

LigoWave DLB Setup for Passive Mobile Download

Contents

- Assumptions 2
- Description 2
- LigoWave/Deliberant Kit Part Numbers 3
- Setup Procedures..... 3
 - Assumptions 3
- LigoWave Default Settings 4
- Login to LigoWave with a PC/Laptop 4
 - Assumptions 4
- Setup LigoWave 6
 - Assumptions: 6
- Master FMU/Passive Mobile NIC Setup 10
- Software Setup 13
 - Select Master FMU as Site 14
 - Select Passive Mobile as Site..... 15
- Install LigoWave 15
- Install Master FMU LigoWave Access Point 15
- Install Passive Mobile LigoWave 17
- Post Installation Tests 19
 - Assumptions 19
 - Steps 19
- Connectivity Test 20
- Considerations When Replacing APC Series Radios with DLB Radios..... 20
- Troubleshooting 20
- Resetting to Defaults..... 21
- Adjusting Effective Isotropic Radiated Power (EIRP) 21
- Change Log: 21
- Hold Harmless Agreement 22

NOTE Although this bulletin covers the use of LigoWave DLB for Passive Mobile Download, the LigoWave DLB radios may be mixed with Deliberant APC radios for these applications.

The purpose of this bulletin is to define a procedure for automatic wireless downloads of Passive Mobile transactions to a Master FMU using LigoWave DLB devices.

NOTE This procedure does not require any interaction from the Passive Mobile driver, nor does it require the CC operator to start the download process. The Passive Mobile may be in motion

throughout the entire download process. Multiple Passive Mobiles may download to a single Master FMU.

Assumptions

This guide assumes the following:

- Passive Mobile/Master Fuel Management Unit (FMU) have firmware .3.69 or later
- For Master FMUs connecting to the Central Controller (CC) via modem (telephone or Two-Way Ringdown Device), the CC software is v5.2.0.38 or later.
- For Master FMUs connecting to the CC via LAN (cable, fiber, or wireless), the software is v5.2.0.39 or later.

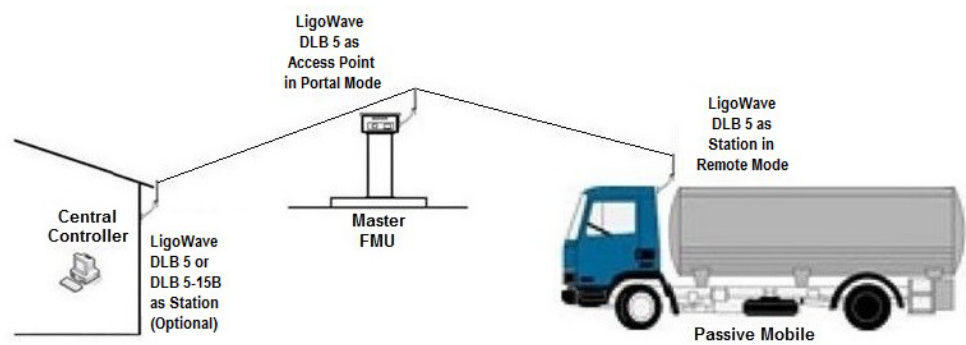


Figure 1. Wireless Path for LigoWave Passive Mobile Downloads

Figure 1 depicts the wireless path from the Passive Mobile to the Master FMU and from the Master FMU to the CC.

NOTE Syntech Systems, Inc. no longer sells the Deliberant APC radio.

The LigoWave DLB radios used in this application both on the Master FMU and on the Passive Mobile are DLB 5 equipped with two Omni Antennas. Previous applications called for a single Omni Antenna on each radio. It has since been found reception is much improved with a second Omni Antenna when two radios using external antennas must communicate to each other. This application permits communications between the Passive Mobile and Master FMU from any location where the Passive Mobile may acquire a wireless connection to the Master FMU.

Description

LigoWave is a small, compact, and inexpensive 5 GHz wireless network transmitter/receiver with an advertised line-of-sight range of 30 miles. When properly installed and configured, the wireless LigoWave DLB installed on the Passive Mobile will continually look for a wireless connection to a LigoWave DLB installed on a Master FMU. When the two radios connect, the transactions in the Passive Mobile will automatically download to the Master FMU, and be stored on the compact flash card. The transactions are retrieved by the CC when the Master FMU is downloaded.

Since the Passive Mobile may be moving when a communications connection is made and the connection may be lost as the vehicle moves, a transaction download will not be recorded until the download is successful. If the communications connection is lost before the download is complete, a full download must be accomplished when communications are restored. Download attempts will continue until a full download is completed.

Changes in the FMU firmware beginning with v3.69 provide these configuration options

- Network Interface Card (NIC) in a Master FMU
- Passive Mobile to Portal (Master FMU auto receives transactions from a Passive Mobile)
- Passive Mobile to Remote (Passive Mobile auto sends transactions to a portal Master FMU)


- Passive Mobile to Normal (Master FMU connects to CC by user initiation)

LigoWave/Deliberant Kit Part Numbers


LigoWave may be programmed for use as an Access Point or a Station. When Passive Mobiles are using LigoWave to download to a Master FMU, the Master FMU is the Access Point, and each Passive Mobile is a Station. Because the Passive Mobiles may be moving, both the Passive Mobile and the Master FMU must have LigoWave radios with omni-directional antennas, so the Passive Mobiles may log on to the Master FMU from any approach angle.

If purchased from Syntech, LigoWave is supplied in kit form as itemized below with a power supply, Power-Over-Ethernet (POE) injector, antenna(s), patch cable, and mount hardware developed for each application. If not purchased in kit form from Syntech, the antenna, 12VDC POE injector, and mount hardware must be purchased separately. The below listed part numbers are Syntech part numbers.

Kit 941H0219B This kit contains everything needed for a Master FMU and one Passive Mobile. It consists of two subordinate kits, 941H0218B and 941H0218D. Additional 941H0218D kits are required for each additional Passive Mobile.

Part #	Part Title	Qty	 <p>Figure 2. Wall/Pole Mount Bracket</p>
264650	LigoWave DLB 5 (Figure 2)	1	
257257	universal wall/pole mount bracket (Figure 3)	1	
251550	antenna, omni, 7 dbi	2	
211052	¼-20 x 0.75 screw	4	
193453	washer	4	

Kit 941H0218D This kit is provided with two omni-directional antennas and 12VDC power supply for use on the Passive Mobile(s).

Part #	Part Title	Qty	 <p>Figure 3. LigoWave DLB 5</p>
264650	LigoWave DLB 5	1	
257257	universal wall/pole mount bracket (Figure 2)	1	
251550	antenna, omni, 7 dbi (Figure 3)	2	
211052	¼-20 x 0.75 screw	4	
193453	washer	4	
21016	¼-20 nut	4	
256692	adapter, direct 12VDC insertion to POE	1	
941B0591	3 ft outdoor patch cable with weather seal	1	
941B0591A	20 ft outdoor patch cable with weather seal	1	

Setup Procedures

There are setup procedures for the Master FMU, Passive Mobile, LigoWave, PC (Laptop and/or Central Controller), and FuelMaster® software.

