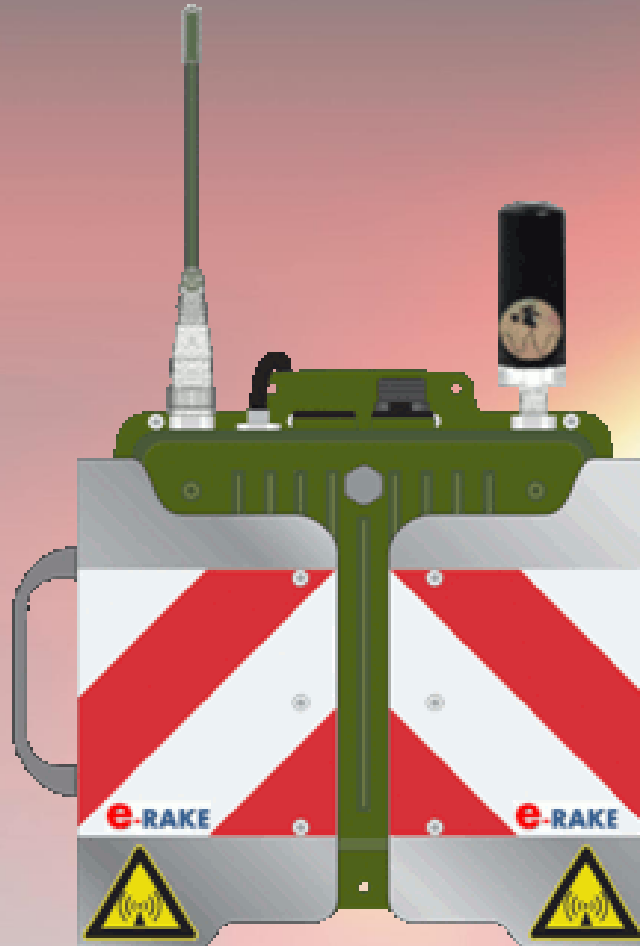




Manuel d'utilisation & de mise en service

Wi10 PWSA041-118 PWS (Station Radio autonome) e-Rake Series
OFDM TDMA Outdoor WAN –LAN Radio PMPT Backbone et accès WiFi



PWS User Manual

Wi10 PWSA041-118 PWS (portable wireless Station) e-Rake Series
Digital OFDM TDMA Outdoor WAN –LAN Wireless PMPT Backbone and WiFi AP

© Hypercable 201

e-RAKE

WIRELESS MOBILE MESH NETWORKS

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \lim_{n \rightarrow \infty} \left(\frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!} \right)$$

Table des matières

Sommaire

1	Introduction	4
1.1	Liste des Abréviations	4
1.2	Precautions de sécurité.....	4
1.3	Sécurité électrique.....	5
1.4	Radiations radio-électriques.....	5
1.4.1	Figure 1.....	6
1.4.2	Figure 2.....	6
2	Emetteur Récepteur Numérique Recommandations importantes	7
2.1	Precautions de sécurité.....	7
3	Guide sommaire de mise en service du Wi10 PWSA041-118.	8
3.1	ATTENTION SPECIALE I.....	8
3.2	ATTENTION SPECIALE II.....	9
3.3	ATTENTION SPECIALE III	9
4	DESCRIPTION MECANIQUE	9
5	TABLEAU DES RACCORDEMENTS.....	10
6	Appendice A: 400MHz TDMA fréquences intermédiaires	11
7	Simply User Guide for the PWSA041-118	11
8	MECHANICAL DESCRIPTION	13
9	Appendix A: 400MHz TDMA Radio Baseband frequency table.....	15
10	APPENDICE A:TABLEAU DES FRÉQUENCES INTERMÉDIAIRES DES RADIO TDMA 400MHZ.	15
11	Tableau d'harmonisation des canaux à utiliser	16
12	Channel plan of the Portable Wireless Station	16
13	Configurations of the 2.4GHz AP/Router	17
13.1	Connecting to the login page	17
14	Status Page.....	17
15	Easy Setup	17
15.1	Operation Mode – AP Bridge.....	18
16	Advanced Setup	18
16.1.1	Management.....	19
16.1.2	Advanced Settings	21

16.1.3 Operation Mode (Only AP Bridge mode works for PWS).....	22
16.2 Firewall Configuration.....	23
16.2.1 MAC/IP/Port Filtering	23
16.2.2 Virtual Server Settings	24
16.2.3 DMZ	26
16.2.4 Firewall	26
16.2.5 Content Filtering	27
16.3 Network Settings.....	28
16.3.1 WAN.....	28
16.3.2 LAN.....	32
16.3.3 Advanced Routing (unavailable in AP Bidge mode).....	33
16.4 Wireless Settings.....	34
16.4.1 Basic.....	34
16.4.2 Security.....	35
17 Appendix B: Demo links setting sample.....	41

Proprietary notice

The information presented in this guide is the property of Hypercable. No part of this document may be reproduced or transmitted without proper permission from Hypercable.

The specifications or information contained in this document are subject to change without notice due to continuing introduction of design improvements. If there is any conflict between this document and compliance statements, the latter will supersede this document.

Hypercable has no liability for typing errors in this document or damages of any kind that result from the use of this document.

To get up to date information about accessories and their availability, please contact sales representative.

Note: FODU/ODU does not contain serviceable parts. Warranty will not be applicable in the event FODU/ODU has been hermetically unsealed.

Note: Hypercable is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

Copyright Notice

Copyright © 2014 Hypercable. All rights reserved.

1 Introduction

Ce manuel décrit les instructions d'utilisation des émetteurs et récepteurs Hypercable

1.1 LISTE DES ABRÉVIATIONS

COFDM- procédé qui associe un codage de canal [OFDM](#) (*Orthogonal Frequency Division Multiplexing*) et une modulation numérique des signaux individualisés (sous-porteuses multiples).

128QAM – 128-Quadrature Amplitude Modulation

16APSK – 16-Amplitude and Phase Shift Keying

32APSK – 32-Amplitude and Phase Shift Keying

64QAM – 64-Quadrature Amplitude Modulation

AC – Alternating Current

ACM – Adaptive Coding and Modulation

AGC – Automatic Gain Control

ASCII - American Standard Code for Information Interchange

BNC connector - Bayonet Neill-Concelman coaxial connector

DC – Direct Current

FODU – Full Outdoor Unit

FTP – File Transfer Protocol

GUI – Graphical User Interface

IEEE - Institute of Electrical and Electronics Engineers

QPSK - Quadrature Phase-Shift Keying

RSL – Received Signal Level

RSSI – Received Signal Strength Indicator

Rx - Receive

SNMP - Simple Network Management Protocol

TCP/IP – Internet Protocol Suite (Transmission Control Protocol / Internet Protocol)

Tx - Transmission

1.2 PRECAUTIONS DE SÉCURITÉ

– l'Installation et l'usage doit être assuré par du personnel ayant reçu la formation appropriée et ayant l'expérience requise pour prévenir tous risques d'accident ou de dommages aux équipements et aux usagers.

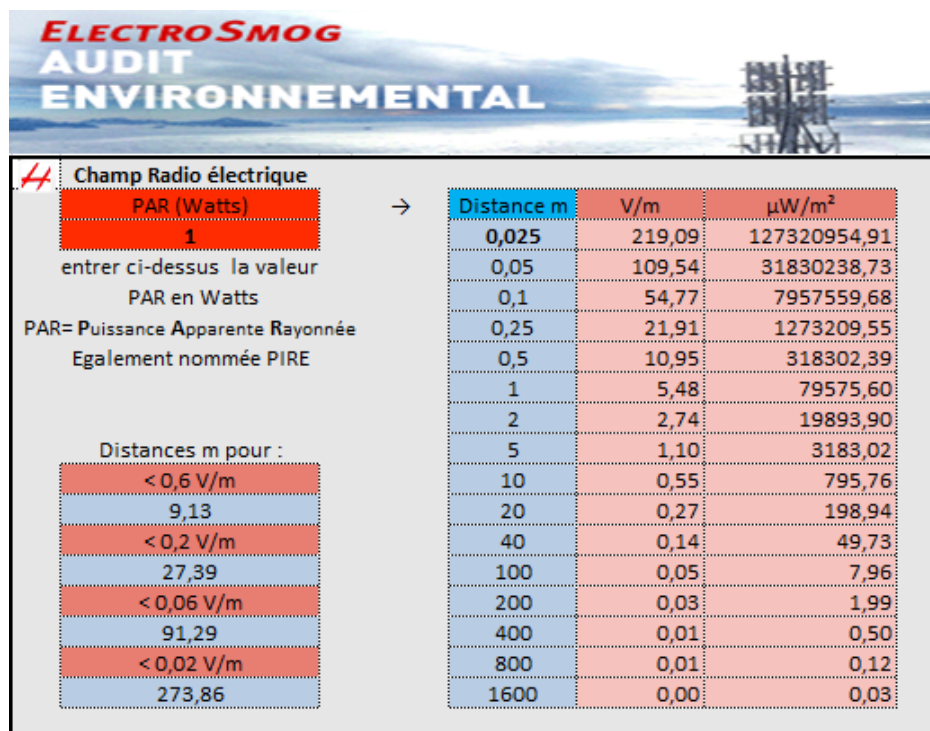
- Utiliser les équipements de secours et de sécurité requis pour le branchement des équipements aux sources électriques appropriées et aux antennes spécialement lors de l'installation des antennes.
- Ne pas utiliser d'autres composants ou visseries ou câbles et antennes qui ne seraient pas fournis ou recommandés par Hypercable.

