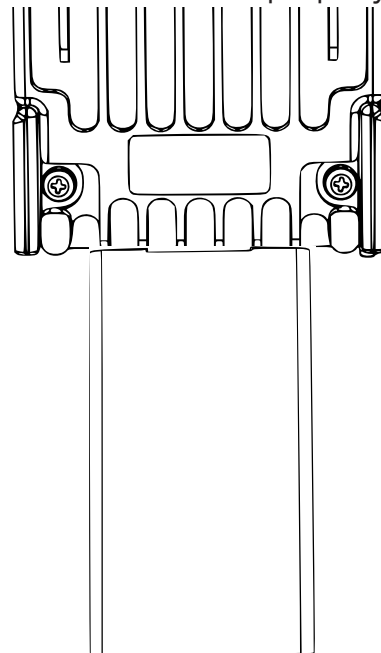
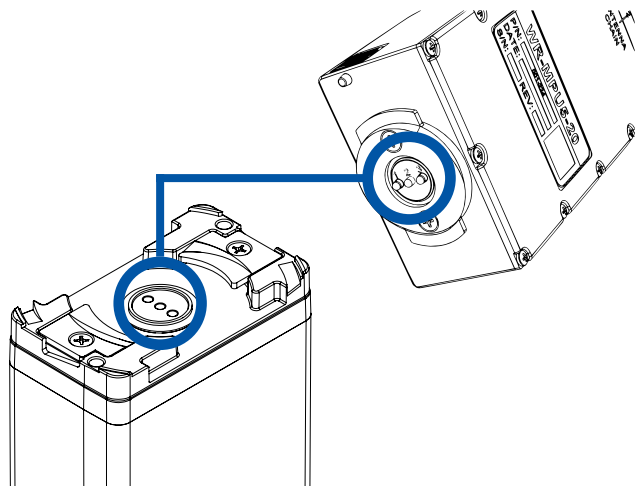
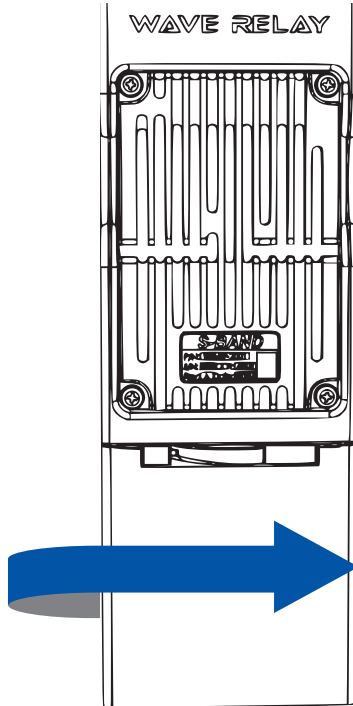


Connecting Power

- 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.



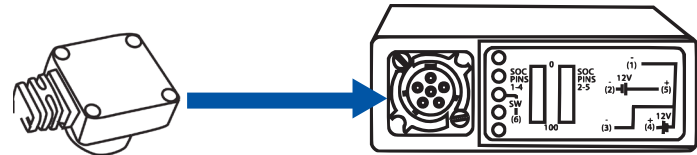
- 4** **Twist** clockwise 90°. You will hear a click when it is locked.



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

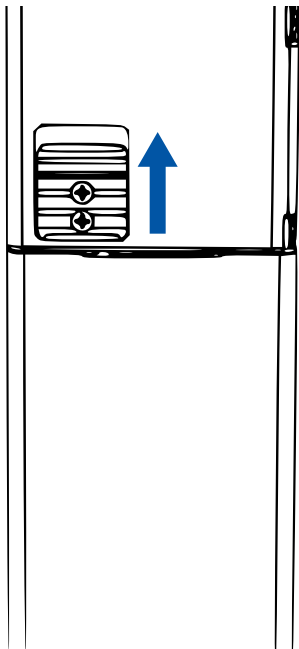


- 6** If you are using a BB Battery Eliminator, plug the **BB plug** into a **BB Battery**.

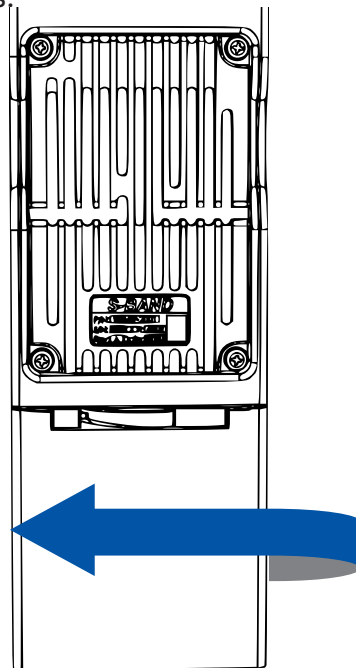


Removing Power

- 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?

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




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

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

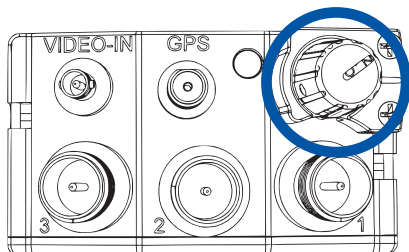
PHYSICAL SETUP: POWER

Powering On the Unit

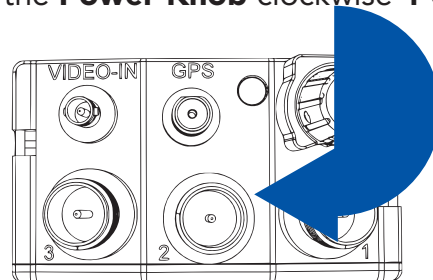
- 1 Ensure that **antennas**, a **radio module**, and an appropriate **power source** are connected.

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

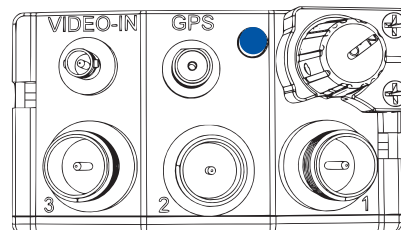
- 2 **Locate** the **Power Knob** on the top of the unit.



- 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

Blue Booting

Yellow Running, no neighbors

Green Running, neighbors

Red Crypto Fail (No key or FIPS)

Orange Low Battery

Purple 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

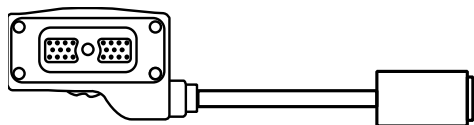


What Will I Learn?

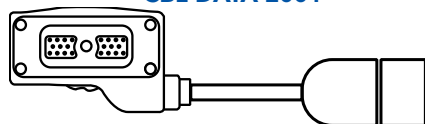
- ▶ How to connect a cable to the MPU5 side connectors



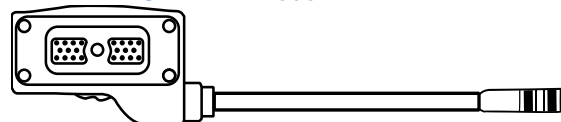
Parts List/Interchangeable Parts



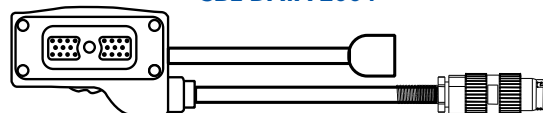
22-Pin to RJ45 Receptacle
CBL-DATA-2001



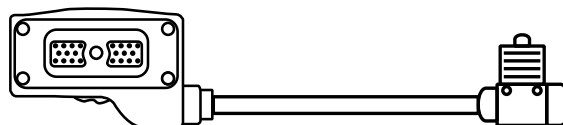
22-Pin to USB 2.0 Type A Receptacle
CBL-DATA-2003



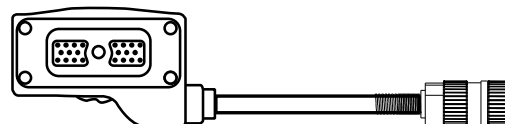
22-Pin to 6-Pin Push Pull USB Tether
CBL-DATA-2004



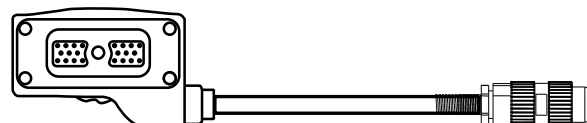
22-Pin to Audio and Video Out
CBL-DATA-3001



22-Pin to U94
CBL-AUD-0003



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



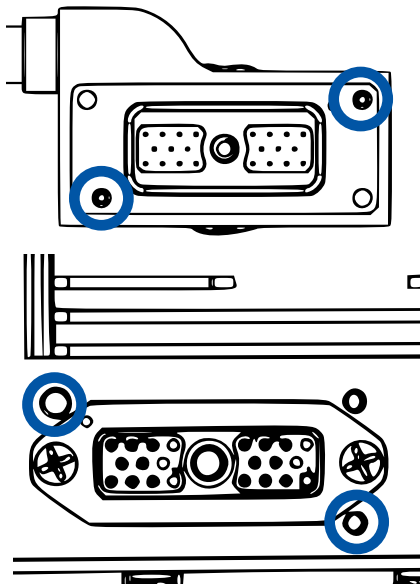
22-Pin to U-328
CBL-AUD-0002

Connecting a Cable to a Side Connector

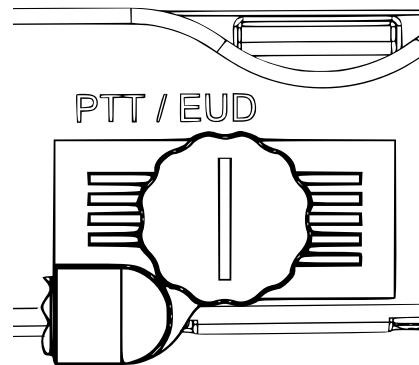
! **WARNING!:** Ensure that the unit is **POWERED OFF** before attaching a cable to a side connector.

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.

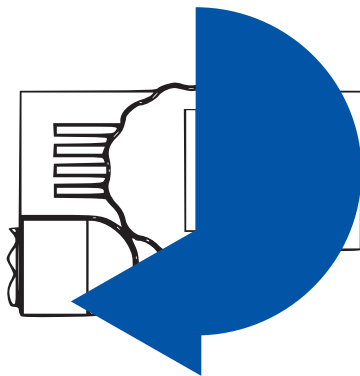
2 To connect a cable to a side connector, **locate** the appropriate side connector.



