Please ensure that when configuring your Amphenol plug, code A is clearly followed.

3.2.12 Solar Power

 Solar Power is recommended for sites where commercial power is not available or is not cost effective to install. The required size for the solar panel and battery system is strongly influenced by the geographic area in which it will be used, and should be calculated by an appropriate engineering effort. Ingenu offers a kit for base station configurations that require solar power which may be appropriate for your application. Contact Ingenu at support@ingenu.com for more information.

3.2.13 Outdoor Installation Hardware

All outdoor installation hardware such as mounting brackets, pipe clamps, u-bolts, bolts, nuts and washers should either be galvanized or stainless steel. This reduces deterioration due to corrosion, oxidation, and rust.

3.2.14 Weather Sealing Antenna System Connections

All exposed antenna system connectors must be sealed against moisture using industry standard techniques.

4 Regulatory Warnings

4.1 Certifications

The AP is designed to meet regulations for world-wide use. For information on the most current certifications, refer to the *Access Point Product Specification (014-0030-00)*.

4.2 Transmit Power Restrictions

Transmit power restrictions vary by country/agency. For details about antenna and transmit power restrictions, refer to the *Access Point Product Specification (014-0030-00)*.

4.3 FCC Warnings – United States

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

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

WARNING :   This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, this equipment may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

4.4 ISED Warnings

CAN ICES-3 (B)/NMB-3(B)

The installer of this radio equipment must ensure that the antenna is located or pointed so that it does not emit RF field in excess of Health Canada limits for the general population. Consult Safety Code 6 which is obtainable from Health Canada's website http://www.hc-sc.gc.ca/index-eng.php.

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

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

Canadian Two Part Warning Statement:

This device complies with Innovation, Science and Economic Development Canada (ISED) licence-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.

L'installateur de cet équipement de radio doit veiller à ce que l'antenne est située ou est pointée de façon à ne pas dégager de champ RF dépassant les limites de Santé Canada pour la population générale. Consulter le Code de sécurité 6 qui peut être obtenu sur le site Web de Santé Canada http://www.hc-sc.gc.ca/index-eng.php

Cet appareil se conforme aux Cahiers des charges sur les Normes Radioélectriques (CNR) d'Industrie Canada applicables aux appareils de radio exempté de licence.   Son fonctionnement se soumis aux deux conditions suivantes :
1) l'appareil ne doit pas produire d' interférences, et
2) l'utilisateur de l'appareil doit accepter tout interférences radioélectrique subi, même si les interférences sont susceptible d'en compromettre le fonctionnement.

Pour réduire les interférences radioélectrique pour les autres utilisateurs, sélectionnez le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (PIRE) ne soit pas supérieure à celle permise pour réussir une communication.

4.5 RF Exposure Statement

For all access point models (ULPAPx110 and RPMAAP10x): This device is only authorized for use in fixed and mobile applications. To meet FCC and other national radio frequency (RF)

exposure requirements, the antenna for this device must be installed to ensure a separation distance of at least 20cm (8 inches) from the antenna to a person.

4.6 CE Mark (ETSI) Warnings

This RPMAAP10E complies with the essential requirements of the European Union Radio and Telecommunications Terminal Equipment Directive (R&TTE) 1995/5/EU and the Restriction of Hazardous Substances Directive (RoHS) directive 2011/65/EU.

The RPMAAP10E has been tested against the requirements for both Generic Short Range Devices and Radio Frequency Identification (RFID) according to EN 300 440. Restrictions for RFID performance follows ERC/REC 70-03, Edition May 27, 2016.

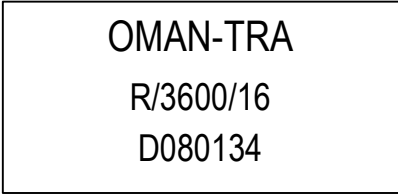## 4.7 Australia (RCM) and New Zealand (R-NZ)

R-NZ

The ULPAP110 and the RPMAAP10 comply with requirements in Australia and New Zealand. All products with EMC and radio communications must have a registered RCM and R-NZ mark on the end product. Registration to use the compliance mark will only be accepted from Australian or New Zealand manufacturers or importers, or their agent, in Australia and New Zealand.
In order to have a RCM/R-NZ mark on an end product, a company must comply with a or b below.
> a. have a company presence in Australia or New Zealand.
> b. have a company/distributor/agent in Australia or New Zealand that will sponsor the importing of the end product.

4.8 Oman
The ULPAPE110 meets the requirements of the TRA in Oman. Equipment label:
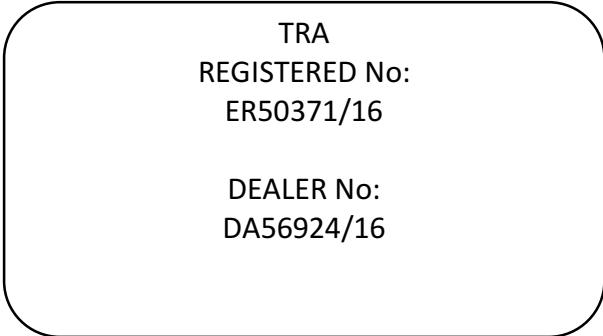
```
┌─────────────────────────┐
│                         │
│       OMAN-TRA          │
│       R/3600/16         │
│       D080134           │
│                         │
└─────────────────────────┘
```

The following are general rules that govern the labeling scheme and the dealer is bound to follow:

1. The label is required to be placed on the equipment and any of the user information document (e.g. User Guide).

2. It is preferable also to place the label on the packing as it is more visible to the consumer. If there is no adequate size on the equipment

4.9 United Arab Emirates - TRA (Telecom Regulatory Authority)

The ULPAPE110 meets the requirements of the TRA as required by United Arab Emirates (UAE).

```
╭─────────────────────────────────╮
│                                 │
│              TRA                │
│          REGISTERED No:         │
│           ER50371/16            │
│                                 │
│           DEALER No:            │
│           DA56924/16            │
│                                 │
╰─────────────────────────────────╯
```

4.10 Taiwan NCC Information

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功
或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改
善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
Under normal operation there are no operational modes that allow the Access Point to violate Administrative Regulations on Low Power Radio Waves Radiated Device.

To maintain NCC compliance do not attempt to modify the equipment. Modifications shall only be performed by trained personnel. Failure to follow these guidelines may violate local regulations.

Warning: modifications including the replacement of components by individuals other than trained personal is strictly prohibited.

5 AP Installation

5.1 AP and Ancillary Equipment

The AP installation includes installing the AP itself and the ancillary equipment listed below:

- Access Point (AP)
- AP antenna
- AP antenna cable (50 ohm coaxial cable)
- AP antenna cable RF surge suppressor (lightning suppressor)
- GPS antenna
- GPS antenna cable (50 ohm coaxial cable)
- PoE injector, powered by 48 VDC
- Site-specific power solution providing 48 VDC to the PoE, if not using the 120/240 VAC powered base station cabinet or the solar powered base station
- Backhaul equipment
- Site-specific mounting hardware

NOTE: Ingenu recommends that a backup power solution be utilized to power the AP in the event of a power failure. The backup power solution should be designed to meet customer requirements for the number of hours of backup power.

5.2 AP Installation Configurations

The small size of the AP (9.1"(231 mm) H x 8.1" (206 mm) W x 4.5"D (114 mm)) and light weight allows for many installation configurations. For basic AP specifications, refer to Appendix C. The AP is designed to be installed indoors or outdoors. It may be mounted in any position indoors but should be mounted with its connectors facing down when installed outdoors. The AP may be installed in an equipment cabinet with its ancillary equipment if desired.
Types of installation configurations include:

- Outdoor non-penetrating roof mounts on building
- Indoor or outdoor wall attachment
- Pipe mounting
- Tower mounting
- Utility pole mounting

5.3 Base Station Configurations

Ingenu offers pre-configured base station packages. For details, refer to Appendix D: Base Station Configuration.

5.4 General Grounding Guidelines

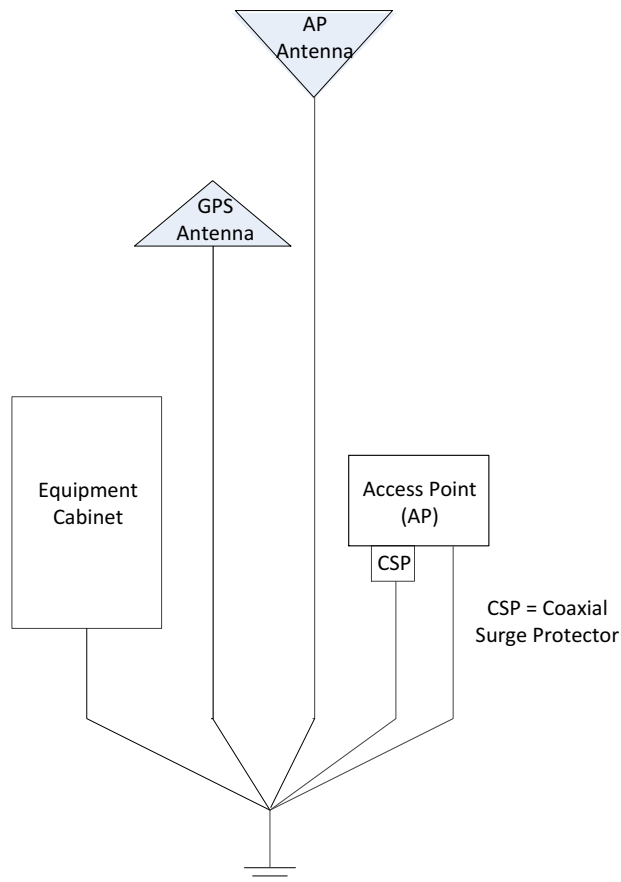The following grounding information is provided as a guideline when installing the AP in any configuration.