Assumptions

These procedures assume the following:

- Your PC (or laptop) is configured with a compatible static IP address

If any questions arise, please contact Syntech Systems, Inc.'s Customer Satisfaction Center at 1-800-888-9136, ext. 2 or email support@myfuelmaster.com.

- When the application includes a Central Controller connection to the wireless network, the Central Controller is configured with a compatible static IP address.

NOTE For instructions on how to do so, please see search online “how to setup a compatible static IP Address.”

LigoWave Default Settings

IP Method:	Dynamic Network mode: Bridge
Wireless mode:	Station (WDS/iPoll2) IP address: 192.168.2.66
Subnet mask:	255.255.255.0
Default gateway:	192.168.2.1 Channel width (MHz): 20/40
TX power (dBm): 25 (of 29 max) SSID:	LigoDLB, broadcasting IEEE mode: 802.11 a/n
Security:	Open

Login to LigoWave with a PC/Laptop

Assumptions

This tutorial assumes the following:

- During connection, you power on one device at a time (unless instructed otherwise).
- Every unit defaults to an IP address of 192.168.2.66.
- You only use a wired connection to the device (Disable wireless on your PC or laptop to avoid connecting to another device during setup).
- Firmware previous to v7.52, requires a browser other than Internet Explorer for login to LigoWave. Both Firefox and Google Chrome have been successfully tested with these devices.

NOTE Important! These radios default to Dynamic IP method. Unlike the previous Deliberant applications, every radio must be changed to the Static IP method.

Mac address may be located by removing the backplate of the device.

1. Run a patch cable from the power injector POE connector to the radio.
2. Run another patch cable from the LAN connector on the power injector to an active RJ-45 LAN receptacle in the PC/laptop.
3. Plug the power supply into a 110 VAC outlet. A green power-on light should illuminate on the power supply, and after it boots, the PWR and LAN LEDs should illuminate on the radio.
4. Enter the URL: <http://192.168.2.66/> into web browser. A Login window will open (Figure 4).

Figure 4. LigoWave Login

5. Enter the login credentials (**username:** admin; **password** admin01). Login credentials may be changed at SYSTEM CONFIGURATION>User accounts.
6. Ensure English is the selected language.
7. Select **Login**. An OPERATING COUNTRY window will open (Figure 5).

Figure 5. Operating Country

NOTE To eliminate the need for FCC licensing, the signal strength of each wireless radio must remain below a maximum Effective Isotropic Radiated Power (EIRP). For a detailed explanation, see Adjusting Effective Isotropic Radiated Power (EIRP) at the end of this bulletin.

8. Upon reading the User agreement, select **I agree**.
9. Select the **Operating country**. Identifying the country determine authorized channels, channel width, output power, Dynamic Frequency Selection (DFS) and Automatic Transit Control (ATC).
10. Enter the **dBi** of the antenna used with the DLB 5 (If using the antenna supplied by Syntech, enter 7). The DLB 5-15B will display 15 in the antenna gain box. The DLB 5 will display 0.

11. Select the **Usage scenario**. Point-to-point indicates the use of one access point and one station. Point-to-multipoint indicates the use of one access point and multiple stations.
12. Select **Change**. The initial firmware screen will display (Figure 6).

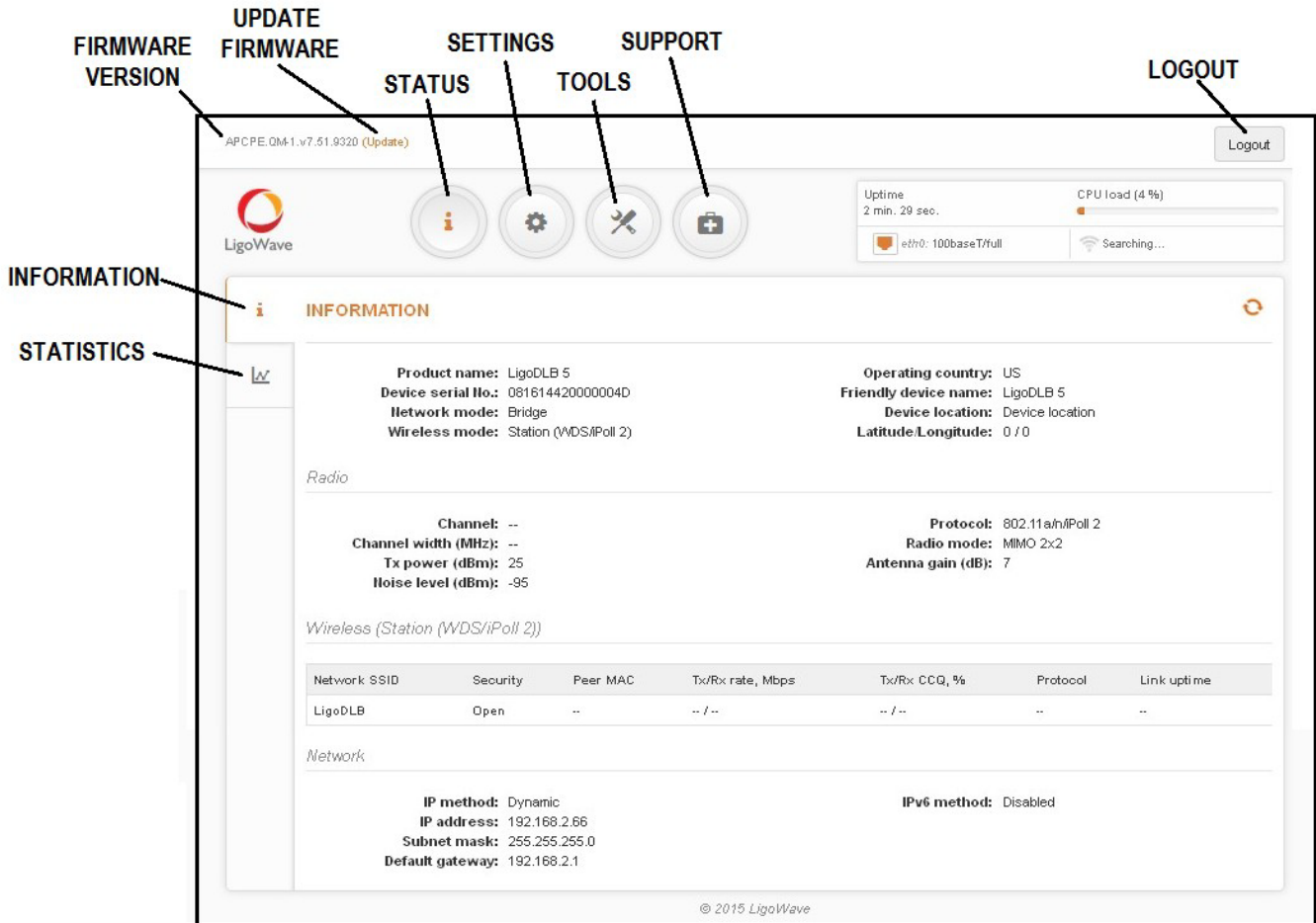


Figure 6. Information Window

Setup LigoWave

Following are procedures for setting up a DLB 5 or DLB 5-15B.

i Some of the following steps may be followed by an information icon, indicating they may not be required for every user of every application. If unnecessary, please skip.

