



# User's Manual

OWL400/410 v1.00

Long Range Outdoor AP/Bridge/CPE

## **Copyright Notice**

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission of 4IPNET, INC.

## **Disclaimer**

4IPNET, INC. does not assume any liability arising out the application or use of any products, or software described herein. Neither does it convey any license under its parent rights not the parent rights of others. 4IPNET further reserves the right to make changes in any products described herein without notice. The publication is subject to change without notice.

## **Trademarks**

4IPNET (4ipnet) is a registered trademark of 4IPNET, INC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Table of Contents

<b>Table of Contents</b> .....	<b>iii</b>
<b>1. Introduction</b> .....	<b>1</b>
1.1 Overview .....	1
1.2 Functionalities .....	3
1.3 Document Conventions .....	4
<b>2. System Overview</b> .....	<b>5</b>
2.1 Package Contents.....	5
2.2 Specifications .....	5
2.3 Panel Function Description .....	6
<b>3. Installation</b> .....	<b>7</b>
3.1 Hardware Installation .....	7
3.2 Basic Configuration .....	8
3.2.1 Introduction to Web Management Interface.....	8
< AP Mode – Default Mode >.....	<b>8</b>
< CPE Mode >.....	<b>11</b>
3.2.2 Quick Configuration .....	13
< AP Mode – Default Mode>.....	<b>13</b>
< CPE Mode >.....	<b>18</b>
<b>4. AP Mode Configuration</b> .....	<b>24</b>
4.1 System .....	26
4.1.1 System Information.....	27
4.1.2 Operating Mode .....	29
4.1.3 Network Settings.....	30
4.1.4 Management Services .....	31
4.2 Wireless .....	33
4.2.1 Virtual AP Overview .....	34
4.2.2 General Settings .....	35
4.2.3 VAP Configuration.....	37
4.2.4 Security Settings .....	38
4.2.5 Repeater Settings .....	42
4.2.6 Advanced Wireless Settings.....	45
4.2.7 Access Control Settings .....	46
4.2.8 Site Survey .....	48
4.3 Utilities .....	49
4.3.1 Change Password .....	50
4.3.2 Network Utilities.....	51
4.3.3 Configuration Save & Restore .....	52
4.3.4 System Upgrade.....	53
4.3.5 Reboot.....	54
4.4 Status .....	55
4.4.1 System Overview .....	56
4.4.2 Associated Client Status.....	58
4.4.3 Repeater Information .....	59
4.4.4 Event Log.....	60
4.5 Online Help .....	61
<b>5. CPE Mode Configuration</b> .....	<b>62</b>
5.1 System .....	64
5.1.1 System Information.....	65
5.1.2 Operating Mode .....	67
5.1.3 Network Settings.....	68
5.1.4 Management Services .....	71

5.2	Wireless .....	73
5.2.1	General Settings .....	74
5.2.2	Advanced Wireless Settings .....	75
5.2.3	Security Settings .....	76
5.2.4	Site Survey .....	78
5.3	Firewall .....	79
5.3.1	IP/ Port Forwarding .....	80
5.3.2	Demilitarized Zone .....	82
5.4	Utilities .....	83
5.4.1	Change Password .....	84
5.4.2	Network Utilities .....	85
5.4.3	Configuration Save & Restore .....	86
5.4.4	System Upgrade .....	87
5.4.5	Reboot .....	88
5.5	Status .....	89
5.5.1	System Overview .....	90
5.5.2	Event Log .....	92
5.5.3	DHCP Leases .....	93
5.5.4	UPnP Status .....	94
5.6	Online Help .....	95
<b>Appendix A. System Management Account Privileges .....</b>		<b>96</b>

# 1. Introduction

## 1.1 Overview

This manual is intended for **system integrators**, **field engineers** and **network administrators** to set up **4ipnet OWL400/410 Long Range Outdoor AP/ Bridge/ CPE** in their network environments. It contains step-by-step procedures and graphic examples to guide users with networking knowledge to complete the installation.



*OWL400 (with N-type connector)*

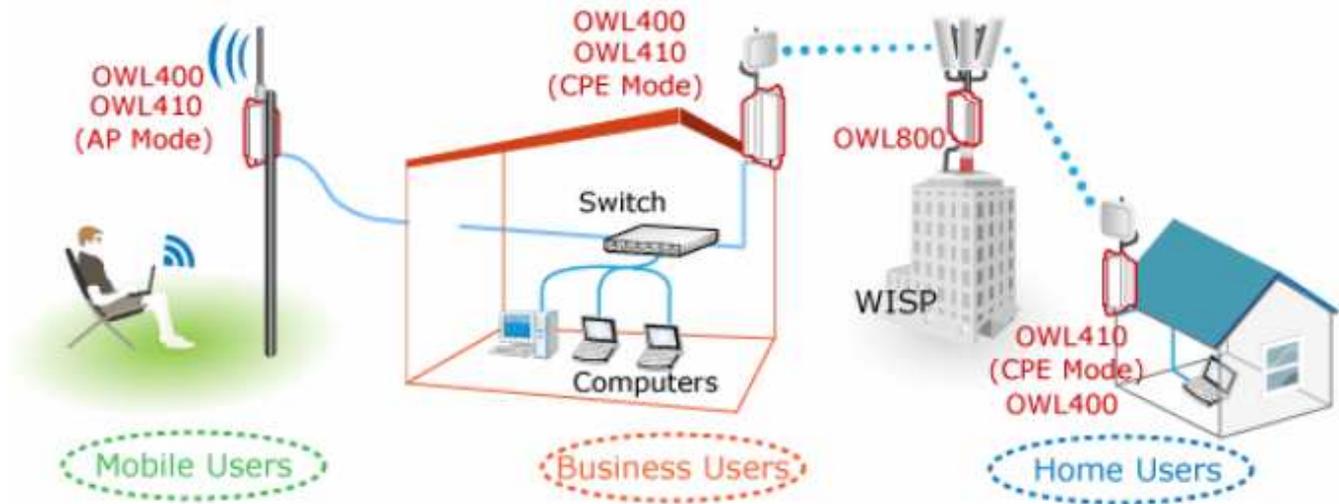


*OWL410 (with built-in 10dBi patch antenna)*

The 802.11 n/a compliant **OWL400/410** is a multi-mode Last-Mile Broadband solution for Wireless Internet Service Provider (WISP). It can be deployed as a traditional fixed wireless Access Point (AP mode) or it can be used as an outdoor Customer Premises Equipment (CPE mode) that connects to the outdoor wireless network of Wireless Internet Service Provider (WISP).

The metal sealed OWL400/410 is compact in size and weatherproof. Coming with a mounting kit, it can be mounted on a pole or wall. It is suitable for both indoor and outdoor usage with its 200mW output power, which is higher than a typical indoor AP (100mW).

The following is a network diagram for a typical WISP application.



The OWL400/410 can be deployed in various environments, for example:

- Hot zones such as business districts, office complexes, airports, hotels, conference centers, recreation areas, and shopping malls.
- Wireless CPE for Multi Dwelling Unit (MDU) /Multi Tenant Unit (MTU), such as apartments, dormitories, and office complexes.
- Outdoor access point for school campuses, enterprise campuses, or manufacture plants.
- Indoor access point for hotels, factories, or warehouses where metal industrial grade devices are preferred.
- Public hotspot operation for café, parks, convention centers, shopping malls, or airports.
- Wireless coverage for indoor and outdoor ground for private resorts, acre estate/home's yards, or gulf course communities.



## 1.2 Functionalities

The metal sealed OWL400/410 is compact in size and weatherproof. Coming with a mounting kit, it can be mounted on a pole or wall. Specifically developed for outdoor use, the fully-hardened, IP68-rated OWL400/410 can withstand wind, rain, lightning, power surges, and extreme temperature.

- Acts as a "**Wireless Modem**" to bring wireless bandwidth to home and office buildings.
- **Wireless Bandwidth Allocation** (uplink/downlink) delivered to each building depending on different subscription plans.
- Full range of **wireless security** mechanisms such as WEP, WPA and WPA2 (802.11i) that are important for enterprise wireless deployments.
- Acts as a **Home Router** for **IP Sharing** and firewall, all-in-one installation solution - no need for extra router.
- Purposely built rugged access point for harsh **outdoor / industrial** conditions.
- **Weatherproof** and watertight from its rugged aluminum housing (IP68 Approved).
- **Power over Ethernet (PoE)** built-in for single cable installation.
- On board **Ethernet surge protection**.
- **Multiple operation modes** :
  - AP Base Station Mode
  - WISP CPE Mode
  - WDS Bridge Mode
  - Universal Repeater Mode

## 1.3 Document Conventions

	Represents essential steps, actions, or messages that should not be ignored.
» <b>Note:</b>	Contains related information that corresponds to a topic.
	Indicates that clicking this button will save the changes you made, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.
	Indicates that clicking this button will clear what you have set before the settings are applied.

