA-2003 may be defective.

**5** Reboot the node.

**4** Your USB accessory may not be compatible. Contact Persistent Systems support.

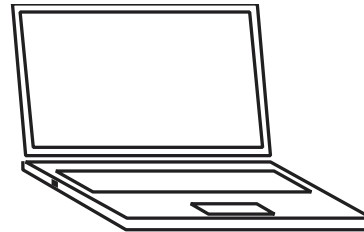


## Install Android™ Apps on the MPU5

### Parts List



.apk file for Android™ App(s)

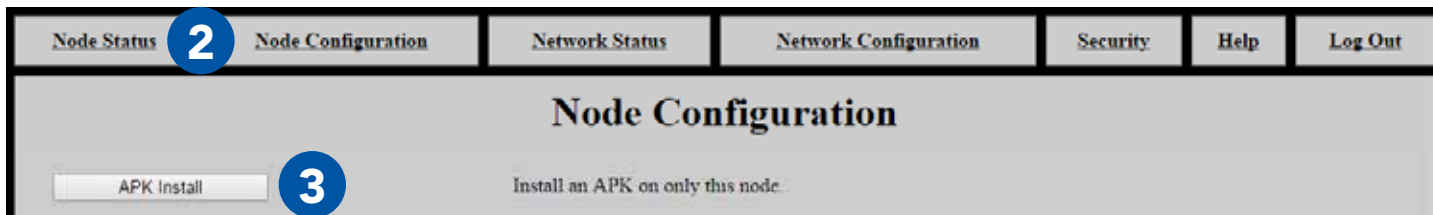


Management Computer

**Note:** the Operating System on the MPU5 is Android™ version 5.0 (Lollipop). Ensure that the app you wish to install is compatible with this version of the Android™ OS.

## DEVICE OPERATION: INSTALLING APPS

- 1 Connect the MPU5 to the Management Computer and log into the Web Management Interface.
- 2 Click the **Node Configuration** tab.
- 3 Click **APK Install**.



**4** Click **Choose File** and navigate to the .apk file you wish to install.

**5** Click **Upload** and wait for the on-screen prompt to say Node APK Install Succeeded. The page will then reload.

### Node APK Install

Install APK on this node:

APK file to install:  No file chosen

**4**

**5**

#### APK Install Status

Started APK Install.

127.0.0.1: Connected to node

127.0.0.1: APK file transferred

127.0.0.1: Ready for APK install

127.0.0.1: APK install successful

Node APK Install Succeeded

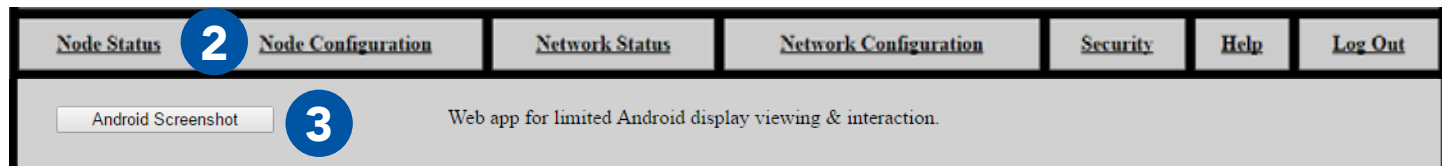
Stand by. Preparing to reload

### View Android™ OS via the Web Management Interface

- ▶ The Android™ Screenshot page allows users to view and control Android™ on the MPU5 via the Web Management Interface

### Accessing the Android™ Screenshot Page

- 1 Connect the MPU5 to the Management Computer and log into the Web Management Interface.
- 2 Click the **Node Status** tab.
- 3 Click the **Android™ Screenshot** button.



## Using the Android™ Screenshot Page



**Mouse Click:** tap/swipe as if using a touch screen EUD

**Reload Screenshot:** refreshes the displayed image of the Android™ OS

**Power:** powers on/off the Android™ display - this will not close apps

**Back:** returns to the previous page

**Home:** returns to the Android™ Home Screen

**App Switch:** allows the user to toggle between open apps

### Network Configuration Tab

The **Network Configuration** tab allows you to perform actions on all nodes in the network.

**Network Node List:** manage the Network Node List

**Network Upgrade:** upgrade firmware on all nodes

**Network Password:** change the Management Password for all nodes

**Network APK Install:** install an APK on all nodes in the network

**Reboot Network:** reboot all nodes in the network

Each action on this tab is the same as the corresponding action on the Node Configuration tab.

Network Upgrade and Network APK install have a box labeled Require All. If this box is checked, the firmware or .apk file will only be installed if and only if all nodes in the Network Node List are able to be contacted. If any node is unable to be contacted, the firmware or .apk file will not be installed on any node. If this box is unchecked, the firmware or .apk file will only be installed on nodes that are able to be contacted. The firmware or .apk file will not be installed on nodes that are unable to be contacted.