NOTE This Passive Mobile application uses a DLB 5 on the truck and Master FMU. When a DLB 5 is used to communicate with another DLB 5, two external antennas will be supplied for each.

If a change is made on any page, **Save Changes** will appear in the upper right corner of the window. Select it before exiting the page to ensure changes are saved.

Assumptions:

You have downloaded the latest firmware version (Filter Downloads box > DLB > 5 GHz > DLB 5 or DLB5-15B) at: <https://www.ligowave.com/downloads>.

NOTE For these applications, do not download the HotSpot or Infinity firmware.

1. Select **Settings**. A WIRELESS CONFIGURATION window will open (Figure 7).
If any questions arise, please contact Syntech Systems, Inc.'s Customer Satisfaction Center at 1-800-888-9136, ext. 2 or email support@myfuelmaster.com.

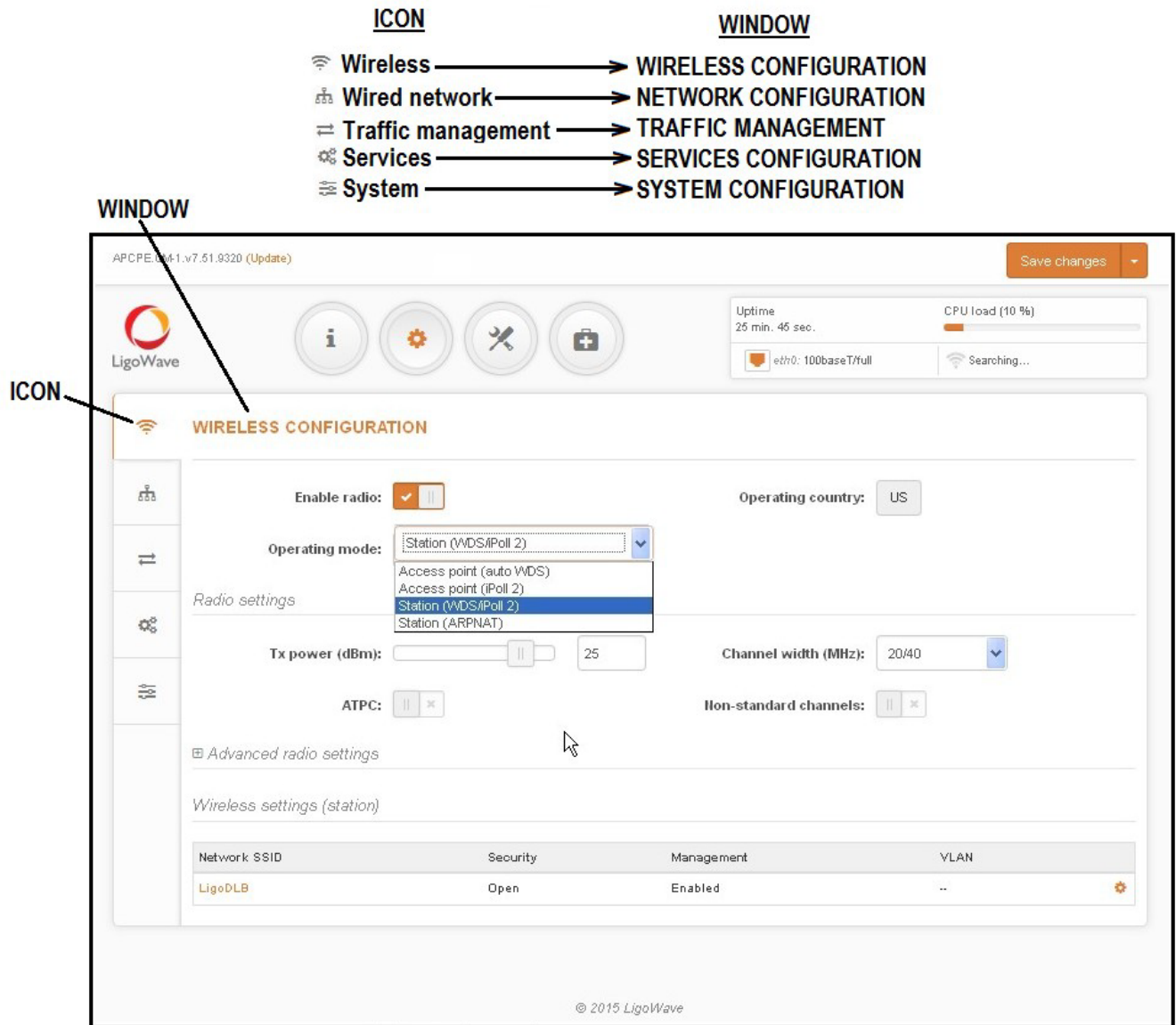


Figure 7. Settings Window


2. Ensure the **Operating mode** is set to desired preference. Only one Access Point may be configured for each network. iPoll2 is a network protocol that only accepts access to other iPoll2 radios. iPoll2 is a point-to-multipoint application. ARP NAT, in short, is a method for encrypting transmitted IP addresses.
3. Ensure the **Tx power (dbm)** (aka Transmit Power) is set to desired preference (default 25).

NOTE The Network SSID must match on all radios assigned to the same network. It is particularly important to look at this setting if the DLB radios are used with the older APC radios.

The Network SSID defaults to LigoDLB (case sensitive) unless the radio was upgraded from a DLB Hotspot to one of the other firmware versions. The Hotspot SSID is Infinity.

4. Ensure the SSID is set to desired preference.
 - a. Select Settings at the bottom right of the WIRELESS CONFIGURATION window. A window will open to permit the change.

NOTE Personal WPA/WPA2 and Enterprise WPA/WPA2 are available in all modes. Whatever security method is chosen has to be set the same in all radios installed in the network.

5. Setup wireless network security. 

- a. In the bottom right of the WIRELESS CONFIGURATION window, select Settings (Figure 11). A WIRELESS STATION SETTINGS window will open (Figure 8).

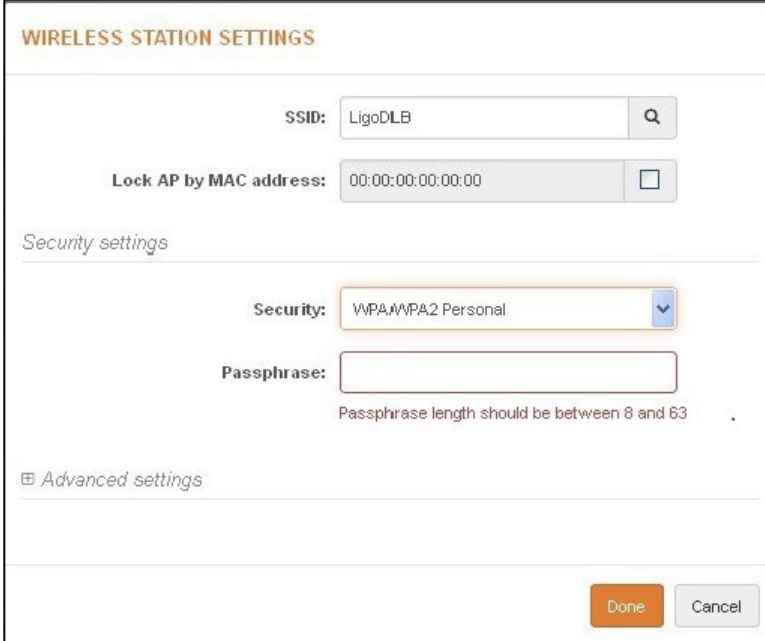


Figure 8. Wireless Network Security Setup

- b. Select the desired **Security Method**. Additional security requirements (example: Passphrase) will appear depending upon the security method chosen.
- c. Supply the required information and, if applicable, **Encryption Method**.
- d. Select **Done**.