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



- 4** **Twist** the spin connector **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 spin connector and the side connector are bent or damaged.
- 4** Ensure that there are no foreign objects in the spin connector 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	This cable allows you to connect the MPU5 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	This cable allows you to connect USB accessories to the unit via a standard USB A port.
CBL-DATA-2004	22-Pin to 6-Pin Push Pull Android™ USB	PTT/EUD	This cable allows you to connect an Android™ EUD or Screen to the unit.
CBL-DATA-3001	22-Pin to Audio and Video Out	PTT/EUD	This cable allows you to connect the unit to a standard HDMI cable to display video on a TV or Monitor as well as connect the unit to a speaker box or headset.
CBL-AUD-0001	22-Pin to U-329	RoIP	This cable allows you to connect the unit to a PTT device with a U-329 connector.

CBL-AUD-0002	22-Pin to U-328	PTT/EUD	This cable allows you to connect the unit to a headset with a U-328 connector.
CBL-AUD-0003	22-Pin to U94	PTT/EUD	This cable allows you to connect the unit to a headset with a U94 connector.



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

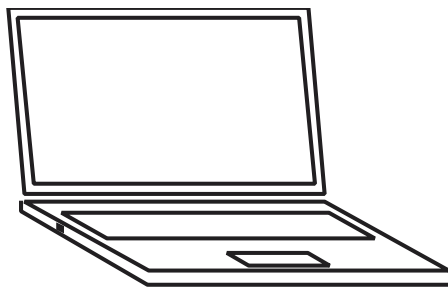


What Will I Learn?

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



Parts List/Interchangeable Parts



Management Computer with Administrator Access

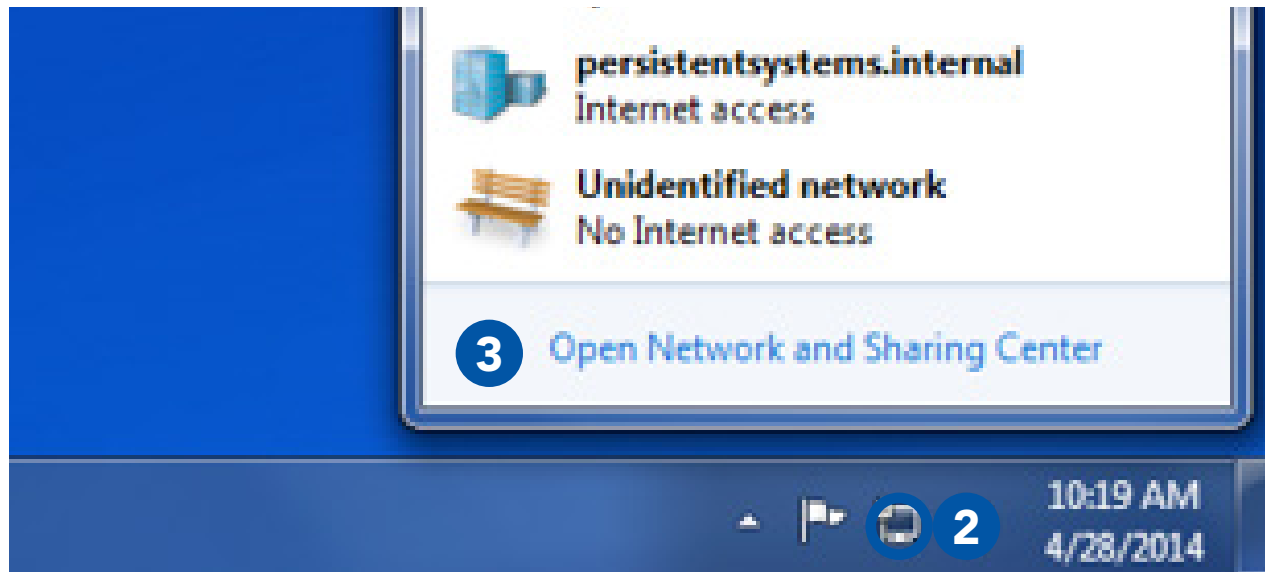


IMPORTANT INFORMATION!:

- ▶ 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**.

Control Panel Home





Change adapter settings

Change advanced sharing settings




View your basic network information and set up connections

 WEDLE-NY1 (This computer)
  Multiple networks
  Internet
 [See full map](#)

View your active networks [Connect or disconnect](#)

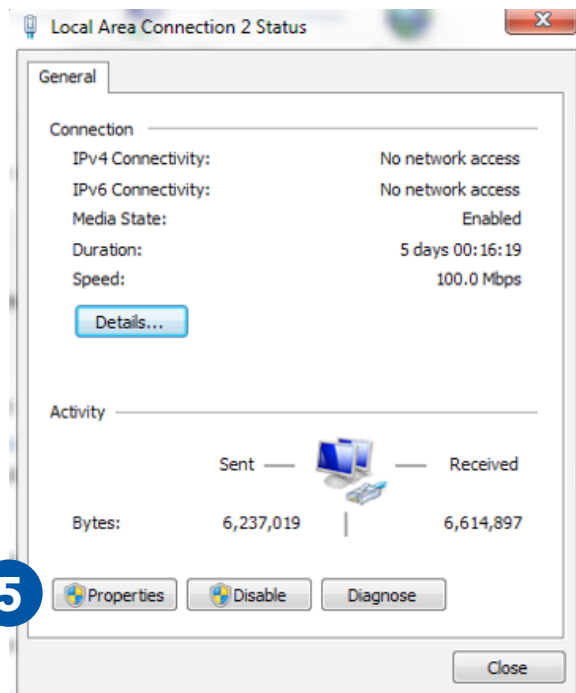
 persistentsystems.internal Domain network	Access type: Internet Connections:  Local Area Connection
 Unidentified network Public network	Access type: No Internet access Connections:  Local Area Connection 2

Change your networking settings

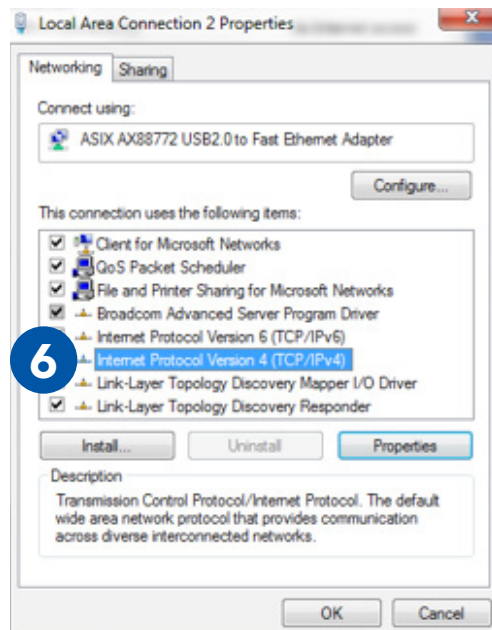
- 
[Set up a new connection or network](#)
 Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
- 
[Connect to a network](#)
 Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
- 
[Choose homegroup and sharing options](#)
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

4

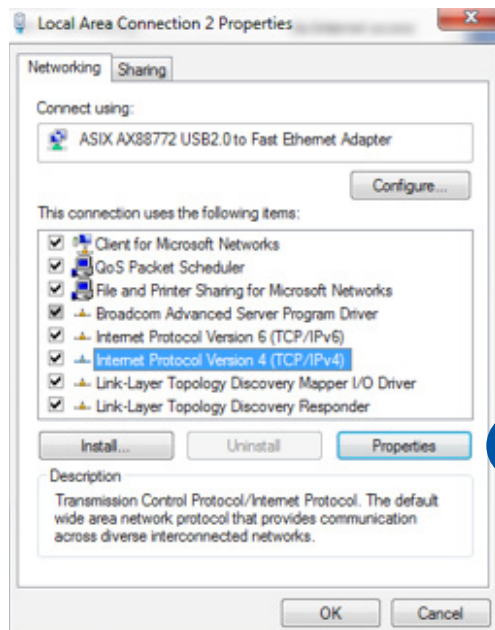
5 Click **Properties**.



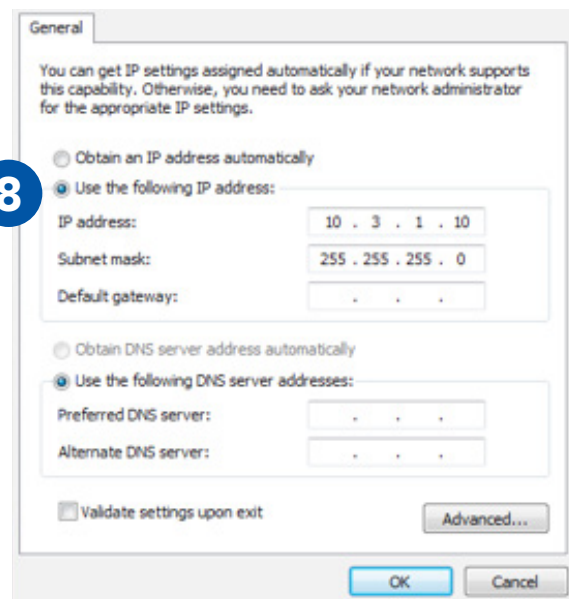
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and ensure that it is highlighted as pictured.