<a href="#">Node Status</a>	<a href="#">Node Configuration</a>	<a href="#">Network Status</a>	<a href="#">Network Configuration</a>	<a href="#">Security</a>	<a href="#">Help</a>	<a href="#">Log Out</a>
-----------------------------	------------------------------------	--------------------------------	---------------------------------------	--------------------------	----------------------	-------------------------

## Network Configuration

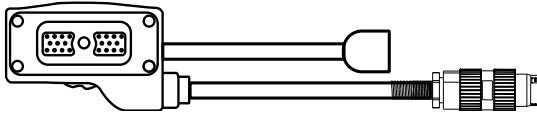
<a href="#">Network Node List</a>	Manage the network node list.
<a href="#">Network Upgrade</a>	Upgrade the firmware on all of the nodes in the network in a single step.
<a href="#">Network Password</a>	Change the management interface password.
<a href="#">Network APK Install</a>	Install an APK on all of the nodes in the network in a single step.
<a href="#">Reboot Network</a>	Reboot all of the nodes in the network.

**Require All (verify connectivity to all in Managed Node List before upgrade)**

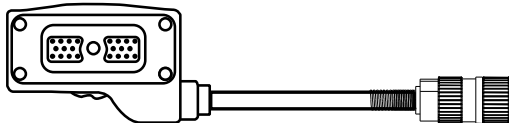
# 🌀 DEVICE OPERATION: CONNECTING A PTT DEVICE

## Connect a PTT Device to the MPU5

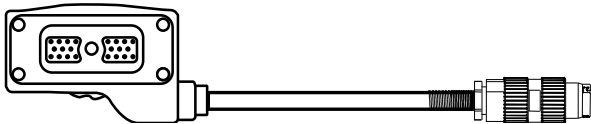
### 🌀 Parts List



22-Pin to audio and Video Out  
**CBL-DATA-3002**



22-Pin to U-329  
**CBL-AUD-0001**

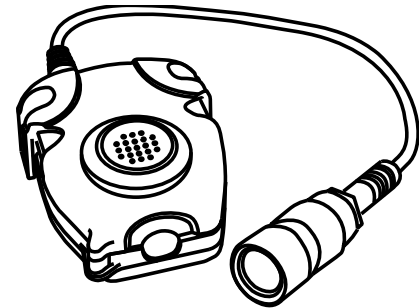


22-Pin to U-328  
**CBL-AUD-0002**



22-Pin to U94 Receptacle  
**CBL-AUD-0003**

The cable you need is dependent on what connector your PTT device has.



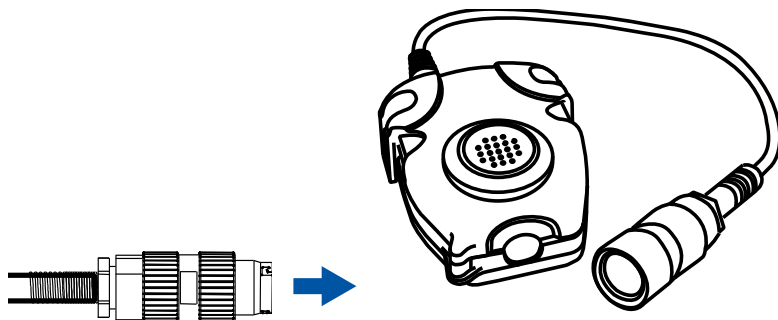
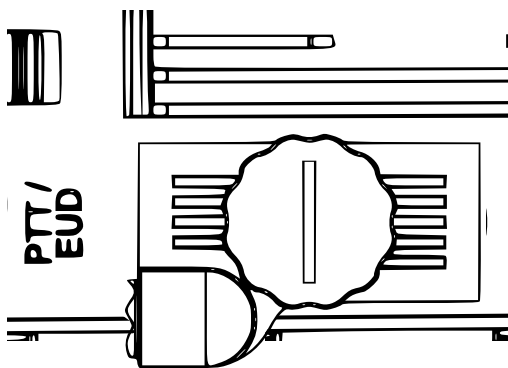
Compatible Push-to-Talk device



## DEVICE OPERATION: CONNECTING A PTT DEVICE

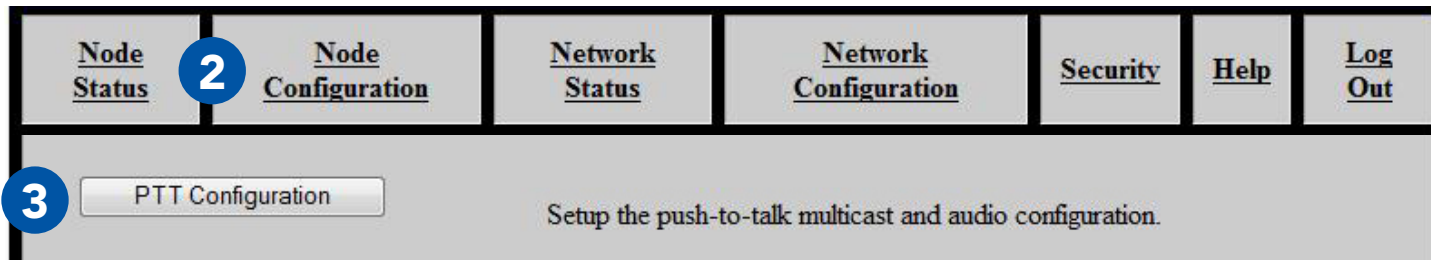
- 1 Connect the cable to the **PTT/EUD** side connector on the MPU5.