6. Change IP Method. 

The DLB radios default to Dynamic IP method. Dynamic must be changed to Static IP method in every radio (Figure 9).

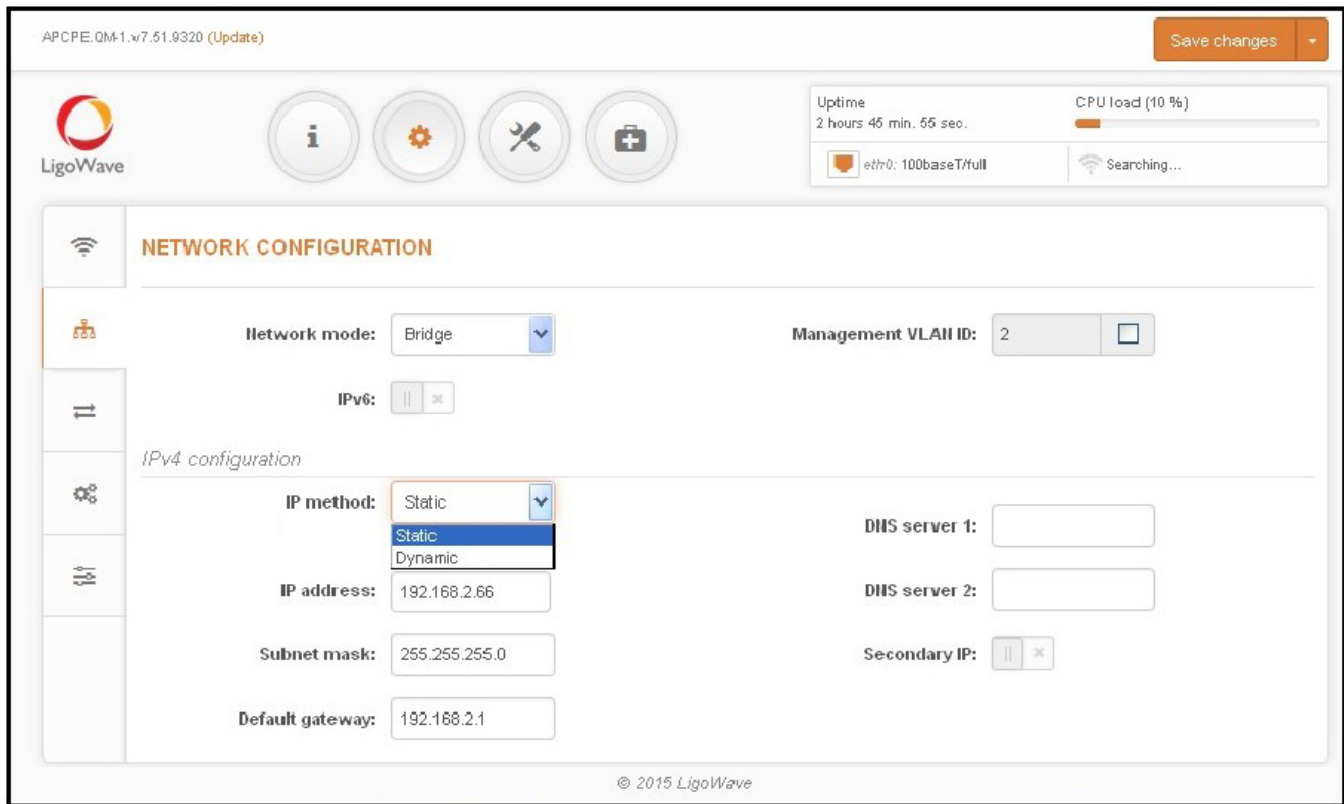


Figure 9. Network Configuration

- a. Under **Settings**, select **Wired Network**.
- b. Under IPv4 configuration, change the **IP Method** to Static.
- c. Select **Save Changes** (top right). A CHANGES window will open with a summary of the changes to be made.
- d. Select **Save**.

7. Change IP address. 

If an IP address change is necessary, perform the following (Figure 9):

- a. Under **Settings**, select **Wired Network**.
- b. Under IPv4 configuration, change the **IP address**, **Subnet mask**, **Default gateway**, **DNS server 1**, and **DNS server 2**, as needed.
- c. Select **Save Changes** (top right). The IP address changes will be saved.

8. Turn Off Client Isolation. 

If you are working with an application requiring a Station to Station communication (e.g., using Central Controller to communicate directly with a Passive Mobile), Client Isolation must be turned off in the Access Point (Master FMU).

- a. With a connection to the Access Point, select **WIRELESS CONFIGURATION** (Figure 7).
- b. Select the **gear icon** (bottom right).

- c. Select **Advanced settings** in the lower left-hand corner (Figure 8). The WIRELESS AP SETTINGS window will expand.
- d. Ensure the **Client isolation** checkbox is not active.
- e. Select **Done** Client isolation is turned off, and saved.



9. Configure a Secondary IP.

This setting can be very useful if your PC/laptop is normally used with a different subnet than what you have set in the LigoWave radios. You won't have to reconfigure the network settings in your PC/laptop to connect to these radios.

- a. Under Settings > NETWORK CONFIGURATION, toggle on **Secondary IP**.
- b. In the appropriate boxes, enter the desired **IP address** and **subnet mask**.
- c. Select **Save changes**.



10. Save backup configuration file.

- a. Select **Settings > System icon (Error! Reference source not found.)**.
- b. Under System functions, select Backup A window will open with the file name used by the firmware.
- c. Select **Save > OK**. The *.cfg file will be saved in the Downloads folder.
- d. Select **Save Changes**. The backup file is created and saved to the Downloads location.

11. Logout from the LigoWave program.

12. Repeat this tutorial as required for additional LigoWave radios.

13. Remove power from the power supply, and disconnect the cables connected to the DLB 5 or DLB 5-15 and the PC. Configuration is complete.

Master FMU/Passive Mobile NIC Setup

The only setup covered herein is the Master FMU and Passive Mobile Network Interface Card (NIC) setup to accommodate this procedure. The Master FMU should otherwise be set up in accordance with the FMU Installation Manual and the FMPlus User Manual. The Passive Mobile should otherwise be set up in accordance with the Passive Mobile Install Manual and the FMPlus User Manual. It is assumed the Master FMU and Passive Mobile(s) have network interface cards (NICs) installed. This setup will permit a Passive Mobile to automatically download transactions to a Master FMU when within wireless range.

If the site was originally setup with LigoWave or Deliberant without Passive Mobiles for wireless communications from the building to the fuel island, a setting change will be necessary in the Master FMU NIC. The steps below preceded with (Master FMU) must be performed to make the necessary change.