## 2. System Overview

### 2.1 Package Contents

The standard package of OWL400/410 includes:

- OWL400/410 x 1
- Quick Installation Guide (QIG) x 1
- CD-ROM (with User's Manual and QIG) x 1
- Power Sourcing Equipment (PSE) x 1
- Mounting Kit x 1



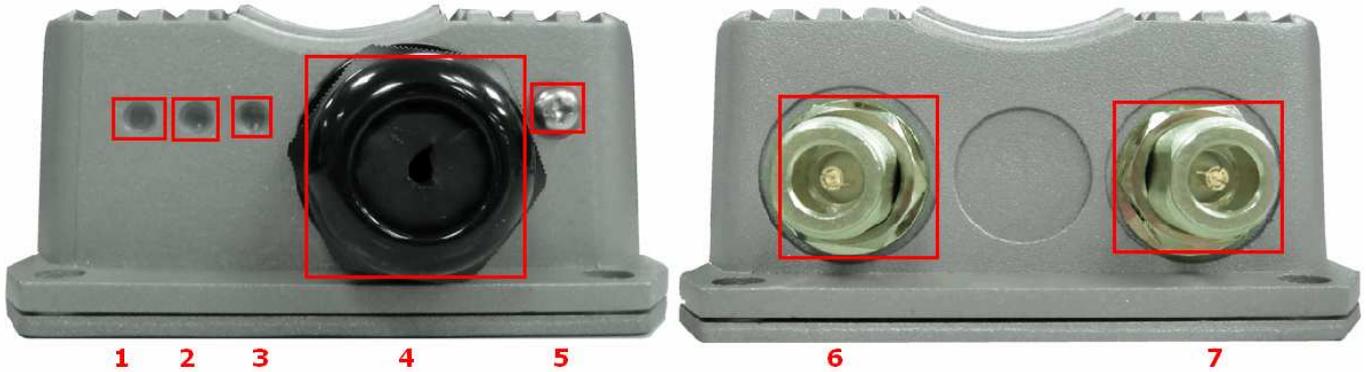
*It is highly recommended to use all the components supplied to ensure best performance of the system.*

### 2.2 Specifications

- **Hardware Specifications**
  - Die cast Metal case: weather proof, compliant with IP68 Standard
  - LED Indication: Power x 1; Ethernet x 1; Wireless x 1
  - Ethernet Port: 10/100 Base-T with Auto MDI/MDX, surge protected
- **Physical and Power**
  - PoE: DC 48V/0.4A
  - Form Factor: Wall or Pole Mountable
  - Dimensions (W x D x H): 6.5" x 3.8" x 1.9" (165 x 96 x 48 mm)
  - Weight: 1.6 lbs (0.72 kg)

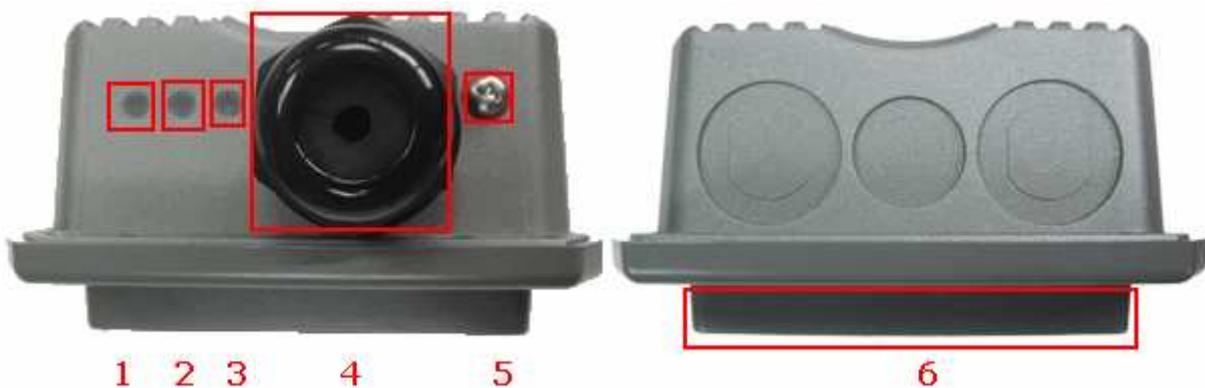
## 2.3 Panel Function Description

### OWL400



1	<b>Power</b>	Green LED <b>ON</b> indicates power on, and <b>OFF</b> indicates power off
2	<b>WLAN</b>	Green LED <b>ON</b> indicates system ready
3	<b>LAN</b>	Green LED <b>ON</b> indicates connection; <b>BLINKING</b> indicates transmitting data; <b>OFF</b> indicates no connection
4	<b>PoE Connector</b>	For connecting to the Power Sourcing Equipment (PSE)
5	<b>Reset</b>	Press more than 5 seconds and release to reset the system to its default settings
6	<b>Primary N-type Antenna Connector</b>	For connecting to an antenna
7	<b>N-type Connector</b>	For connecting to an antenna

### OWL410

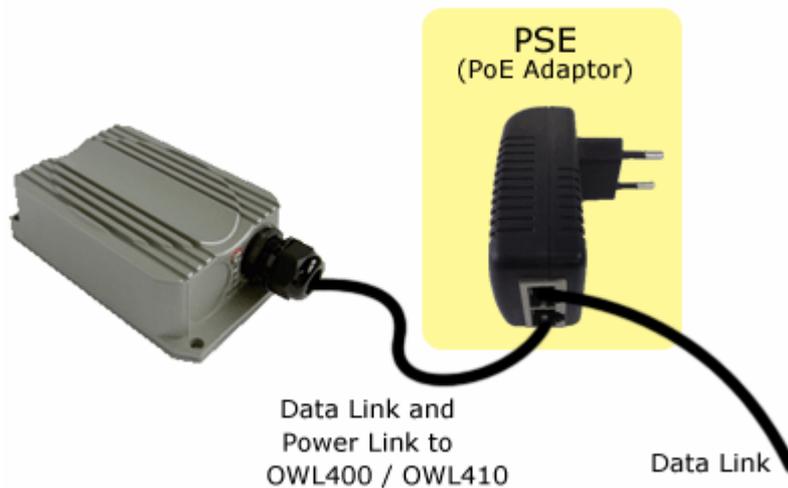
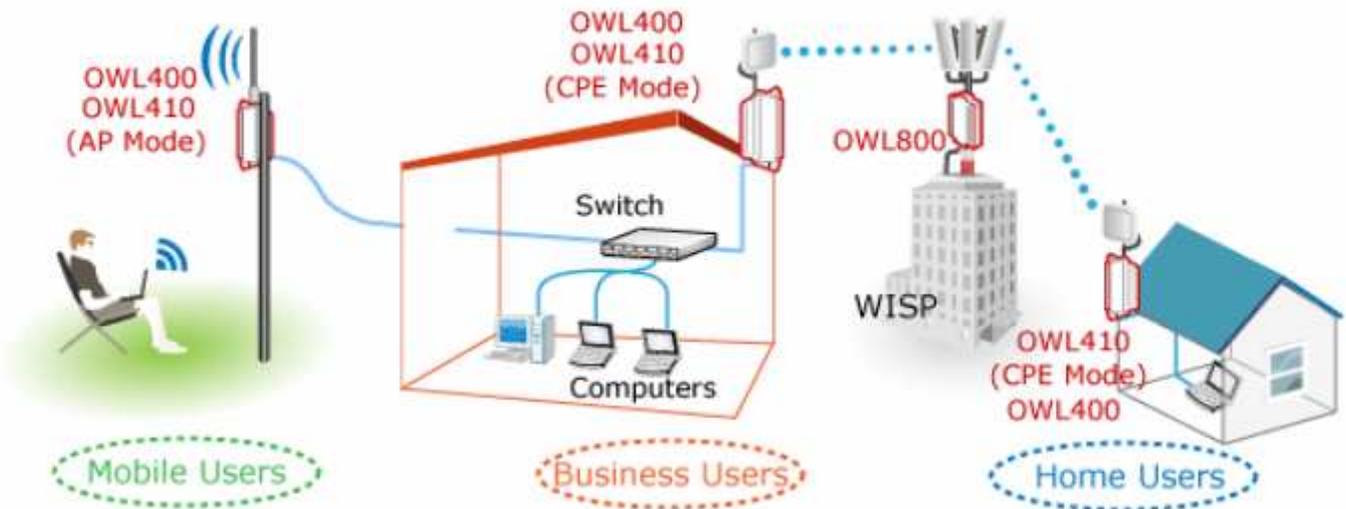


1	<b>Power</b>	Green LED <b>ON</b> indicates power on, and <b>OFF</b> indicates power off
2	<b>WLAN</b>	Green LED <b>ON</b> indicates system ready
3	<b>LAN</b>	Green LED <b>ON</b> indicates connection; <b>BLINKING</b> indicates transmitting data; <b>OFF</b> indicates no connection
4	<b>PoE Connector</b>	For connecting to the Power Sourcing Equipment (PSE)
5	<b>Reset</b>	Press more than 5 seconds and release to reset the system to its default settings
6	<b>Built-in patch antenna</b>	14 dBi (Horizontal: 25 degree; Vertical: 25 degree)

### 3. Installation

#### 3.1 Hardware Installation

The following diagram is a **basic network topology** which can be used for testing and configuring the OWL400/410.



#### Installation Steps:

- Step 1.** Connect the antennas to the connectors (applicable for OWL400 only).
- Step 2.** Connect the Ethernet Port of OWL400/410 to POWER & DATA OUT Port of the PSE.
- Step 3.** Connect one end of an Ethernet cable to the Data Port of PSE and the other end to the computer.
- Step 4.** Plug the PSE in order to supply power to the OWL400/410.