1.3 SÉCURITÉ ÉLECTRIQUE

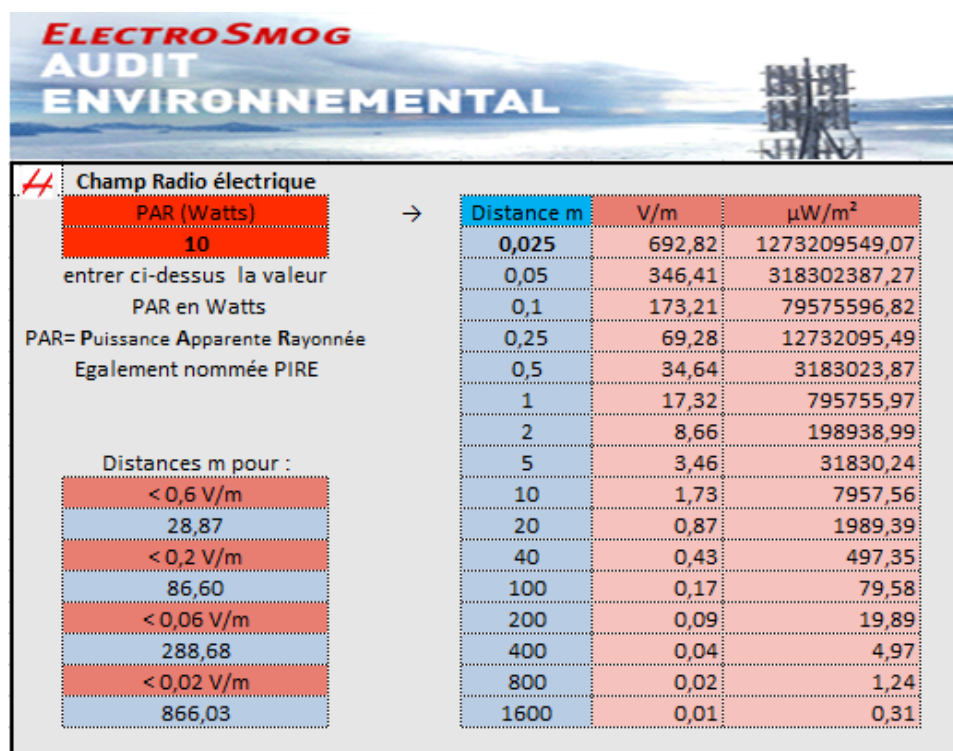
- Les équipements sont conformes a la norme I EN 60950 (protection contre les chocs électriques).
- Tous les circuits externes sont définis selon EN 60950.
- Tous les équipements sont reliés a la terre (ou équivalent) et aux antennes avant le raccordement a la source d'énergie et a la mise sous tension
- Pour la sécurité électrique l'alimentation secteur vers DC dispose d'une isolation renforcée.

1.4 RADIATIONS RADIO-ÉLECTRIQUES

- L'émetteur doit être éteint avant la déconnexion des antennes.
 - Il n'existe pas de radiation présentant un quelconque risque a proximité des antennes. Toutefois selon la puissance utilisée il est déconseillé de séjourner dans un champ de niveau supérieur à 28 volts/mètre. (Figure 1 pour 1 watt, Figure 2 pour 10 watts)



1.4.1 FIGURE 1.



1.4.2 FIGURE 2.

2 Emetteur Récepteur Numérique Recommandations importantes

2.1 PRECAUTIONS DE SÉCURITÉ

- L'installation et l'usage doit être assuré par du personnel ayant reçu la formation appropriée et ayant l'expérience requise pour prévenir tous risque d'accident ou de dommages aux équipements et aux usagers.
- Utiliser les équipements de secours et de sécurité requis pour le branchement des équipements aux sources électriques appropriées et aux antennes spécialement lors de l'installation des antennes.
- Ne pas utiliser d'autres composants ou visseries ou câbles et antennes qui ne seraient pas fournis ou recommandés par Hypercable.

Ce manuel explique les fonctions basiques de votre système fait « sur mesure ». Lisez le soigneusement avant l'utilisation des équipements.

Nous ne sommes pas responsables des dommages subis par les équipements en raison d'un usage inapproprié ou d'une erreur de manipulation.

Attention! Il est interdit d'utiliser ces produits pour créer des brouillages ou intercepter des messages ou des images dont vous n'êtes pas le destinataire. Référez vous aux règlements en vigueur dans votre pays.

Attention! Maintenez a une distance de l'ordre de 1.5 metres des antennes TX et RX de ces équipements d'autres antennes de type Télémétrie 968 Mhz ou autres systemes RF en harmonique 2, afin d'éviter des interférences par transmodulation de champs RF excessifs

Attention! Importantes recommandations concernant l'usage des batteries rechargeables , Lisez avec attention ! :

1. » utiliser le chargeur livré et recommandé pour le type de batteries
2. » Ne pas recharger hors contrôle et surveillance.
3. » En raison de la Haute densité d'énergie les batteries peuvent brûler ou exploser en cas de détérioration par surcharge ou de court circuit
4. » Tenir les enfants éloignés
5. » Lire le manuel avant usage
6. » installer en conformité avec le produit!

Battery type	NiMH-LSD	Li-Ion	LiFePO4
Self-discharge per month	1-2%	1-2%	3-5%
Charging level for storage	40-60%	50-70%	50-70%
Storage temperature	10-20°	15-25°	10-20°C
Re-charging interval	every year	every 2 years	every year

Intervales de recharge d'entretien

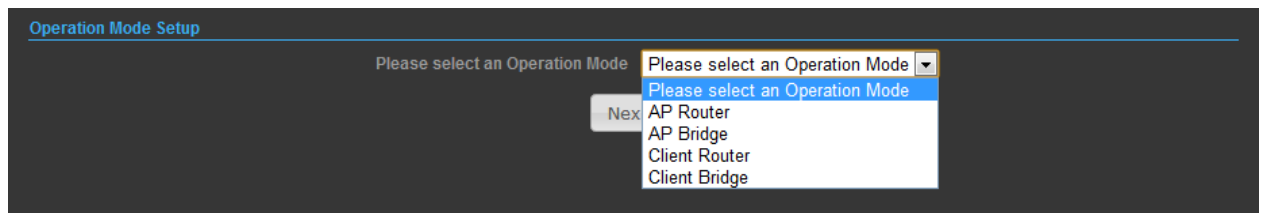
Une fois tous les ans

Une fois tous les 2 ans

une fois tous les ans

3 Guide sommaire de mise en service du Wi10 PWSA041-118.

1. Dans cet envoi 3 PWS sont déjà préconfigurés 1*BS et 2*CPE. Voir en dernière page l'Appendice B: configuration de test
2. La connexion via le port RJ-45 est connecté de prime abord a la radio 802.11 b/g/n 2.4GHz AP et ensuite renvoyé par le switch de l'AP WiFi vers la radio 400MHz. Le mode de fonctionnement de l'AP 2.4 GHz doit être ajusté en "AP Bridge mode" pour assurer que la connexion vers la radio 400MHz radio est bien ouverte.



3. Réglages par défaut du 2.4GHz AP
Default IP address: 192.168.2.1
User name: admin
Password: admin
4. Réglages par défaut du 400MHz TDMA radio
Default IP address: 192.168.2.2
User name: admin
Password: password

3.1 ATTENTION SPECIALE I

5. La bande de fréquence intermédiaire des radio 400MHz (440 ~ 500MHz) TDMA Radio est (2392 ~ 2452 MHz). Les performances du système sont altérées si la fréquence intermédiaire du 400/550 MHz est identique à celle utilisée pour le 802.11b/g/n 2.4GHz. Il est donc préférable de séparer de 10 Mhz les fréquences dans un même PWS.

Se référer aux fréquences intermédiaires Bande de base dans l'appendice

Appendice A : Tableau des fréquences intermédiaires des radio TDMA 400MHz.

3.2 ATTENTION SPECIALE II

Veiller avant toute mise sous tension à ce que les bonnes antennes sur les bonnes fréquences soient bien raccordées aux embases N coaxiales respectives

6. Alimentation "on" PWSA041-118:

Connecter le bloc radio sur la batterie via le câble équipé des connecteurs M12. Aux deux extrémités

Alimentation "off" PWSA041-118:

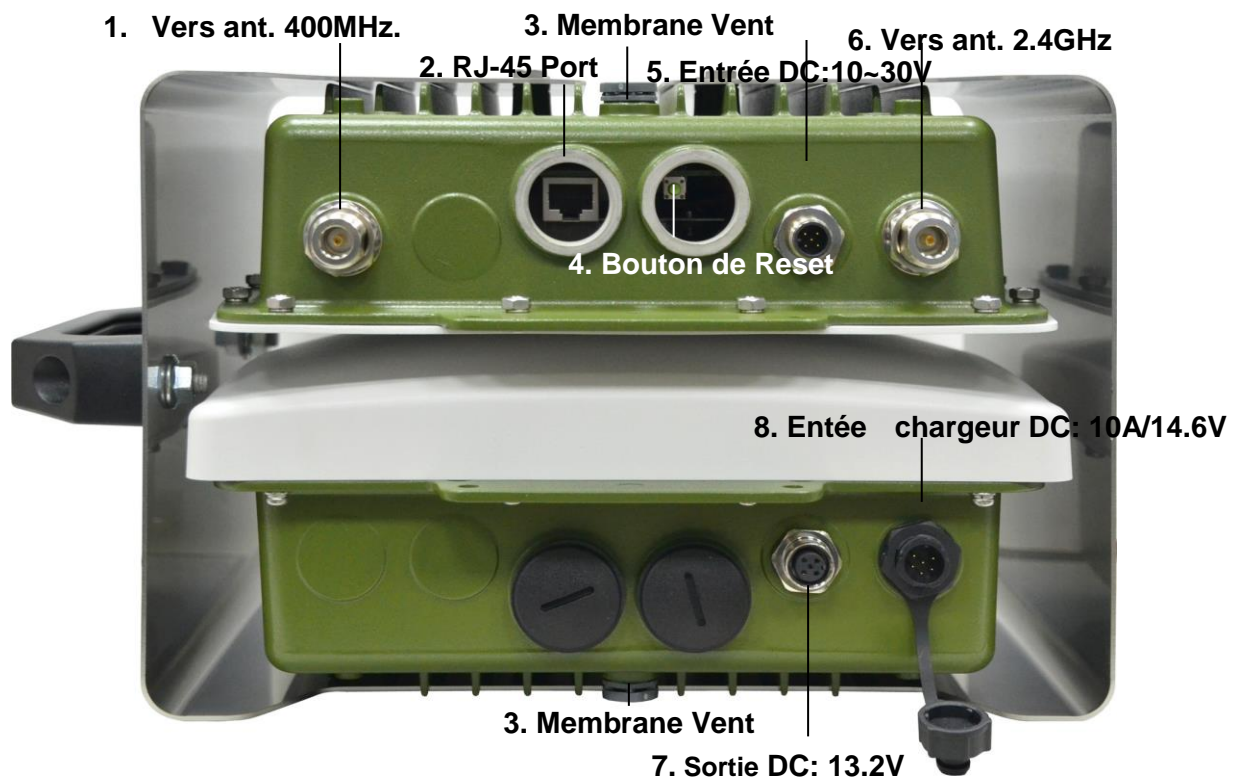
Déconnecter la radio de la batterie.