Initial NIC settings must be configured with a laptop connection. After the initial configuration, changes may be accomplished with a Supervisor Key.

NOTE There may be some variation in the commands shown depending upon the firmware in use in the FMU. Firmware version 3.74a was used in developing these procedures.

Until the networking equipment is set up and installed, there may be error messages stating No Link, Unable to Establish Network Link, FMU Is Not in Network Mode, etc.

1. Make a laptop connection in accordance with Product Bulletin 111.
2. Verify the network interface card is detected.
3. Use Ctrl-D to connect to the FMU.
4. Issue an F1 Command. A display similar to the following will appear (Figure 10).

NOTE There may be some variation in the commands shown depending upon the firmware in use in the FMU. Firmware version 3.74a was used in developing these procedures.

Until the networking equipment is set up and installed, there may be error messages stating No Link, Unable to Establish Network Link, FMU Is Not in Network Mode, etc.

```

NETWORKING CONFIGURATION

Hardware Address: 00-50-C2-2D-84-39
Link Status: OK

10 => Use DHCP:                disabled
15 => Domain Name:              localdomain
20 => IP Address:                0.0.0.0
30 => Subnet Mask:              255.255.255.0
40 => Default Gateway:          0.0.0.0
45 => Domain Name Server #1:    0.0.0.0
46 => Domain Name Server #2:    0.0.0.0
50 => Broadcast IP Address:     enabled
60 => Re-Broadcast IP at Midnight: enabled
70 => UDP Broadcast port:       3000
=> FTP Server:                  enabled
85 => Portal/Remote Configuration
90 => Reset Networking Configuration
95 => Display Network Statistics
0   => QUIT
Enter Selection: 0

```

Figure 10. Networking Configuration

5. If 10 => Use **DHCP** reflects enabled, at the prompt, enter 10 to disable DHCP.
6. At the prompt, enter 20 to change the **IP address**. A prompt, Set New IP Address: will appear.

```

Enter Selection: 20
Set New IP Address: 192.168.2.150

```

Figure 11. Set New IP Address

8. Enter an **IP address** that matches the application. The IP addresses for LigoWave, the PC or network switch, and the FMU NIC must be in the same subnet. After the IP address is entered, the NETWORKING CONFIGURATION will display similarly to Figure 10 but with a new IP address. As required, at the prompt, enter the **Subnet Mask, Default Gateway, Domain Name Server #1, and Domain Name Server #2**.

9. The wireless link between the Master FMU and the Passive Mobile requires some additional settings. At the prompt, enter 85 to change the Portal/Remote Configuration (Figure 12).

```

PORTAL/REMOTE CONFIGURATION
1 => Client Type:NORMAL
2 => UDP Comm Port: 4242
3 => Portal Timeout Period: 15
0 => QUIT
Enter Selection: 0

```

Figure 12. Portal/Remote Configuration

NOTE A longer Portal Timeout Period is preferred. The longer timeout will provide a lower frequency, clearer signal. The timeout is too long if the Passive Mobile is only in range of the Master FMU for a very short duration, and the download cannot be completed. In this case, reduce the timeout period until the download is successful.

- a. Perform the following for the Master FMU:
- 1) At the prompt, enter 1 to change **Client Type** to PORTAL (Figure 13).

```

PORTAL/REMOTE CONFIGURATION
=> Client Type: PORTAL
2 => UDP Comm Port: 4242
3 => Portal Timeout Period: 120
=> Remote IP Addresses: 255.255.255.255
4 => Add New Remote IP Address
5 => Remove Remote IP Address
0 => QUIT
Enter Selection:

```

Figure 13. Client Type Changed to Portal

- 2) At the prompt, increase the **Portal Timeout Period** to 120 seconds, or as far as is practical.
 - 3) Remote is for Passive Mobile(s). The Remote IP Address of 255.255.255.255 will allow the Master FMU to connect to any Passive Mobile remote IP address. If this is a problem and you want the Master FMU to pick up only designated IP addresses, at the prompt, enter 4 and all desired IP addresses.
 - 4) If you want to remove remote IP addresses from the Master FMU, at the prompt, enter 5 and all unwanted remote IP addresses.
- b. Perform the following for each Passive Mobile.
- 1) At the prompt, enter 1, and repeat until 1 => Client Type changes to REMOTE (Figure 14).

```

PORTAL/REMOTE CONFIGURATION

=> Client Type:          REMOTE

2 => UDP Comm Port:      4242
3 => Portal Timeout Period: 120

0 => QUIT

Enter Selection: 0

```

Figure 14. Client Type Changed to Remote PORTAL/REMOTE CONFIGURATION

- 2) At the prompt, increase the **Portal Timeout Period** to 120 seconds or as far as practical.
- c. When the setting changes are complete, enter 0 to **QUIT** and exit the PORTAL/REMOTE CONFIGURATION.
3. At the prompt, enter 0 to **QUIT**, and exit the NETWORKING CONFIGURATION.
4. The FMU NIC is configured. Disconnect in accordance with Product Bulletin 111.
5. Repeat steps 1 through 10, as required, for additional Master FMUs or Passive Mobiles.

Software Setup

The only software setup covered herein is the setup to accommodate this procedure. The software should otherwise be set up in accordance with the FMPlus User Manual. Changes to accommodate wireless downloads of Passive Mobiles are made in two screens: 1) Site ID, and 2) Go Online with FMUs.

1. Set the Site ID to identify where the transaction originated.
 - a. From the main window of the software, select the **Site** icon. A Site List window will open.
 - b. In the Site List window, open an existing site, or add a new site. A Site ID window will open (**Error! Reference source not found.**).

Figure 15. Software Site ID Window

- c. Enter a unique **Site ID**. The FMU dropdown will become active.
 - d. Select an **FMU**.
 - e. Select the **FMU Type** (Mobile or Passive).
 - f. Select **LAN**.
 - g. Select **Configure**. A LAN Connection Config Dialog window will open.
 - h. Activate the **IP address** checkbox.
 - i. Enter the **IP address** of the network card. Depending upon the selection made in the Type: box, the IP address should correspond to the IP address of the applicable Fixed FMU or Passive Mobile network card
 - j. Select **OK**.
 - k. In the Site ID window, complete the remaining configuration information in accordance with the FMPlus User Manual.
 - l. Select **Apply** > **OK**. The Site ID window will close.
 - m. Repeat these steps for each Master FMU and Passive Mobile to be configured for wireless Passive Mobile downloads.
2. Go Online with FMUs. See Figure 16. The software developed for the Passive Mobile download application has a change in the Go Online with FMUs window. There is a selection for Download Transactions, and another selection for Download Passive Mobile Transactions. These choices are dependent upon the site selected to start the download from, either the Master FMU or the Passive Mobile.

Select Master FMU as Site. Selecting the Master FMU as the site, and clicking on just the Download Transactions check box will download Master FMU transactions only. If you select just Download Passive Mobile Transactions you will download Passive Mobile transactions already downloaded from the Passive Mobile and stored in the Master FMU. Select both Download Transactions and Download Passive Mobile Transactions to download both FMU and Passive Mobile transactions (downloaded and in the FMU) with one action.