## 3.2 Basic Configuration

### 3.2.1 Introduction to Web Management Interface

OWL400/410 provides a user friendly web management interface for configuration. As OWL400/410 is a dual-mode system which can be configured as either an access point (AP Mode) or a gateway (CPE Mode) based on your needs, it is required to follow the respective installation procedures provided to properly set up the desired mode for this system.

- **Default IP Address of Web Management Interface:**

The default IP address and Subnet Mask for the AP mode and CPE mode are as follows:

Mode	AP Mode	CPE Mode
IP Address	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0

In addition, there are two system management accounts for AP & CPE mode to maintain the system, **root** and **admin**, and each has different levels of management capabilities. The **root** account is empowered with full privileges while the **admin** account is with partial ones. And there is only one management account for AP mode, **root**. For more information on the privileges of these two accounts, please refer to **Appendix A. System Management Account Privileges**.

- **Default User Name and Password:**

The default **User name** and **Password** for both the **root** and **admin** account are as follows:

Mode	AP Mode	CPE Mode	
Management Account	Root Account	Root Account	Admin Account
User Name	root	root	admin
Password	admin	admin	admin

#### < AP Mode – Default Mode >

##### **Step 1: IP Segment Set-up for Administrator PC**

Set a static IP address on the same subnet mask as OWL400/410 in TCP/IP of the administrator PC, such as the following example. Do not duplicate the IP address used here with the IP address of OWL400/410 or any other devices within the same network.

##### **>> Example of IP Segment:**

The valid range of IP address is 1 ~ 254. However, **1** must be avoided as it is already used by OWL400/410. Below depicts an example of using **100** (the underlined value can be changed as desired).

- IP Address: 192.168.1.100
- Subnet Mask: 255.255.255.0

**Step 2: Launch Web Browser**

Launch a web browser to access the web management interface of AP mode by entering the default IP address, **http://192.168.1.1/**, in the URL field, and then press **Enter**.



Using an incorrect default IP address will result in no Login page shown on the web browser. Please make sure a correct IP address is used; refer to **Section 3.2.1 Instruction to Web Management Interface** for detailed default IP addresses.

**Step 3: System Login**

The system manager Login Page will then appear.

Enter "**root**" in the *User name* field and "**admin**" in the *Password* field, and then click **Login** to log in.



**Step 4: Login Success**

The **System Overview** page will appear after a successful login.

To logout, simply click on the Logout button on the top right hand corner of the management interface.

Home > Status > System Overview

### System Overview

**System**

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.8-1.2628
Location	CA, US
Site	EN-A
Device Time	1999/12/31 16:10:40
System Up Time	0 days, 0:10:40
Operating Mode	AP

**Radio Status**

MAC Address	00:1F:D4:00:31:40
Band	802.11a
Channel	36
TX Power	Highest

**LAN Interface**

MAC Address	00:1F:D4:00:30:F9
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

**AP Status**

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:31:40	OWL400-1	None	0

## &lt; CPE Mode &gt;

**Step 1: Launch Web Browser**

Launch a web browser to access the web management interface of CPE mode by entering the default IP address, **http://192.168.1.1/**, in the URL field, and then press **Enter**.



*Using an incorrect default IP address will result in no Login page shown on the web browser. Please make sure a correct IP address is used.*

**Step 2: System Login**

The system manager Login Page will then appear.

Enter "**root**" in the *User name* field and "**admin**" in the *Password* field, and then click **Login** to log in.

Below depicts an example of using the **root** manager account.

**Step 3: Login Success**

After a successful login into OWL400/410, a **System Overview** page of web management interface will appear.

To logout, simply click on the **Logout** button at the upper right hand corner of the interface.

System Overview | Event Log | DHCP Lease | UPnP

System | Wireless | Firewall | Utilities | Status

System Overview | Event Log | DHCP Lease | UPnP

Home > Status > System Overview

## System Overview



### System

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.8-1.2628
Location	CA, US
Site	EN-A
Device Time	2000/01/01 13:29:24
System Up Time	0 days, 21:29:24
Operating Mode	CPE



### Radio Status

Status	Disable
SSID	N/A
MAC Address	N/A
Channel	56
Signal Strength	12
Security	None



### LAN Interface

MAC Address	00:1F:D4:00:30:F9
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled



### WAN Interface

Mode	Static
MAC Address	00:1F:D4:00:31:40
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
Bandwidth	Down: Unlimited / UP: Unlimited

### 3.2.2 Quick Configuration

OWL400/410 is a dual-mode system which can be configured as either an access point (**AP Mode**) or a gateway (**CPE Mode**) based on deployment needs. This section provides a step-by-step configuration procedure for installing CPE mode and AP mode respectively.

< **AP Mode – Default Mode** >

**Step 1: Mode Confirmation**

The screenshot shows the web interface navigation menu with 'System', 'Wireless', 'Utilities', and 'Status' buttons. The 'Status' button is highlighted with a red border. Below the menu, the 'System Overview' page is displayed. The 'System' section shows the following details:

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.8-1.2628
Location	CA, US
Site	EN-A
Device Time	1999/12/31 16:10:40
System Up Time	0 days, 0:10:40
Operating Mode	AP

The 'Radio Status' section shows:

MAC Address	00:1F:D4:00:31:40
Band	802.11a
Channel	36
TX Power	Highest

The 'AP Status' section shows a table with the following data:

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:31:40	OWL400-1	None	0

The 'LAN Interface' section shows:

MAC Address	00:1F:D4:00:30:F9
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

- Ensure that the *Operating Mode* is currently at **AP** mode.
- Click on the **Status** button and then select the **System Overview** tab. The *Operating Mode* is at the **System** section on the **System Overview** page.

▶ **Note:** For more information on switching to AP mode, if it is not currently active, please refer to **AP Mode Section 4.1.2 Operating Mode**.

**Step 2: Change Password**

System Wireless Utilities Status

Change Password Network Utilities Config Save & Restore System Upgrade Reboot

Home > Utilities > Change Password

### Change Password

Name : root

Old Password :

New Password :  \*up to 32 characters

Re-enter New Password :

- Click on the **Utilities** button and then select the **Password** tab.
- Enter a new password in the *New Password* field and retype it in the *Re-enter New Password* field.
- Click **SAVE** to save the changes.

**Step 3: Network Settings**

System Information Operating Mode **Network** Management

Home > System > Network Interface

### Network Settings

**Mode :**  Static  DHCP

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

**Layer2 STP :**  Disable  Enable

【Settings here are for example only.】

- Click on the **System** button and then select the **Network** tab.
- Enable *Static*, and then enter the related information in the fields marked with red asterisks.
- Click **SAVE** to save the settings.

**Step 4: SSID Settings**

Home > Wireless > General

### General Settings

Band : 802.11a

Short Preamble :  Disable  Enable

Channel : 64

Max Transmit Rate : Auto

Transmit Power : Auto

Beacon Interval : 100 \*(100 - 500ms)

- Click on the **Wireless** button and then select the **General** tab.
- **Band:** Select an appropriate band from the drop-down list box.

Home > Wireless > VAP Config

### VAP Configuration

Profile Name : VAP-1

VAP :  Disable  Enable

Profile Name : VAP-1

ESSID : OWL400-1

VLAN ID :  Disable  Enable

VLAN ID : \*( 1 - 4094 )

- Click on the **Wireless** button and then select the **VAP Config** tab.
- **ESSID:** Enter respective ESSID for each VAP in the *ESSID* field or use the default. **ESSID (Extended Service Set Identifier)** is a unique identifier used for networking devices to get associated with OWL400/410.
- Click **SAVE** to save the settings.

**Step 5: Security Settings**

The screenshot shows the 'Security Settings' configuration page. At the top, there are four main navigation buttons: 'System', 'Wireless' (highlighted with a red box), 'Utilities', and 'Status'. Below these are several sub-tabs: 'VAP Overview', 'General', 'VAP Config', 'Security' (highlighted with a red box), 'Repeater', 'Advanced', 'Access Control', and 'Site Survey'. The breadcrumb path is 'Home > Wireless > Security'. The main title is 'Security Settings'. A 'Profile Name' dropdown is set to 'VAP-1'. The 'Security Type' dropdown is set to 'WEP'. A note states: 'Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.' Under '802.11 Authentication', 'Open System' is selected. 'WEP Key Length' is set to '64 bits', 'WEP Key Format' is set to 'ASCII', and 'WEP Key Index' is set to '4'. There are four 'WEP Keys' input fields; the first contains '1234' and the others are empty.

- Click on the **Wireless** button and then select the **Security** tab.
- Select the desired *VAP Profile and Security Type* from the drop-down list boxes. The above figure depicts an example of selecting VAP-1 and **WEP**.
- Enter the information required in the blank fields.

 *You must use the same information provided here to configure the network devices that are to be associated with OWL400/410.*

- Click **SAVE** to save all settings configured so far. All updated settings will take effect upon reboot.

**Congratulations!**

The AP mode is now successfully configured.

< CPE Mode >

**Step 1: Mode Confirmation**

The screenshot shows the 4IPNET web interface. At the top, there are navigation buttons for System, Wireless, Firewall, Utilities, and Status. The Status button is highlighted with a red box. Below these are sub-tabs for System Overview, Event Log, DHCP Lease, and UPnP. The System Overview tab is selected and highlighted with a red box. The breadcrumb path is Home > Status > System Overview. The main content area is titled 'System Overview' and contains four sections: System, Radio Status, LAN Interface, and WAN Interface. In the System section, the 'Operating Mode' is set to 'CPE' and is highlighted with a red box.