7 Click **Properties**.



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

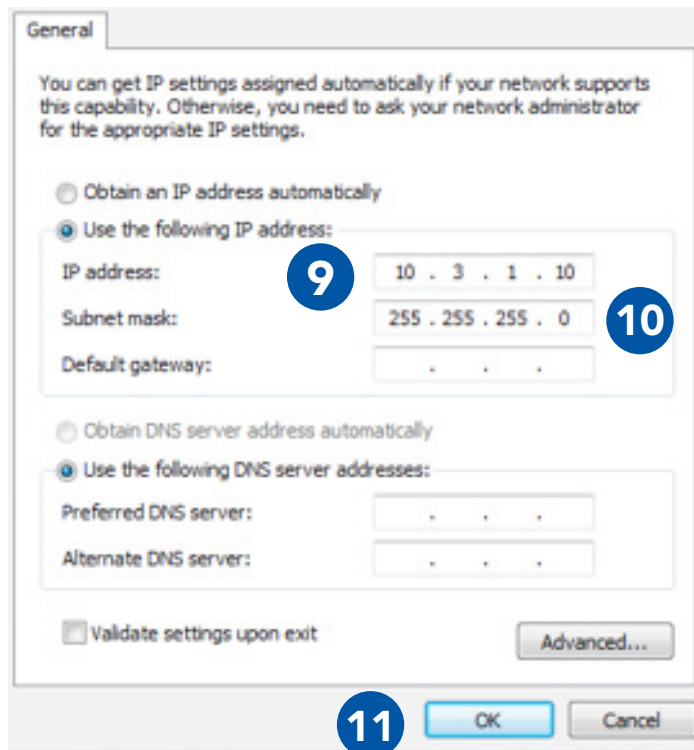


SOFTWARE SETUP: MANAGEMENT COMPUTER

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

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

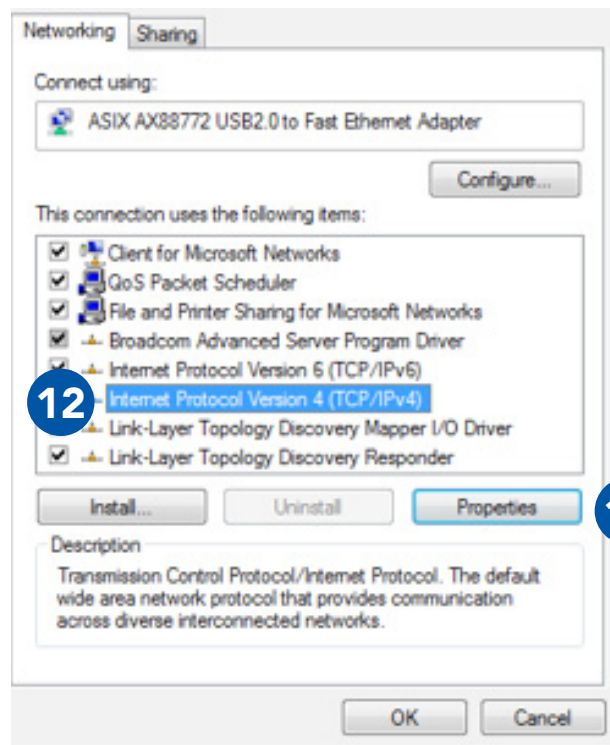
11 Click **OK**.



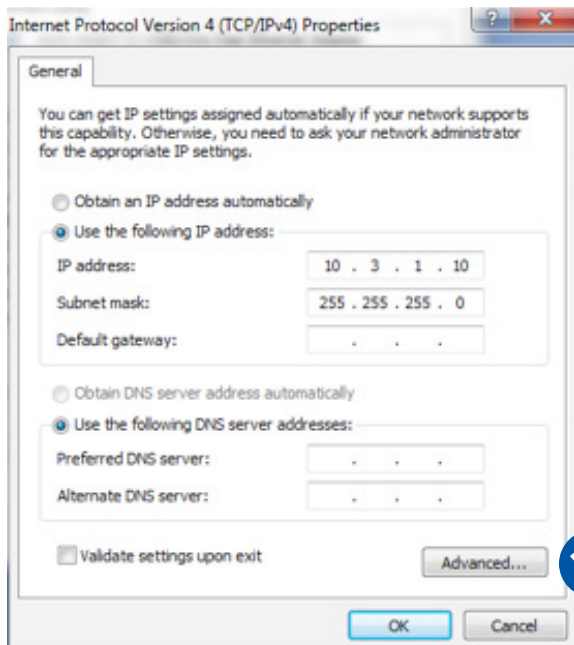
The screenshot shows a 'General' network configuration window. At the top, a text box explains that IP settings can be assigned automatically or manually. Below this, there are two radio button options: 'Obtain an IP address automatically' (unselected) and 'Use the following IP address:' (selected). Under the selected option, there are three input fields: 'IP address' (containing '10 . 3 . 1 . 10' with callout 9), 'Subnet mask' (containing '255 . 255 . 255 . 0' with callout 10), and 'Default gateway' (containing three dots). Below these, there are two more radio button options: 'Obtain DNS server address automatically' (unselected) and 'Use the following DNS server addresses:' (selected). Under the selected option, there are two input fields: 'Preferred DNS server' and 'Alternate DNS server', both containing three dots. At the bottom left, there is a checkbox for 'Validate settings upon exit' (unchecked). At the bottom right, there is an 'Advanced...' button. At the very bottom, there are 'OK' and 'Cancel' buttons, with callout 11 pointing to the 'OK' button.

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

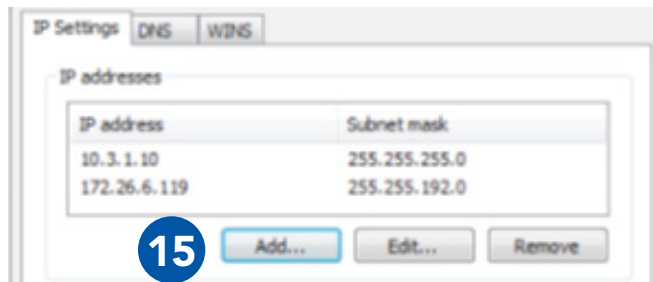
13 Click **Properties**.



14 Click **Advanced...**



15 Under **IP addresses**, click **Add...**

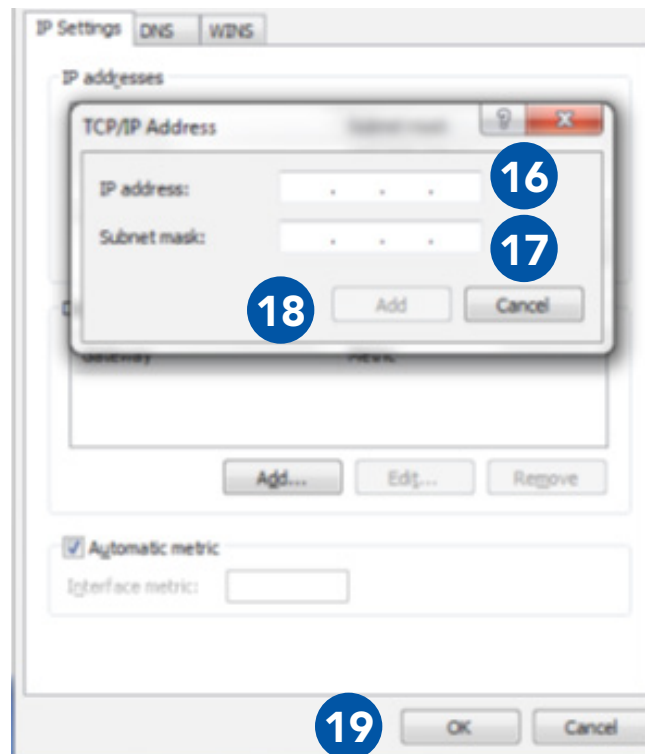


16 In the **IP address field**, enter **10.3.1.10**.

17 In the **Subnet mask field**, enter **255.255.255.0**

18 Click **Add**.

19 Click **OK**.



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`
- 4 **Type:**
`sudo ip addr add 10.3.2.10/24 dev eth0`

What Can I Do Now?

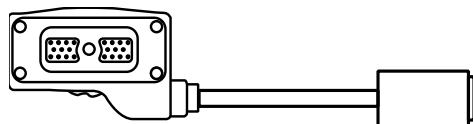
- ▶ Configure computers to be able to communicate with Wave Relay® devices.
- ▶ Have a computer that is able to configure a Wave Relay® device.

Connecting the MPU5 to the Management Computer

What Will I Learn?

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

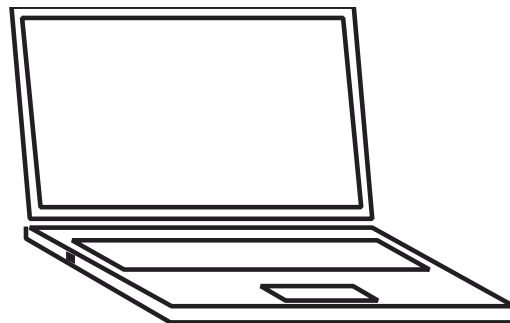
Parts List/Interchangeable Parts



22-Pin to RJ45 Receptacle
CBL-DATA-2001



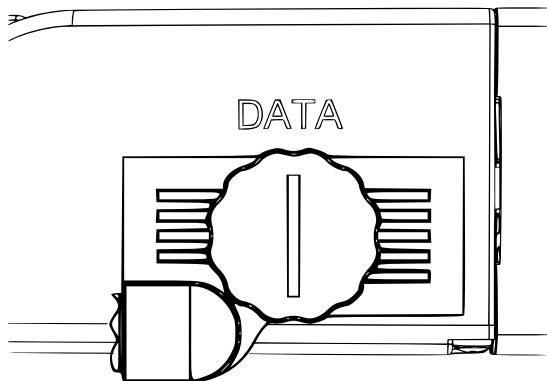
Standard RJ45 Ethernet Cable



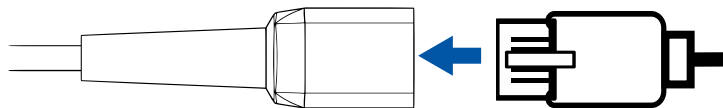
Properly Configured Management Computer

SOFTWARE SETUP: MANAGEMENT COMPUTER

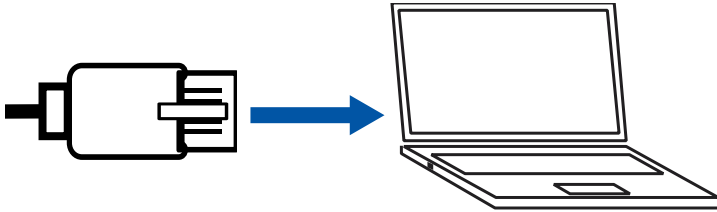
- 1 Connect **CBL-DATA-2001** to the **DATA** side connector on the MPU5.



- 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

Accessing the Web Management Interface



What Will I Learn?