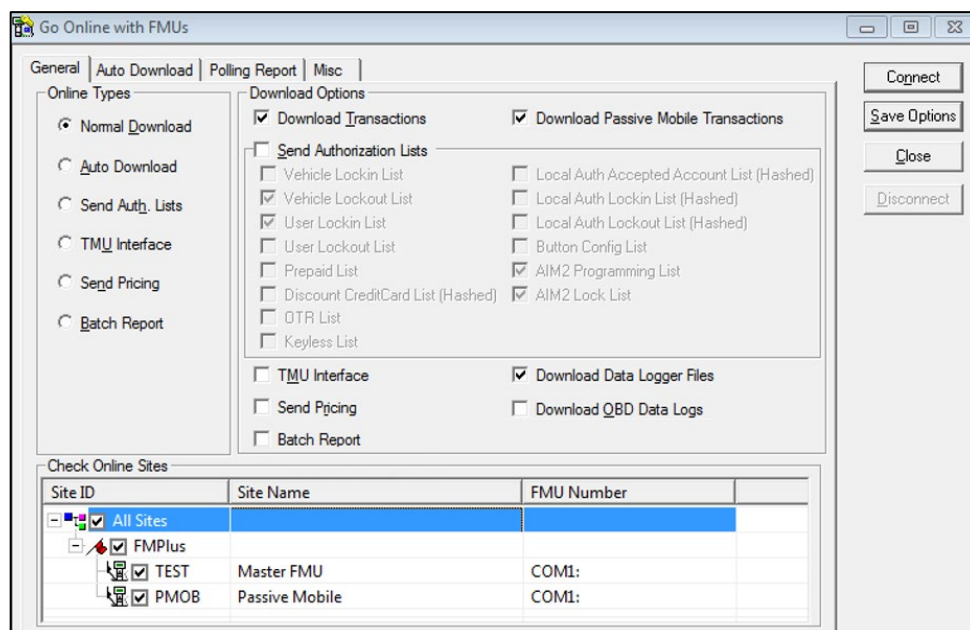


Figure 16. Go Online with FMUs

Select Passive Mobile as Site. If the Passive Mobile site is selected, clicking on the Download Transactions box will poll the Passive Mobile directly from the Central Controller for its transactions. Clicking on Download Passive Mobile Transactions from within a Passive Mobile site will do nothing. Since the connection is dependent upon a good wireless connection, no transactions will be downloaded if unable to connect to the Passive Mobile. If only a partial download from the Passive Mobile occurs such as when the Passive Mobile may drive out of range of the wireless network, the download will not complete. All transactions will remain in the Passive Mobile until a complete download occurs.

Install LigoWave

When LigoWave is used to download Passive Mobiles, different installation scenarios may be encountered. In all cases, a LigoWave must be installed on the Passive Mobile(s). In some cases, the same LigoWave on the Master FMU used to download transactions from Passive Mobiles may also be used to wirelessly download transactions from the Master FMU to the Central Controller. In some cases, there may not be a Master FMU.

Product Bulletin 228 describes the installation of LigoWave to communicate from the Central Controller to a Master FMU. In Product Bulletin 228, the LigoWave connected to the Central Controller was configured as an Access Point, and the LigoWave connected to the Master FMU was configured as a Station. When the Passive Mobiles are added, the LigoWave on each Passive Mobile is a Station. The LigoWave on the Master FMU is reconfigured as an Access Point, and the LigoWave connected to the Central Controller is reconfigured as a Station.

If there is no Master FMU, the LigoWave connected to the Central Controller remains an Access Point, and the LigoWave on each Passive Mobile is a Station.

The Syntech installation kits for FMUs and Passive Mobiles described on pages 3 and 4 include everything we found necessary to complete the installations. If purchased from other sources, be sure you purchase what is listed in the kit breakdowns on pages 3 and 4.

Install Master FMU LigoWave Access Point

If a LigoWave was previously installed on the Master FMU, the only change required is to reconfigure it to be an Access Point in accordance with [LigoWave Setup](#). If a complete installation is required, perform the following:

1. Ensure the Master FMU LigoWave is configured as an Access Point in concordance with [LigoWave Setup](#).
2. Find a suitable location for mounting the LigoWave.

CAUTION Exercise caution when selecting an FMU mount location for the antenna bracket and entry point for the patch cable (connected to power supply/POE in FMU). Mounting or entry holes must not interfere with or damage FMU internal components or mount points, and must not allow the entry of water through any new entry holes. If in a hazardous location, abide by the National Electric Codes.

NOTE If the FMU is an AIM FMU, do not mount anything between the FMU AIM antennas and the fueling point. It will interfere with AIM RF reception.

3. To mount the LigoWave directly on the FMU, perform the following (otherwise, skip to step 4).

NOTE If a mount location is selected that allows the mount screws to be installed without removing the Backplate Assembly, it is possible to exercise caution and drill holes into the FMU upper cabinet without removing the Backplate Assembly.

- a. Remove FMU power.
- b. If necessary, remove the Backplate Assembly in accordance with Product Bulletin 052.
- c. Using caution, install something to prevent drill shavings from falling on circuit boards or connectors.
- d. Mark and drill holes for the antenna mount bracket and patch cable strain relief (Figure 17).



Figure 17. Strain Relief

- e. Remove all drill shavings.
 - f. Install the mount bracket and run the patch cable. The Metal Washer of the Strain Relief may be discarded, and the rubber seal may be split to permit installation over Cat 5 cable. The End Cap and Rubber Seal of the Strain Relief should be outside the FMU.
 - g. As required, reinstall the FMU Backplate Assembly in accordance with Product Bulletin 052.
 - h. Securely mount the LigoWave on the mount bracket.
 - i. Remove and disassemble the LigoWave Compression Fitting.
 - j. Route the patch cable RJ-45 connector through the External Fitting, stretch the Rubber Bushing over the RJ-45, thread the RJ-45 through the Internal Fitting and Rubber Washer of the Compression Fitting, and plug the RJ-45 into the LigoWave RJ-45 POE receptacle.
 - k. Leaving some slack in the POE patch cable, push the remainder of the cable into the FMU through the Strain Relief (the POE cable may be secured to the antenna mount/FMU to prevent wind lash).
 - l. Tighten the External Fitting to seal the Compression Fitting against water intrusion.
4. To mount the LigoWave on another surface, perform the following (if already mounted, skip to step 5).
 - a. Mount the LigoWave in the desired location.
 - b. Run a POE cable from the LigoWave to the FMU. If the cable is entering a hazardous area, an explosion-proof conduit and sealoffs will be necessary to enclose the cable. The 182834 Strain Relief (Figure 17) supplied with the parts kit must be used to provide a weatherproof entry point for cable entry into the FMU.

CAUTION If the cable is entering a hazardous area, an explosion-proof conduit and sealoffs must be used to enclose the cable. The 182834 Strain Relief (Figure 17) supplied with the parts kit must be used to provide a weatherproof entry point for cable entry into the FMU.

- c. Ensure internal components are protected from damage and metal shavings when drilling the entry hole in the FMU for the Strain Relief. The small end of the Barrel is $\frac{3}{4}$ inch, and is inserted from outside through the Seal Washer and a hole drilled/punched in the FMU upper cabinet. Discard the Metal Washer and split the Rubber Seal to permit an RJ-45 connector to be inserted through the Strain Relief.
- d. Run the POE cable into the FMU through the Strain Relief, and tighten the End Cap to seal against water intrusion.