System	
System Name	OWL400
Firmware Version	1.00.00
Build Number	1.8-1.2628
Location	CA, US
Site	EN-A
Device Time	2000/01/01 13:29:24
System Up Time	0 days, 21:29:24
Operating Mode	CPE

Radio Status	
Status	Disable
SSID	N/A
MAC Address	N/A
Channel	56
Signal Strength	12
Security	None

LAN Interface	
MAC Address	00:1F:D4:00:30:F9
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

WAN Interface	
Mode	Static
MAC Address	00:1F:D4:00:31:40
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
Bandwidth	Down: Unlimited / UP: Unlimited

- Ensure that the *Operating Mode* is currently at **CPE** mode.
- Click on the **Status** button and then select the **System Overview** tab. The *Operating Mode* is at the **System** section on the **System Overview** page.

➤ **Note:** For more information on switching to CPE mode, if it is not currently active, please refer to **Section 5.1.2 Operating Mode**.

**Step 2: Change Password**

Home > Utilities > Change Password

### Change Password

**Name :** root

**Old Password :**

**New Password :**  \*up to 32 characters

**Re-enter New Password :**

**Name :** admin

**New Password :**  \*up to 32 characters

**Re-enter New Password :**

- Click on the **Utilities** button and then select the **Change Password** tab.
- **Change Root Account Password**
  - Enter the old password in the *Old Password* field, which default password is “**admin**”.
  - Enter a new password in the *New Password* field and retype it in the *Re-enter New Password* field.
- **Change Admin Account Password**
  - Enter a new password in the *New Password* field and retype it in the *Re-enter New Password* field.
- Click **SAVE** to save the changes.

**Step 3: Site Survey**

System Wireless Firewall Utilities Status

General Advanced Security Site Survey

Home > Wireless > Site Survey

### Scan Result

Scan Again!

SSID	MAC Address	Channel	Signal	Security	Setup / Connect
------	-------------	---------	--------	----------	-----------------

【The scan result displayed here is an example only.】

- Click on the **Wireless** button and then select the **Site Survey** tab.
- The system will automatically scan and display all APs in the same OWL400/410's coverage area.
- Click **Scan Again** if the APs to be associated with are not listed on the **Scan Result** list.

**Step 4: Select AP to be Associated**

- Select an AP to be associated with from the **Scan Result** list provided in **Step 3**.

**Step 5: Security Settings**

Home > Wireless > Site Survey

### Scan Result

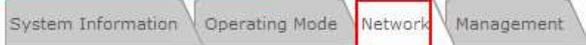
[Scan Again!](#)

SSID	MAC Address	Channel	Signal	Security	Setup / Connect
b0b24b	00:0B:6B:DD:A7:EE	36	20	WEP	<a href="#">Setup</a>
9595d5	00:0B:6B:DD:27:A6	36	34	WEP	<a href="#">Setup</a>
rh-OWL410-none	00:1F:D4:00:31:78	56	15	NONE	<a href="#">Connect</a>
471f2a	00:0B:6B:DD:27:B9	56	10	WEP	<a href="#">Setup</a>

- The above figure depicts an example of selecting one SSID (encrypted via one security type).
- Click **Setup**, and then a related encryption configuration box will appear.
- Enter the information required in the configuration box. Information to be entered must be exactly the same as configured in this **AP**.
- Click **Connect** to start the connection.

**Step 6: Network Interface Configuration**

- Click on the **System** button and then select the **Network** tab.



Home > System > Network Interface

### WAN Configuration

Mode :  Static  DHCP

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

Bandwidth Limit :

Download :  ▼

Upload :  ▼

### Dynamic DNS (DDNS)

DDNS :  Disable  Enable

Provider :

Host Name :

User Name / E-mail :

Password / Key :

### LAN Configuration

IP Address :  \*

Netmask :  \*

DHCP Server :  Disable  Enable

Start IP :  \*

End IP :  \*

Preferred DNS Server :  \*

Alternated DNS Server :

WINS Server IP :

Domain Name :

Lease Time :  ▼

【Settings here are for example only.】

**WAN Configuration**

- Enable *Static*, and then enter the related information in the fields marked with red asterisks.
- Click **SAVE** to save the settings.

**Dynamic DNS Configuration**

- The **Dynamic DNS** section is on the same page as **WAN Configuration** section.

- When enabled, choose the service *Provider* with provided *Host Name*, *User Name/E-mail*, and *Password/Key*.
- Click **SAVE** to save all settings configured so far. All updated settings will take effect upon reboot.

#### **LAN Configuration**

- The **LAN Configuration** section is on the same page as **WAN Configuration** section.
- Provide the information to the required field by entering IP address/Netmask of the LAN port.
- Click **SAVE** to save all settings configured so far. All updated settings will take effect upon reboot.

### ***Congratulations!***

The CPE mode is now successfully configured.

## 4. AP Mode Configuration

When AP mode is activated, the system can be configured as an Access Point or an Access Point with Repeater depending on deployment needs. This chapter will guide you through setting up the AP mode with graphical illustrations. The following table shows all the functions of OWL400/410 in its AP mode.

OPTION	System	Wireless	Utilities	Status
<b>FUNCTION</b>	System Information	Virtual AP Overview	Change Password	System Overview
	Operating Mode	General Settings	Network Utilities	Associated Client Status
	Network Settings	VAP Configuration	Configuration Save & Restore	Repeater Information
	Management Services	Security Settings	System Upgrade	Event Log
		Repeater Settings	Reboot	
		Advanced Wireless Settings		
		Access Control Settings		
		Site Survey		

**AP Mode Functions**

System      Wireless      Utilities      Status

Overview   Clients   Repeater   Event Log

Home > Status > System Overview

## System Overview

### System

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.8-1.2628
Location	CA, US
Site	EN-A
Device Time	1999/12/31 16:10:40
System Up Time	0 days, 0:10:40
Operating Mode	AP

### Radio Status

MAC Address	00:1F:D4:00:31:40
Band	802.11a
Channel	36
TX Power	Highest

### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:31:40	OWL400-1	None	0

### LAN Interface

MAC Address	00:1F:D4:00:30:F9
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

AP Mode Main Page

## 4.1 System

This section provides information for configuring the following functions: **System Information**, **Operating Mode**, **Network Settings**, and **Management Services**.

System Information    Operating Mode    Network    Management

Home > System > General

### System Information

**Name :**  \*

**Description :**

**Location :**

### Time

**Device Time :** 1999/12/31 16:10:48

**Time Zone :**  ▼

**Time :**  Enable NTP     Manually set up

**NTP Server 1 :**  \*

**NTP Server 2 :**

---

► **Note:** A system restart is required when a reminding message appears after clicking the **SAVE** button; all settings entered and saved will take effect only after the system restart.

---

## 4.1.1 System Information

For maintenance purpose, it is required to specify the system name, its location and corresponding basic parameters. Fields such as *Name*, *Description* and *Location* are used for mnemonic purpose. It is recommended to have different values in each AP.

System Information | Operating Mode | Network | Management

Home > System > General

### System Information

Name : OWL400 \*

Description : 4IPNET, INC.

Location : CA, US

### Time

Device Time : 1999/12/31 16:10:48

Time Zone : (GMT-08:00)Pacific Time(US&Canada),Tijuana

Time :  Enable NTP  Manually set up

NTP Server 1 : tock.stdtime.gov.tw \*

NTP Server 2 :

- **System Information**

For maintenance purpose, it is recommended to have the following information stated as clearly as possible. Fields Name, Description, and Location are used for mnemonic purpose. It is recommended to have different values in each wireless device.

- **Name:** The system name used to identify this system.
- **Description:** Further information of the system.
- **Location:** The information on geographical location of the system for the administrator to locate the system easily.

- **Time**

Time settings allow the system time synchronized with NTP server or manually set.

- **Device Time:** Display the current time of the system.
- **Time Zone:** Select an appropriate time zone from the drop-down list box.
- **Synchronization:** Synchronize the system time either by NTP server or manual setup.

(1) **Enable NTP:**

By selecting **Enable NTP**, OWL400/410 can synchronize its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address or domain name must be provided. If FQDN (full qualified domain name) is used as the IP address of NTP server, the DNS server must also be activated (please refer to **4.1.3 Network Settings**).

**Time**

Device Time : 1999/12/31 17:21:04

Time Zone : (GMT-08:00)Pacific Time(US&Canada),Tijuana

Time :  Enable NTP  Manually set up

NTP Server 1 : tock.stdtime.gov.tw \*

NTP Server 2 :

(2) **Manually set up:**

By selecting **manually set up**, the administrator can manually set the system date and time.