- 2 Connect the PTT device to the connector on the end of the cable.



## Configure PTT Settings

- 1 Connect the MPU5 to the Management Computer and log into the Web Management Interface.
- 2 Click the **Node Configuration** tab.
- 3 Click the **PTT Configuration** button.



## Enable Push-to-Talk

- 1 In the **Run PTT Subsystem** drop-down menu, select **Enabled**.
- 2 To disable Push-to-Talk, select **Disabled**.

Run PTT subsystem

## Set Earpiece Volume

- 1 Next to Volume, **check** the **Network Default** box to use the Network Default earpiece volume.
- 2 To customize earpiece volume, **uncheck** the **Network Default** box.
- 3 In the **Volume** field, enter a value **0 - 125**. Values above 100 are digitally amplified.

Volume   Network Default

### Set Microphone Level

- 1** Next to Microphone Level, **check** the **Network Default** box to use the Network Default microphone level.
- 2** To customize microphone level, **uncheck** the **Network Default** box.
- 3** In the **Microphone Level** field, enter a value:
  - auto:** Uses automatic gain control for microphone input - recommended for most users
  - 0 - 100:** valid microphone level volumes

Microphone Level   Network Default

## Set Transmit Mode

- 1 Select a setting from the **Transmit Mode** drop-down menu:

**OnKeyPress:** audio is transmitted only when the PTT button is pressed on the headset

**Continuous:** audio is continuously transmitted.

**Note:** other nodes may monitor the channel only. Selected Channel audio transmissions will interrupt monitored continuously transmitted audio.

Transmit Mode

### Set Transmit or Receive Audible Checktone

- 1 From the **Tones on Transmit** and **Tones on Receive** drop down menus, select:
  - Quiet:** no audible checktone
  - Beep:** audible checktone will be set to a beep
  - Voice:** audible checktone will be a vocalized "one"
  - Network Default:** audible checktone will be set to the network default setting

Tones on Transmit	Network Default (Beep) ▼
Tones on Receive	Network Default (Beep) ▼

## Enable/Disable Low Battery Audible Notification

1

Select a setting in the **Low Battery** drop-down menu:

**Enabled:** when the battery is depleted to 5%, the node will play an audible notification every 5 minutes.

**Disabled:** no low battery audible notification will occur.

**Network Default:** network default setting

Audible Low Battery Notify Network Default (Enabled) ▼

### Selecting Channels

- 1 In the **Selected** column, click the circle for the channel(s) you wish to transmit on.
- 2 In the **Monitor** column, check the box for each channel you wish to monitor. You will be able to hear PTT audio on the monitored channel.

**Pro Tip:** you may select any number of channels to monitor. In the Monitor column, check the box for each channel you wish to monitor. You will NOT be able to transmit PTT audio on channels other than the one you selected in Step 3.

### Customize a PTT Channel

- 3 In the **Channel** field, uncheck the **Network Default** box and enter the desired channel name.
- 4 In the **Multicast Address** field, uncheck the **Network Default** box and enter the desired multicast address and multicast port in the form <multicast address>:<multicast port>.

**Note:** valid multicast address values are in the range **224.0.0.0 - 239.255.255.255**

**Note:** valid multicast port values are in the range **1 - 65534**

**Note:** each channel **MUST** have a unique multicast address and multicast port.

- 5 Scroll to the bottom of the page and click **Save**.