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



Parts List/Interchangeable Parts



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



Management Computer with properly con-
figured IP address and subnet mask

SOFTWARE SETUP: WEB MANAGEMENT INTERFACE

- 1 Open the web browser



Microsoft Internet Explorer 7+



Google Chrome

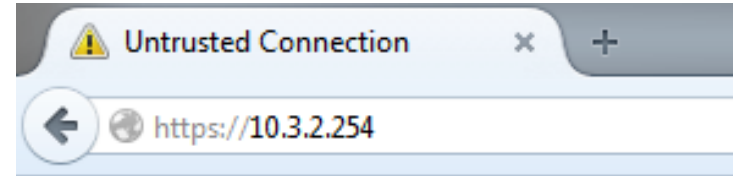


Mozilla Firefox 3+

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



Microsoft Internet Explorer 7+



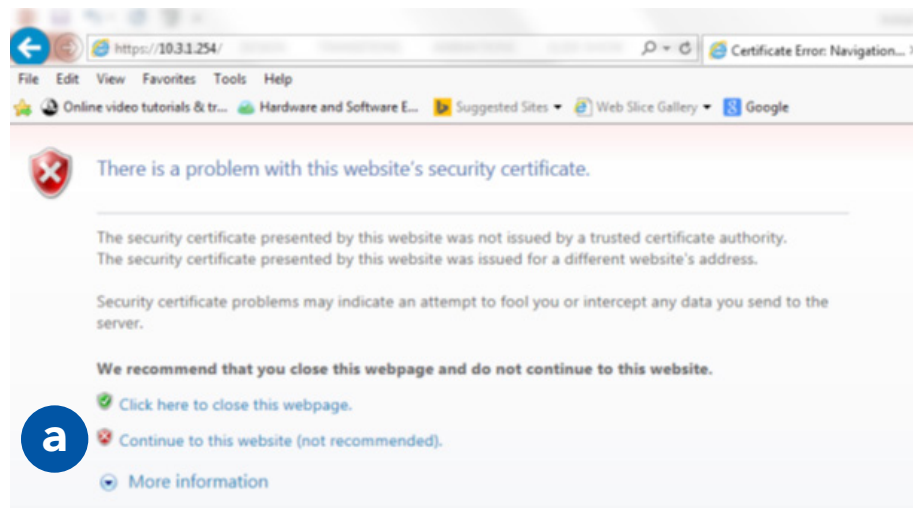
Mozilla Firefox 3+



Google Chrome

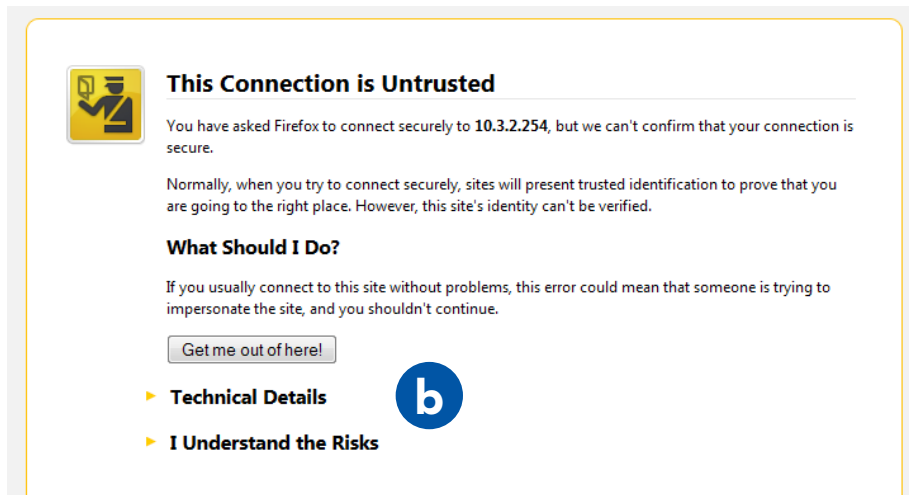
3 The web browser will ask you to accept a security certificate.

In Internet Explorer:



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

In Firefox:



The screenshot shows a Firefox warning dialog titled "This Connection is Untrusted". It features a yellow shield icon with a red 'X' and a lock. The text explains that the connection to 10.3.2.254 cannot be confirmed as secure. It provides a "What Should I Do?" section with a button "Get me out of here!". Below this are two options: "Technical Details" and "I Understand the Risks". A blue circle with a white 'b' is positioned to the right of the "I Understand the Risks" option.

This Connection is Untrusted

You have asked Firefox to connect securely to **10.3.2.254**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

 Click **I Understand the Risks**

SOFTWARE SETUP: WEB MANAGEMENT INTERFACE

▼ I Understand the Risks

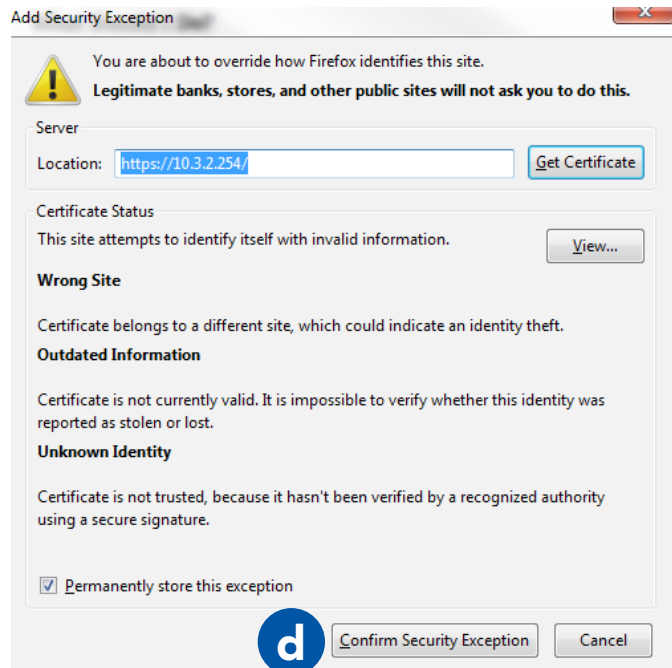
If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...



Click **Add Exception**



Click **Confirm Security Exception**

SOFTWARE SETUP: WEB MANAGEMENT INTERFACE

In Chrome:



Your connection is not private

Attackers might be trying to steal your information from **10.3.2.254** (for example, passwords, messages, or credit cards).



[Advanced](#)

[Back to safety](#)



Click **Advanced**

This server could not prove that it is **10.3.2.254**; 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.



[Proceed to 10.3.2.254 \(unsafe\)](#)

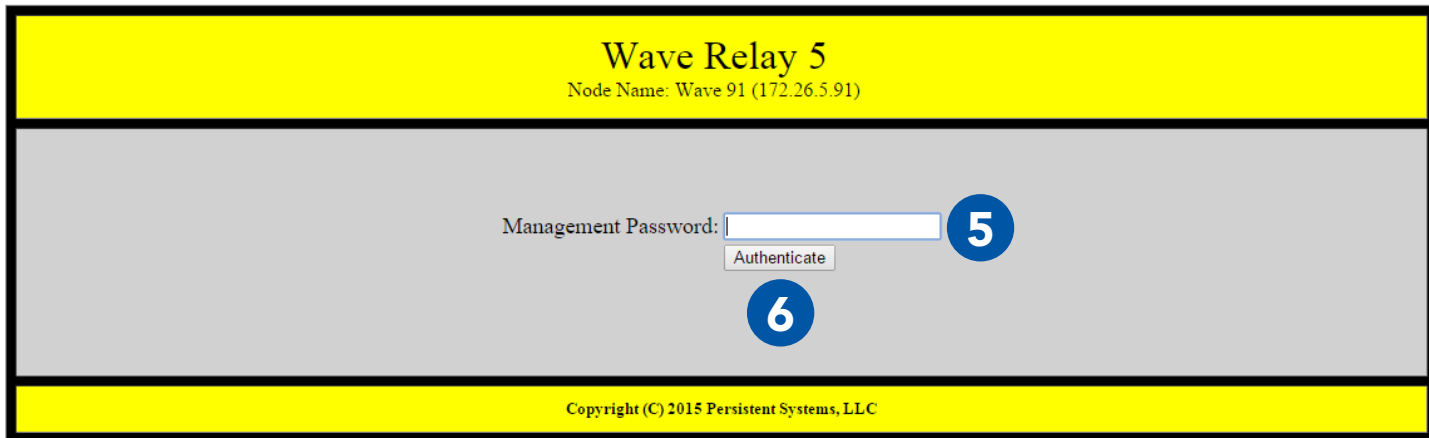
NET::ERR_CERT_AUTHORITY_INVALID



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 5
Node Name: Wave 91 (172.26.5.91)

Management Password: **5**

6

Copyright (C) 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.

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.

Wave Relay 5

Node Name: Wave 91 (172.26.5.91)

[Node Status](#)

[Node Configuration](#)

[Network Status](#)

[Network Configuration](#)

1 [Security](#)

Security

Status

Operational

Display Key

2 Set Key

Update:

Node

Crypto Mode: Recommended: 256-bit AES-CTR with HMAC-SHA-256 (Suite-B)

3

Enter key:

4

6 Set (in hex with optional whitespace between bytes)

Random key:

Generate



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



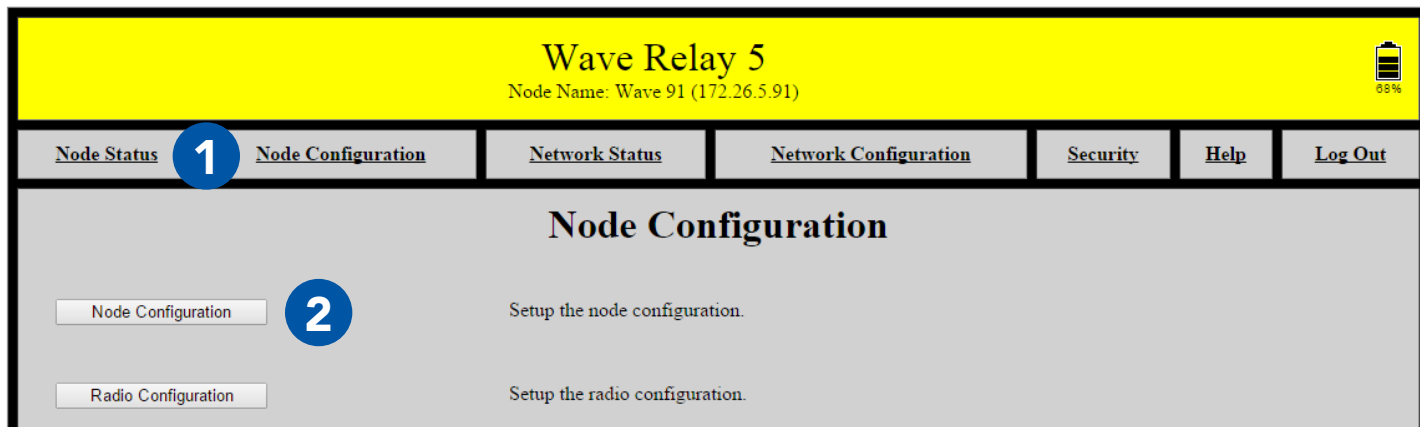
What Will I Learn?