7. Charger la batterie à l'aide du câble d'alimentation équipé du connecteur M12 a 8 broches.

3.3 ATTENTION SPECIALE III

Pour la recharge et pour l'alimentation en floating de la radio utiliser exclusivement le chargeur intelligent fourni avec les équipements

4 DESCRIPTION MECANIQUE



Aspect supérieur du PWS Portable Wireless Station

5 TABLEAU DES RACCORDEMENTS

1	Vesr ant ; 400MHz	Fixer convenablement l'antenne 400 MHz à ce connecteur N femelle.
2	RJ-45 Port	Connecter ce port à votre PC pour la configuration du système et les connexions LAN Ethernet filaires.
3	Membrane Vent	<ol style="list-style-type: none"> 1. Goretex spécifique évite la condensation et l'humidité dans les ODU. 2. Equilibre les pressions internes et externes afin d'éviter les contraintes aux éléments scellés internes .
4	Bouton de Reset	En dévissant le capot plastique avec une pièce de monnaie l'on accède au bouton de reset. Une pression maintenue entre 6 et 9 secondes remet les équipements en configuration Usine..
5	Entrée DC:10~30V	Connecter avec la M12 à 4 pins du câble fourni depuis le connecteur M12 côté batterie.
6	Vers ant. 2.4GHz	Fixer une antenne 2.4GHz adaptée à ce connecteur N
7	Sortie DC:13.2V	Connecter la M12 4pins connector vers la radio via le cable équipé des connecteurs M12 aux deux extrémités.
8	Entrée DC:10A / 14.6V	Connecte le chargeur intelligent à la batterie LiFePO4 avec le câble spécifique M12 8 pins



Capuchon étanche

Scellé sans fonction actuelle.

6 Appendice A: 400MHz TDMA fréquences intermédiaires

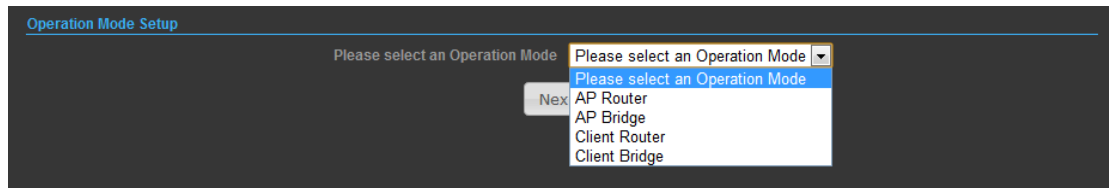
Channel no.	Operating frequency	Baseband frequency
1	440 MHz	2392 MHz
2	445 MHz	2397 MHz
3	450 MHz	2402 MHz
4	455 MHz	2407 MHz
5	460 MHz	2412 MHz
6	465 MHz	2417 MHz
7	470 MHz	2422 MHz
8	475 MHz	2427 MHz
9	480 MHz	2432 MHz
10	485 MHz	2437 MHz
11	490 MHz	2442 MHz
12	495 MHz	2447 MHz
13	500 MHz	2452 MHz

7 Simply User Guide for the PWSA041-118

8. 3 Radios in this shipment was set to be 1*BS to 2*CPE demo links already.

Please refer to the **Appendix B: Demo links setting sample**

- The RJ-45 port of the Radio is connected to the 802.11 b/g/n 2.4GHz AP first and then forwarded to 400MHz Radio by the switch of the 2.4GHz AP. And the operation mode of the 2.4GHz AP must be set to “AP Bridge mode” to ensure the path to 400MHz radio is open.



- Default settings of the 2.4GHz AP

Default IP address: 192.168.2.1

User name: admin

Password: admin

- Default settings of the 400MHz TDMA radio

Default IP address: 192.168.2.2

User name: admin

Password: password

- Base band of the 400MHz (440 ~ 500MHz) TDMA Radio is (2392 ~ 2452 MHz).

That may affects the system performance when the baseband frequency is same as the 802.11b/g/n 2.4GHz. It's better to separate the two frequencies in the same radio for 10MHz at least.

Please refer to the baseband frequency table in **Appendix A: Baseband frequency table of the 400MHz TDMA Radio.**

13. Power on PWSA041-118:

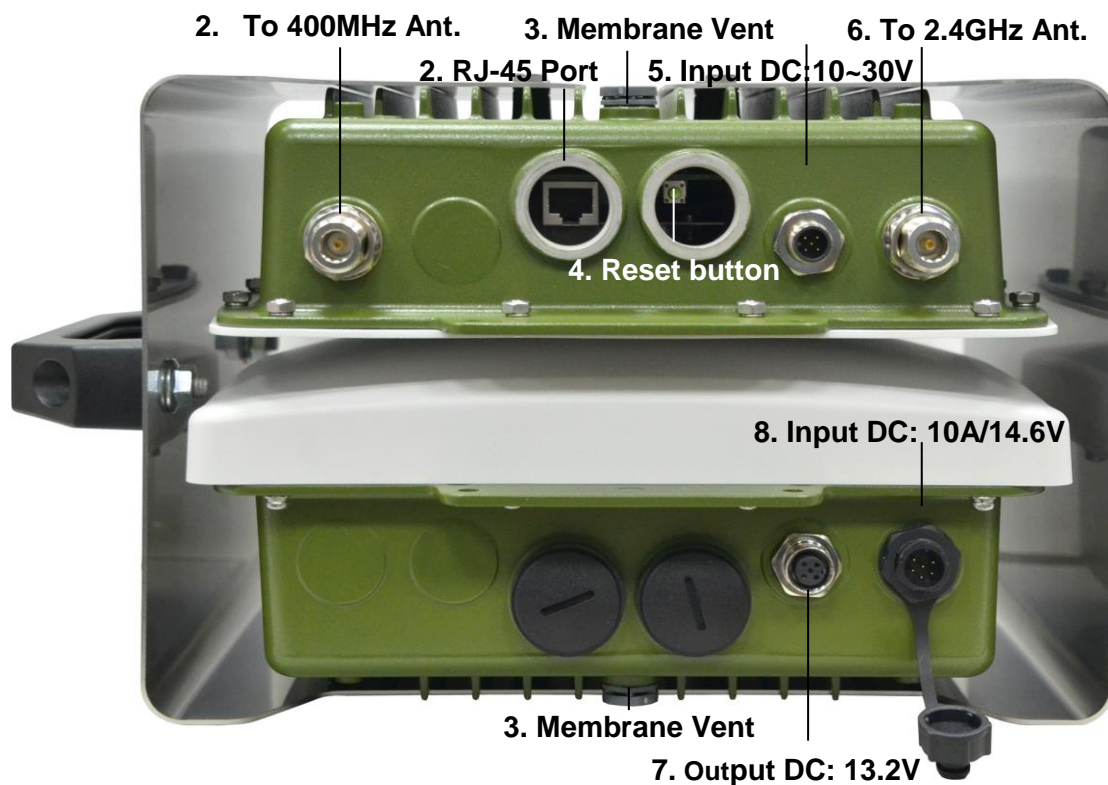
Connect the radio and battery by the power cable with M12 connectors for both ends.

Power off PWSA041-118:

Disconnect the radio and battery.

14. Charging the battery by the power cable with M12 8 pins connector for one end.

8 MECHANICAL DESCRIPTION



Portable Wireless Station Figure

1	To 400MHz Ant.	Attach proper 400MHz antenna to this N-type connector
2	RJ-45 Port	Connect this port to your PC for system configuration.
3	Membrane Vent	3. Moisture vapor permeable to help aid in condensation and fogging reduction in the ODU. 4. High airflow allows pressure equalization to prevent stress on enclosure seals
4	Reset button	Revolve the plastic cap by coin, you will see the reset button. Press it and hold the for 6~9 seconds, both of the radio will back to factory default settings.
5	Input DC:10~30V	Connect to the M12 4pins connector of the battery by the attached power cable with M12 connectors at both ends.
6	To 2.4GHz Ant.	Attach proper 2.4GHz antenna to this N-type connector
7	Output DC:13.2V	Connect to the M12 4pins connector of the radio by the attached power cable with M12 connectors at both ends.
8	Input DC:10A / 14.6V	Connect to the LiFePO4 battery charger by the attached power cable.



Water-proof cap

Sealed. No function this time.

9 Appendix A: 400MHz TDMA Radio Baseband frequency table

10 APPENDICE A: TABLEAU DES FRÉQUENCES INTERMÉDIAIRES DES RADIO TDMA 400MHz.

Channel no.	Operating frequency	Baseband frequency
1	440 MHz	2392 MHz
2	445 MHz	2397 MHz
3	450 MHz	2402 MHz
4	455 MHz	2407 MHz
5	460 MHz	2412 MHz
6	465 MHz	2417 MHz
7	470 MHz	2422 MHz
8	475 MHz	2427 MHz
9	480 MHz	2432 MHz
10	485 MHz	2437 MHz
11	490 MHz	2442 MHz
12	495 MHz	2447 MHz
13	500 MHz	2452 MHz

11 Tableau d'harmonisation des canaux à utiliser

12 CHANNEL PLAN OF THE PORTABLE WIRELESS STATION

To make sure the system works in best condition, below is the recommended channel plan list for your reference.