## DEVICE OPERATION: CONFIGURING PTT SETTINGS

Channel Selected	Monitor Name	Multicast Address
0	<input checked="" type="checkbox"/> Channel 0	<input checked="" type="checkbox"/> Network Default 239.192.60.0:60000 <input checked="" type="checkbox"/> Network Default
1	<input type="checkbox"/> Channel 1	<input checked="" type="checkbox"/> Network Default 239.192.60.1:60001 <input checked="" type="checkbox"/> Network Default
2	<input type="checkbox"/> Channel 2	<input checked="" type="checkbox"/> Network Default 239.192.60.2:60002 <input checked="" type="checkbox"/> Network Default
3	<input type="checkbox"/> Channel 3	<input checked="" type="checkbox"/> Network Default 239.192.60.3:60003 <input checked="" type="checkbox"/> Network Default
4	<input type="checkbox"/> Channel 4	<input checked="" type="checkbox"/> Network Default 239.192.60.4:60004 <input checked="" type="checkbox"/> Network Default
5	<input type="checkbox"/> Channel 5	<input checked="" type="checkbox"/> Network Default 239.192.60.5:60005 <input checked="" type="checkbox"/> Network Default
6	<input type="checkbox"/> Channel 6	<input checked="" type="checkbox"/> Network Default 239.192.60.6:60006 <input checked="" type="checkbox"/> Network Default
7	<input type="checkbox"/> Channel 7	<input checked="" type="checkbox"/> Network Default 239.192.60.7:60007 <input checked="" type="checkbox"/> Network Default
8	<input type="checkbox"/> Channel 8	<input checked="" type="checkbox"/> Network Default 239.192.60.8:60008 <input checked="" type="checkbox"/> Network Default
9	<input type="checkbox"/> Channel 9	<input checked="" type="checkbox"/> Network Default 239.192.60.9:60009 <input checked="" type="checkbox"/> Network Default
10	<input type="checkbox"/> Channel 10	<input checked="" type="checkbox"/> Network Default 239.192.60.10:60010 <input checked="" type="checkbox"/> Network Default
11	<input type="checkbox"/> Channel 11	<input checked="" type="checkbox"/> Network Default 239.192.60.11:60011 <input checked="" type="checkbox"/> Network Default
12	<input type="checkbox"/> Channel 12	<input checked="" type="checkbox"/> Network Default 239.192.60.12:60012 <input checked="" type="checkbox"/> Network Default
13	<input type="checkbox"/> Channel 13	<input checked="" type="checkbox"/> Network Default 239.192.60.13:60013 <input checked="" type="checkbox"/> Network Default
14	<input type="checkbox"/> Channel 14	<input checked="" type="checkbox"/> Network Default 239.192.60.14:60014 <input checked="" type="checkbox"/> Network Default
15	<input type="checkbox"/> Channel 15	<input checked="" type="checkbox"/> Network Default 239.192.60.15:60015 <input checked="" type="checkbox"/> Network Default

**5**

### Using Wave Relay® Push-to-Talk

- 1 Ensure that your PTT device is connected and channel settings have been configured properly and as desired.
  - 2 **Press and hold** the PTT button on the PTT device.
  - 3 Wait to hear a single beep.
  - 4 Talk.
  - 5 **Release** the PTT button when you are finished talking.
- ▶ You may talk or listen, but you may not do both simultaneously.
  - ▶ Transmissions from an individual user are broadcast to all other users on the network using the same channel.
  - ▶ Only one person may talk on a channel at one time. If you try to PTT while another user is transmitting, you will hear a busy signal.
  - ▶ Selected Channel audio will interrupt Monitored Channel audio.
  - ▶ Flash Override audio will interrupt both Selected Channel and Monitored Channel audio.

## Using Flash Override

Flash Override is a feature that allows a user to transmit audio to all nodes on the network regardless of which channel they are operating on.

Flash Override audio will interrupt all audio on all channels.

- 1** To activate Flash Override, **"tap-tap-hold"** the PTT button (**press and release** the PTT button quickly in succession, then **press and hold** the PTT button for the duration of the transmission)
- 2** The transmitting user and all receiving users will hear three beeps.
- 3** Talk.
- 4** **Release** the PTT button when you are finished talking.

The following notes refer to these part numbers:

Persistent Systems P/N	Description	FCC ID	IC ID
RF-2100	S-Band Radio Module	2AG3J-RF2100	20968-RF2100
RF-5100	Upper C-Band Radio Module	2AG3J-RF5100	20968-RF5100

*This device complies with part 15 of the FCC rules and Industry Canada license-exempt RSS standard(s). 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.*

*Le présent appareil est conforme aux la partie 15 des règles de la FCC et CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

**NOTE:** THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

**NOTE II:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

**OPERATING FREQUENCY:** Operating frequency is determined by the installer. It is important that the frequency configured meets local regulations.

# PROFESSIONAL INSTALLER – COMPLIANCE

**P/N:** RF-2100

**FCC ID:** 2AG3J-RF2100

**IC ID:** 20968-RF2100

## US and Canada Power Limits

Mode:	SISO: Only One Port Active		MIMO (2x2): 2 Ports Active Power Setting / Port		MIMO (3x3): All 3 Ports Active Power Setting / Port	
	Max. Power Setting Approved (dBm)	Max. EIRP (dBm)	Max. Power Setting Approved (dBm)	Max. EIRP (dBm)	Max. Power Setting Approved (dBm)	Max. EIRP (dBm)
CHANNEL: 1	28	32	26	31	24.5	31
2	30	35	26	32	24.5	31
3	30	36	26	32	24.5	31
4	30	36	26	32	24.5	31
5	30	36	26	32	24.5	31
6	30	36	26	32	24.5	31
7	30	36	26	32	24.5	31
8	30	36	26	32	24.5	31
9	30	36	26	32	24.5	31
10	30	33	26	32	24.5	31
11	29	32	26	31	24.5	31