**Time**

Device Time : 1999/12/31 17:21:04

Time Zone : (GMT-08:00)Pacific Time(US&Canada),Tijuana

Time :  Enable NTP  Manually set up

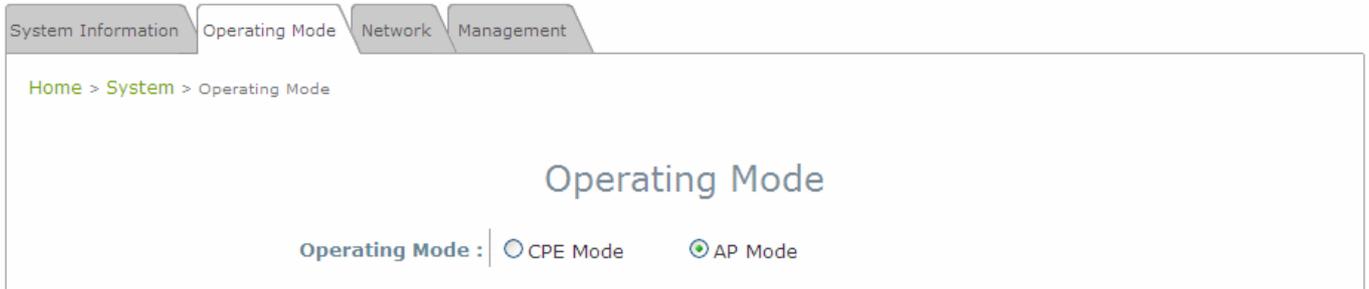
Set Date : Year Month Day

Set Time : Hour Min Sec

- *Set Date:* Select the appropriate *Year*, *Month*, and *Day* from the drop-down list box.
- *Set Time:* Select the appropriate *Hour*, *Min*, and *Sec* from the drop-down list box.

## 4.1.2 Operating Mode

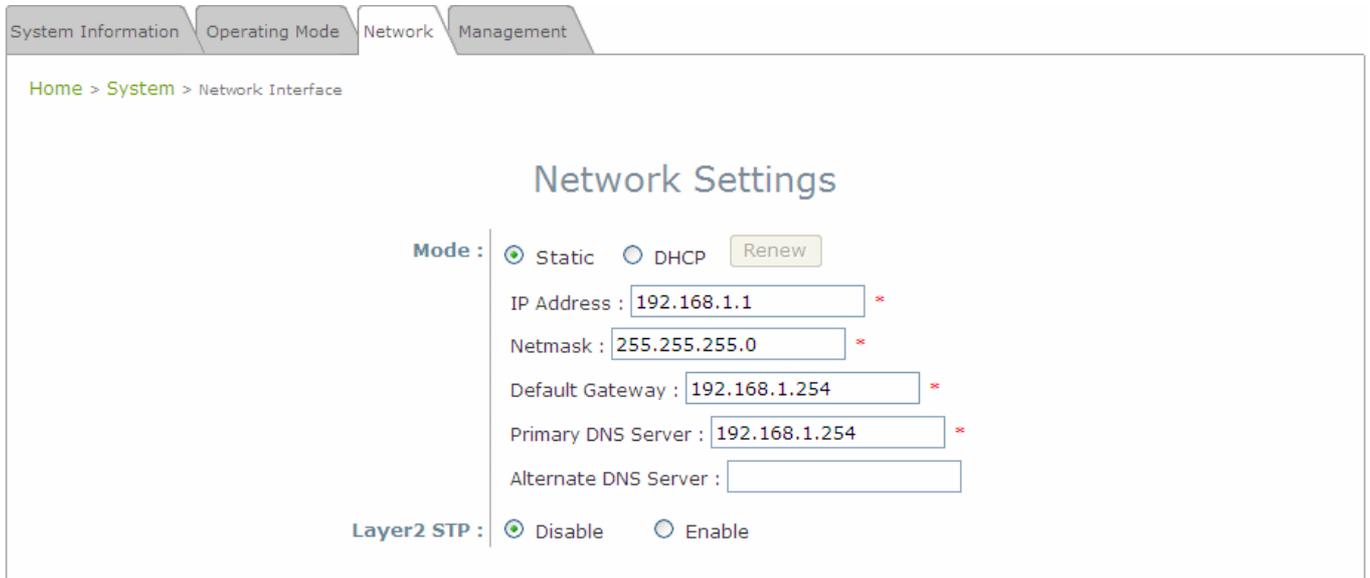
OWL400/410 supports two operation modes: AP mode and CPE mode. The administrator can set the desired mode on this page, and then configure the system according to deployment needs.



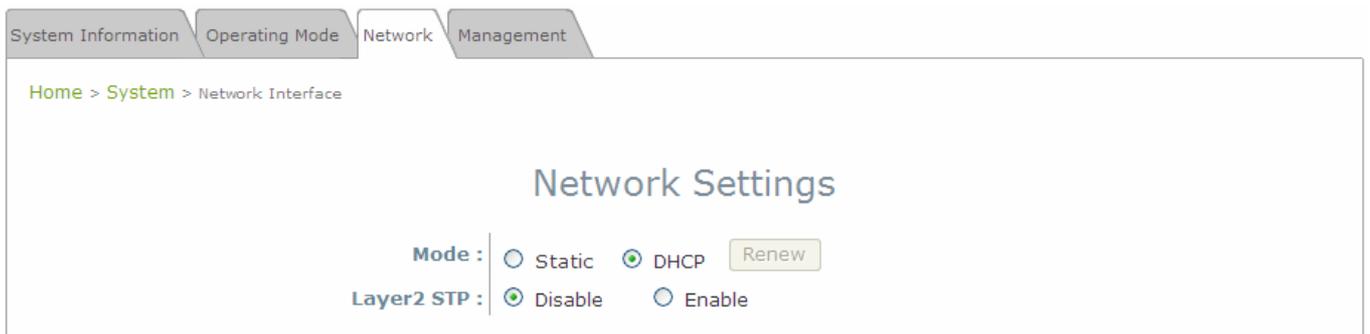
- **Operating Mode:** Select the desired mode and then click **SAVE** to save the setting.

### 4.1.3 Network Settings

LAN settings can be configured on this page.



- **Mode:** Determine the way to obtain the IP address, by *DHCP* or *Static* manually set.
  - **Static:** Static setting is set these parameters manually. The basic parameters need to provide such as IP address, subnet mask and Gateway.
    - **IP Address:** The IP address of the LAN port.
    - **Netmask:** The Subnet mask of the LAN port.
    - **Gateway:** The Gateway IP address of the LAN port.
    - **Primary/Secondary DNS Server:** Please provide at least on DNS server's IP address.
  - **DHCP:** The option is provided when a DHCP server is provided in the network. The following IP address/Netmask/Gateway setting will be disabled.



- **Layer 2 STP:** Depending on the configuration of the system including wired and wireless settings, when it is configured to bridge several networks, it is suggested to enable STP.

## 4.1.4 Management Services

The system supports **VLAN**, **SNMP**, **Remote Syslog**, and **Auto Reboot** functions for easy management. These functions can be configured on this page.

- **VLAN for Management:** The Ethernet traffic from the system can be tagged with VLAN tag with specific ID.
- **SNMP Configuration:** By enabling SNMP service, the remote SNMP manager could obtain the system status.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to deactivate it.
  - **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system.
    - **Read:** Enter the community string to access the MIB with Read privilege.
    - **Write:** Enter the community string to access the MIB with Write privilege.
  - **Trap:** When enabled, events such as Cold Start, Interface UP & Down, and etc can be reported to an assigned server.
    - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to deactivate it.
    - **Server IP Address:** Enter the IP address of the assigned server for receiving the trap report.

- **Syslog Configuration:** By enabling this function, specify a remote syslog server which could accept system log messages from the system remotely. Therefore, by reading the syslog message in the remote server, the administrator can review activities of all installed systems in the network.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to deactivate it.
  - **Server IP:** The IP address of the Syslog server for receiving the reported events.
  - **Server Port:** The port number of the Syslog server.
  - **Log Level:** Select the desired level of received events from the drop-down list.
  
- **Auto Reboot:** The option can be enabled to reboot system automatically with preferred Reboot Time from drop-down list.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to deactivate it.
  - **Reboot Time:** Select an appropriate time from the drop-down list. Since all users on the network will be disconnected during reboot, it is suggested to set the reboot time during an off-peak period to reduce impacts on online users.

## 4.2 Wireless

The administrator can configure the following wireless settings on this page: **VAP Overview, General Settings, VAP Configuration, Security Settings, Repeater Settings, Advanced Wireless Settings, Access Control Settings,** and **Site Survey**. The system supports up to seven Virtual Access Points (VAPs). Each VAP can have its own settings including ESSID, VLAN ID, security settings, etc. Such VAP capability enables different levels of service to meet actual requirements.

The screenshot shows the 4IPNET web interface. At the top, there are four main menu buttons: System, Wireless (highlighted with a red border), Utilities, and Status. Below these are sub-menus for VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. A breadcrumb trail reads 'Home > Wireless > VAP Overview'. The main content area is titled 'VAP Overview' and contains a table with the following data:

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	OWL400-1	Enabled	None	Disabled	<a href="#">Edit</a>
2	OWL400-2	Disabled	None	Disabled	<a href="#">Edit</a>
3	OWL400-3	Disabled	None	Disabled	<a href="#">Edit</a>
4	OWL400-4	Disabled	None	Disabled	<a href="#">Edit</a>
5	OWL400-5	Disabled	None	Disabled	<a href="#">Edit</a>
6	OWL400-6	Disabled	None	Disabled	<a href="#">Edit</a>
7	OWL400-7	Disabled	None	Disabled	<a href="#">Edit</a>

## 4.2.1 Virtual AP Overview

An overall status is collected in this page, including *Enable/Disable State*, *Security Type*, *MAC ACL* state, and *Advanced Settings*. The system has 7 VAPs; each has its own settings. In this table, please click on the hyperlink for further configuration of each VAP respectively.