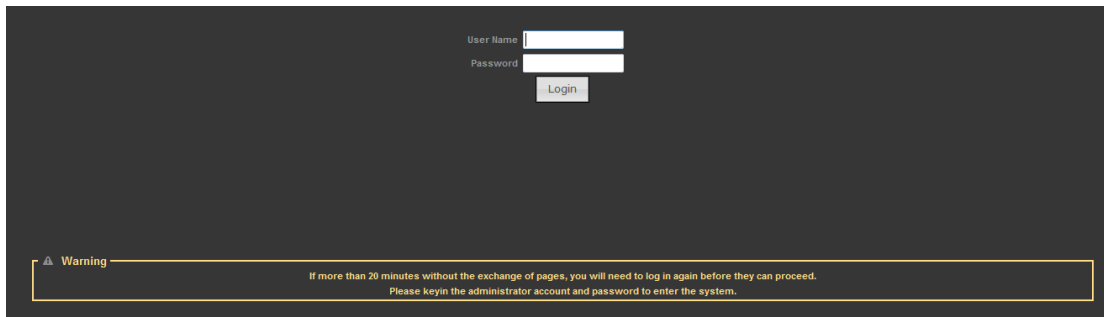
Channel no. of 400MHz TDMA Bridge	Operating frequency of 400MHz TDMA Bridge	Recommended 2.4 GHz AP Channels
1	440 MHz	Ch1 ~ Ch13
2	445 MHz	Ch1 ~ Ch13
3	450 MHz	Ch1 ~ Ch13
4	455 MHz	Ch2 ~ Ch13
5	460 MHz	Ch3 ~ Ch13
6	465 MHz	Ch4 ~ Ch13
7	470 MHz	Ch1 & Ch5 ~ Ch13
8	475 MHz	Ch1 ~ Ch2 & Ch6 ~ Ch13
9	480 MHz	Ch1 ~ Ch3 & Ch7 ~ Ch13
10	485 MHz	Ch1 ~ Ch4 & Ch8 ~ Ch13

13 Configurations of the 2.4GHz AP/Router

13.1 CONNECTING TO THE LOGIN PAGE

To access the 2.4GHz 802.11b/g/n AP/ROUTER's management web GUI interface, following these steps please:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.2.1.
2. Log in by entering the default user name "admin" and password "admin," then click Login.



The screenshot shows a login interface with two input fields labeled 'User Name' and 'Password', and a 'Login' button. Below the fields is a warning message: 'Warning: If more than 20 minutes without the exchange of pages, you will need to log in again before they can proceed. Please keyin the administrator account and password to enter the system.'

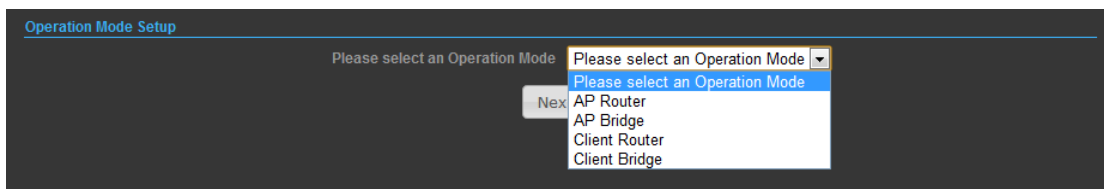
14 Status Page

After logging in to the web interface, the Status page displays. The Home page top-menu-bar shows the Status, Easy Setup, Advanced and Language.

15 Easy Setup

The Easy Setup is designed to help you to configure the basic settings required to get the 2.4GHz 802.11b/g/n AP/ROUTER up and running. There are only a few basic steps you need to set up the 2.4GHz 802.11b/g/n AP/ROUTER to get the connection.

Click on Easy Setup to bring up the wizard

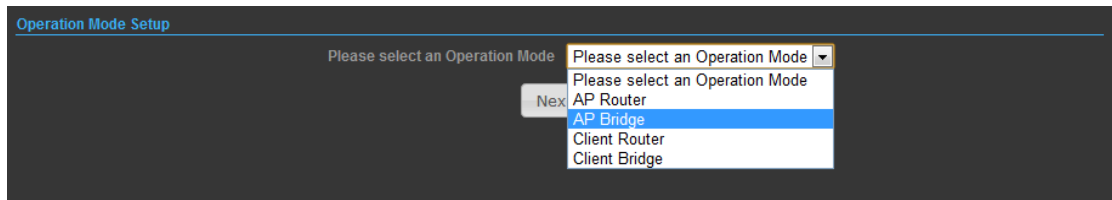


The screenshot shows the 'Operation Mode Setup' page. It features a dropdown menu labeled 'Please select an Operation Mode' with a 'Next' button. The dropdown menu is open, showing the following options: 'AP Router', 'AP Bridge', 'Client Router', and 'Client Bridge'.

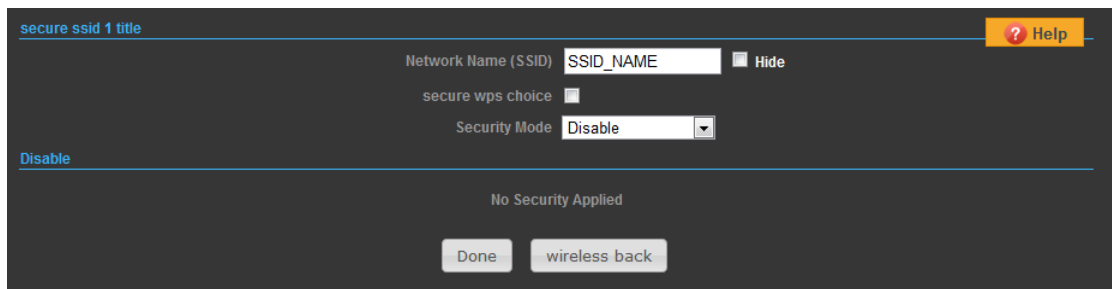
✘Note: Only AP Bridge mode can runs the PWS normally, you won't get reply from the 400MHz TDMA bridge by other operation modes.

15.1 OPERATION MODE – AP BRIDGE

Choose menu “Easy Setup” and select AP Bridge if you want to configure to an access point.



1)

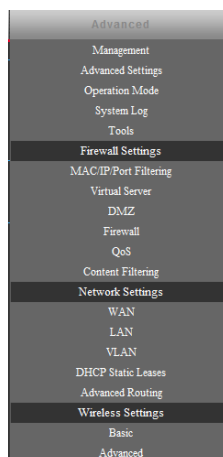


Network Name (SSID) — SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, Open, Shared, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-PSK_WPA2-PSK, WPA, WPA2, WPA1_WPA2, 802.1X; Default: Disabled)

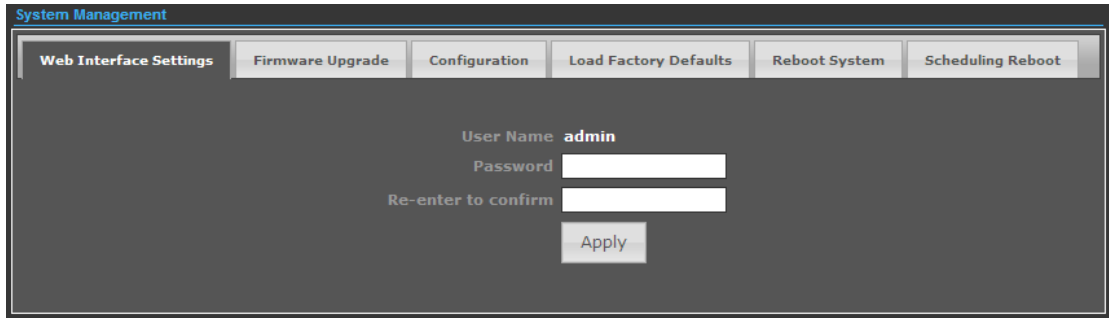
16 Advanced Setup

In the Advanced Manual Bar, it includes all the settings such as firmware upgrade, LAN, WAN and wireless settings that change the RF behaviors. It is important to read through this section before attempting to make changes.



16.1.1 MANAGEMENT

The Management section is provided for configuration of administrative needs such as language type, user name / Password, firmware upgrade, export and import settings, load factory defaults and reboots system.



System Management

Web Interface Settings | Firmware Upgrade | Configuration | Load Factory Defaults | Reboot System | Scheduling Reboot

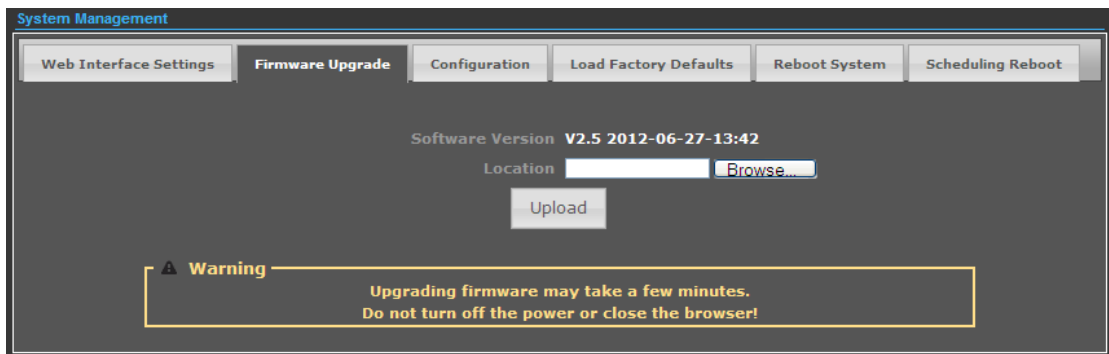
User Name **admin**

Password

Re-enter to confirm

Apply

◆ **Password** — The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.



System Management

Web Interface Settings | **Firmware Upgrade** | Configuration | Load Factory Defaults | Reboot System | Scheduling Reboot

Software Version **V2.5 2012-06-27-13:42**

Location **Browse...**

Upload

Warning Upgrading firmware may take a few minutes.
Do not turn off the power or close the browser!