**P/N:** RF-5100

**FCC ID:** 2AG3J-RF5100

**IC ID:** IC ID: 20968-RF5100

**Antenna Type and Gain (dBi):** Omnidirectional / 3.5 dBi

## USA

Freq (MHz)	Channel (WLAN)	Channel Width (MHz)	SISO Max. Power Setting Approved (dBm)	2x2 Max. Power Setting Approved (dBm)	3x3 Max. Power Setting Approved (dBm)	Max. EIRP Approved (dBm)
5180	36	20	17.0	14.0	11.5	21
5200	44	20	17.0	14.0	11.5	21
5240	48	20	17.0	14.0	12.0	21
5745	149	20	29.5	26.5	24	36
5787	157	20	29.5	26.5	24	36
5825	165	20	29.5	26.5	24	36

## Canada

SISO Max. Power Approved (dBm)	2x2 Max. Power Approved (dBm)	3x3 Max. Power Approved (dBm)	Max. EIRP Approved (dBm)
n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a
29.5	26.5	24	36
29.5	26.5	24	36
29.5	26.5	24	36

## PROFESSIONAL INSTALLER – COMPLIANCE

Operations outside of the FCC grant will require special licensing.

### Approved Antennas:

*The radio transmitters listed in the table below have been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.*

Part Number	FCC ID	IC ID	Antenna Type	Max. Gain Approved (dBi)
RF-2100	2AG3J-RF2100	20968-RF2100	Omni	7.4
RF-5100	2AG3J-RF5100	20968-RF5100	Omni	3.5

**EIRP** (Isotropic Radiated Power) = Power Setting + Antenna Gain - Cable Loss

National regulations may require that operations may be limited to portions of the frequency range shown in the channel selection page of the interface.



Minimum Safe Distance (MSD)			
	Antenna Gain (dBi)	*Occupational Exposure Distance (cm)	Non Occupational Exposure Distance (cm)
<b>Dipole (Omnidirectional)</b>	2.1	7.0	20.0
	3.5	7.0	20.0
	4.0	8.0	20.0
	7.4	**11.0	**25

In addressing the MSD for operation of the RF-2100 S-Band (2200 MHz – 2500 MHz) radio module with **FCC ID 2AG3J-RF2100** and **IC ID 20968-RF2100** and the RF-5100 Upper C-Band (5100 MHz – 6000 MHz) radio module with **FCC ID 2AG3J-RF5100** and **IC ID 20968-RF5100**, the applicable Maximum Permissible Exposure (MPE) limits were obtained IAW the FCC rules for radio frequency radiation exposure limits under **FCC Title 47, Chapter 1 Subpart 1 Article 1.1310** and **Industrial Canada RSS-102, Section 2.6**.

En abordant la MSD pour le fonctionnement des RF-2100 S-Band (2200 MHz - 2500 MHz) module radio avec **FCC ID 2AG3J-RF2100** et **IC ID 20968-RF2100** et RF-5100 Upper C-Band (5100 MHz – 6000 MHz) avec **FCC ID 2AG3J-RF5100** et **IC ID 20968-RF5100**, l'exposition maximale admissible applicable (MPE) limites ont été obtenus conformément à la FCC règles pour les limites d'exposition aux radiations de fréquences radio sous **FCC Titre 47, Chapitre 1 partie 1 article 1,1310** et **industriel Canada RSS-102, Section 2.6**.

For compliance information, contact Persistent Systems' Quality Management Department.  
 Pour plus d'informations de conformité, le service de qualité contact Persistent Systems.  
 (212)-561-5895  
 support@persistentsystems.com

### Notes:

\*Occupational/controlled exposure limits apply in situations in which persons are exposed as a consequence of their employment provided those persons are fully aware of the potential for exposure and can exercise control over their exposure. Limits for occupational/controlled exposure also apply in situations when a person is transient through a location where occupational/controlled limits apply provided he or she is made aware of the potential for exposure. The phrase *fully aware* in the context of applying these exposure limits means that an exposed person has received written and/or verbal information fully explaining the potential for RF exposure resulting from his or her employment. With the exception of *transient* persons, this phrase also means that an exposed person has received appropriate training regarding work practices relating to controlling or mitigating his or her exposure. Such training is not required for *transient* persons, but they must receive written and/or verbal information and notification (for example, using signs) concerning their exposure potential and appropriate means available to mitigate their exposure. The phrase *exercise control* means that an exposed person is allowed to and knows how to reduce or avoid exposure by administrative or engineering controls and work practices, such as use of personal protective equipment or time averaging of exposure.

\*\* Cable loss is the minimum cable loss that may exist between the antenna port and the 7.4dBi antenna. 0.50dB cable loss was taken into consideration when calculating minimum distance.