Figure 8. High Level Grounding Diagram

5.4.1 Grounding the AP and Antenna Cable Surge Suppressor

A ground wire may be attached underneath one of the AP mounting bolts. A ground wire must be attached to the ground terminal on the inline coaxial surge protector which is inserted between the AP's type N female antenna connector and the AP antenna cable. An example is shown in the following figure.
Note that the "Grounding for the AP" is shown for the ULPAPx110 model. For chassis grounding on the RPMAAP10x, refer to Figure 4 RPMAAP10x Grounding Stud.
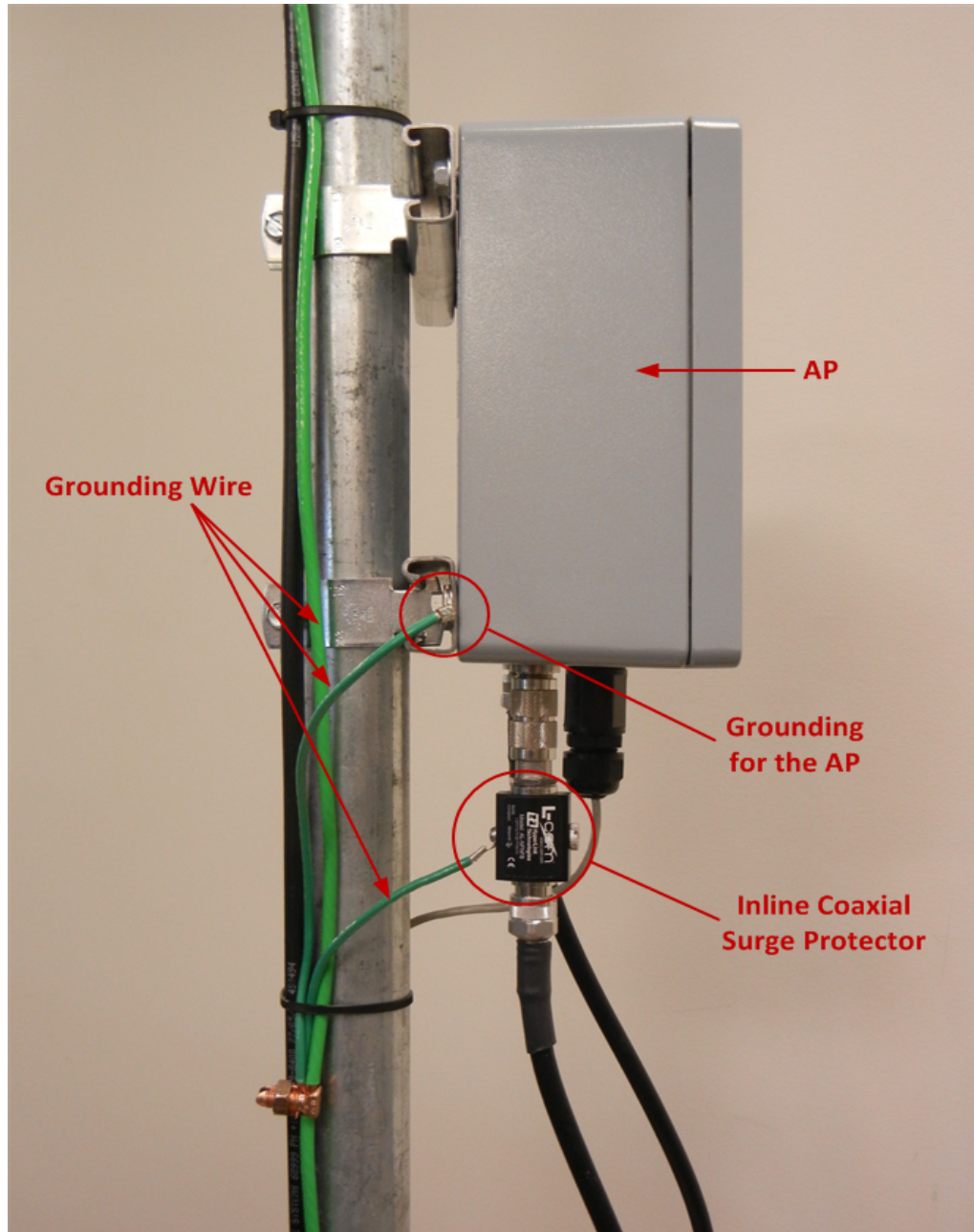
Figure 9. Grounding the AP (models ULPAPx110 only)

5.4.2 Grounding the AP and GPS Antennas

If the AP and GPS antennas are not attached to grounded metal structures a #6 AWG or larger ground wire should be attached to the base of both antennas. An example of grounding these two antennas is shown in the following figure.
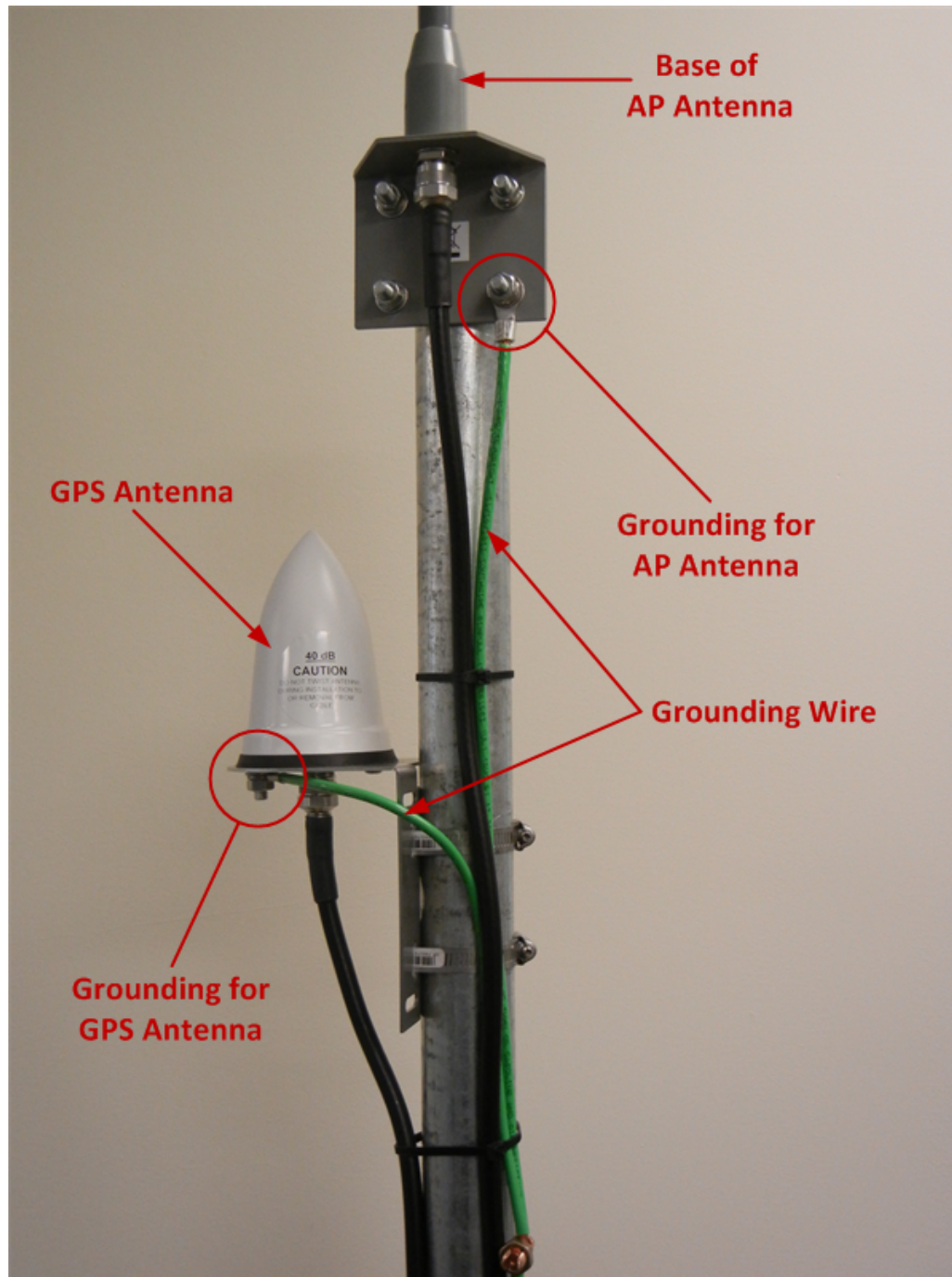

Figure 10. Grounding the GPS and AP Antennas

5.5 AP Mounting Details

APs are typically mounted using one of the three methods described below:

5.5.1 AP Mounting Tabs

The AP is supplied with four mounting tabs that facilitate attaching the AP to a wall, in a cabinet, or to a strut channel, if required. The mounting tabs are attached to the AP by the installer using four provided, 5/16 inch, hex head bolts.
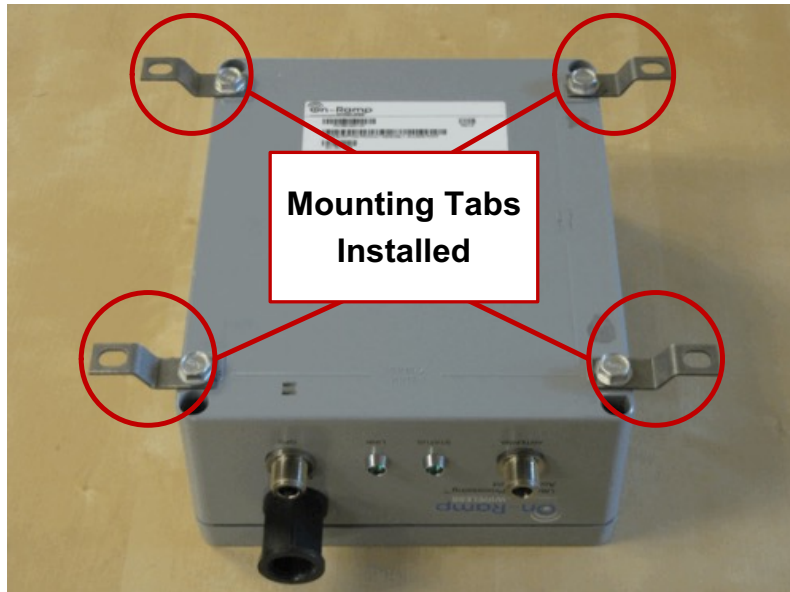

Figure 11. AP with Mounting Tabs Installed

5.5.2 AP Direct Attachment

The AP may be directly attached to a 19" equipment shelf or other mounting arrangement using the four tapped mounting holes in its enclosure. The four provided 5/16 inch, hex head bolts. are used for this mounting option.

5.5.3 AP Pipe Mount Option

Ingenu offers an optional pipe mount kit for the AP. This kit provided two 8-inch lengths of strut channel that have been drilled to allow attachment to the top and bottom holes on the back of the AP. The four provided 5/16 inch, hex head bolts are used to attach the strut channel in place of the mounting tabs. After attaching the strut channel to the AP, it can now be attached to any size of pipe using standard strut channel pipe clamps or conduit clamps.

5.6 Outdoor AP Installations

The AP is enclosure is IP66 rated and may be installed outdoors in a secure location. When installing the AP outdoors the flowing requirements must be observed:

- The AP must be mounted with the connectors facing down toward the ground.
- The Ingenu approved waterproof Ethernet cable restraint must be used to weather seal the AP's PoE connector. On AP's using the plastic PoE connector housing, the connector housing must be held with a wrench to prevent it from turning while the water proof cable restrain is installed. <u>The installation instructions provided with the waterproof cable restraint must be followed.</u>
- The RF Surge protector must be installed with the male connector end marked "Protect" connected to the APs RPMA antenna connector.
- The RF surge protector and the AP enclosure must be grounded using #10 AWG or larger, stranded, insulated conductors connected to a nearby grounding point. A ground wire with a 5/16" ring terminal may be placed under one of the four AP mounting bolts to ground it.
- The RPMA and GPS antenna connections to the AP and the RF surge protector must be completely weather sealed with wireless industry approved methods. The most common methods are:
  - Butyl tape wrapped with a, UV rated, high quality 3/4" electrical tape such as 3M Scotch 33+
  - Heavy duty adhesive lined heat shrink tubing applied with a heat gun
- See section 3.2.13 Outdoor Installation Hardware for additional weatherproofing plug for RJ-45 Amphenol connector (furnished by others) when installing RPMAAP10x.

6 Hardware Installation Verification

6.1 Power Verification

Prior to applying power to the AP, confirm with a Digital Voltmeter (DVM) that the DC voltage is correct at the PoE injector. The DC voltage should be between 48 VDC and 54 VDC.

> **NOTE:** The AP its self is not polarity sensitive, however, it is recommended that the barrel of the PoE power plug be at ground potential if the power system is grounded.

6.2 AP Antenna and GPS Cable DVM Test

Prior to weather sealing the AP antenna and GPS antenna connectors, disconnect both cables at both ends and verify continuity between center pins and verify that neither cable is shorted.
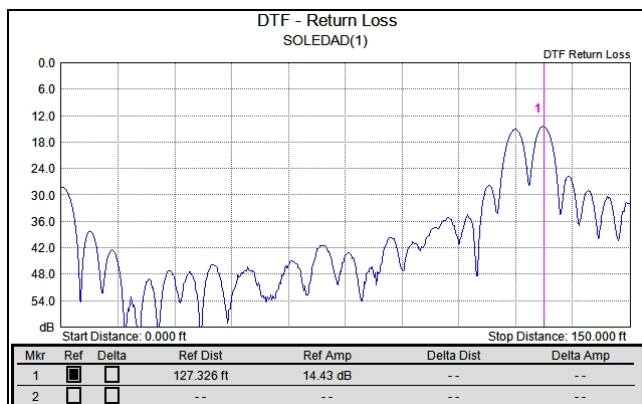
6.3 Antenna System Sweep Testing

The combined RPMA antenna system (including the antenna, cables, and lightning suppressor) should be "sweep tested" for Return Loss and Attenuation using an antenna analyzer such as an Anritsu Site Master™. The antenna system should be swept across the frequencies of interest, 2.400 GHz – 2.500 GHz. The Return Loss should be greater than 17 dB across the frequency range and the total attenuation should be as low as possible, generally less than 5 dB. The antenna system attenuation (loss) should be noted for use when configuring the AP within the EMS system.

If the Return Loss is not acceptable, the antenna should be disconnected and the antenna line should be terminated with a 50 ohm load. The Return Loss test should be repeated. If the antenna line Return Loss is now greater than 20 dB and is flat across the frequency range, the antenna should be replaced. If the Return Loss is not acceptable, the antenna cable system should be tested using the Distance to Fault (DTF) capability in the antenna analyzer to locate the problem.

Figure 12. Return Loss
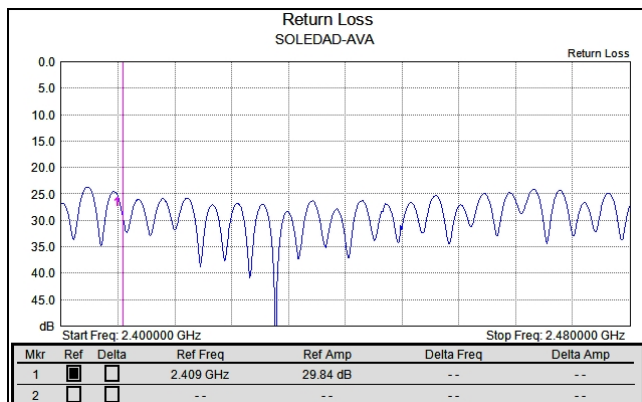
Notes:

- Measurement is required to be > 20 dB for coaxial cable and connectors.
- Overall return loss with antenna should be > 17 dB.

Figure 13. Distance to Fault

6.4 Grounding

Verify that the mounting hardware, AP, antenna cable, and lightning suppressor are properly grounded.

6.5 Connector Weather Sealing

Verify that all outdoor connectors are properly weather sealed.

6.6 Mounting Hardware

Verify that all mounting hardware is tight and secure.

Notes:

- Measurements should be taken with the antenna as well as with a 50Ω terminating load.
- Type and length of coaxial cable should be recorded for each run.

7 AP Software Configuration via Web Interface

The AP web interface can be accessed with a web browser connected locally at the data port of the PoE injector or remotely through the backhaul network. Ingenu recommends that you use one of the following internet browsers when using the AP web interface:

- Microsoft Internet Explorer® 8 or higher
- Mozilla Firefox®, any version
- Google Chrome™, any version
    NOTE: The AP web interface described in this chapter is compatible with AP software version 8.X and System Release 3.0.X.

7.1 Initial AP Network Configuration Prior to Installation

The AP is shipped with the following factory default IP Network Settings:

- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Default Router: 192.168.1.254

This section covers the minimum IP network configuration required to establish remote connectivity with the AP. This configuration must be performed prior to AP installation or on-site immediately following the physical AP installation. In most cases, it is strongly recommended that the initial configuration be performed prior to installation.

Refer to Figure 7 for the connections required to configure an AP. If the AP is being installed with a 3/4G wireless modem for backhaul, refer to section 7.1.1. If the AP is being installed with any other type of customer-provided IP backhaul, refer so section 7.1.2.

7.1.1 Initial AP Network Configuration for 3/4G Wireless Backhaul Modem

When activating the 3/4G wireless modem, a static IP address is required from the wireless carrier. The LAN side of the 3G modem can be configured to support the default IP network settings of the AP. This avoids the need to change these default settings in the AP. After the AP is installed, a connection to the AP can be established using the IP address of the 3/4G modem and the AP can be configured remotely. Refer to the *RPMA 3/4G Modem Configuration Guide* for additional information.