◆ **Software Version** - This displays the current firmware version.

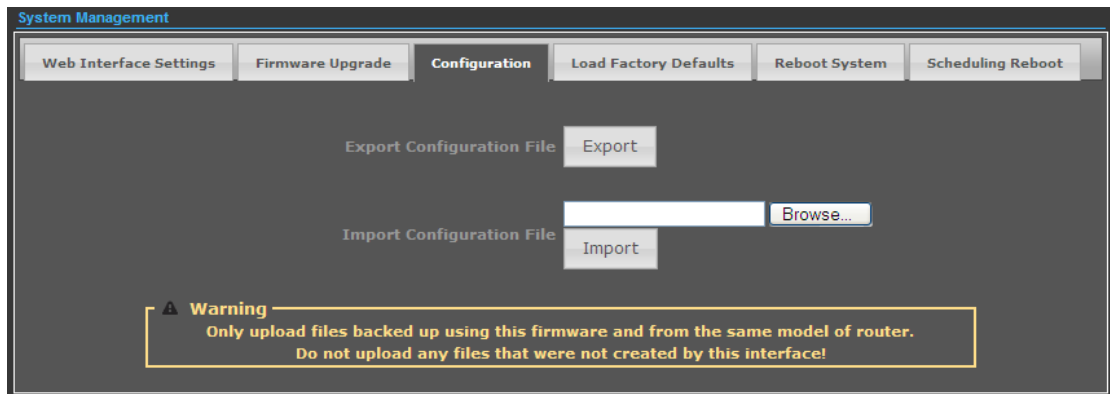
To upgrade the firmware, follow these instructions below:

1. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.
2. Click the **Upgrade** button.

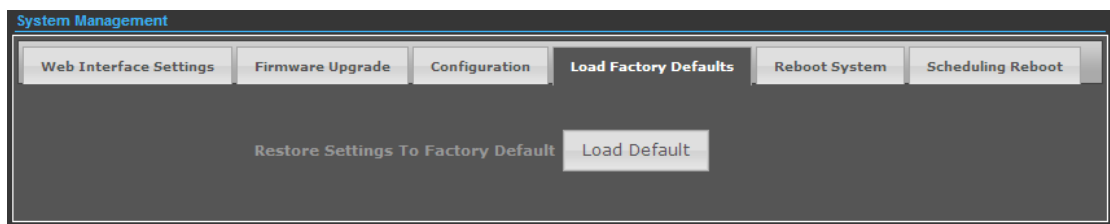
✂ **Note:**

1. When you upgrade the firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.

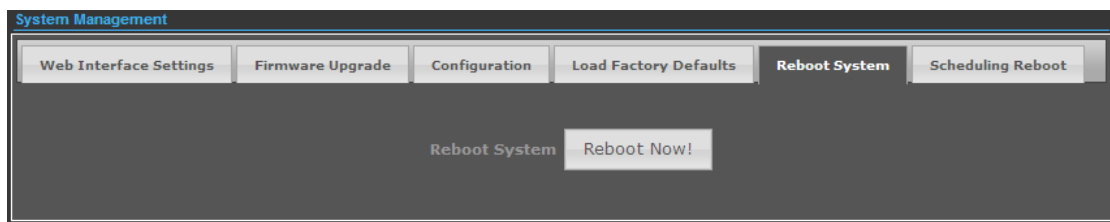
3. Do not turn off the Radio or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.
4. The Router will reboot after the upgrading has been finished.



- ◆ **Export Settings** — Click the Export button to export current configurations to your PC.
- ◆ **Import Settings** — Click the Browse button to browse for the configuration file that is currently saved on your PC, and then click Import button to overwrite the current configurations of the radio.



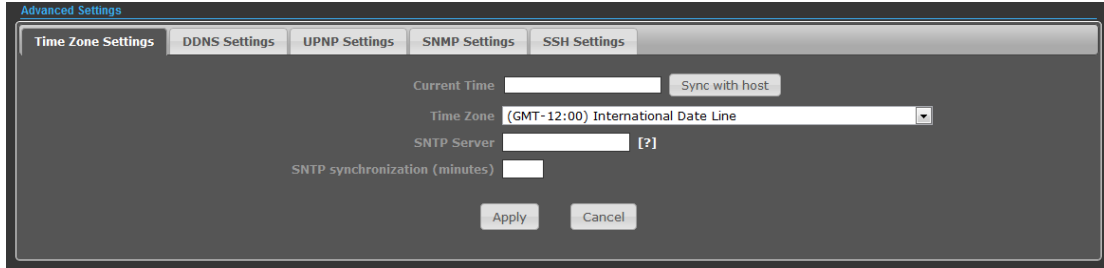
- ◆ **Load Factory Defaults** — If you have problems with 2.4GHz 802.11b/g/n AP/ROUTER, which might be because of changing some settings but you are not sure about that. You can restore the radio back to the factory defaults by clicking the Load Default Button.



- ◆ **Reboot System** — If you want to reboot the 2.4GHz 802.11b/g/n AP/ROUTER, click the Reboot Now Button.

16.1.2 ADVANCED SETTINGS

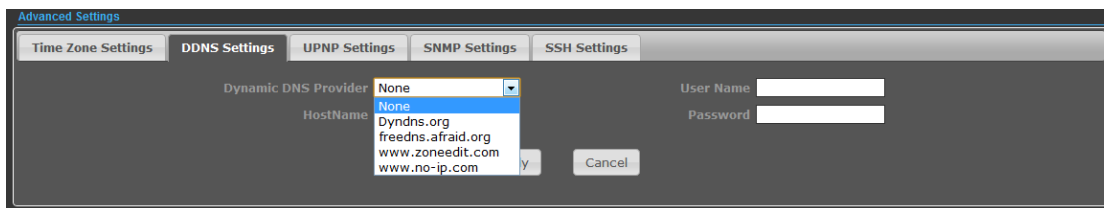
The Advanced Settings section is provided for configuration of Time Zone, DDNS, UPnP, SNMP, and SSH.



◆ **Time Zone Settings** — The Time Zone Settings allows you to configure, update and maintain the correct time on the 2.4GHz 802.11b/g/n AP/ROUTER's internal system clock.

◆ **SNTP Server** — Enter the address of an SNTP server to receive time updates.

◆ **SNTP synchronization (minutes)** — Specify the interval between SNTP server updates.

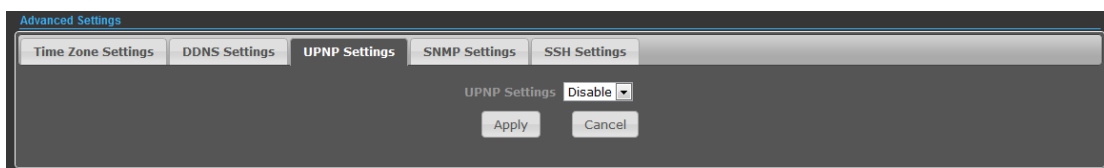


DDNS Settings — DDNS lets you assign a fixed host and domain name to dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the 2.4GHz 802.11b/g/n AP/ROUTER. Before using this feature, you need to sign up for DDNS service at www.dyndns.org, a DDNS service provider.

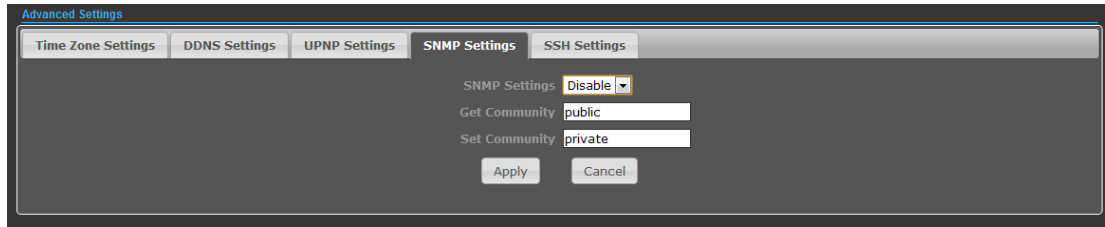
◆ **User Name** — Sets the DDNS user name for the connection.

◆ **Password** — Sets a DDNS password for the connection.

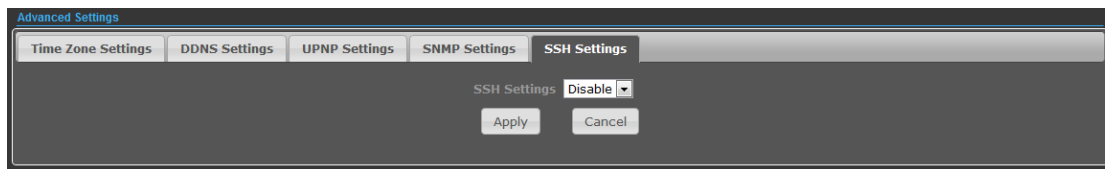
◆ **HostName** — The host name that you selected from the DDNS service provider.



UPNP Settings – UPnP permits network devices to discover other network device(s) preference and establish functional network services for data sharing, communication, and entertainment. Default setting is Disabled.



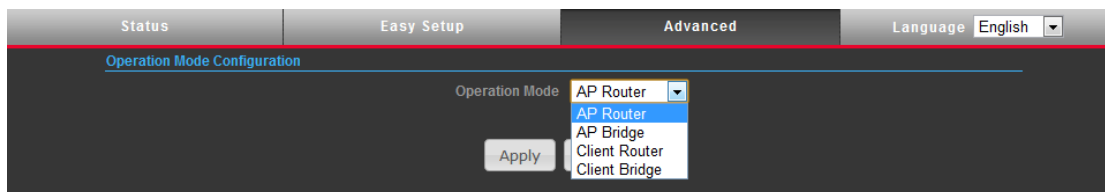
SNMP Settings – Managing devices on IP networks. Default setting is Disabled.



SSH Settings – Secure Shell. Enable your 2.4GHz 802.11b/g/n AP/ROUTER unit to access secure shell (SSH) based network device. Default setting is Disabled.