# PROFESSIONAL INSTALLER – COMPLIANCE

**Country:** Japan (Government)

**Mode of Operation:** MIMO 3x3

**Antenna Types and Gain (dBi)**

**Antenna 1:** Omnidirectional / 3.5 dBi

**Antenna 2:** Blade / 9 dBi

**Antenna 3:** Patch 4x4 / 13 dBi

**Japan Power Limits**

Channel (MHz)	Channel Width (MHz)	Antenna 1		Antenna 2		Antenna 3	
		Max. Power Approved (dBm)	Max. EIRP Approved (dBm)	Max. Power Approved (dBm)	Max. EIRP Approved (dBm)	Max. Power Approved (dBm)	Max. EIRP Approved (dBm)
5660	20	25.2	36	22.2	36	18.2	36
5655	10	25.2	36	22.2	36	18.2	36
5665	10	25.2	36	22.2	36	18.2	36
5675	10	25.2	36	22.2	36	18.2	36
5680	20	25.2	36	22.2	36	18.2	36
5685	10	25.2	36	22.2	36	18.2	36
5695	10	25.2	36	22.2	36	18.2	36
5700	20	25.2	36	22.2	36	18.2	36
5705	10	25.2	36	22.2	36	18.2	36
5715	10	25.2	36	22.2	36	18.2	36
5720	20	25.2	36	22.2	36	18.2	36
5725	10	25.2	36	22.2	36	18.2	36
5740	10	25.2	36	22.2	36	18.2	36
5745	20	25.2	36	22.2	36	18.2	36
5750	10	25.2	36	22.2	36	18.2	36

## BAT-06 Technical Datasheet

Rechargeable, Lithium-Ion Battery

### Features

- Communicates using a Single Wire DQ interface.
- UN/DOT 38.3 Rating: 73Wh
- Comparable to: BT-70716BE

### Typical Applications

- Wave Relay System
- AN/PRC-148
- TRC-9110

### Recommended Charging Platforms

Charger Part Number	Required Adapter Part Number
BTC-70801	BTA-70810
BTC-70844	BTA-70810
BTC-70819, -1, -3	BTA-70810
BTC-70836	BTA-70830, BTA-70830-1
BTC-70870, -1, -3	BTA-70830, BTA-70830-2
BTC-70824-1	BTA-70810S
BTC-70663	BTA-70810S
BTC-70716-1	Not Required

**Technical Specifications**

<b>National Stock Number</b>	Pending
<b>BT Part Number</b>	BT-70716BG
<b>Dimensions</b>	Length: 2.8 in. (71 mm) Width: 1.6 in. (41 mm) Height: 3.4 in. (86 mm)
<b>Weight</b>	0.75 lbs (0.34 kg)
<b>Nominal Voltage</b>	10.8V
<b>Maximum Voltage</b>	12.6V
<b>Capacity</b>	6.4Ah
<b>Discharge</b>	6A Max Continuous
<b>Pulse Discharge</b>	40A ≤ 1 ms
<b>Operating Temperature</b>	-30°C to +60°C (-22°F to +140°F)
<b>Recommended Storage Temperature</b>	-40°C to +40°C (-40°F to +104°F)
<b>Connector</b>	Flat Contacts (bottom), Fly Wheel Connection (top)
<b>State of Charge Indicator</b>	Not Applicable
<b>Disposal</b>	Check local regulations (Contains 0% Mercury or Cadmium)



**MATERIAL SAFETY DATA SHEET**

**From:** Bren-Tronics Inc.  
10 Brayton Court  
Commack, N.Y. 11725

**Telephone:** 631-499-5155  
**Fax:** 631-499-5504  
**www.bren-tronics.com**

**Emergency Telephone:** If no answer above, contact Chem-Tel Corporation at 1-800-255-3924 or 1-813-248-0585

Effective Date: 01 Jan 2013

**BT-70716BE** (BT-70716BE-PS, BT-70716BE-TB, BT70716BE-TG,  
BT-70716BE-TT, BT-70716BG)

**1. Product Identification**

**Product Name:** Lithium-Ion Battery  
**Chemical System:** Lithium-Ion (Carbon/Lithiated Metal Oxide)  
**NSN:** n/a  
**Nominal Weight:** 0.380kg (0.84 lbs)  
**Nominal Voltage:** 10.8V

## 2. Composition/Information on Ingredients

Although the chemical composition of the various cell manufacturers is proprietary, the following is typical of the chemistry.