7.1.2 Initial AP Network Configuration for Customer Backhaul Modem

The default IP network settings for the AP must be changed to allow connection to the AP over the customer's IP network. To make these changes, perform the following steps:

- Log into the AP as described in section 7.2.
- After successfully logging into the AP, select "Admin" in the upper right corner of the screen.

- From the Admin menu, select the Network submenu.
- Follow the instructions in section 7.7.2 to make the required changes to the IP address, Netmask, and Default Router.
- When you have completed the changes, be sure to click on the **Save** button and then click on the **Reboot Access Point** button.
- After these changes are made and the customer's firewall and routers have been properly configured, the AP can be remotely configured.

For additional support with AP configuration, contact the Ingenu's Network Operations Center (NOC) Team at support@ingenu.com.

7.2 Login

The AP has a factory default IP Address of 192.168.1.1 which allows connection to the AP configuration page using https protocol on port 443.

- To access the AP configuration page, ensure the following:
- You are on the same subnet with the AP or your router can route to the AP IP address. The AP's default router setting is 192.168.1.254.
- You have access to port 443 on the firewall
- Open your web browser.
- In the address bar of the browser, type https://192.168.1.1. A dialog box opens that looks similar to the following:
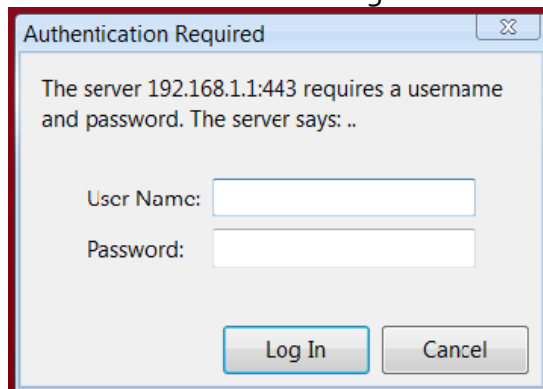

Figure 14. Username and Password Prompt

- Enter the default User Name and Password.
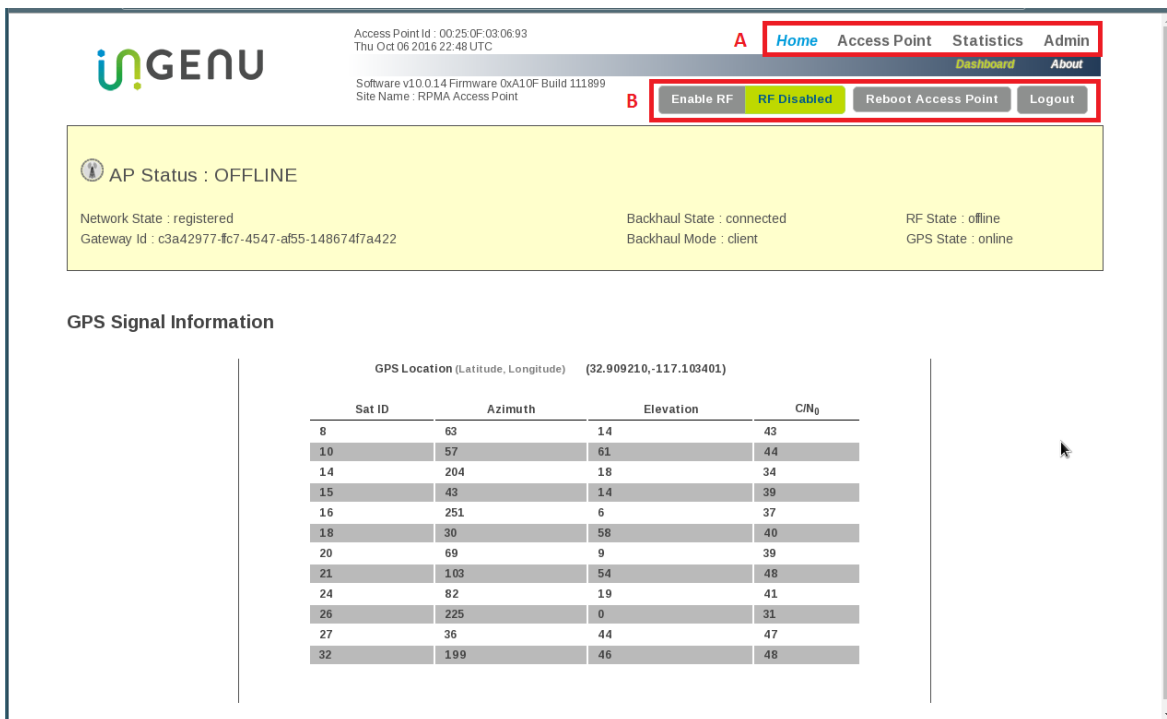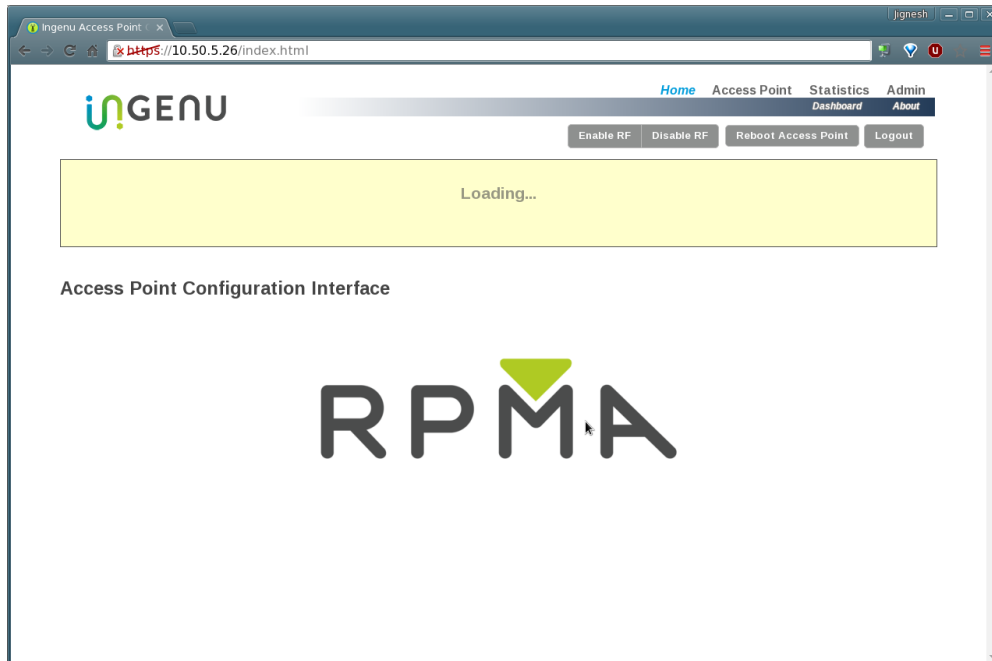
    User Name: `admin`

    Password: `onramp`

- Click on the **Log In** button.

    NOTE: After you log in, Ingenu strongly recommends that you change from the default password to a personalized password. For instructions on how to do this, refer to section 7.7.1 Security Submenu.

7.3 AP Web Pages

- After logging in, the page shown below is briefly displayed while the Home page is loaded.

The following information is displayed at the top of the Home page and all other web pages, Access Point ID, current date, software and firmware versions, and site name.

Additionally, there is a "status box" that provides AP status, network state, Gateway ID, backhaul state, backhaul mode, RF state, and GPS state.

Block A above shows the four main menus (i.e., Home, Access Point, Statistics, and Admin) that can be used to navigate to different configuration pages. Below **Block A** are the Home page submenus, Dashboard and About.

Block B shows four buttons that allow you to do the following:

- **Enable/Disable RF**
  If the RF is disabled, the AP is still connected to the Gateway.
- **Reboot the AP**
  After making configuration changes, this button is used to reboot the Access Point in order for the changes to take effect.
- **Logout**
  This button allows you to completely log out of the system.

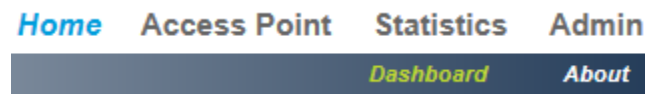All of the menus and their submenus are described in the following sections.

NOTE:

7.4 Home Page

Home	Access Point	Statistics	Admin
	Dashboard	About	
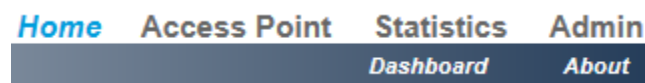
On the Home Page, there are two submenus—Dashboard and About.

7.4.1 Dashboard Submenu

Home	Access Point	Statistics	Admin
	Dashboard	About	

The Dashboard is the initial screen that is displayed after logging in (shown below). The Dashboard displays GPS signal information and is the initial submenu displayed after logging in. (shown below)

GPS Signal Information

GPS Location (Latitude, Longitude)   (33.014244,-117.094604)

| Sat ID	Azimuth	Elevation	C/N$_0$
7	313	53	36
6	61	23	33
20	177	9	31
19	109	27	38
3	81	34	35
13	69	76	41
28	216	15	33
23	120	55	38
16	40	19	34
8	282	31	35
10	282	36	40
5	324	2	19

If the GPS antenna is connected to the AP GPS information is shown.