- ▶ 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.



Wave Relay 5
Node Name: Wave 91 (172.26.5.91) 88%

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

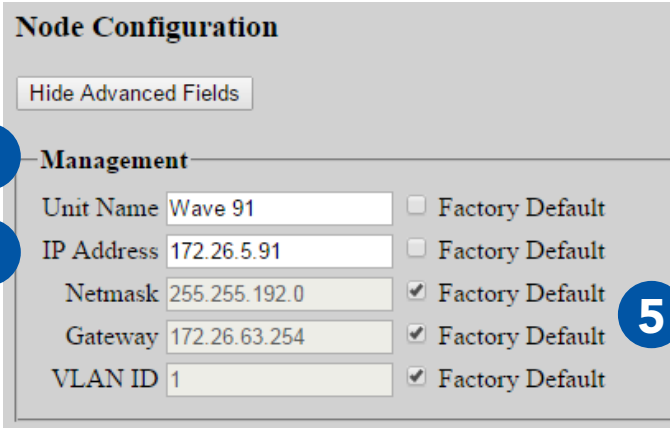
Node Configuration

2 Setup the node configuration.

Setup the radio configuration.

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	Wave 91	<input type="checkbox"/> Factory Default
IP Address	172.26.5.91	<input type="checkbox"/> Factory Default
Netmask	255.255.192.0	<input checked="" type="checkbox"/> Factory Default
Gateway	172.26.63.254	<input checked="" type="checkbox"/> Factory Default
VLAN ID	1	<input checked="" type="checkbox"/> Factory Default

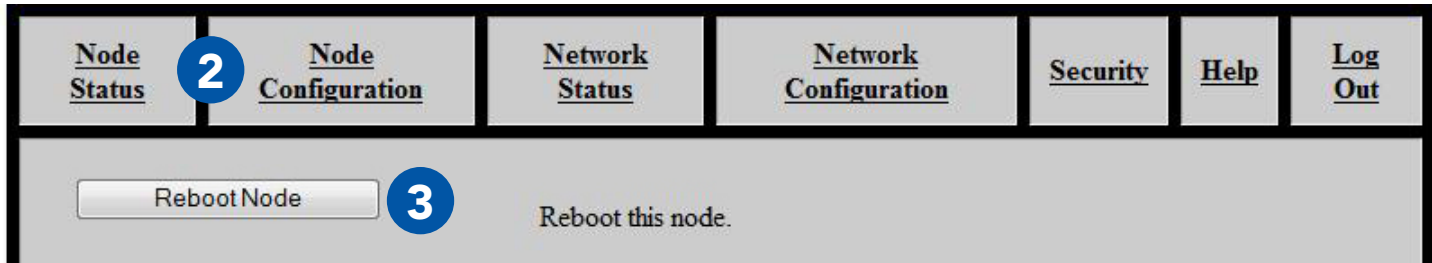
5

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.



Part III: Testing Connectivity

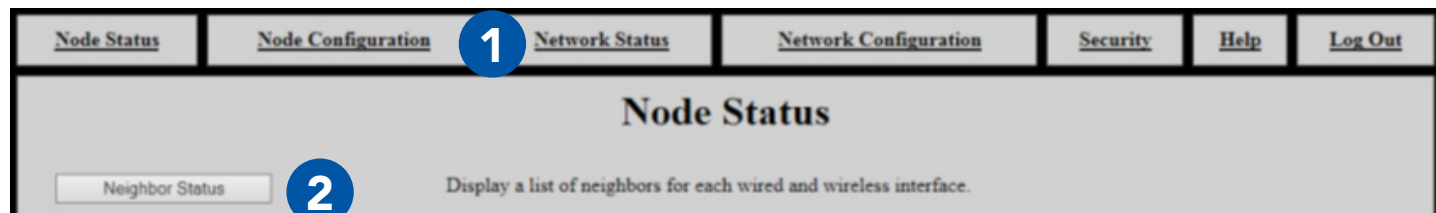
What Will I Learn?

- ▶ 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 (Receiver) (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.
- 4 **Check** or **uncheck** the **Upload only test** box. If this box is checked, only upload speed to the destination node will be tested.
- 5 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.
-  **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](#)

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

Network TCP Throughput Testing

3 **Destination:** **4** ☐ Upload only test

5 **Test Duration:** Seconds

6

TCP Throughput test to 172.26.5.68 for 5 seconds =

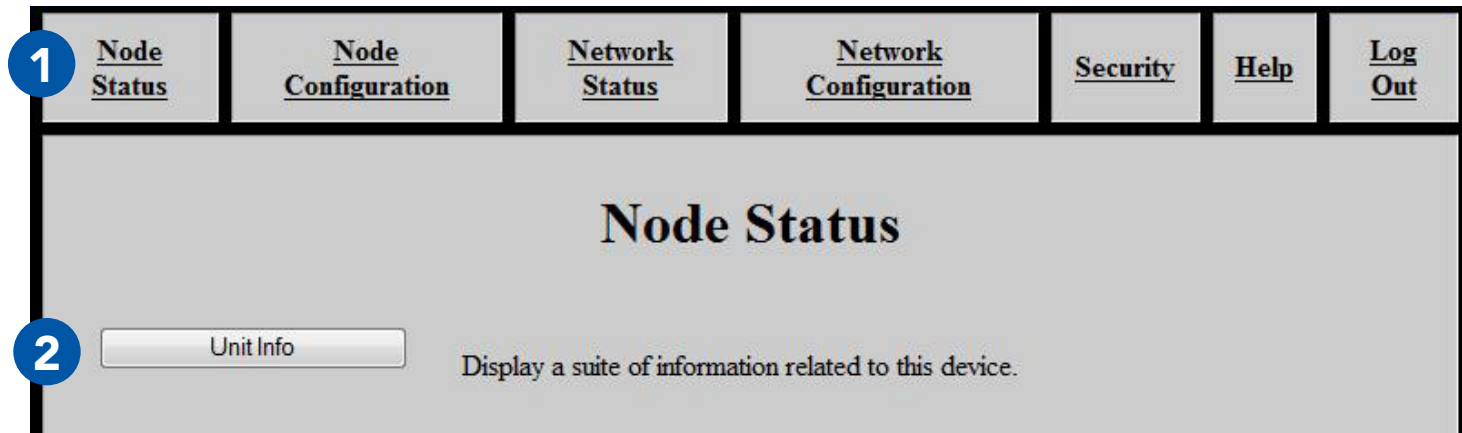
Upload	7	Download
20.0 Mbits/sec		21.3 Mbits/sec

Part IV: Using the Web Management Interface

View Individual Node Information

1 Click the **Node Status** tab.

2 Click the **Unit Info** button.



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

Firmware Version: 19-dev-20150612

Wave Relay Model: Wave Relay 5

Serial No.: 00016558

Uptime: 00:07:35

Temperature: Power Board: 34.250 C

Main Board CPU: 32.000 C

MIMO Radio Chain 1: 25.125 C

MIMO Radio Chain 2: 25.375 C

MIMO Radio Chain 3: 25.437 C

Input Power Voltage: Unavailable

Battery Status: 67% remaining

Battery Temperature: 20 < T < 30 degrees Celsius

Real Time Clock Battery: Unavailable

Current System Time: UTC Time: Sat Jan 3 15:33:27 GMT 1970

Warning: Unit does not save clock across reboots

Management HW MAC Address: 00:18:A6:00:40:AE

Radio 1 HW MAC Address: 00:18:A6:A0:00:09 (Persistent L-Band (1.3 GHz))

Ethernet 1 HW MAC Address: 00:18:A6:E0:00:5B

Refresh

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="Wave84"/>	<input type="checkbox"/> Factory Default
Frequency	<input type="text" value="1.360 GHz"/>	
Bandwidth	<input type="text" value="20Mhz"/>	
Max Link Distance	<input type="text" value="1.0 mi - 1.6 km"/>	
Channel Density	<input type="text" value="Medium"/>	
Radio Preference	<input type="text" value="Factory Default (None)"/>	
Max Transmit Power	<input type="text" value="5.0 dBm - 3 mW"/>	
Transmit Chain Select	<input type="text" value="Network Default (Auto)"/>	
Receive Chain Select	<input type="text" value="Network Default (Auto)"/>	

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

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: Adjust transmit power of the radio



WARNING!: User **MUST** refer to the **Professional Installer – Compliance** Section of this manual for approved power levels and approved channels

Transmit Chain Select: Choose which RF chains to use to transmit - you may select one, two, or three chains.


Receive Chain Select: Choose which RF chains to use to receive - you may select one, two, or three chains


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**.

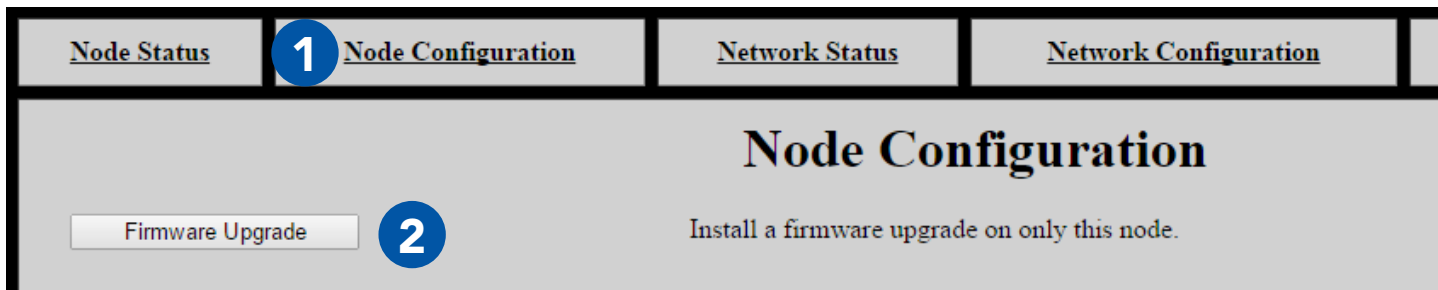
 **WARNING!:** A firmware upgrade will cause the node to be reconfigured, an operation that causes a period of downtime. Do not perform a firmware upgrade during mission critical operations that cannot tolerate such disruptions. Perform firmware upgrades only during scheduled maintenance or other appropriate 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® devices (MPU4, MPU3, QUAD).