VAP Overview
General
VAP Config
Security
Repeater
Advanced
Access Control
Site Survey

[Home](#) > [Wireless](#) > VAP Overview

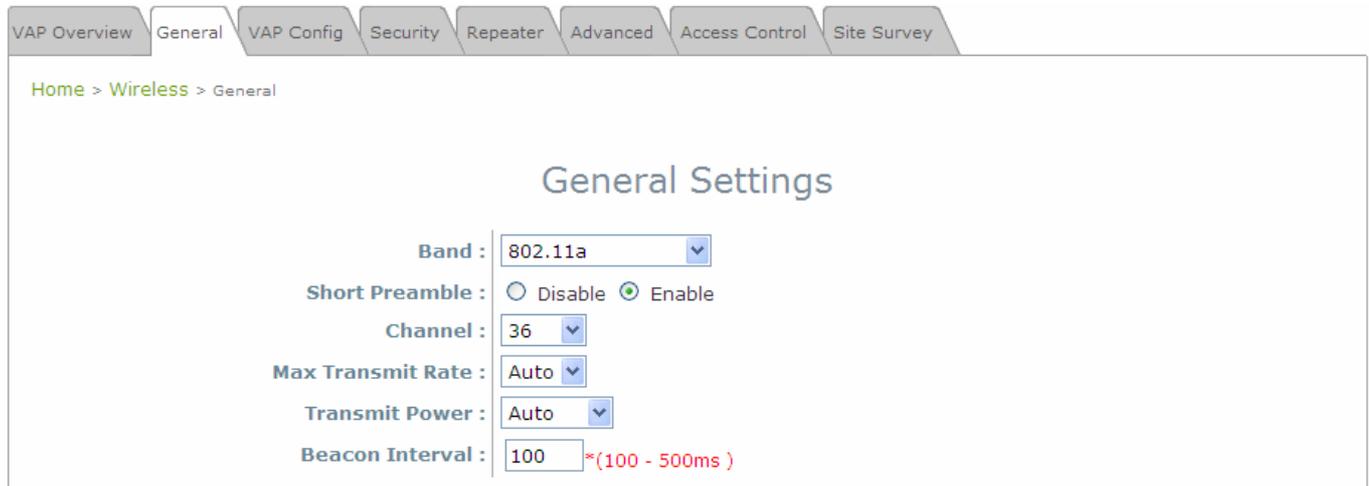
### VAP Overview

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	OWL400-1	<a href="#">Enabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
2	OWL400-2	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
3	OWL400-3	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
4	OWL400-4	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
5	OWL400-5	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
6	OWL400-6	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
7	OWL400-7	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>

- **State:** The hyperlink showing *Enabled* or *Disabled* connects to the screen of **VAP Configuration**.
- **Security Type:** The hyperlink showing security type connects to the screen of **Security Settings**.
- **MAC ACL:** The hyperlink showing *Allow* or *Disabled* connects to the screen of **Access Control Settings**.
- **Advanced Settings:** The hyperlink of advanced settings connects to the screen of **Advanced Wireless Settings**.

## 4.2.2 General Settings

This section is for configuring the system RF settings.



Home > Wireless > General

### General Settings

Band : 802.11a

Short Preamble :  Disable  Enable

Channel : 36

Max Transmit Rate : Auto

Transmit Power : Auto

Beacon Interval : 100 \*(100 - 500ms )

- **Band:** Select an appropriate wireless frequency band of this system. Select one frequency band from *Disable*, *802.11a*, or mixed mode *802.11a+802.11n*.
- **Short Preamble:** The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select *Enable* to use Short Preamble or *Disable* to use Long Preamble with a 128-bit synchronization field.
- **Short Guard Interval (802.11a + 802.11n):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. With 802.11n, short guard interval is half of what used to be to increase throughput. Select *Enable* to use Short Guard Interval or *Disable* to use normal Guard Interval.
- **Channel Width (802.11a + 802.11n):** For 802.11n in 5GHz, double channel bandwidth to 40 MHz is supported to enhance throughput.
- **Channel Width Extension:** Either Above or Below (the primary channel) can be selected for the extension channel when channel width is 40MHz.
- **Channel:** Select the appropriate channel from the drop-down list box to correspond with your network settings.
- **Max Transmit Rate:** Select transmit rate from *6M* to *54M* (802.11a), *6M* to *MCS 15* (802.11a + 802.11n), or *Auto*.
- **Transmit Power:** Select from the lowest to highest power level or choose *Auto*.
- **Beacon Interval:** Provide the value of Beacon Interval from 100 to 500ms.

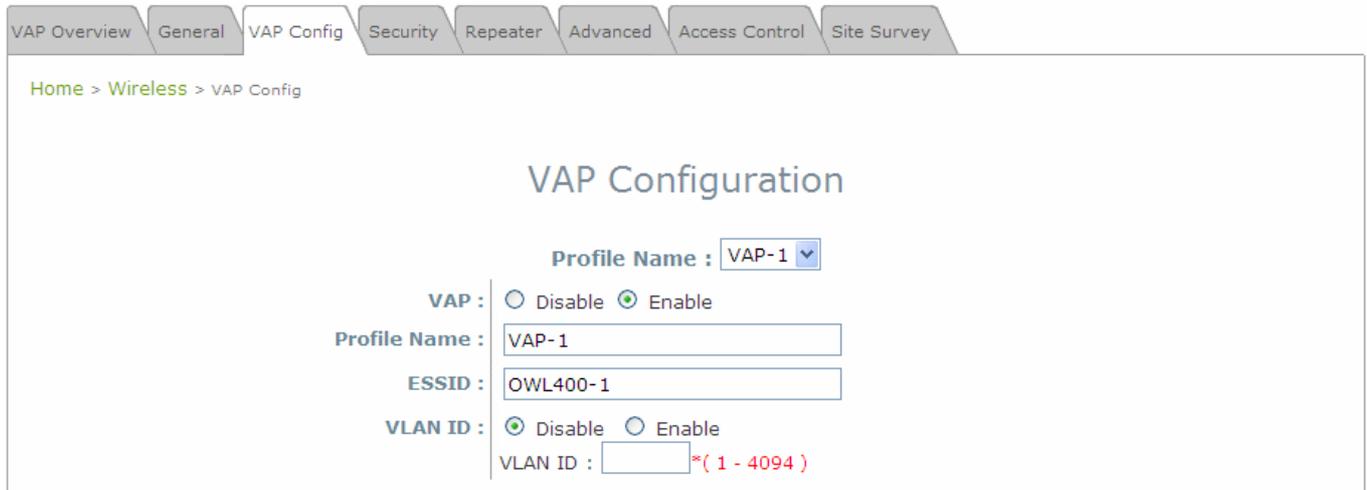
The RF settings in this page will be applied to all VAPs.

Under normal circumstances, the available RF configurations are illustrated as below:

◆ **RF Configurations (under normal circumstances in certain countries)**

Band	Channel	Max Transmit Rate	Transmit Power
Disable	N/A	N/A	N/A
802.11a	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	Auto, Lowest, Low, Medium, High, Highest
802.11a+802.11n	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~15	

## 4.2.3 VAP Configuration



Home > Wireless > VAP Config

### VAP Configuration

Profile Name : VAP-1

VAP :  Disable  Enable

Profile Name : VAP-1

ESSID : OWL400-1

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

To enable each VAP, the administrator must configure each VAP manually. The settings of each VAP are collected as its profile.

- **Enable VAP:** Enable or disable the respective VAP.
- **Profile Name:** The profile name of each VAP for identity/management purpose.
- **ESSID:** ESSID (Extended Service Set ID) indicates a unique SSID used by a client device to associate with a specified VAP. ESSID determines the service level assigned to a client.
- **VLAN ID:** The system supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP must have a unique VLAN ID; valid values are ranged from 1 to 4094.

## 4.2.4 Security Settings

The system supports various user authentication and data encryption methods in each VAP profile. Thus the administrator can depend on the need to provide different service levels to clients. The security type includes **None**, **WEP**, **802.1X**, **WPA-PSK**, and **WPA-RADIUS**.

- **None:** No authentication is required.

The screenshot shows the 'Security Settings' page in a web interface. At the top, there are navigation tabs: VAP Overview, General, VAP Config, Security (selected), Repeater, Advanced, Access Control, and Site Survey. Below the tabs is a breadcrumb trail: Home > Wireless > Security. The main heading is 'Security Settings'. Underneath, there is a 'Profile Name' dropdown menu set to 'VAP-1'. Below that is a 'Security Type' dropdown menu set to 'None'.

- **WEP:** WEP (Wired Equivalent Privacy) supports key length of 64/128 bits.

The screenshot shows the 'Security Settings' page with 'Security Type' set to 'WEP'. The 'Profile Name' dropdown is still 'VAP-1'. Below the 'Security Type' dropdown, there is a red note: 'Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.' Underneath the note are several settings: '802.11 Authentication' with radio buttons for 'Open System' (selected), 'Shared Key', and 'Auto'; 'WEP Key Length' with radio buttons for '64 bits' (selected) and '128 bits'; 'WEP Key Format' with radio buttons for 'ASCII' (selected) and 'Hex'; and 'WEP Key Index' with a dropdown menu set to '1'. At the bottom, there are four input fields labeled 'WEP Keys' numbered 1 through 4.