NOTE: GPS status verification MUST occur after completion of physical AP installation. The columns on this screen are defined in the following table. The rows show the number of GPS satellites to which the AP receiver is currently locked. Five satellites are required for GPS synchronization but a minimum of nine satellites are required for reliable operation.

Table 3. Fields on the Access Point Screen

Column Heading	Description
Sat ID	The Sat ID column provides the name of the GPS satellite to which the AP is locked or is tracking.
Azimuth	The Azimuth is the direction of a GPS satellite, measured clockwise around the observer's horizon from north. Azimuth and altitude or elevation are usually used together to give the direction of an object in the topocentric coordinate system.
Elevation	The elevation (sometimes called altitude) is the angle at which we see the satellite when we look up into the sky.
C/N_o	Carrier to Noise (C/N_o) density ratio is the ratio of the carrier or signal power to the white-noise spectral density. For the AP GPS receiver to lock to the GPS satellite, the C/N_o should be greater than 20 dB-Hz.

7.4.2 About Submenu
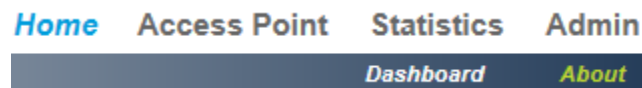
The About screen displays device specifications for the AP such as manufacturer, device type, MAC address of the AP, hardware, firmware, and software versions. There is nothing to configure on this screen, therefore the fields cannot edited.

Device Specification

Manufacturer	On-Ramp Wireless Inc.
Device Type	Access Point
MAC Address	00:25:0F:03:06:93
Hardware Version	AP_MAIN : 510-0000-00 REV 0
	AP_RF : 510-0000-00 REV 0
Firmware Version	0xa10f
Software Version	10.0.14

7.5 Access Point Menu

The Access Point menu has the following submenus:

- RPMA Config
- Field Config
- Backhaul Config
- Site Survey

7.5.1 RPMA Config Submenu

The RPMA Configuration screen (shown below) displays network configuration parameters at the time the AP was deployed.

The following table defines the fields on this screen. To edit these fields, click on the **Disable RF** button. After you make the changes, click on the **Save** button and then the **Enable RF** button.
NOTE: If you disable the RF, the AP is still connected to the Gateway.

Table 4. Fields on the RPMA Configuration Screen

Field	Unit	Description
AP ID	Decimal	The identification number for the AP. Range is 1 – 255.
Deployment Region ID	Decimal	The identification number for the region where the AP is deployed. Number range is 0 – 4228250625.
System ID	Decimal	The System Identification Number. Range is 0 – 255.
Channel	Decimal	The channel on which the AP communicates. Range is 1 – 41.
Reuse Code	Decimal	Different Reuse Codes allow two APs to operate on the same Channel and System ID without interference. Range is 0 – 255.
Center Frequency	MHz	This field is not editable. The value for center frequency is determined from the setting for the Channel field.

Field	Unit	Description
Broadcast Gold Code	Hex	This field is not editable. The value for the broadcast gold code is determined from the information provided in the following fields: ■ System ID ■ Channel ■ Reuse Code
Max Uplink PDUs (High Capacity)	Decimal	The maximum number of PDUs allowed on the uplink. Range is 4 – 16. The default setting is 4.
Max Uplink PDUs (Low Latency)	Decimal	The maximum number of PDUs allowed on the uplink. Range is 2 – 16. The default setting is 16.
UL Overload Alarm Threshold	dBm	This alarm triggers when the threshold for uplink capacity has been reached. Range is 0 – 31.
Interference Alarm Threshold	dBm	This alarm triggers when the threshold for interference on the uplink has been reached. Range is 0 – 31.

7.5.2 Field Config Submenu

The Field Configuration screen (shown below) displays RF configuration parameters that are set during AP configuration. These parameters are set to meet regulatory requirements in the country where the AP is deployed.

The following table defines the fields on this screen. To edit these fields, click on the **Disable RF** button. After you make the changes, click on the **Save** button and then the **Enable RF** button.

NOTE 1: If you disable the RF, the AP is still connected to the Gateway.

NOTE 2: The maximum transmit power for the AP and the Node is based on the setting in the **Regulatory Domain** field.

Table 5. Parameters on the Field Configuration Screen

Field	Unit/Format	Description
Reset Broadcast Margin	Boolean	Resets the broadcast margin. The AP stays in this state until the next time it is rebooted.
Force Scan Day	yyyy/mm/dd	The date to perform a Force Scan.
Broadcast Spreading Factor	N/A	Options are: ■ 2048 (High Capacity) ■ 256 (Low Latency)
Online Duration Without GPS Fix	seconds	The length of time allowed for the AP not to have a GPS fix. The default is 600 seconds.
AP Transmit Parameters *(These parameters are based on regulatory domain, AP cable loss, and target excess SNR)*		
Regulatory Domain	string	The regulatory domain where the AP is deployed. The regulatory domain limits the maximum transmit power for the AP.
Filter	Boolean	The default value is set according to country-specific regulatory requirements.
Filter Type	N/A	Options are: ■ cavity ■ diplexer

Diplexer Type	N/A	Options are:
		■ Channel 1 = SBAND1 & Channel 2 = SBAND4
		  − Ingenu PN 250-0041-00, or equivalent
		■ Channel 1 = SBAND1 & Channel 2 = SBAND3
		  − Ingenu PN 250-0046-00, or equivalent
		■ Channel 1 = SBAND2 & Channel 2 = SBAND4
		  − Ingenu PN 250-0047-00, or equivalent
		  where:
		    ▪ SBAND1 = 2401.5-2406.5MHz
		    ▪ SBAND2 = 2421.4-2428.4MHz
		    ▪ SBAND3 = 2445.2-2452.2Mhz
		    ▪ SBAND4 = 2471.1-2476.2Mhz

Diplexer Channel	N/A	Options are: ■ Channel 1 ■ Channel 2
Channel	Decimal	The channel on which the AP communicates. Range is 1 – 45 depending on Regulatory Domain and Diplexer Type.

Field	Unit/Format	Description
AP Maximum EiRP Target	dBm	The maximum EiRP output targeted for the AP.
AP Cable Loss	dB	AP cable loss measured in dB.
AP Antenna Gain	dBi	This is the gain specified for the AP antenna installed.
AP Antenna Height	String	This stores the height of AP Antenna
AP Maximum Transmit Power at internal SMA	dBm	This field is not editable. The value is determined by the settings for the other AP Transmit Parameters.
Node Transmit Parameters *(These parameters are based on regulatory domain, Node cable loss, and target excess SNR)*		
Node Type	String	Options are: ■ unode1 ■ phoenix
Node Transmit Constraint Type	N/A	This field is not editable. The value is determined by the settings for Regulatory Domain.
Node Transmit Constraint Limit	dBm	This field is not editable. The value is determined by the settings for Regulatory Domain.
Node Transmit Constraint Limit 2	dBm	This field is not editable. The value is determined by the settings for Regulatory Domain.
Node Transmit Constraint Antenna Gain Threshold	dBm	This field is not editable. The value is determined by the settings for Regulatory Domain.
Node Maximum EiRP Target	dBm	The maximum EiRP output targeted for the Node.
Node Cable Loss	dB	Default setting is 0 dB. Contact Ingenu (support@ingenu.com) prior to changing this parameter.
Node Antenna Gain	dBi	Default setting is 2 dBi. Contact Ingenu (support@ingenu.com) prior to changing this parameter.
Node Maximum Transmit Power	dBm	This field is not editable. The value is determined by the settings for Regulatory Domain and the other Node Transmit Parameters.
Power Control Parameters		
Target Excess SNR	dB	Default setting is 1 dB. Contact Ingenu (support@ingenu.com) prior to changing this parameter.
Maximum BCH Power Control Target	dB	The default value is set according to country-specific regulatory requirements.
Minimum BCH Power Control Target	dB	The default value is set according to country-specific regulatory requirements.
Link Budget		
Uplink	dB	This field shows the total amount of link budget available for the uplink and is not editable.
Downlink	dB	This field shows the total amount of link budget available for the downlink and is not editable.

Field	Unit/Format	Description
AP Maximum EiRP (Actual)	dBm	The actual maximum EiRP output for the AP.
Node Maximum EiRP (Actual)	dBm	The actual maximum EiRP output for the Node.

7.5.3 Backhaul Config Submenu

The Backhaul Configuration screen (shown below) displays configuration parameters that were set at the time the AP was deployed.

The following table defines the fields on this screen. To edit these fields, click on the *Disable RF* button. After you make the changes, click on the *Save* button and then the *Enable RF* button.
NOTE: If you disable the RF, the AP is still connected to the Gateway.