16.1.3 OPERATION MODE (ONLY AP BRIDGE MODE WORKS FOR PWS)

The Operation Mode content four modes: AP Bridge, AP Router, Client Router and Client Bridge.



◆-**AP Bridge** — The wired Ethernet and wireless are bridged together. Once the mode is selected, all WAN related functions will be disabled.

◆-**AP Router** — The WAN port is used to connect with ADSL/Cable modem and the wireless is used for your private WLAN. The NAT is existed between the 2 RJ45 ports and all wireless clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is DHCP client

◆-**Client Router** — In the Client Router mode is also known as WISP. The 2.4GHz 802.11b/g/n AP/ROUTER wireless side is connected to the remote AP (Base-Station) as in Client Infrastructure mode. Between the wireless and LAN is the IP sharing router function. The WAN is on the wireless side.

◆-**Client Bridge** — If you want to configure your 2.4GHz 802.11b/g/n AP/ROUTER as a WiFi client.

16.2 FIREWALL CONFIGURATION

16.2.1 MAC/IP/PORT FILTERING

MAC/IP/Port filtering restricts connection parameters to limit the risk of intrusion and defends against a wide array of common hacker attacks. MAC/IP/Port filtering allows the unit to permit, deny or proxy traffic through its MAC addresses, IP addresses and ports. The 2.4GHz 802.11b/g/n AP/ROUTER allows you define a sequential list of permit or deny filtering rules. This device tests ingress packets against the filter rules one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is either accepted or dropped depending on the default policy setting.

The screenshot shows the configuration page for MAC/IP/Port Filtering. At the top, there are tabs for 'Status', 'Easy Setup', 'Advanced', and 'Language' (set to English). Under 'Basic Settings', the 'MAC/IP/Port Filtering' is set to 'Disable'. To the right, the 'Default Policy' is set to 'Accepted'. Below these settings are 'Apply' and 'Reset' buttons. A table titled 'Current MAC/IP/Port filtering rules in system' is shown with columns: No., MAC address, DIP, SIP, Protocol, DPR, SPR, Action, and Comment. Below the table, it says 'Others would be accepted'.

◆-**MAC/IP/Port Filtering** — Enables or disables MAC/IP/Port Filtering.

◆-**Default Policy** — When MAC/IP/Port Filtering is enabled, the default policy will be enabled. If you set the default policy to "Dropped", all incoming packets that don't match the rules will be dropped. If the policy is set to "Accepted," all incoming packets that don't match the rules are accepted. (Default: Dropped)

◆-**MAC Address** — Specifies the MAC address to block or allow traffic from.

◆-**DIP** — Destination IP Address. Specifies the destination IP address to block or allow traffic from.

◆-**SIP** — Source IP Address. Specifies the source IP address to block or allow traffic from.

- ◆ **Protocol** — Specifies the destination port type, TCP, UDP or ICMP.
- ◆ **Destination Port Range** — Specifies the range of destination port to block traffic from the specified LAN IP address from reaching.
- ◆ **Source Port Range** — Specifies the range of source port to block traffic from the specified LAN IP address from reaching.
- ◆ **Action** — Specifies if traffic should be accepted or dropped. (Default: Accept)
- ◆ **Comment** — Enter a useful comment to help identify the filtering rules.
- ◆ **Current Filtering rules** — The Current Filter Table displays the configured IP addresses and ports that are permitted or denied access to and from.
 - **No.** — The table entry number.
 - **MAC Address** — Displays a MAC address to filter.
 - **Destination IP Address (DIP)** — Displays the destination IP address.
 - **Source IP Address (SIP)** — Displays the source IP address.
 - **Protocol** — Displays the protocol type.
 - **Destination Port Range (DPR)** — Displays the destination port range.
 - **Source Port Range (SPR)** — Displays the source port range.
 - **Action** — Displays if the specified traffic is accepted or dropped.
 - **Comment** — Displays a useful comment to identify the filter rules.

16.2.2 VIRTUAL SERVER SETTINGS

Virtual Server (sometimes referred to as Port Forwarding) is the act of forwarding traffic from one network node to another based on received protocol port number. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside through a NAT enabled router. (Maximum 32 entries are allowed.)

Virtual Server

Virtual Server

Virtual Server Settings

IP Address

Private Port

Public Port

Protocol

Comment

(The maximum rule count is 32.)

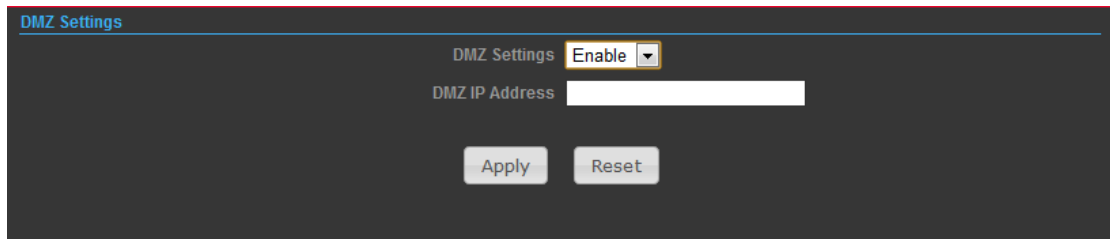
Current Virtual Servers in system

No.	IP Address	Port Mapping	Protocol	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>				

- ◆ **Virtual Server** — Selects between enabling or disabling port forwarding the virtual server.
(Default: Disable)
- ◆ **IP Address** — Specifies the IP address of a server on the local network to allow external access.
- ◆ **Private Port** — The protocol port number on the local server.
- ◆ **Public Port** — The protocol port number on the router’s WAN interface.
- ◆ **Protocol** — Specifies the protocol to forward, either TCP, UDP, or TCP&UDP.
- ◆ **Comment** — Enter a useful comment to help identify the port forwarding service on the network.
- ◆ **Current Virtual Servers in System** — The Current Port Forwarding Table displays the entries that are allowed to forward packets through the 2.4GHz 802.11b/g/n AP/ROUTER’s firewall.
 - **No.** — The table entry number.
 - **IP Address** — The IP address of a server on the local network to allow external access.
 - **Port Mapping** — displays the port mapping for the server.
 - **Protocol** — Displays the protocol used for forwarding this port.
 - **Comment** — Displays a useful comment to identify the nature of the port to be forwarded.

16.2.3 DMZ

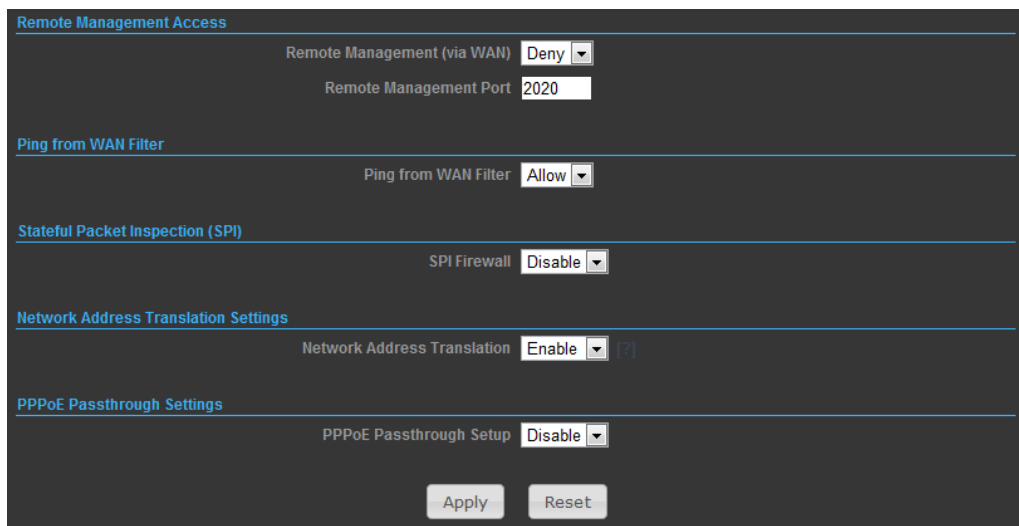
DMZ is to specified host PC on the local network to access the Internet without any firewall protection. Some Internet applications, such as interactive games or video conferencing, may not function properly behind the firewall. By specifying a Demilitarized Zone (DMZ) host, the PC's TCP ports are completely exposed to the Internet, allowing open two-way communication. The host PC should be assigned a static IP address (which is mapped to its MAC address) and this must be configured as the DMZ IP address.



- ◆ **DMZ Settings** — Sets the DMZ status. (Default: Disable)
- ◆ **DMZ IP Address** — Specifies an IP address on the local network allowed unblocked access to the WAN.

16.2.4 FIREWALL

Firewall functions which will help to protect your network and computer. You can utilized firmware functions to protect your network from hackers and malicious intruders.

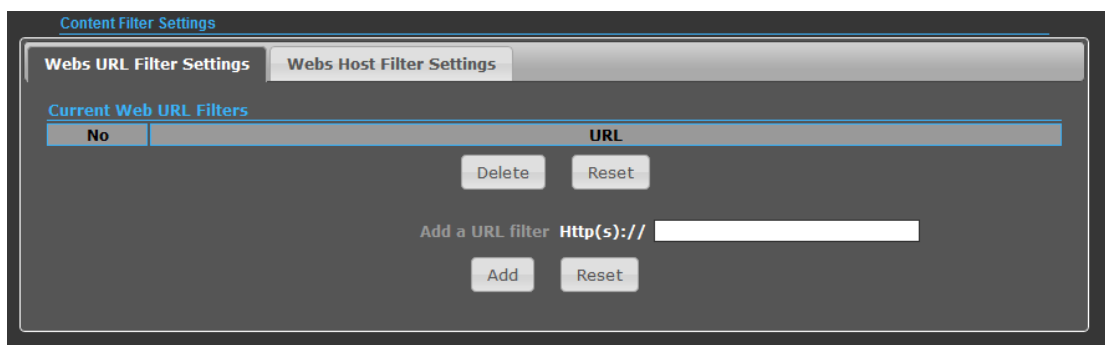


- ◆ **Remote Management (via WAN)** — allow or deny to manage the router from anywhere on the Internet.