- **802.11 Authentication:** Select from *Open System*, *Shared Key*, or *Auto*.
- **WEP Key Length:** Select from *64-bit* or *128-bit* key length.
- **WEP Key Format:** Select from *ASCII* or *Hex* format for the WEP key.
- **WEP Key Index:** Select a key index from 1 through 4. The WEP key index is a number that specifies which WEP key to use for the encryption of wireless frames during data transmission.
- **WEP Keys:** Provide WEP key value; the system supports up to 4 sets of WEP keys.

- **802.1X:** Provide RADIUS authentication and enhanced WEP.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : 802.1X

Dynamic WEP :  Disable  Enable

WEP Key Length :  64 bits  128 bits

Rekeying Period : 300 second(s)

Primary RADIUS Server :

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :

➤ **Dynamic WEP Settings:**

- **Dynamic WEP:** By enabling this function, the system will automatically generate WEP keys for encryption.
- **WEP Key Length:** Select from *64-bit* or *128-bit* key length.
- **Rekeying Period:** The time interval for the WEP key to be updated; the time unit is in second.

➤ **Primary RADIUS Server Settings:**

- **Host:** Enter the IP address or domain name of the RADIUS server.
- **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
- **Secret Key:** The secret key for the system to communicate with the RADIUS server.

- **WPA-PSK:** Provide shared key authentication with WPA data encryption.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : WPA-PSK

Cipher Suite : TKIP (WPA)

Pre-shared Key Type :  PSK(Hex)\*( 64 chars )  Passphrase\*( 8 - 63 chars )

Pre-shared Key :

Group Key Update Period: 600 second(s)

- **Cipher Suite:** Select an encryption method from *TKIP (WPA)*, *AES (WPA)*, *TKIP(WAP2)*, *AES (WAP2)*, or *Mixed*.
- **Pre-shared Key Type:** Select a pre-shared key type: *PSK (Hex)* or *Passphrase*.
- **Pre-shared Key:** Enter the key value for the pre-shared key; the format of the key value depends on the key type selected.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in second.

- **WPA-RADIUS:** Authenticate users by RADIUS and provide WPA data encryption.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Security

## Security Settings

Profile Name : VAP-1 ▼

Security Type : WPA-RADIUS ▼

Cipher Suite : TKIP (WPA) ▼

Group Key Update Period: 600 second(s)

Primary RADIUS Server :

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :

➤ **WPA Settings:**

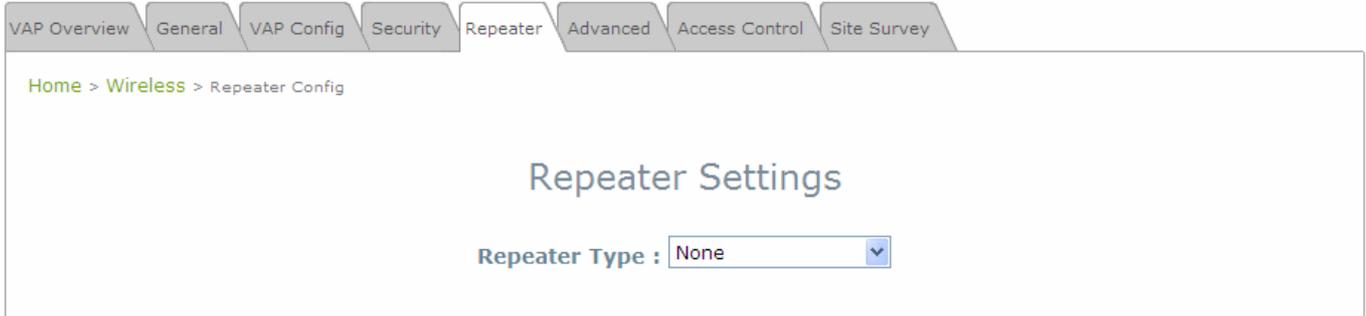
- **Cipher Suite:** Select an encryption method from *TKIP (WPA)*, *AES (WPA)*, *TKIP(WAP2)*, *AES (WAP2)*, or *Mixed*.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in second.

➤ **Primary RADIUS Server Settings:**

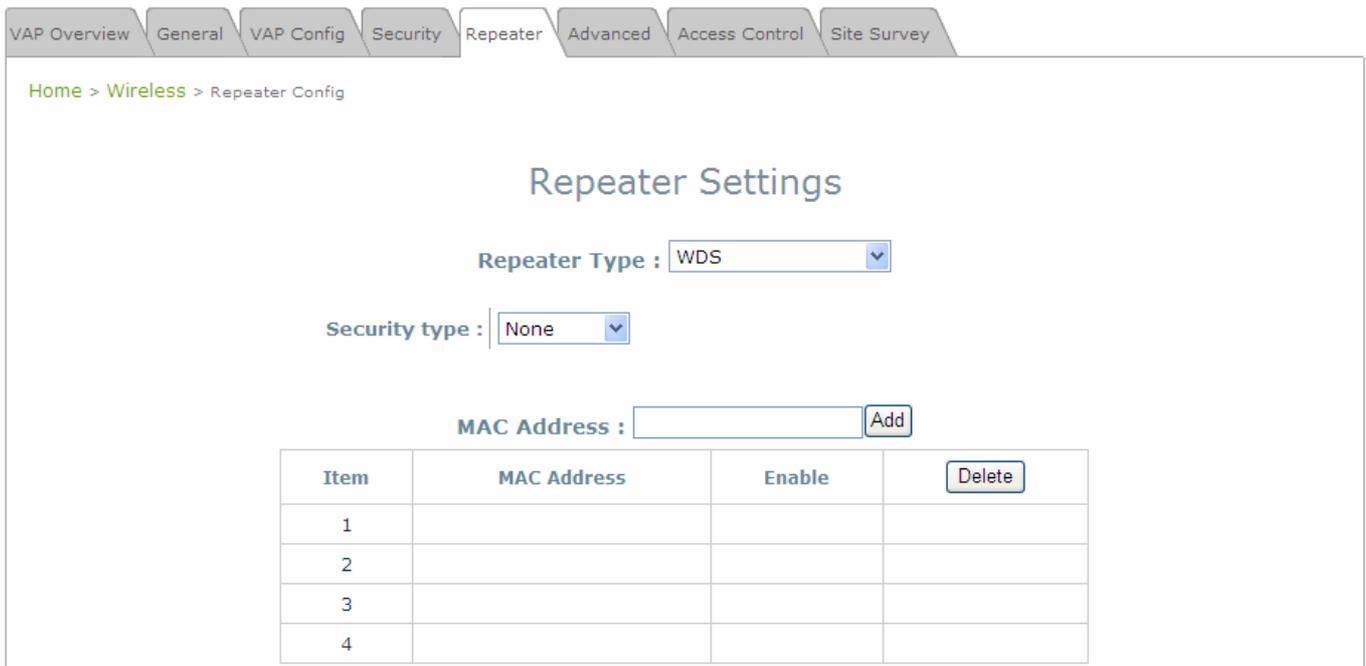
- **Host:** Enter the IP address or domain name of the RADIUS server.
- **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
- **Secret Key:** The secret key for the system to communicate with the RADIUS server.

## 4.2.5 Repeater Settings

The system can serve as an Access Point or an Access Point with Repeater depending on deployment needs. Select a *Repeater Type* from the drop-down list box and proceed with the related settings.



- **None:** When *None* is selected, the system is acting as an Access Point only; therefore, no further configuration is required here.
- **WDS:** The device supports up to 4 WDS peers. After providing WDS peer's MAC address, click on **Add** to add this link to the table shown on UI.



- **MAC:** Enter the MAC address of the WDS peer. Click **Add** to add it into the list.
- **MAC Address:** Display the MAC address of the WDS peer.
- **Enable:** Check **Enable** to activate the specified WDS link.
- **Delete:** Check **Delete** box and click **Delete** button to remove the specified WDS peer from the list.
- **Security Type:** Select an appropriate security type for the WDS link, either **None**, **WEP** or **WPA-PSK**; the type selected needs to be the same as the one configured at the WDS peer.

- Universal Repeater:** If Universal Repeater is chosen, please provide the SSID of upper-bound AP for uplink connection; Security Type (None, WEP, or WPA-PSK) can be configured for this Repeater connection. Please note the security type configured here needs to be the same as upper-bound AP to be connected.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Repeater Config

### Repeater Settings

Repeater Type :

The SSID of Upper-Bound AP : \*

Current wireless channel of the system is set at 36. Repeater connection may fail if the system is set to connect to upper AP with different channels

Security Type :

- **The SSID of Upper-Bound AP:** Specify the SSID of the upper-bound AP that the system is used to extend that AP's wireless service coverage.
- **Security Type:** Select the security type used by the upper-bound AP, **None**, **WEP** or **WPA-PSK**. Security settings configured here must be the same as the upper-bound AP.

### Repeater Settings

Repeater Type :

The SSID of Upper-Bound AP : \*

Current wireless channel of the system is set at 36. Repeater connection may fail if the system is set to connect to upper AP with different channels

Security Type :

Note!!!  
If you set WEP security for Universal Repeater the security of AP will also change to WEP and use the same settings.