Table 6. Fields on the Backhaul Configuration Screen

Field	Unit	Description
Control Socket Mode	N/A	Options for this field are as follows: ■ **Server:** When the AP is set to work in Server mode, it listens for a TCP connection with the RPMA Gateway on port number 2021. See descriptions below for setting the following fields. ■ **Client:** When the AP is set to work in Client mode, the AP requests service from the RPMA Gateway. See the field descriptions below for setting the following fields.
Control Server Port Number	N/A	The port number when the AP is set to Server mode. When the AP is in Server mode, this field should be set to 2021. The AP listens on port 2021 for a TCP connection with the RPMA Gateway. Ensure that port 2021 is allowed on the firewall in your network.
Gateway Hostname/IP Address	N/A	■ For Server mode, this field is grayed out and not accessible. ■ For Client mode, the RPMA Gateway IP Address or Fully Qualified Domain Name (FQDN) should be entered here.
Gateway Port Number	N/A	■ For Server mode, this field is grayed out and not accessible. ■ For Client mode, this field should be set to 5051. Ensure that port number 5051 is allowed on the network firewall.
Enable HTTP Tunneling?	N/A	Options for this field are: Yes or No. When **Yes** is selected, the following option is available: **Use HTTP Tunneling Proxy?** The options for this parameter are also Yes or No. When **Yes** is selected, the following parameters are available to configure: ■ **HTTP Proxy IP Address:** The IP address of the http proxy server to use ■ **HTTP Proxy Port Number:** The port number of the http proxy server to use ■ **HTTP Proxy User Name:** This is optional. ■ **HTTP Proxy Password:** This is optional.
Online Duration Without Backhaul Connection	seconds	The length of time allowed for the AP not to have a GPS fix. The default is 600 seconds.
Keep-Alive Interval	seconds	The number of seconds allowed for the interval where the AP checks the link to the network to determine whether the link is still "alive" or broken.
Message Tx Timeout	seconds	The number of seconds allowed before the AP times out and stops trying to transmit a message.

7.5.4 Site Survey Submenu

The Site Survey screen (shown below) allows you to run a site survey, select the appropriate channel on which the AP operates, and determine the number of frames per channel. It also allows you to download survey results (sorted by RSSI or channel) and download diagnostic results.

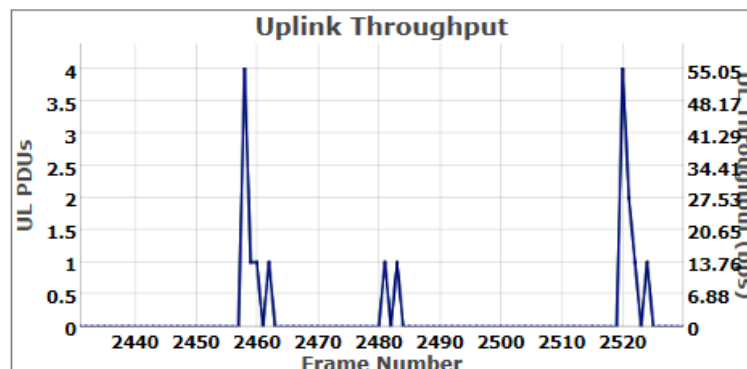**Site Survey**

7.6 Statistics Menu

The Statistics menu has the following submenus:

- Throughput
- Counters

7.6.1 Throughput Submenu

The Throughput screen (shown below) provides a graph of uplink throughput in bits per second.

Total Reach Network Link Statistics

7.6.2 Counters Submenu

The AP Counters screen (shown below) provides various counters for uplink and downlink.

AP Counters

Counters	Value
Missed UL Count	0
Uplink Pdu Count	0
Downlink Pdu Count	0
Uplink Control Sdu Count	0
Downlink Control Sdu Count	0
Downlink Acked Control Sdu Count	0
Uplink Data Sdu Count	0
Uplink Stream1 Data Sdu Count	0
Uplink Stream2 Data Sdu Count	0
Downlink Data Sdu Count	0
Downlink Acked Data Sdu Count	0

7.7 Admin Menu

Home	Access Point	Statistics	Admin
	Security	Network	Logs

The Admin menu has the following submenus:

- Security
- Network
- Logs

7.7.1 Security Submenu

The following Security Configuration screen provides information related to system services, administrator password, and SNMP configuration.

The following table defines the fields on this screen.

Table 7. Parameters on the Security Configuration Screen

Field	Description
System Services	
Preferences	Options are: ■ Disable Tenet login? ■ Enable SSL for Sockets?
Change 'admin' Password	
Old Password	To change the password, you must first enter the old password.

Field	Description
New Password	Enter the new password.
Re-type to Confirm	Re-type the new password to confirm the change.
SNMP Configuration	

Version	Options are:
	■ **Enable SNMPv2c?**
	If this is selected, the following options are available:
	  ❒ Transport
	  ❒ Community
	  ❒ Write Community
	These options are defined below.
	■ **Enable SNMPv3?**
	If this is selected, the following options, in addition to those listed above for SNMPv2C, are available:
	  ❒ Minimum Security Level
	  ❒ User Name
	  ❒ Authentication Protocol
	  ❒ Authentication Password
	  ❒ Privacy Protocol
	  ❒ Privacy Password
	These options are defined below.

Transport	Options are: ■ **Enable SNMP over UDP?** If this is selected, enter the port number. ■ **Enable SNMP over TCP?** If this is selected, enter the port number.
Community	Specifies SNMPv2c community string (password) for read-only access to the full tree of SNMP managed objects on the AP. Default value is **Public**.
Write Community	Specifies SNMPv2c community string (password) for read-write access to the full tree of SNMP managed objects. The default value is **Private**.
Minimum Security Level	Specifies SNMPv3 minimum security level. From the dropdown menu, the options are: ■ **No Auth No Priv** Allows unauthenticated requests. ■ **Auth No Priv** Allows authenticated requests without privacy or encryption. ■ **Auth Priv** Allows authenticated requests with privacy to enforce use of encryption.
User Name	Specifies an SNMPv3 user that will be allowed read-only or read-write access to the full tree of SNMP-managed objects on the AP.
Authentication Protocol	Specifies the hash algorithm to use for authentication of SNMPv3 requests. From the dropdown menu, the options are: ■ **MD5:** The cryptographic hash function as specified by IETF RFC 1321. ■ **SHA:** The Secure Hash Algorithm function as specified by NIST standard FIPS 180-4.
Authentication Password	Specifies the passphrase used for authentication of SNMPv3 requests.

Field	Description
Privacy Protocol	Specifies the privacy protocols to use for encryption of SNMPv3 requests. From the dropdown menu, the options are: ■ **DES:** The Data Encryption Standard algorithm for encryption as specified by NIST standard FIPS 46-3. ■ **AES:** The Advanced Encryption Standard algorithm for encryption as specified by NIST standard FIPS PUB 197.
Privacy Password	Specifies the passphrase used for encryption of SNMPv3 requests.

NOTE: To increase network security, it is recommended that you check the boxes to *"Disable Telnet login"* and *"Enable SSL for Sockets."* It is also recommended that you change the default passwords for the following fields:

- ❑ Admin Password
- ❑ Community
- ❑ Write Community
- ❑ Authentication Password
- ❑ Privacy Password

7.7.2 Network Submenu

The Network Configuration screen (shown below) allows you to change the AP IP address, netmask, and default router as well as other network configuration parameters such as Ethernet speed and MTU, duplex mode, and DNS and NTP servers.

Network Configuration

IPv4 Settings	Automatic (DHCP)	**Manual (Static IP)**
IP Address	192.168.1.1	
Netmask	255.255.255.0	
Default Router	192.168.1.254	
Ethernet Speed	Auto ▾	
Duplex Mode	Auto ▾	
Ethernet MTU	1500	
DNS Servers	10.141.123.18	
NTP Servers	ntp.m2m	
	Save	

The following table defines the fields on this screen.

Table 8. Fields on the Network Configuration Screen

Field	Description
IPv4 Settings	Currently the AP only supports two IP settings for TCP/IP Versions: ■ **Automatic (DHCP):** This setting is used to request a dynamic IP address from a local DHCP server. ■ **Manual (Static IP):** This setting is used for configuring a fixed IP address.
IP Address	IP address of the AP (e.g., default is 192.168.1.1)
Netmask	The default is 255.255.255.0.
Default Router	The default is 192.168.1.254.
Ethernet Speed	The speed at which data travels over the Ethernet connection. Setting options are: Auto, 10 Mbit, and 100 Mbit. The default setting is "Auto" which monitors the connection and displays the current speed.
Duplex Mode	Setting options are: Auto, Half-Duplex, and Full-Duplex. The default setting is "Auto" which displays the current duplex mode.
Ethernet MTU	The largest frame size that can be transmitted over the network. The default setting is 1500 bytes. Messages longer than the Ethernet MTU indicated in this field must be divided into smaller frames.
DNS Servers	The IP address of the DNS server can be set in this text field. Multiple DNS servers can be configured for an AP by separating the IP addresses of each DNS server with a comma when entering them into the text field. The following DNS server addresses are the defaults: ■ `208.67.222.222` ■ `208.67.220.220` ■ `8.8.8.8` ■ `8.8.4.4`
NTP Servers	The AP should be configured with valid NTP servers for correct time synchronization. If the AP is not configured, it may have problems connecting to the RPMA Gateway using SSL. The following NTP server addresses are the defaults: ■ `nist1-nj.ustiming.org` ■ `nist1-atl.ustiming.org` ■ `nist1-la.ustiming.org` ■ `nist1-sj.ustiming.org` ■ `nist1-lv.ustiming.org` ■ `time.nist.gov` As with DNS server configuration, multiple NTP server IP addresses can be entered into this text field separated with commas.