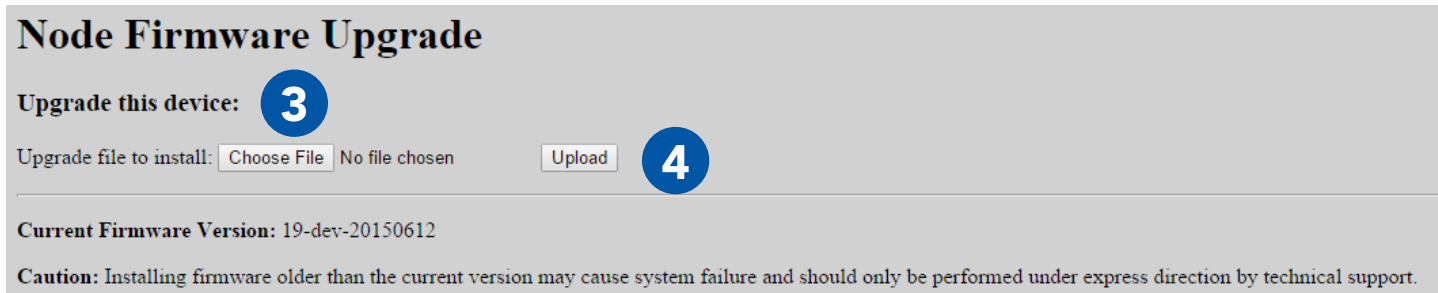
USING THE WEB MANAGEMENT INTERFACE: UPGRADING FIRMWARE



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

Node Configuration

Firmware Upgrade **2** Install a firmware upgrade on only this node.



Node Firmware Upgrade

Upgrade this device: **3**

Upgrade file to install: Choose File No file chosen Upload **4**

Current Firmware Version: 19-dev-20150612

Caution: Installing firmware older than the current version may cause system failure and should only be performed under express direction by technical support.

Creating a Configuration File

- 1 Click the **Node Configuration** tab.
 - 2 Click the **Config Management** button.
 - 3 Click the **Store** button.
 - 4 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.

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".

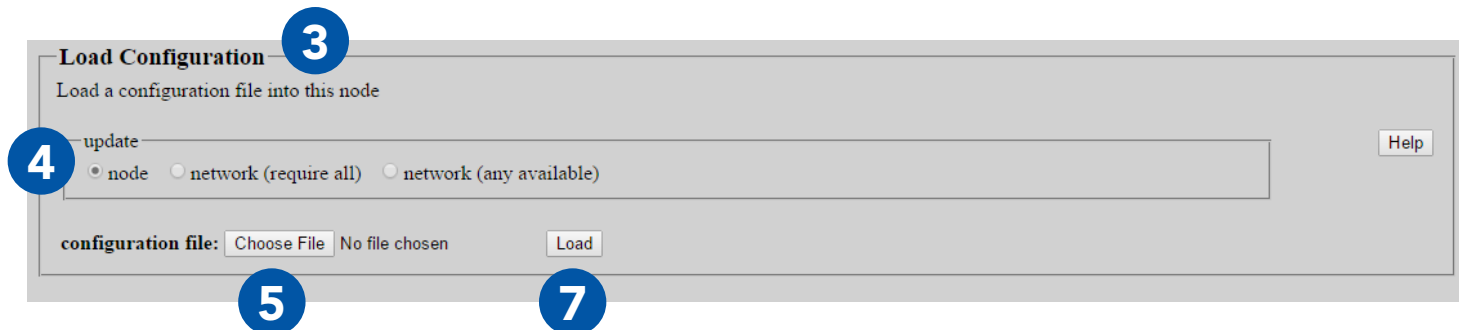
Store

3

Loading Settings from a Configuration File

- 1 Click the **Node Configuration** tab.
- 2 Click the **Config Management** button.
- 3 Scroll to the **Load Configuration** section.
- 4 In the **update** section, select **node**.
- 5 Click **Choose File**.
- 6 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.



The screenshot shows the 'Load Configuration' section of a web management interface. It includes a title bar with the text 'Load Configuration' and a subtitle 'Load a configuration file into this node'. Below this is an 'update' section with three radio button options: 'node', 'network (require all)', and 'network (any available)'. A 'Help' button is located to the right of these options. At the bottom, there is a 'configuration file:' label followed by a 'Choose File' button, the text 'No file chosen', and a 'Load' button. Numbered callouts are placed over the interface: '3' is over the title bar, '4' is over the 'node' radio button, '5' is over the 'Choose File' button, and '7' is over the 'Load' button.

USING THE WEB MANAGEMENT INTERFACE: RESET TO FACTORY CONFIG

Reset Node to Factory Configuration

- 1 Click the **Node Configuration** tab.
- 2 Click the **Config Management** button.
- 3 Check the **box** at the bottom of the page to retain the current Node Name and Management IP configuration after the reset. Otherwise, **all** custom configuration will be removed and the IP address will be reset to 10.4.1.254. The node's security key will **not** be zeroized.
- 4 When you are ready to remove all custom configuration and restore the node to factory settings, click the **Factory Reset** button.

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.)

☒ Keep current Node Name and Management IP configuration (IP, Netmask, Gateway)

Factory Reset

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 above sea level of the node

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

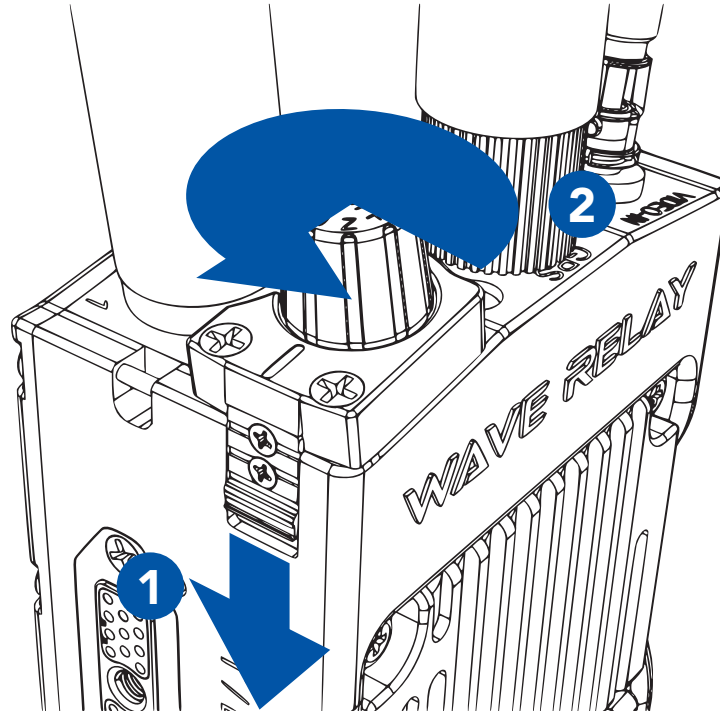
[Return to Menu](#)

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 past the home position.

DEVICE OPERATION: ZEROIZE THE SECURITY KEY

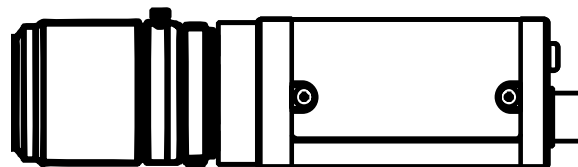


Connect a Camera to the MPU5

Parts List/Interchangeable Parts



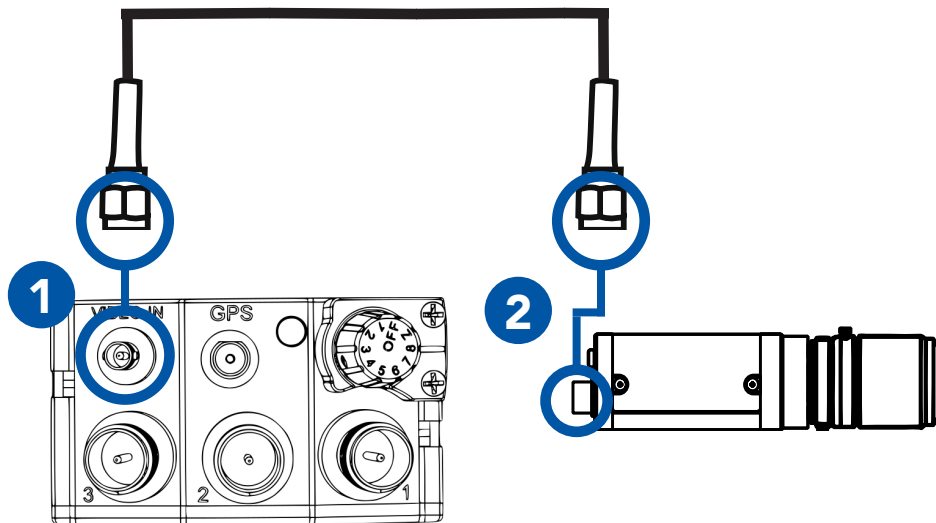
HD-BNC to BNC Cable (CBL-VID-2001)



Camera with BNC output

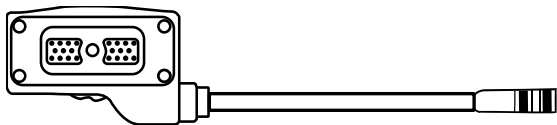
DEVICE OPERATION: CONNECTING A CAMERA

- 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.
- 3 Streaming video will be available on the network.