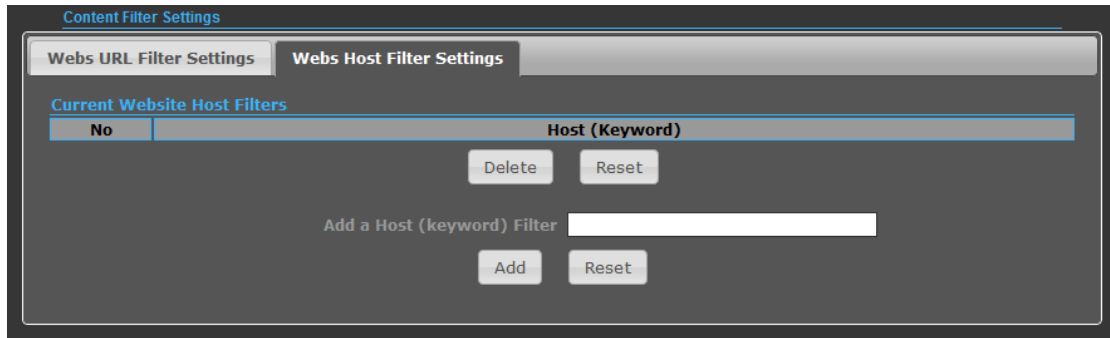
- ◆ **Remote Management Port** — The port that you will use to address the management from the Internet. For example, if you specify port 2020, then to access the 2.4GHz 802.11b/g/n AP/ROUTER from Internet, you would use a URL of the form: `http://xxx.xxx.xxx.xxx:2020/`
- ◆ **Ping from WAN Filter** — When Allow, the 2.4GHz 802.11b/g/n AP/ROUTER does not respond to ping packets received on the WAN port.
- ◆ **SPI Firewall** — SIP firewall help to keep track of the state of network connections (such as TCP streams, UDP communication) traveling across it. It is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.
- ◆ **Network Address Translation** — NAT is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

16.2.5 CONTENT FILTERING

The 2.4GHz 802.11b/g/n AP/ROUTER provides a variety of options for blocking Internet access based on content, URL and host name.



- ◆ **Web URL Filter Settings** — By filtering inbound Uniform Resource Locators (URLs) the risk of compromising the network can be reduced. URLs are commonly used to point to websites. By specifying a URL or a keyword contained in a URL traffic from that site may be blocked.
- ◆ **Current URL Filters** — Displays current URL filter.
- ◆ **Add a URL Filter** — Adds a URL filter to the settings.
- ◆ **Delete a URL Filter** — Deletes a URL filter entry from the list.



Web Host Filter Settings — Allows Internet content access to be restricted based on web address keywords and web domains. A domain name is the name of a particular web site. For example, for the address www.HOST.com, the domain name is HOST.com. Enter the Keyword then click “Add.”

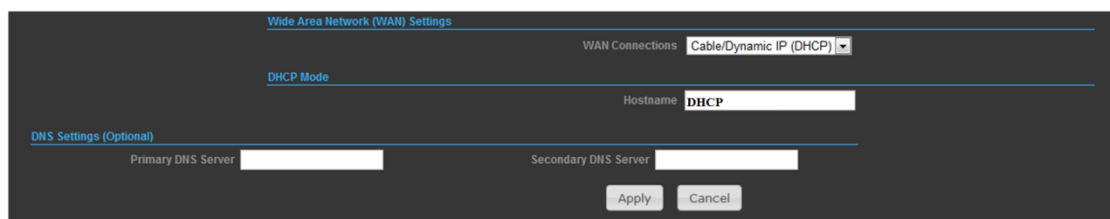
- ◆ **Current Host Filters** — Displays current Host filter.
- ◆ **Add a Host Filter** — Enters the keyword for a host filtering.
- ◆ **Delete a Host Filter** — Deletes a Host filter entry from the list.

16.3 NETWORK SETTINGS

16.3.1 WAN

In this section, there are several connection types to choose from; Static IP, DHCP, PPPoE, PPTP and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

CABLE/DYNAMIC IP (DHCP)



- ◆ **Hostname** — Specifies the host name of the DHCP client.
- ◆ **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- ◆ **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

PPPoE (ADSL)

Wide Area Network (WAN) Settings

WAN Connections: PPPoE (ADSL)

PPPoE Mode

User Name: pppoe_user

Password:

Verify Password:

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period: 60 Seconds

MTU: 1492 bytes (Default=1492)

DNS Settings (Optional)

Primary DNS Server:

Secondary DNS Server:

Apply Cancel

◆-**User Name** — Sets the PPPoE user name for the WAN port.

(Default: pppoe_user; Range: 1~32 characters)

◆-**Password** — Sets a PPPoE password for the WAN port.

(Default: pppoe_password; Range: 1~32 characters)

◆-**Verify Password** — Prompts you to re-enter your chosen password.

◆-**Operation Mode** — Enables and configures the keep alive time and configures the on-demand idle time.

STATIC IP (FIXED IP)

Wide Area Network (WAN) Settings

WAN Connections: Static (Fixed IP)

Static Mode

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Default Gateway:

DNS Settings

Primary DNS Server:

Secondary DNS Server:

Apply Cancel

◆-**IP Address** — Sets the static IP address.

◆-**Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0)

◆-**Default Gateway** — The IP address of a router that is used when the requested destination IP address is not on the local subnet.

◆-**Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆ **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

PPTP

PPTP Mode

Server IP: pptp_server

User Name: pptp_user Password:

Address Mode: Static IP

IP Address:

Subnet Mask:

Operation Mode: Keep Alive Keep Alive Mode: Redial Period: 60 Seconds

DNS Settings (Optional)

Primary DNS Server: Secondary DNS Server:

Apply Cancel

◆ **Server IP** — Sets the PPTP server IP Address. (Default: pptp_server)

◆ **User Name** — Sets the PPTP user name for the WAN port.

(Default: pptp_user; Range: 1~32 characters)

◆ **Password** — Sets a PPTP password for the WAN port.

(Default: pptp_password; Range: 1~32 characters)

◆ **Address Mode** — Sets a PPTP network mode. (Default: Dynamic IP)

◆ **Operation Mode** — Enables and configures the keep alive time.

◆ **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆ **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

IPSec

The screenshot shows the 'Wide Area Network (WAN) Settings' window with 'WAN Connections' set to 'IPSEC'. The 'wan ipsec mode' section includes the following fields:

- Connection address family: IPv4
- IPSec Connection Type: Road Warrior Tunnel
- IPSec Authentication: SHA-1
- SA connection Life Time: [] hours
- Local IP Address: []
- Local Subnet: []
- Local Gateway: []
- IPSec Tunnel Name: accCONN
- IPSec Key Life time: 12h hours
- NAT Transversal:
- IPSec Compression:
- IPSec Operation Mode: add
- PFS/DH Group: modp1024
- IPSec Encryption: AES
- IKE Key Tries: 3 times
- Peer IP Address: []
- Peer Subnet: []
- Peer Gateway: []
- IPSec Secret Key: PSK
- Perfect Forward Secrets:
- IPSec Conn. Keep Alive:

At the bottom, there are 'DNS Settings (Optional)' for Primary and Secondary DNS Servers, and 'Apply' and 'Cancel' buttons.

Verify the desired settings and use scroll down for more options.

- ◆-IPSec Connection Type – Use drop down menu to select from Road Warrior Tunnel, Host to Host Tunnel, Subnet to Subnet Tunnel, Host to Host Transport, Pass through, Drop, or Reject. Default setting is Road Warrior Tunnel
- ◆-IPSec Authentication – Use drop down menu to select from SHA-1, or MD5. Default setting is SHA1.
- ◆-SA Connection Life Time – Specify how often each SA should be rekeyed, measured in hour.
- ◆-Local IP address / Subnet / Gateway – Local end point IP address, Subnet, and Gateway IP address.
- ◆-IPSec Operation Mode – Use drop down menu to select from Add, Route Start, Manual, or Ignore. Default setting is Add.
- ◆-IKE Key Retry –Specify maximum retry limits for negotiate key to Internet Key Exchange.
- ◆-Peer IP address / Subnet / Gateway – Remote end point IP address, Subnet, and Gateway IP address.

L2TP

L2TP Mode

Server IP

User Name

Password

Address Mode

IP Address

Subnet Mask

Operation Mode

Keep Alive Mode: Redial Period Seconds

DNS Settings (Optional)

Primary DNS Server

Secondary DNS Server

◆ **Server IP** — Sets the L2TP server IP Address. (Default: l2tp_server)

◆ **User Name** — Sets the L2TP user name for the WAN port.

(Default: l2tp_user; Range: 1~32 characters)

◆ **Password** — Sets a L2TP password for the WAN port.

(Default: l2tp_password; Range: 1~32 characters)

◆ **Address Mode** — Sets a L2TP network mode. (Default: Dynamic IP)

◆ **Operation Mode** — Enables and configures the keep alive time.

◆ **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆ **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

16.3.2 LAN

In this section, the LAN settings are configured based on the IP Address and Subnet Mask. The IP address is also used to access this Web-based management interface. It is recommended to use the default settings if you do not have an existing network.

◆ **-IP Address** — The IP address of 2.4GHz 802.11b/g/n AP/ROUTER on the local area network.

(Default: 192.168.2.1)

◆ **-Subnet Mask** — The subnet mask of 2.4GHz 802.11b/g/n AP/ROUTER on the local area network

◆ **-DHCP Server** — The DHCP Server is to assign private IP address to the 2.4GHz 802.11b/g/n AP/ROUTER in your local area network(LAN). The default LAN IP address is 192.168.2.1, changing IP address will also change the DHCP server's IP subnet.

16.3.3 ADVANCED ROUTING (UNAVAILABLE IN AP BIDGE MODE)

In this section, allow to configure routing feature in the 2.4GHz 802.11b/g/n AP/ROUTER.

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	192.168.2.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	

◆ **-Destination** — The IP address of packets that can be routed.