5. Mount the power supply/POE injector in the FMU to permit connection of the POE cable.

CAUTION If mounting close to any circuit board, anchor the power supply with industrial Velcro or some other mounting method to prevent contact with the circuit boards. Ensure the mounting location supports connection to a 110 VAC outlet, and permits patch cables to be routed to the FMU NIC.

If mounting close to any circuit board, anchor the power supply with industrial Velcro or some other mounting method to prevent contact with the circuit boards. Ensure the mounting location supports connection to a 110 VAC outlet, and permits patch cables to be routed to the FMU NIC.

6. Connect the POE cable to the power supply/POE injector POE port.
7. Run a patch cable from the FMU network interface card to the power supply LAN connector.
8. Plug the power supply into a 110 VAC power receptacle. A green PWR and LAN light will illuminate on the LigoWave.
9. Seal any holes where the patch cable exits the FMU.

Install Passive Mobile LigoWave

This installation includes a non-weatherproof 12VDC POE injector, which must be installed out of the weather where one Cat5 patch cable can be routed from it to LigoWave, and another can be routed from it to the Passive Mobile NIC. It will also require a wire connection to 12VDC switched power.

The LigoWave-antenna placement should be low enough to not interfere with anything in the path of the Passive Mobile (garage doors, fuel site canopies, etc.) but high enough to provide line-of-sight when the Passive Mobile is moving within RF range of the Master FMU LigoWave. It should not be placed where it will interfere with refilling the fuel tank on the Passive Mobile.

A variety of mounting positions have been used for Passive Mobiles. Some are mounted inside the truck cab. Some are mounted outside the cab, which requires weatherproofing. Keeping with these considerations, perform the following to install LigoWave on Passive Mobiles.

1. Ensure the Passive Mobile LigoWave is configured as a **Station**.
2. Find a suitable location for mounting the LigoWave.

CAUTION If an external Cat5 connection is not provided on the Passive Mobile, an entry point must be made for the patch cable into the Passive Mobile cabinet. Exercise caution when selecting the entry point. Creating mounting or entry holes must not damage or interfere with FMU internal components or mount points.

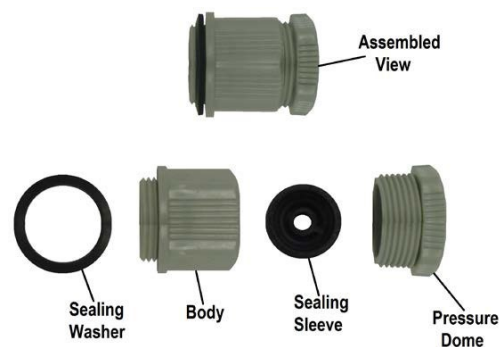


Figure 18. LigoWave Cable Gland

NOTE Locate LigoWave so as not to block AIM RF reception between the Passive Mobile antennas and fueling vehicles. Most Passive Mobiles fuel from a fixed mount hose reel.

Two Patch Cables with Weatherseals (see Figure 18) are provided with the install kit. One intended for connection between the POE Injector and Passive Mobile NIC is 3 feet long. The other for connection between the POE Injector and LigoWave is 20 feet long. If not needed, it is not necessary to remove the Weatherseal from the Patch Cable.

3. Find a location for mounting the Wall/Pole Mount Bracket, and if applicable, make an entry hole in the Passive Mobile cabinet for the Patch Cable Weatherseal. The Patch Cable Weatherseal will require a 5/8-inch hole where the patch cable enters the FMU.
4. If holes must be made in the Passive Mobile cabinet:
 - a. Remove Passive Mobile power and remove/protect the Backplate Assembly.
 - b. Mark and drill holes for the Wall/Pole Mount Bracket and Patch Cable Weatherseal. The Patch Cable for the LAN connection is 3 feet long and must reach the POE Injector.
 - c. Remove all drill shavings.
 - d. Install the Wall/Pole Mount Bracket, and run the Patch Cable. The Weatherseal should be installed so the Passive Mobile cabinet is sandwiched between the O-Ring and Locknut with the O-Ring and End Cap outside the FMU.
 - e. As required, reinstall the FMU Backplate Assembly.
5. Securely mount the LigoWave.
6. Install the POE Injector requires a 12VDC input. Recommend a switched power source to avoid the possibility of vehicle battery drain. The top of the POE Injector has two RJ-45 receptacles marked Network and Equip+PoE.

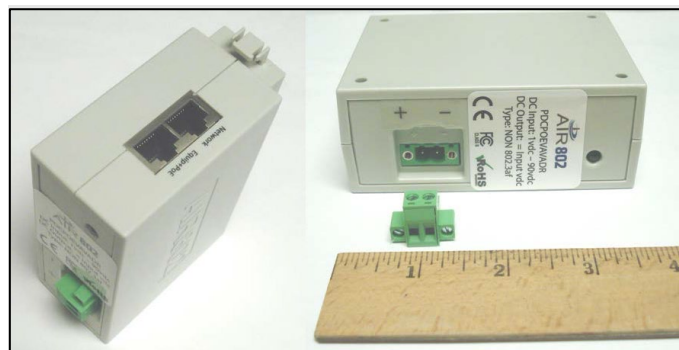


Figure 19. 12VDC POE Injector

- a. Find a weatherproof mounting location for the 256692 POE Injector. It has a removable DIN rail mount that may be removed, if not needed. For this application, industrial strength Velcro may be a good mounting choice.
- b. Run a two-conductor cable from a switched (switched off when the ignition switch is off) 12VDC power source to the POE Injector.
- c. Connect the 12VDC switched power source to the POE Injector. The two-pin connector on the POE Injector is removable, if necessary, and the connection points are labeled + and -.
7. Connect the 3-foot Patch Cable from the POE Injector Network receptacle to the Passive Mobile NIC.
8. Connect the end of the 20-foot Patch Cable inside the Passive Mobile to the POE Injector Equip+PoE receptacle.
9. Route the other end of the 20-foot Patch Cable to the LigoWave.

- a. Remove and disassemble the LigoWave Cable Gland.
 - b. Route the patch cable RJ-45 connector through the Pressure Dome, stretch the Sealing Sleeve over the RJ-45, thread the RJ-45 through the Body and Sealing Washer of the Cable Gland, and plug the RJ-45 into the LigoWave RJ-45 POE receptacle (Figure 19).
 - c. Leaving some slack in the POE Patch Cable, coil the excess inside the Passive Mobile, and secure the POE cable to prevent wind lash.
 - d. Tighten the External Fitting to seal the Compression Fitting against water intrusion.
10. Tighten the End Cap of the 20-foot Patch Cable Weatherseal to prevent water intrusion into the Passive Mobile cabinet.
 11. Repeat these steps for second and subsequent Passive Mobiles.



Figure 20. Patch Cable Weatherseal

Post Installation Tests

This test is only verifying Passive Mobile downloads to the Master FMU and Central Controller.