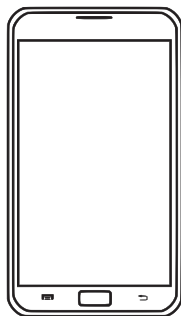
Connect an EUD or Handheld Display to the MPU5

Parts List/Interchangeable Parts



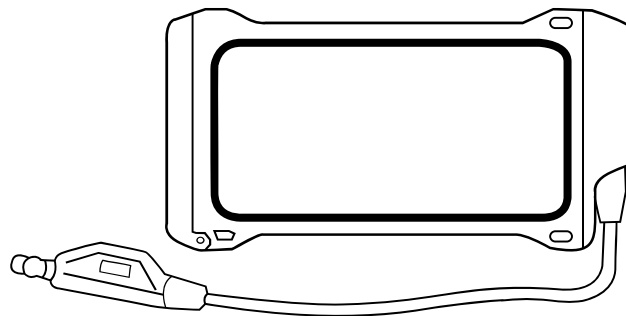
22-Pin to 6-Pin USB Push Pull Android™ Tether Cable

CBL-DATA-2004



Android™ EUD

ACC-EUD-0001

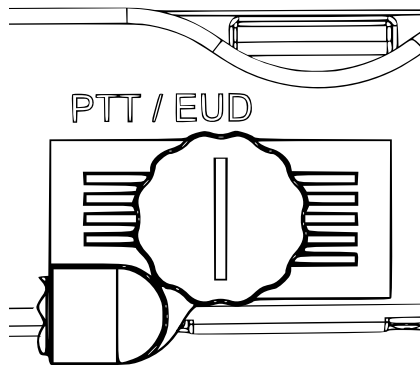


EUD IP67 Enclosure

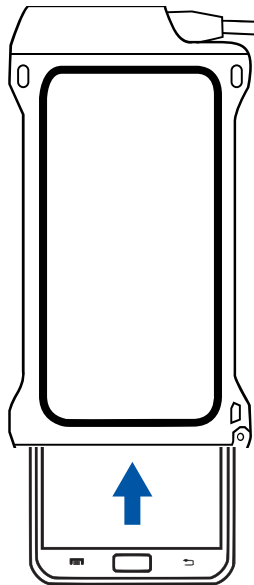
MOLLE-IP67-N3

DEVICE OPERATION: CONNECTING AN EUD OR HANDHELD DISPLAY

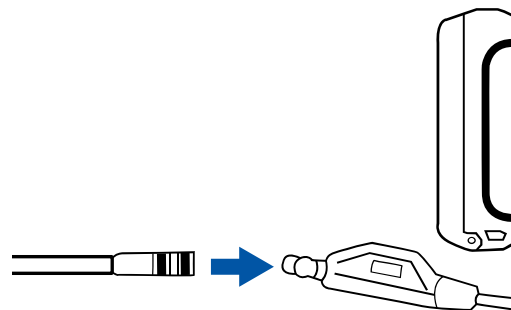
- 1** Connect **CBL-DATA-2004** to the **PTT/EUD** side connector on the MPU5.



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



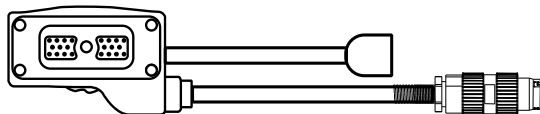
- 3** Connect the **6-Pin Push Pull connector** on the Juggernaut Case to the **6-Pin Push Pull connector** on **CBL-DATA-2004**.



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

Connect a Monitor or TV to the MPU5

Parts List/Interchangeable Parts



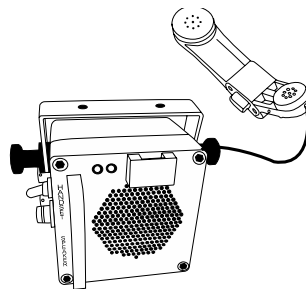
22-Pin to Audio and Video Out
CBL-DATA-3001



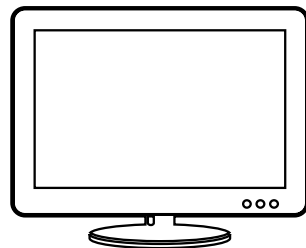
MyDP to HDMI
ACC-VID-1002



Standard HDMI Cable



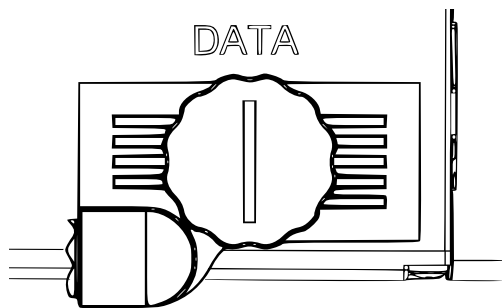
Speaker Box or Headset with U-328 Connector



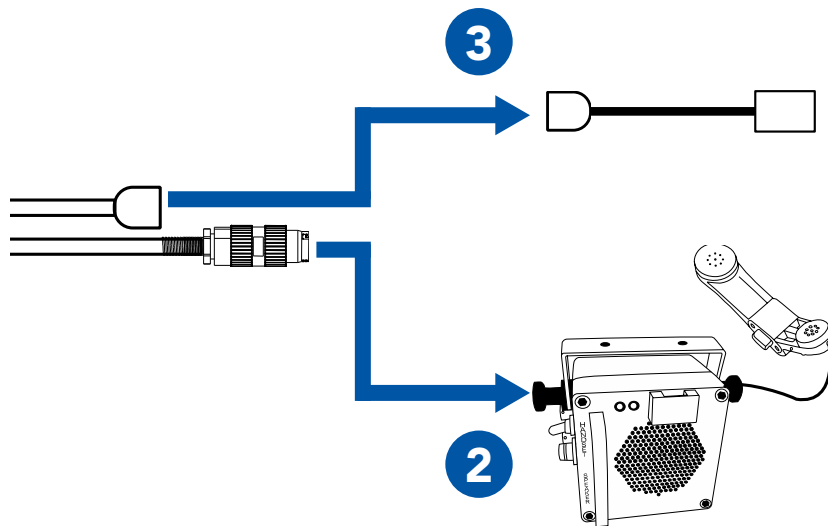
Monitor or TV with HDMI Input

DEVICE OPERATION: CONNECTING A MONITOR OR TV

- 1 Connect **CBL-DATA-3001** to the **DATA** side connector on the MPU5.

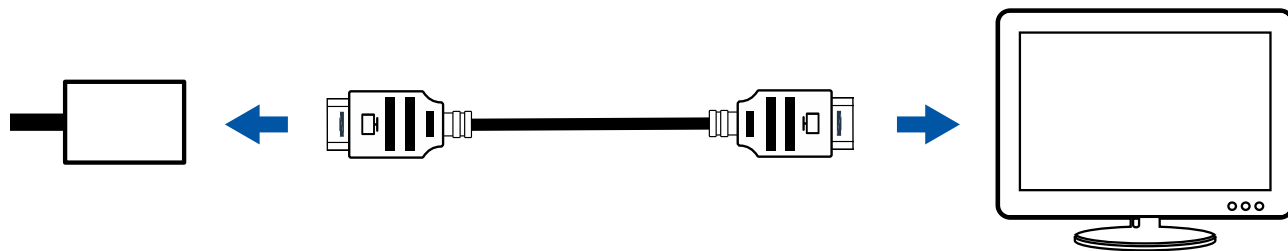


- 2 Connect the speaker box or headset to the **U-328 audio connector** on **CBL-DATA-3001**.



DEVICE OPERATION: CONNECTING A MONITOR OR TV

- 4** Connect one end of the standard HDMI cable to the **HDMI receptacle** on of **CBL-DATA-3001**.
- 5** Connect the other end of the standard HDMI cable to the **HDMI input** on the Monitor or TV.
- 6** The MPU5 Android™ OS will be displayed on the Monitor or TV.

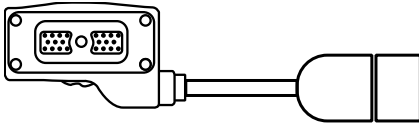


Why can't I see video on my Monitor or TV?

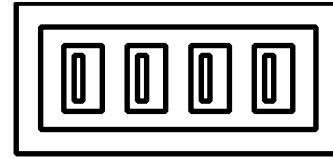
- 1** Ensure that the Monitor or TV is powered on.
- 2** Ensure that all cables are connected properly.
- 3** Ensure that the Monitor or TV is set to the correct HDMI input.
- 4** Reboot the node.

Connect USB Accessories to the MPU5

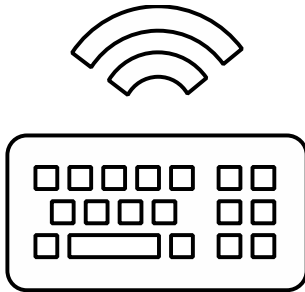
≈ Parts List/Interchangeable Parts



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



USB Hub
(Optional)



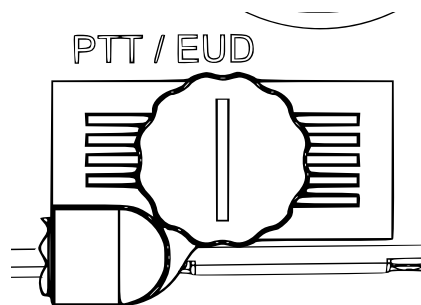
USB Keyboard
(Optional)



USB Mouse
(Optional)

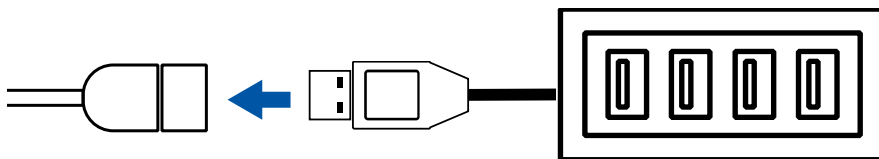
DEVICE OPERATION: USB ACCESSORIES

- 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.