◆ **-Type** — Defines the type of destination. (Host: Signal IP address / Net: Portion of Network)

◆ **-Netmask** — Displays the subnetwork associated with the destination.

◆ **-Gateway** — Defines the packets destination next hop

- ◆ **-Interface** — Select interface to which a static routing subnet is to be applied
- ◆ **-Comment** — Help identify the routing
- ◆ **-RIP** — Enable or disable the RIP(Routing Information Protocol) for the WAN or LAN interface.

16.4 WIRELESS SETTINGS

16.4.1 BASIC

Basic Wireless Settings

Wireless Mode: Access Point

Multiple SSID:

Country Code: Germany

Frequency (Channel): 2437 MHz (Channel 6)

Site Survey:

Network Mode: WiFi 11gn HT20

Extension Channel: Upper Channel

Distance: 0.8 miles (km)

ACK Timeout: 35

SSID Security Settings

Network Name (SSID): SSID NAME Hide

WPS Choice:

Encryption Settings: Disable

- ◆ **-Wireless On/Off** — Enables or Disable the radio. (Default: Turn On)
- ◆ **-Wireless Mode** — There are 4 wireless mode, those are Access Point, WDS Access Point, WDS Repeater and WDS Client

✂ **Note:**

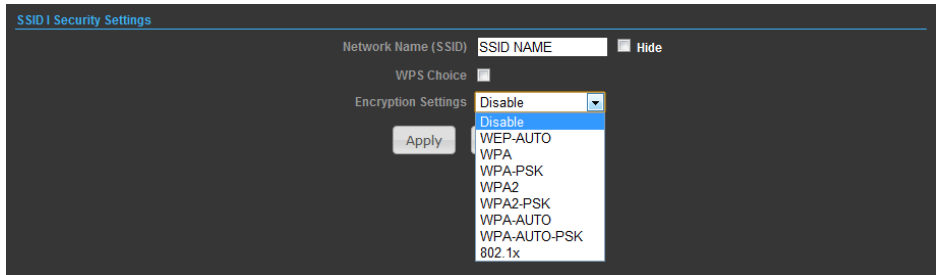
If WEP authentication is selected for WDS communication, you will then only have one set of encryption for the entire channel.

- ◆ **-Network Name (SSID)** — The name of the wireless network service provided by the 2.4GHz 802.11b/g/n AP/ROUTER. Clients that want to connect to the network must set their SSID to the same as that of 2.4GHz 802.11b/g/n AP/ROUTER. (Range: 1-32 characters)
- ◆ **-Multiple SSID** — One additional VAP interface supported on the device. (Default: no name configured; Range: 1-32 characters)
- ◆ **-Frequency (Channel)** — The radio channel that the 2.4GHz 802.11b/g/n AP/ROUTER uses to communicate with wireless clients.

◆ **-Network Mode** — Defines the radio operating mode.(Default: 11an HT20)

◆ **-Packet Aggregate** — The process of joining multiple packets together into a single transmission unit, in order to reduce the overhead associated with each transmission.

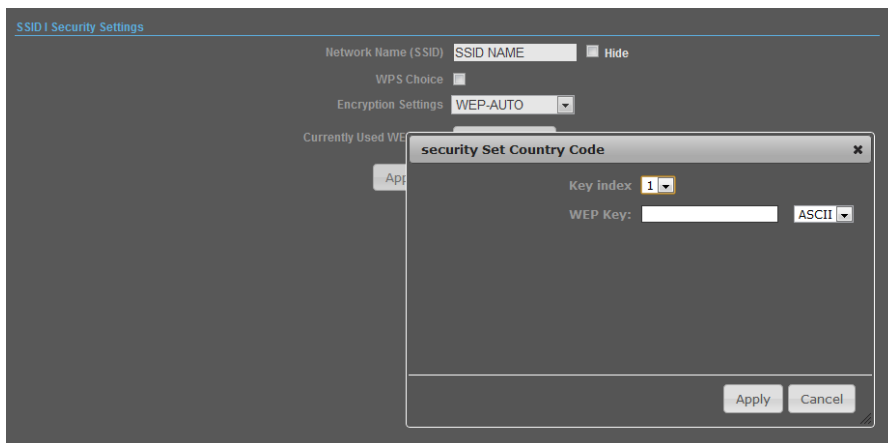
16.4.2 SECURITY



WIRED EQUIVALENT PRIVACY (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

When you select to use WEP, be sure to define at least one static WEP key for user authentication or data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.



◆ **-WEP-AUTO** — Allows wireless clients to connect to the network using

Open-WEP (uses WEP for encryption only) or Shared-WEP (uses WEP for authentication and encryption).

- ◆ **Encrypt Type** — Selects WEP for data encryption (OPEN mode only).
- ◆ **Security Key Index** — Selects the WEP key number to use for authentication or data encryption. If wireless clients have all four WEP keys configured to the same values, you can change the encryption key to any of the settings without having to update the client keys. (Default: 1; Range: 1~4)
- ◆ **WEP Keys** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. (Default: Hex, no preset value)

✂**Note:**

If WEP authentication is selected for WDS communication, you will then only have one set of encryption for the entire channel.

WPA & WPA2

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA.

The screenshot shows a configuration window titled "SSID I Security Settings". It contains the following fields and options:

- Network Name (SSID): SSID NAME (with a "Hide" checkbox)
- WPS Choice:
- Encryption Settings: WPA (dropdown menu)
- WPA Algorithms: TKIP, CCMP(AES), Auto
- Key Renewal Interval(Seconds): 60
- IP Address: [empty text box]
- Port: [empty text box]
- Shared Secret: [empty text box]
- Buttons: Apply, Cancel

- ◆ **WPA** — Clients using WPA for authentication.
- ◆ **WPA2** — Clients using WPA2 for authentication.
- ◆ **WPA-Auto** — Clients using WPA or WPA2 for authentication.
- ◆ **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

■ **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

■ **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

■ **Auto** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆ **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

RADIUS Server — Configures RADIUS server settings.

◆ **IP Address** — Specifies the IP address of the RADIUS server.

◆ **Port** — The User Datagram Protocol (UDP) port number used by the

RADIUS server for authentication messages. (Range: 1024-65535;

Default: 1812)

◆ **Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

WPA-PSK & WPA2-PSK

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation. For small home or office networks, WPA and WPA2 provide a simple “personal” operating mode that uses just a pre-shared key for network

access. The **WPA Pre-Shared Key (WPA-PSK)** mode uses a common password phrase for user authentication that is manually entered on the access point and all wireless clients. Data encryption keys are automatically generated by the access point and distributed to all clients connected to the network.

The screenshot shows the 'SSID Security Settings' window. It includes the following fields and options:

- Network Name (SSID): SSID NAME (with a 'Hide' checkbox)
- WPS Choice:
- Encryption Settings: WPA2-PSK (dropdown menu)
- WPA Algorithms: TKIP [?], CCMP(AES), Auto
- Key Renewal Interval(Seconds): 60
- Pre-Shared Key: [text input] (with a 'Generator' button)
- Buttons: 'Apply' and 'Cancel'

◆ **-WPA-PSK** — Clients using WPA with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is TKIP.

◆ **-WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is AES.

◆ **-WPA- Auto-PSK** — Clients using WPA or WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type is TKIP/AES.

◆ **-WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

■ **-TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

■ **-AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

■ **-Auto** — Uses either TKIP or AES keys for encryption. WPA and

WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

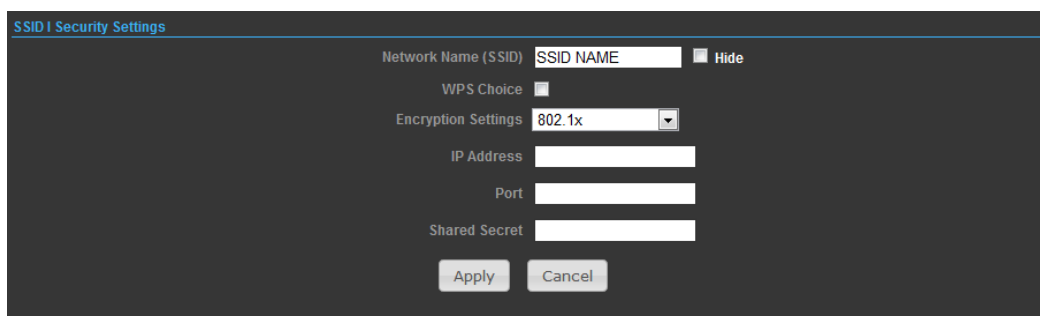
◆ **-Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

◆ **-Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

IEEE 802.1X AND RADIUS

IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the client can access the network. Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires network access.

The WPA and WPA2 enterprise security modes use 802.1X as the method of user authentication. IEEE 802.1X can also be enabled on its own as a security mode for user authentication. When 802.1X is used, a RADIUS server must be configured and be available on the connected wired network.



The screenshot shows a configuration window titled "SSID Security Settings". It contains the following fields and controls:

- Network Name (SSID): A text input field containing "SSID NAME" and a "Hide" checkbox.
- WPS Choice: A checkbox.
- Encryption Settings: A dropdown menu currently set to "802.1x".
- IP Address: A text input field.
- Port: A text input field.
- Shared Secret: A text input field.
- Buttons: "Apply" and "Cancel" buttons at the bottom.

802.1X WEP: Selects WEP keys for data encryption. When enabled, WEP encryption keys are automatically generated by the RADIUS server and distributed to all connected clients. (Default: Disabled)

RADIUS Server — Configures RADIUS server settings.

◆ **IP Address** — Specifies the IP address of the RADIUS server.

◆ **Port** — The User Datagram Protocol (UDP) port number used by the

RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

◆ **Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

Wi-Fi PROTECTED SETUP (WPS) --- No Available in PWS (Portable Wireless Station)

Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the 2.4GHz 802.11b/g/n AP/ROUTER can be pressed at any time to allow a single device to easily join the network. The WPS Settings page includes configuration options for setting WPS device PIN codes and activating the virtual WPS button.

Click on “Wireless Settings,” followed by “WPS”.

17 Appendix B: Demo links setting sample