Hazardous Components (Specific Chemical Identity, Common Name(s))	%	CAS Number	LD <sub>50</sub> (mg/kg) (oral-rat)	LC (mg/L)
Aluminum foil	0.1-1 w/w	7429-90-5	N/AV	A/AV
Biphenyl (BP)	0 -0.3 w/w	92-52-4	2400	N/AV
Copper foil	0.1 -0.3 w/w	7440-50-8	3.5(ipr-mouse)	N/AV
Dioxathiolane 2,2-Dioxide (DTD)	0 -3 w/w	1072-53-3	1600	N/AV
Linear and Cyclic Carbonic Solvents (See other information)	5 -17 w/w	N/APP	≈11000 (weighted avg)	N/AV
Graphite Powder	10-30 w/w	7440-44-0	440 (ivr-mouse)	N/AV
Lithium Carbonate	0 -0.3 w/w	554-13-2	525	N/APP
Lithium cobaltite (LiCoO <sub>2</sub> )	01-3- w/w	12190-79-3	N/AV	N/AV
Lithium hexafluorophosphate (LiPF <sub>6</sub> )	1-5 w/w	21324-40-3	1702	Rat: >20
Poly (vinylidene fluoride) (PVDF)	0.1 -1 w/w	24937-79-9	N/AV	N/AV
Propane Sulfone (PS)	0-3 w/w	1120-71-4	100	N/AV
Steel, nickel and inert polymer	Balance	N/APP	N/APP	N/APP

These chemicals and metals are contained in a sealed can.

### 3. Hazards Identification

#### Routes of Entry:

Inhalation? Not anticipated. Respiratory (and eye) irritation may occur if fumes are released due to heat or an abundance of leaking batteries.

Skin? Yes

Ingestion? Yes

#### Potential Health Effects:

These chemicals are contained in a sealed can. Risk of exposure occurs only if the battery is mechanically or electrically abused. The most likely risk is acute exposure when a cell vents. Propylene Carbonate is mildly irritating upon eye and skin contact. Contact of electrolyte and extruded lithium with skin and eyes should be avoided. Inhalation or ingestion of lithium trifluoromethane sulfonate may be harmful.

#### Signs/Symptoms of Exposure:

Skin and eye irritation may occur following exposure to a leaking battery.

#### Medical Conditions Generally Aggravated by Exposure:

An acute exposure will not generally aggravate any medical condition.

### 4. First Aid Measures

#### Emergency & First Aid Procedures:

If battery is leaking and material contacts eyes, flush with copious amounts of clear, tepid water for thirty (30) minutes, exposed skin for at least fifteen (15) minutes. Contact Physician at once. Leaking contents may be irritating to respiratory passages. Remove to fresh air. Contact physician if irritation persists. If ingested, rinse mouth and surrounding area with clear, tepid water for at least fifteen (15) minutes. Consult physician immediately for treatment and to rule out involvement of the esophagus and other tissues.



## 5. Fire Fighting Measures

### **Extinguishing Media:**

Water spray, Carbon Dioxide, dry chemical powder or appropriate foam. Use agent appropriate for surrounding materials.

### **Special Fire Fighting Procedures:**

In burning, wear self-contained breathing apparatus and protective clothing to prevent contact with skin and eyes.

### **Unusual Fire and Explosion Hazards:**

Organic components will burn if cell incinerated. Combustion of cell contents will cause evolution of extremely corrosive Hydrogen Fluoride gas.

## 6. Accidental Release Measures

### **Ventilation:**

None under normal use conditions.

### **Protective Gloves:**

None under normal use conditions. Use butyl gloves when handling leaking batteries.

### **Eye Protection:**

None under normal use conditions. Wear safety glasses when handling leaking batteries.

## 7. Handling and Storage

### **Precautions to be Taken in Handling and Storage:**

For best service life: store batteries in a cool (below 70° F, 21°C) dry area that is subject to little temperature changes; do not place near heating equipment, nor exposed to direct sunlight for long periods. Elevated temperatures can result in reduced battery service life.

### **Other Precautions:**

Do not disassemble battery or battery pack. Do not puncture, crush or dispose of in fire.

## 8. Exposure Controls/Personal Protection

### **Steps to be Taken in Case Material is Released or Spilled:**

Notify safety personnel of large spills. Evacuate the area and allow vapors to dissipate. Increase ventilation. Avoid eye or skin contact. **DO NOT** inhale vapors. Clean up personnel should wear appropriate protective gear. Remove spilled liquid with absorbent and contain for disposal.

Transport containers outdoors. Hold burned cells and fire cleanup solids for disposal as potential hazardous waste. Unburned cells are not hazardous waste. A fire with over 100 kg of burned cells will likely require reporting to environmental offices. Always consult and obey all international, federal and local environmental laws.

## 9. Physical and Chemical Properties

### **Appearance:**

Rectangular box shape

## 10. Stability and Reactivity

### Stability:

Stable

### Conditions to Avoid:

Do not heat, crush, disassemble, short-circuit or recharge.

### Hazardous Decomposition or By-products:

Thermal degradation may produce hazardous fumes of manganese and lithium, hydrofluoric acid, oxides of carbon and sulfur and other toxic by-products.

### Hazardous Polymerization:

Will not occur.