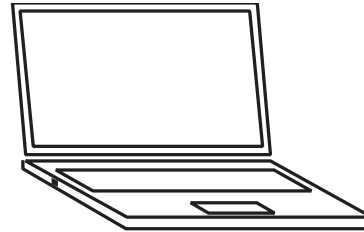
Install Android Apps on the MPU5



Parts List/Interchangeable Parts



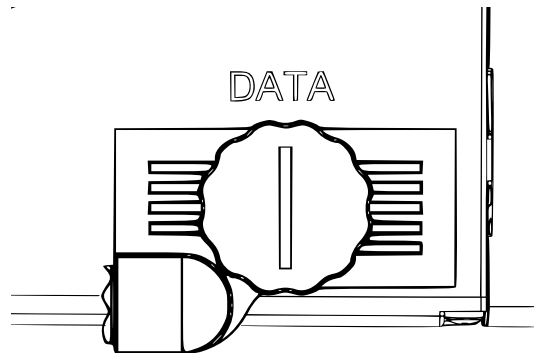
.apk file for Android™ App(s)



Management Computer

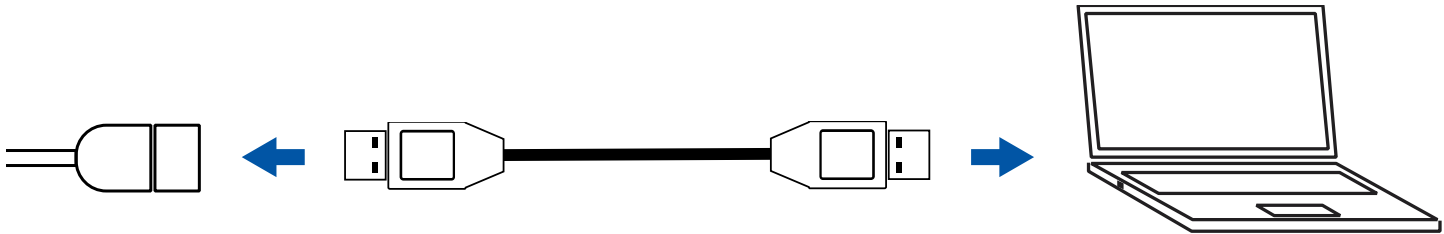
DEVICE OPERATION: INSTALLING APPS

- 1 Attach an EUD to the MPU5.
- 2 Connect **CBL-DATA-2003** to the **Data** side connector on the MPU5.



3 Connect one end of the USB extension cable to the **USB receptacle** on CLB-DATA-2003.

4 Connect the other end of the USB extension cable to a **USB port** on the Management Computer. Wait for drivers to automatically install.



DEVICE OPERATION: INSTALLING APPS

- 5 Download and install the **Android Debug Bridge (ADB)**.
- 6 Open **Command Prompt**.
- 7 Navigate to the folder containing ADB.
- 8 To run ADB, type: `adb`

```
Z:\Firmware\Android\apk\win32-android-tools>adb
Android Debug Bridge version 1.0.31
```

- 9 Type: `adb devices`
The MPU5 will appear.
- 10 Type: `adb install <file path>`
Replace `<file path>` with the path to the .apk file you wish to install.
Wait for the app to install.

```
Z:\Firmware\Android\apk\win32-android-tools>adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached
0018a6e0005b    unauthorized
```

9

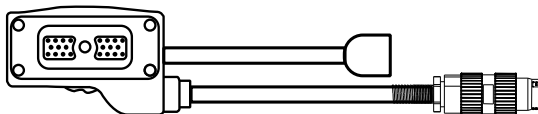
```
Z:\Firmware\Android\apk\win32-android-tools>adb install <path to .apk file>
```

10

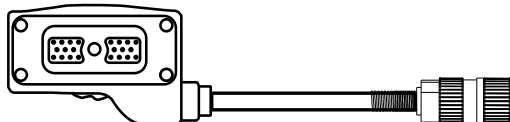
- 11 A message will appear on the EUD asking if you want to allow USB debugging.
Click **OK**.

Connect a PTT Device to the MPU5

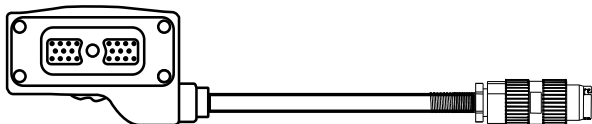
Parts List/Interchangeable Parts



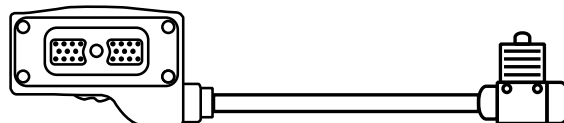
22-Pin to audio and Video Out
CBL-DATA-3001



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

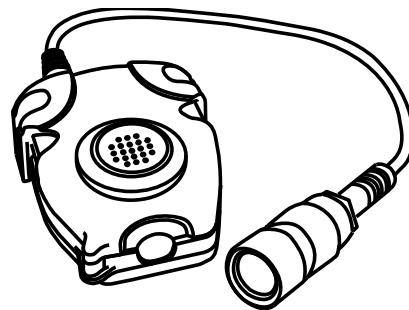


22-Pin to U-328
CBL-AUD-0002



22-Pin to U94 Receptacle
CBL-AUD-0003

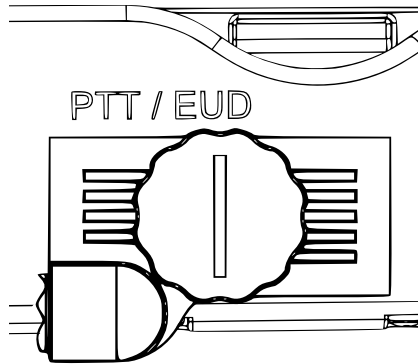
The cable you need is dependent on what connector your PTT device has.



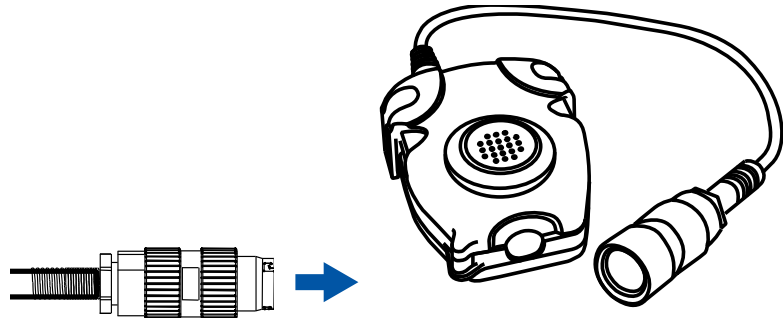
Compatible Push-to-Talk device

DEVICE OPERATION: CONNECTING A PTT DEVICE

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

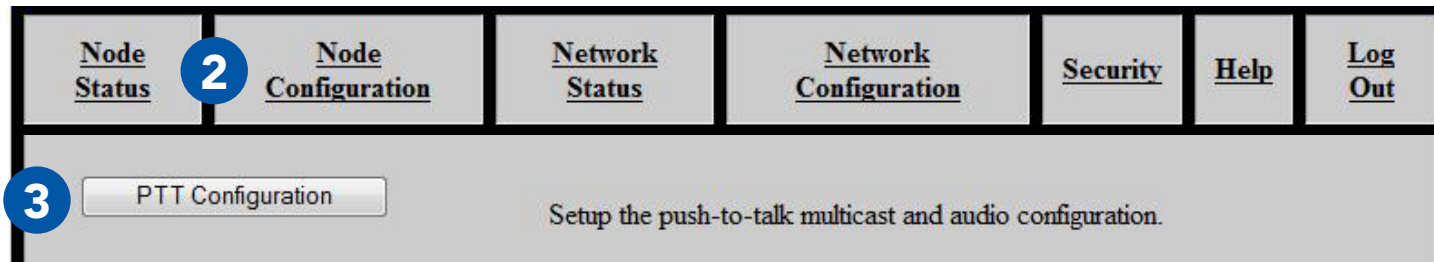


- 2 Connect the PTT device to the connector on the end of the cable.



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 **Load Audio Daemon** drop-down menu, select **Enabled**.
- 2 To disable Push-to-Talk, select **Disabled**.

Load Audio Daemon Network Default (true) ▼

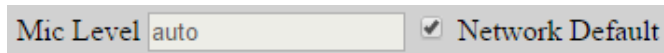
Set Earpiece Volume

- 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 80 ☒ 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



Mic Level auto ☒ 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 Network Default (OnKeyPress) ▼

Set Transmit or Receive Audible Checktone

- 1 From the **Courtesy TX** and **Courtesy RX** 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

Courtesy TX	Network Default (Beep) ▼
Courtesy RX	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 Channel** field, enter the channel(s) you wish to transmit on.
- 2 In the **Monitor** column, check the left 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

2

Monitor

☒ ☐ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

☐ ☒ Network Default

1

Selected Channel

☒ Factory Default

3

Name>>

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

4

Multicast Address

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ Network Default

☒ 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: RF-2001

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.

US- 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	
CHANNEL:	Max. Power Setting Approved (dBm)	Max. EIRP (dBm)	Max. Power Setting Approved (dBm)	Max. EIRP (dBm)	Max. Power Setting Approved (dBm)	Max. EIRP (dBm)
1	28	32	26	31	24	30.5
2	30	35	26	32	24	30.5
3	30	36	26	32	24	30.5
4	30	36	26	32	24	30.5
5	30	36	26	32	24	30.5
6	30	36	26	32	24	30.5
7	30	36	26	32	24	30.5
8	30	36	26	32	24	30.5
9	30	36	26	32	24	30.5
10	30	33	26	32	24	30.5
11	29	32	26	31	24	30.5

Approved Antenna Type:

- Dipole Antenna with up to 7.4 dBi gain

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)
Dipole (Omnidirectional)	2.1	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 (2200MHz – 2500MHz) radio module, 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**.

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.

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

National Stock Number	Pending
BT Part Number	BT-70716BG
Dimensions	Length: 2.8 in. (71 mm) Width: 1.6 in. (41 mm)
	Height: 3.4 in. (86 mm)
Weight	0.75 lbs (0.34 kg)
Nominal Voltage	10.8V
Maximum Voltage	12.6V
Capacity	6.4Ah
Discharge	6A Max Continuous
Pulse Discharge	40A \leq 1 ms
Operating Temperature	-30°C to +60°C (-22°F to +140°F)
Recommended Storage Temperature	-40°C to +40°C (-40°F to +104°F)
Connector	Flat Contacts (bottom), Fly Wheel Connection (top)
State of Charge Indicator	Not Applicable
Disposal	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 ₅₀ (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 (ivm-mouse)	N/AV
Lithium Carbonate	0 -0.3 w/w	554-13-2	525	N/APP
Lithium cobaltite (LiCoO ₂)	01-3- w/w	12190-79-3	N/AV	N/AV
Lithium hexafluorophosphate (LiPF ₆)	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

Carcinogenicity:	NTP?	IARC Monograph?	OSHA Regulated?
	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 2.0



303 Fifth Avenue Suite 306
New York, NY 10016

www.persistentsystems.com