Assumptions

This tutorial assumes:

- The Passive Mobile(s) and Master FMU have been properly installed
- The applicable post installation tests/Acceptance Test Procedures have been performed

Steps

1. Bring each Passive Mobile (one at a time) within RF range of the Master FMU, and perform a test transaction with each Passive Mobile. The Passive Mobile should download its test transaction to the Master FMU as soon as the transaction completes. A prompt will appear on the Passive Mobile display, PREPARING TO UPLOAD TRANSACTIONS and will remain until the transaction(s) has been uploaded to the Master FMU.
2. When a test transaction has been run on each Passive Mobile, go to the Central Controller, and select the Online icon.
3. In the Go Online with FMUs window, select **Download Passive Mobile Transactions**.
4. Select the **Site ID** for the Master FMU.
5. Select **Connect**. The Central Controller should connect with the Master FMU. Each test transaction should download and appear in the Polling Report.

Connectivity Test

There are fewer tools presently available for the DLB series radios. If both ends of a wireless connection are properly configured, the signal strength indicators will illuminate when power is applied and a link is made. This could be tested while the radios are being configured in an office environment, installed, and powered using those same configurations.

Considerations When Replacing APC Series Radios with DLB Radios

The only conflict we have been made aware of occurs when an APC series radio is configured to an iPoll mode, and asked to link to a DLB radio. If this occurs, the APC radio firmware must be upgraded to the same firmware as used by the DLB radio.

Troubleshooting

For more information, including news on updates to the equipment and firmware, visit <https://www.ligowave.com/wiki/>.

Unlike the previous Deliberant radios, these LigoWave radios are defaulted to Dynamic IP method. All radios must be configured to Static IP method to work with the available FuelMaster software settings.

If you are unable to connect to a LigoWave device with any IP address, perform Resetting to Defaults. The procedure will restore LigoWave to the manufacturer's original default configuration.

A satisfactory Repeater configuration has not yet been found, but alternatives to a Repeater have been discovered. A Deliberant Repeater was attempted between an Access Point and a Station, but wouldn't work. Deliberant support suggested we move the Access Point to the Repeater position, and make both end positions Stations. Ping would not work from the Repeater to either Station.

When all three radios were turned on, communications passed from the first Station (on a building) to the Access Point, then to the Station on the FMU. Ping was also successful from the first Station through to the second Station, and from the second Station back to the first Station.

When you make a PC connection to a LigoWave device, remember it takes a moment for the device to boot up. It is not immediately available as soon as the connections are made and power is applied.

Verify the two (or more) units are configured correctly. They, and the devices they are connected to, must be on the same subnet. They must be using the same SSID. They cannot be using the same IP address.

The DLB 5-15B has a directional antenna. If being used as an access point for several FMUs, and is not communicating to all of them, the signal may not be reaching all the FMUs. This may be tested by performing the Antenna Alignment procedure. It may be necessary to replace the DLB 5-15B with a DLB 5 and omni antenna.

If the PC is presently on a network, it will have to be reconfigured with a static IP address as opposed to Obtain an IP address automatically. The static IP address must be on the same subnet as the LigoWave radios.

After any changes are made to the configuration of the radios, be sure they are saved correctly. Do not remove power while a save or reboot is in progress.

If wireless security is enabled, verify it is configured with the same settings so all the devices will communicate with each other. Wireless security passkeys are case sensitive.

If troubleshooting doesn't resolve communicate conflicts, reset all devices to their default settings and re-accomplish configuration. A simple typographical error in one setting can be very difficult to find, and can prevent communications.

Resetting to Defaults

With the POE cable connected and power applied (green Power LED illuminated), press and hold the reset button for 5- 10 seconds (Figure 21).

1. Then release. The radio will reboot and be accessible using the default IP address of 192.168.2.66.

NOTE If the reset button was not closed long enough, the radio will still reboot but will not reset.



Figure 21. Reset Button

Adjusting Effective Isotropic Radiated Power (EIRP)

To eliminate the need for FCC licensing, the signal strength of each wireless radio must remain below a maximum Effective Isotropic Radiated Power (EIRP). The EIRP is measured by adding the antenna dBi to the radio output power (example: 7 dBi antenna + 29 dBm radio output power = 36 EIRP).

Point-to-point (one access point to one station) cannot exceed 53 EIRP. Point-to-multipoint (one access point to multiple stations) cannot exceed 36 EIRP. When first logging in to the DLB radios, you will be asked to enter the gain of the antenna, as well as whether it will be used for point-to-point, or point-to-multipoint. The maximum transmit power of the DLB radios is 29 dBm when the EIRP is not exceeded. The radio firmware will automatically reduce the maximum transmit power to keep the EIRP within the maximum permitted by the FCC.

TIP

If any questions arise, contact Syntech Systems, Inc.'s Customer Satisfaction Center (CSC) at 1-800-888-9136, ext. 2, or email support@myfuelmaster.com.

Change Log:

Date	Description
11/9/2015	Original
3/24/2016	Revised - Added explanation and instructions for disabling Client Isolation, pages 13 and 14.
11/6/2020	Rebranded/Reformatted
03/30/2020	Edited for conciseness

Hold Harmless Agreement

Users of wireless networking equipment should be aware there is a potential for hackers to access a wireless network. The best network security cannot stop the best hackers. Though the FuelMaster fuel management system and software should contain no secure information, the PC may be connected to a network, which may contain secure information. Syntech Systems, Inc., cannot be responsible for unauthorized access achieved through the use of this equipment. A Hold Harmless Agreement (attached to the end of this document) is provided for the installer to present to the customer. Installation should not be completed until the Agreement is acknowledged. The setup procedures herein cover the setup of network security with this wireless networking equipment.

HOLD HARMLESS AGREEMENT (to be completed when installing wireless networking equipment)

TO:

SUBJECT: Potential Security Breaches Through Wireless Network Connections to FuelMaster

FuelMaster Fuel Management Units (FMUs) and software do not contain personal information subject to the Privacy Act of 1974. However, when added to a network the FMU may provide a link to other resources which do contain personal or privileged information. Cable or fiber optic network connections are not easily accessible. Wireless networks operate on radio waves that can be intercepted by anyone with the right equipment and within range of the transmitter. Without proper wireless network security, outside users can access your network to attain such valuable information as social security numbers, credit card numbers, bank account numbers, and countless other private information sources stored on your network. If accessibility is achieved, outside users can access anything stored in your network, not just FuelMaster related information.

Though the physical installation of the equipment may be accomplished by anybody with the knowledge and experience, the responsibility for the network, IP addresses, wireless components and devices, access points and network configuration rests entirely on the customer and, where applicable, his/her Information Technology (IT) person(s) or Network Administrator(s) for that site.

Syntech Systems, Inc., cannot emphasize enough the potential damage that may result from a breach in network security. When a wireless network connection to FuelMaster is established, Syntech Systems, Inc, cannot prevent accessibility by outside users. As such, this HOLD HARMLESS AGREEMENT is prepared to remove liability from Syntech Systems, Inc., and the installer/installing company for any breach of security resulting from the development of a wireless network connection to FuelMaster. Please acknowledge receipt and concurrence with the terms of this agreement by signing below. Thank you.

ACKNOWLEDGEMENT:

I acknowledge receipt and concurrence with the terms of this agreement:

(Signature of Authorized Representative)