### Incompatible Materials:

Contents incompatible with strong oxidizing agents.

## 11. Toxicological Information

<b>Carcinogenicity:</b>	<b>NTP?</b>	<b>IARC Monograph?</b>	<b>OSHA Regulated?</b>
	No	No	No

## 12. Ecological Information

N/A

## 13. Disposal Considerations

- Batteries must be completely discharged prior to disposal and/or the terminals must be taped or capped to prevent short circuit.
- Disposal of large quantities of batteries containing lithium cells may be subject to Federal, State or local regulations.

**14. Transportation Information:** This lithium-ion battery is regulated as a Class 9 Misc hazardous material (dangerous goods). The UN number for the US is UN 3090; International is UN 3480. Equivalent Lithium Content, (ELC), per battery is 6.12g max. The Watt-hour rating is 73 Wh max. The battery and component cells conform to the requirements of Section 38.3 of the UN Manual of Tests and Criteria, (T1-T8 tests). The battery must be packaged and shipped according to the following regulations starting on January 1, 2013):

**Domestic Transportation within the U.S. - All Modes: See 49 CFR Section 173.185; Special Provision 188:**

Battery is "excepted" from Class 9 Hazardous Materials Regulations because it contains less than 8g ELC.

Battery must be packaged in a manner TO PREVENT SHORT CIRCUITS and in a strong outer package.

For quantities of 13 or more in one package, 1) mark "LITHIUM-ION BATTERIES INSIDE" on the package and that special procedures should be followed if package is damaged; (or IATA label shown below); 2) Accompany with a document indicating same information; 3) Package must be capable of being dropped 1.2 meters in any orientation without damage to cells or batteries contained in the package, without shifting of the contents that would allow short circuiting, and without release of package contents; 4) The maximum gross weight of the package may not exceed 30 kg (66lbs). *Note: these requirements will reflect Int'l regs below later in 2013. However, some U.S. carriers may require compliance now.*

**International Transportation – All Modes: IMDG Code, ADR, ICAO Technical Instructions, IATA Dangerous Goods Regulations:**

**IMDG Code and ADR, Special Provision 188:** Battery is "excepted" from Class 9 Dangerous Goods Regulations because it has a rating of less than 100 Wh. Battery must be packaged in a manner TO PREVENT SHORT CIRCUITS.

Battery must be packed in inner packagings that completely enclose the battery, then placed in a strong outer package capable of withstanding a 1.2m drop test in any orientation without damage to the batteries, shifting of contents to allow battery to battery contact or release of contents. Package must carry label similar to the IATA lithium battery handling label shown below. Package must be accompanied with a document such as an air waybill with an indication that the package contains lithium-ion batteries, must be handled with care, that a flammability hazard exists if the package is damaged, special procedures should be followed in the event the package is damaged, to include inspection and repacking if necessary, and a telephone number for additional information. Package may not exceed 30 kg (66 lbs) gross weight.

**IATA Dangerous Goods Regulations / ICAO Technical Instructions: Packing Instruction 965, Section II.**

No more than 2 batteries per package. Packaging and documentation requirements are same as shown above for IMDG and ADR. IATA and ICAO specifically require lithium ion battery handling label shown below. No package weight limit.

**IATA Dangerous Goods Regulations / ICAO Technical Instructions: Packing Instruction 965, Section IB.**

More than 2 batteries per package. Packaging and documentation requirements are same as shown above for IMDG Code and ADR *and* package must carry Class 9 label and lithium battery handling label shown below. In addition, shipment must be offered to airline as fully-regulated Class 9 dangerous goods, accompanied with shipper's declaration for dangerous goods (or alternative document with similar entries) and employees must have dangerous goods training. Package may not exceed 10 kg (22 lbs) gross weight.



- Label dimensions: 120 x 110 mm (4.75" x 4.35") or 74 X 105 mm (2.9" x 4.13") if package cannot accommodate larger label
- Border color: Red on a contrasting background
- Pictogram colors: Glass, batteries, and flame can be black
- Label also can be used to comply with 49 CFR and IMDG Code

**15. Regulatory Information**

Batteries are considered to be "articles" and thus are exempt from TSCA regulation.

**16. Other Information**

Avoid mechanical or electrical abuse. **DO NOT** short circuit or install incorrectly. Batteries may explode, pyrolyze or vent if disassembled, crushed, recharged incorrectly or exposed to high temperatures. Install batteries in accordance with equipment instructions.

This information and recommendations set forth are made in good faith and believed to be accurate as of the date of preparation. Bren-Tronics Inc. makes no warranty, expressed or implied, regarding the accuracy of the data or the results to be obtained from the use thereof.

**MPU5**  
**BASIC OPERATOR MANUAL**  
**VERSION 2.5**



303 Fifth Avenue Suite 306  
New York, NY 10016

[www.persistentsystems.com](http://www.persistentsystems.com)