❐
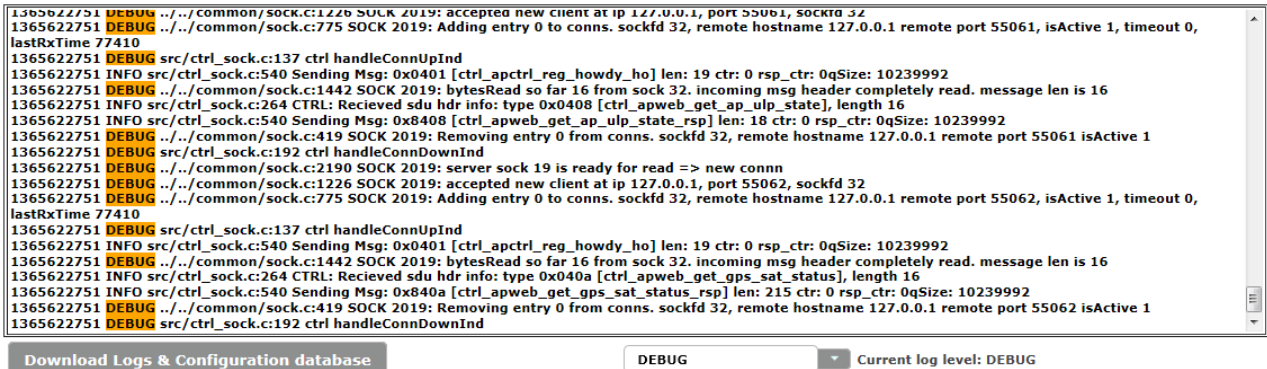
7.7.3 Logs Submenu

The Logs screen (shown below) allows you to download AP logs. By clicking on a dropdown menu, you can choose from five log levels that provide various levels of detail:
- ■ *Critical:* This setting shows only critical log information.
- ■ *Error:* This setting shows error and critical log information.
- ■ *Warning:* This setting shows warning, error, and critical log information.
- ■ *Informational:* This setting shows informational, warning, error, and critical log information.

- **_Debug:_** This setting shows debug, informational, warning, error, and critical log information.

```
1365622751 DEBUG ../../common/sock.c:1226 SOCK 2019: accepted new client at ip 127.0.0.1, port 55061, sockfd 32
1365622751 DEBUG ../../common/sock.c:775 SOCK 2019: Adding entry 0 to conns. sockfd 32, remote hostname 127.0.0.1 remote port 55061, isActive 1, timeout 0,
lastRxTime 77410
1365622751 DEBUG src/ctrl_sock.c:137 ctrl handleConnUpInd
1365622751 INFO src/ctrl_sock.c:540 Sending Msg: 0x0401 [ctrl_apctrl_reg_howdy_ho] len: 19 ctr: 0 rsp_ctr: 0qSize: 10239992
1365622751 DEBUG ../../common/sock.c:1442 SOCK 2019: bytesRead so far 16 from sock 32. incoming msg header completely read. message len is 16
1365622751 INFO src/ctrl_sock.c:264 CTRL: Recieved sdu hdr info: type 0x0408 [ctrl_apweb_get_ap_ulp_state], length 16
1365622751 INFO src/ctrl_sock.c:540 Sending Msg: 0x8408 [ctrl_apweb_get_ap_ulp_state_rsp] len: 18 ctr: 0 rsp_ctr: 0qSize: 10239992
1365622751 DEBUG ../../common/sock.c:419 SOCK 2019: Removing entry 0 from conns. sockfd 32, remote hostname 127.0.0.1 remote port 55061 isActive 1
1365622751 DEBUG src/ctrl_sock.c:192 ctrl handleConnDownInd
1365622751 DEBUG ../../common/sock.c:2190 SOCK 2019: server sock 19 is ready for read => new connn
1365622751 DEBUG ../../common/sock.c:1226 SOCK 2019: accepted new client at ip 127.0.0.1, port 55062, sockfd 32
1365622751 DEBUG ../../common/sock.c:775 SOCK 2019: Adding entry 0 to conns. sockfd 32, remote hostname 127.0.0.1 remote port 55062, isActive 1, timeout 0,
lastRxTime 77410
1365622751 DEBUG src/ctrl_sock.c:137 ctrl handleConnUpInd
1365622751 INFO src/ctrl_sock.c:540 Sending Msg: 0x0401 [ctrl_apctrl_reg_howdy_ho] len: 19 ctr: 0 rsp_ctr: 0qSize: 10239992
1365622751 DEBUG ../../common/sock.c:1442 SOCK 2019: bytesRead so far 16 from sock 32. incoming msg header completely read. message len is 16
1365622751 INFO src/ctrl_sock.c:264 CTRL: Recieved sdu hdr info: type 0x040a [ctrl_apweb_get_gps_sat_status], length 16
1365622751 INFO src/ctrl_sock.c:540 Sending Msg: 0x840a [ctrl_apweb_get_gps_sat_status_rsp] len: 215 ctr: 0 rsp_ctr: 0qSize: 10239992
1365622751 DEBUG ../../common/sock.c:419 SOCK 2019: Removing entry 0 from conns. sockfd 32, remote hostname 127.0.0.1 remote port 55062 isActive 1
1365622751 DEBUG src/ctrl_sock.c:192 ctrl handleConnDownInd
```

| Download Logs & Configuration database | | DEBUG ▼ | Current log level: DEBUG |

Only the last 100 log entries are shown on this screen. To see additional log entries, you can download the logs and configuration database by clicking on the "**_Download Logs & Configuration database_**" button. When you click on this button, a pop-up dialog box appears asking whether you would like to open or save the "ap.tgz" file. The compressed tar file contains two folders: "onramp" and "tmp." The file structure is shown below.

```
AP
├── onramp
│       └── db
│               └── config.db
└── tmp
        └── ap.log
```
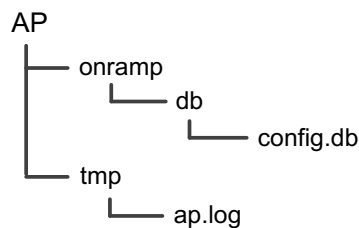
The "config.db" file is the configuration file for the SQLite database used in the AP and the "ap.log" file is the log file for the AP.

8 AP Communication Troubleshooting

Before you leave the installation site, contact your network operations center (NOC) to verify that the AP is online and successfully communicating. If remote communication with the AP is not possible, perform the following steps:

1. Manually configure the following on a laptop:
   - ❑ The IP address of the Ethernet port
   - ❑ Netmask setting
   - ❑ The Default Router setting
2. Unplug the backhaul connector from the data port of the PoE and connect the laptop to that port.
3. Verify that you can locally log in to the AP as described in section 7.2.
   - ❑ If you can successfully log in, further testing of the backhaul and its configuration is needed.
   - ❑ If you cannot log in, check the IP setting of your laptop.
   - ❑ If no problems are found, refer to the Chapter 9: Troubleshooting Guide.

The following figure illustrates a method for detailed on-site debugging of an AP installation. The Ethernet hub allows the user to "sniff" Ethernet traffic between the backhaul port and the AP to troubleshoot and resolve any issues.
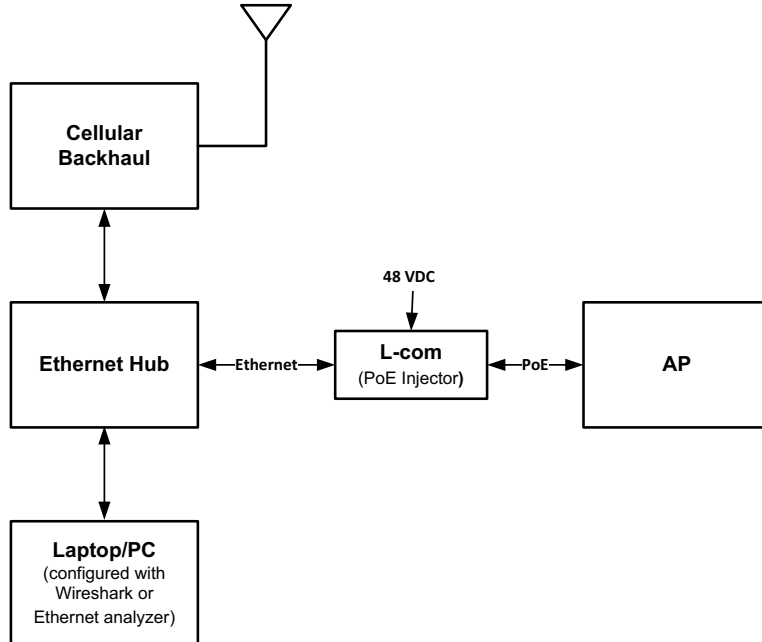
Figure 15. Sample Method for On-site Debugging of an AP Installation

9 Troubleshooting Guidelines

Use the following table to help troubleshoot a problem.

Table 9. Troubleshooting Guide

Problem	Action
AP does not power up (Status LED is not illuminated or flashing)	■ When the AP is powered, the Status LED illuminates or flashes. If not, check the Ethernet cable and connector for damage. ■ Verify that the PoE injector is connected properly (i.e., the AP is connected to Data + Power side). ■ Verify that a nominal voltage of 48 VDC is present at the power connector of the PoE. ■ Verify that the PoE injector is not defective by substituting another known working PoE. ■ Verify that the backhaul cable from the Data connector on the PoE injector is connected to a router, backhaul device, or laptop that is powered up. Connectivity is not required but the port must be active. ■ Contact Ingenu for assistance
AP does not acquire GPS	■ Verify that the GPS antenna cable and the AP antenna cable are connected and have not been swapped. If the connectors were swapped, it is necessary to power cycle the AP. ■ Disconnect both ends of the GPS. Verify continuity and that the cable is not shorted. ■ Verify the GPS antenna is not defective by substituting a known working GPS antenna. ■ Power cycle the AP ■ Contact Ingenu for assistance.
Link problem	■ Is the Link LED blinking? If not, check the Ethernet cable and connector for damage. ■ Verify that the PoE injector is connected to the WAN. ■ Connect a properly configured laptop to the data port on the PoE, as described in chapter 8, and attempt to log into the AP. If successful, troubleshoot the backhaul. ■ Contact Ingenu for assistance.

10 Preventive Maintenance

The recommended preventive maintenance schedule for the AP is shown in the following table. For additional assistance, contact Ingenu Customer Support at (858) 592-6008 or support@ingenu.com.

NOTE: Do NOT open the AP enclosure. Doing so voids the product warranty.

Table 10. Preventive Maintenance Schedule

Task	Frequency
1. Verify that all connections are tight and secure.	Annually
2. Verify that there is no visible damage to any wires or cables.	Annually
3. Ensure that the exposed connectors are properly sealed against weather conditions.	Annually
4. Verify that the AP door screws are tight and that the warranty seal is in place	Annually
5. Verify that all required grounds are connected and tight.	Annually
6. Verify that all mounts and bracket are securely attached.	Annually

Appendix A Site Survey Worksheet

Site Survey	Required Information	✓ Completed
Site name		
AP ID		
Site street address or other location information		
Site access information		
Landlord contact information		
Specific landlord requirements (Attach another sheet if there is significant information)		
Latitude		
Longitude		
Site type (building, tower, pole, or other)		
Height of existing structure		
AP equipment mounting location		
AP antenna mounting location and height		
Antenna line length required		
GPS mounting location		
GPS line length		
AP power type, commercial power, or solar solution		
Distance to commercial power, if available		
Photos of site including antennal location, AP location, and overall site (Attach all photos to this worksheet.)	See attachments.	
Other site-specific information		

010-0148-00 Rev D

Appendix B AP Configuration Worksheet

AP Configuration Parameter	Required information	✓ Completed
Site name		
AP Name		
AP ID		
Deployment Region ID		
AP physical configuration *(Outdoor, indoor, standalone, in cabinet, or other)*		
AP antenna gain		
AP antenna downtilt		
AP antenna cable type		
AP antenna cable length		
AP antenna cable loss		
Backhaul type		
Backhaul configuration information		
AP Static or DHCP IP address (Static or Dynamic?)		
AP IP address	(Default: 192.168.1.1)	
Netmask setting	(Default: 255.255.255.0	
Default router	(Default: 192.168.1.254)	
DNS servers		
NTP servers		
AP Socket mode, Server or Client	For System Release 2.1, the Client mode is always used.	
Server port number	This is not used for System Release 2.1.	
RPMA Gateway IP address		
RPMA Gateway port number	(Default: 5051)	
SNMP server address		
Channel assignment		
Reuse Code		

AP Configuration Parameter	Required information	✓ Completed

Appendix C Basic AP Specifications

The following table provides the basic specification information for the AP. For detailed product specifications, refer to the *Access Point Product Specification (014-0030-00).*

Size	Inches: 9.1"H x 8.1"W x 4.5"D Millimeters: 231mm H x 206 mm W x 114 mm D
Maximum Weight	Pounds: 9.6 Kilograms: 4.35
Operating Environment	Outdoors or indoors
Enclosure	IP66
Operating Temperature Range	-40°C to +80°C
Power Source Voltage Range (PoE)	38 – 56 VDC, Nominal 48 VDC Power over Ethernet
Current Consumption	0.35A maximum @ 48 VDC, .29A typical
Power Dissipation	17 Watts (maximum)
Antenna Connector	Type N, female
GPS Connector	Type N, female
GPS Antenna Type	Powered
Data and Power Connector	RJ45
GPS Power	3.3 VDC @ 50 mA maximum over coaxial cable

Appendix D Base Station Configuration

Table 11. RPMA Base Station Configuration Options

Base Station Option	Description	Applications	Required RPMA Hardware	Additional Items Required
Outdoor Cabinet Base Station AC Powered	■ Outdoor base station ■ 120/240 VAC powered system with 8 hours of battery backup ■ AP is located in the equipment cabinet along with a 4G modem and battery backup	Outdoor locations with AC power requiring 4G modem backhaul. For example: ■ Communication sites ■ Transmission Towers ■ Wood distribution poles ■ Outdoor Wall mount	■ Access Point ■ Outdoor equipment cabinet powered by 120/240 VAC and contains: ❒ One Integrated GPS antenna ❒ One 4G modem ❒ Two integrated 4G modem antennas ❒ Antenna surge suppressor ❒ Backup battery ❒ Alarm monitor ■ AP antenna	■ Customer-provided 4G Digi modem (WR-21) ■ Site-specific cable for the AP antenna ■ Site-specific installation hardware
Outdoor Cabinet Base Station DC Powered for Solar Applications	■ Outdoor base station ■ 12 VDC powered ■ AP is located in the equipment cabinet along with a 4G modem	Outdoor locations without AC power requiring 4G modem backhaul. For example: ■ Transmission Towers	■ Access Point ■ Outdoor equipment cabinet powered by 12 VDC and contains: ❒ One Integrated GPS antenna ❒ One 4G modem ❒ Two integrated 4G modem antennas ❒ Antenna surge suppressor ❒ Alarm monitor ■ AP antenna	■ Customer-provided Solar Power System designed for area of operation ■ Customer-provided 4G Digi modem (WR-21) ■ Site-specific cable for the AP antenna ■ Site-specific installation hardware

Base Station Option	Description	Applications	Required RPMA Hardware	Additional Items Required

Rack Mounted Base Station Kit (Indoor AP)	■ Indoor rack-mounted base station
	■ Contains a 19-inch rack 3RU shelf
	■ AP is mounted on the shelf
	■ Powered by either 120/240 VAC or 48 VDC
		Indoor rack mount environment with access to power and corporate IP network.
		For example:
		■ Communication site shelters
		■ IT equipment rooms
		■ Substation equipment rooms
			■ Access Point
			■ A 19-inch rack 3RU shelf including:
			  ❑ 120/240 VAC power supply
			  ❑ 48 VDC terminal strip/cable
			■ Antenna surge suppressor
			■ GPS antenna
			■ AP antenna
				■ Site-specific cables for the AP antenna and the GPS antenna
				■ Site-specific installation hardware

Rack Mounted Base Station Kit (Outdoor AP)	■ Rack-mounted base station
	■ Contains a 19-inch rack 3RU shelf
	■ Powered by either 120/240 VAC or 48 VDC
	■ AP is mounted outdoors
		Secure locations with indoor rack mount environment, power and access to corporate IP network. For example:
		■ Rooftop outdoor AP
		■ Tower-mounted AP
		■ Wood pole-mounted AP
			■ Access Point
			■ A 19-inch rack 3RU shelf including:
			  ❑ 120/240 VAC power supply
			  ❑ 48 VDC terminal strip/cable
			■ Antenna surge suppressor
			■ GPS antenna
			■ AP antenna
				■ Site-specific cables for the AP antenna and the GPS antenna
				■ Site-specific Ethernet cable between the shelf and the AP
				■ Site-specific installation hardware
				■ AP pipe mount (optional)

NOTE: All base stations require an external AP antenna. Specific country regulatory requirements may determine antenna type and gain. See examples below; ■ United States - 9 dBi omni, antenna with ≥3dBi cable loss normally used, other antenna gains may be used as long is 36 dBi maximum ERP is not exceeded ■ China – 10 dBi gain omni antenna required (Model OA-102425, or equivalent), +17dBm EIRP (Maximum) ■ Japan – 2 dBi or 4 dBi gain omni antennas normally used				

For information about any of these packages, contact your Ingenu representative at support@ingenu.com.

Appendix E Abbreviations and Terms

Abbreviation/Term	Definition
AP	Access Point. The RPMA component geographically deployed over a territory.
DL	Downlink
DNS	Domain Name System
DTF	Distance to Fault
DVM	Digital Voltmeter
EIRP	Equivalent Isotropically Radiated Power
EMS	Element Management System. The network component that provides a concise view of controls and alarms on the RPMA network.
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
GW	Gateway
IC	Industry Canada
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
NID	Node ID
NIST	National Institute of Standards and Technology
Node	The wireless RPMA Radio module developed by Ingenu that integrates with OEM sensors and communicates sensor data to an Access Point.
NTP	Network Time Protocol
PV	Photovoltaic
RF	Radio Frequency
RFID	Radio Frequency Identification
RPMA	Ingenu's proprietary wireless communication technology and network.
RSSI	Receive Signal Strength Indicator
SSL	Secure Socket Layer
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
UL	Uplink
UTP	Unshielded Twisted Pair