WEP Key Type :  Open  Shared  Auto

WEP Key Length :  64 bits  128 bits

WEP Key Format :  ASCII  Hex

WEP Key Index :

WEP Keys :

1

2

3

4

## Repeater Settings

Repeater Type :

The SSID of Upper-Bound AP :

Current wireless channel of the system is set at 36. Repeater connection may fail if the system is set to connect to upper AP with different channels

Security Type :

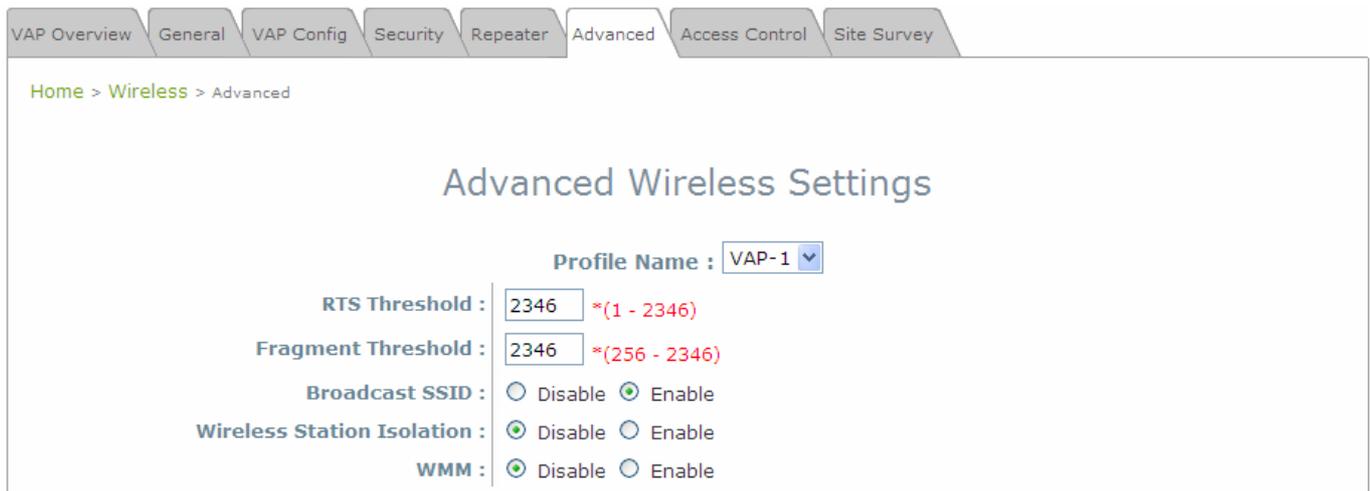
Cipher Suite :

Pre-shared Key Type :  PSK(Hex) \*( 64 chars )  Passphrase \*( 8 - 63 chars )

Pre-shared Key :

## 4.2.6 Advanced Wireless Settings

The advanced wireless settings for the system's VAP profiles allow customization of data transmission settings. The administrator can tune the following parameters to improve network communication performance if a poor connection occurs.



Home > Wireless > Advanced

### Advanced Wireless Settings

Profile Name : VAP-1

RTS Threshold : 2346 \*(1 - 2346)

Fragment Threshold : 2346 \*(256 - 2346)

Broadcast SSID :  Disable  Enable

Wireless Station Isolation :  Disable  Enable

WMM :  Disable  Enable

- **RTS Threshold:** To control station access to the medium and to alleviate this effect of the hidden terminal problem, the administrator can tune this RTS threshold value. A lower RTS Threshold setting can be useful in areas where many client devices are associating with OWL400/410 or in areas where the clients are far apart and can detect only OWL400/410 and not each other.
- **Fragmentation Threshold:** A unicast frame larger than this threshold will be fragmented before transmission. If a significant number of collisions are occurring, the administrator can try to set a smaller value of the threshold to see whether it helps. A smaller value results in smaller packets but allows a larger number of packets in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.
- **Broadcast SSID:** Disabling this function will prevent the system from broadcasting its SSID. If you disable broadcast of the SSID, only devices that have the correct SSID can connect to the system.
- **Wireless Station Isolation:** By enabling this function, all stations associated with the system can only communicate with the system.
- **WMM:** The default is *Disable*. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than voice and video. In short, WMM decides which data streams are the most important and assign them a higher traffic priority.

#### < To receive the benefits of WMM QoS >

- The application must support WMM.
- You must enable WMM in this system.
- You must enable WMM in the wireless adapter in your computer.

## 4.2.7 Access Control Settings

The administrator can restrict the wireless access of client devices based on their MAC addresses.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( Range: 1 ~ 32 )

Access Control Type : Disable Access Control

- **Maximum Number of Clients**

The system supports various methods of authenticating clients for using wireless LAN. The default policy is unlimited access without any authentication required. To restrict the station number of wireless connections, simply change the **Maximum Number of Stations** to a desired number. For example, while the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

- **Access Control Type**

The selected **Access Control Type** will be the activated policy while the rest will be omitted. The following is a list of the supported methods for MAC ACL control:

- (1) **Disable Access Control**

No MAC address check required.

(2) **MAC ACL Allow List**

Deny all except those in the Allow List. When selecting *MAC ACL Allow List*, all wireless connections to the specified VAP will be denied except the MAC addresses listed in the Allow List (“allowed MAC addresses”). The administrator can disable any allowed MAC address to connect to the VAP temporarily by checking *Disable*. For example, 11:22:33:44:55:66 is in the Allow List; to temporarily deny its access, check *Disable* in the **State** section.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients :  \*( Range: 1 ~ 32 )

Access Control Type : MAC ACL Allow List

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
3	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

(3) **MAC ACL Deny List**

Allow all except those in the Deny List. When selecting *MAC ACL Deny List*, all wireless connections to the specified VAP will be allowed except the MAC addresses listed in the Deny List (“denied MAC addresses”). The administrator can allow any denied MAC address to connect to the VAP temporarily by checking *Disable*.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

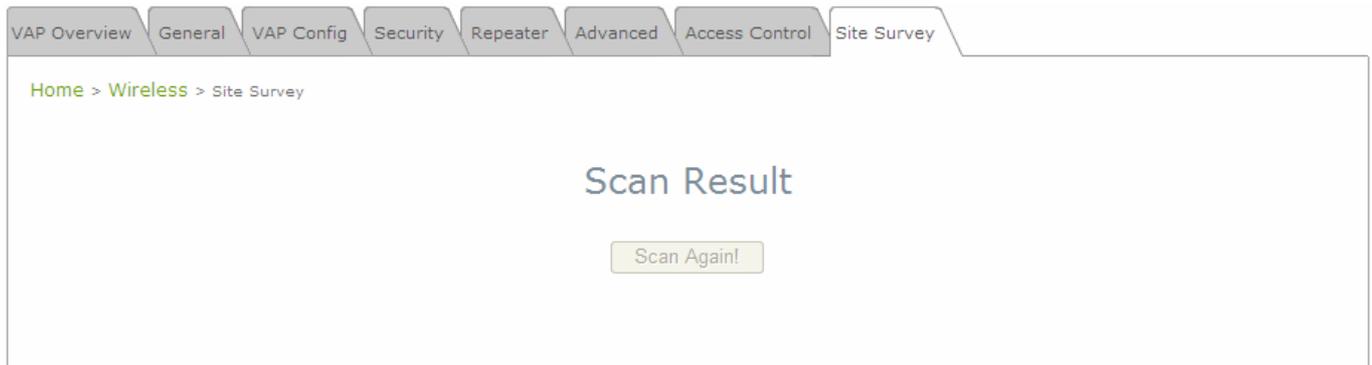
Maximum Number of Clients :  \*( Range: 1 ~ 32 )

Access Control Type : MAC ACL Deny List

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
3	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

## 4.2.8 Site Survey

The system can scan and display all surrounding available access points (APs) when Universal Repeater is enabled. Site Survey is a useful tool to provide information about the surrounding wireless environment; available APs are shown with their respective SSID, MAC Address, Channel, Rate setting, Signal reading and Security type. The administrator can click Setup or Connect to establish the wireless connection for Universal Repeater according to the mentioned readings.



*Site Survey- when repeater function is disabled.*

- **SSID:** The SSID (Service Set ID) of the AP found in the system's coverage area.
- **MAC Address:** The MAC address of the respective AP.
- **Channel:** The channel number currently used by the respective AP or repeater.
- **Rate:** The transmitting rate of the respective AP.
- **Signal:** The signal strength of the respective AP.
- **Security:** The encryption type used by the respective AP.
- **Setup/ Connect:**
  - **Connect:** Click **Connect** to associate with the respective AP directly; no further configuration is required.
  - **Setup:** Click **Setup** to configure security settings for associating with the respective AP.
    - **WEP:** Click **Setup** to configure the WEP setting for associating with the target AP.
    - **WPA-PSK:** Click **Setup** to configure the WPA-PSK setting for associating with the target AP.

### 4.3 Utilities

The administrator can maintain the system on this page: **Change Password, Network Utilities, Configuration Save & Restore, System Upgrade, and Reboot.**

The screenshot shows the 4IPNET web interface. At the top, there are four main menu buttons: System (with a blue router icon), Wireless (with a green antenna icon), Utilities (with a hammer icon and highlighted by a red border), and Status (with a document icon). Below these are sub-menu tabs: Change Password, Network Utilities, Config Save & Restore, System Upgrade, and Reboot. The breadcrumb trail reads: Home > Utilities > Change Password. The main heading is "Change Password". The form contains the following fields and labels:

- Name : root
- Old Password :
- New Password :  \*up to 32 characters
- Re-enter New Password :

At the bottom of the form are two yellow buttons: SAVE and CLEAR.

### 4.3.1 Change Password

The administrator can update or change password. The system provides one management account for AP mode, root account. The administrator can change password on this page.

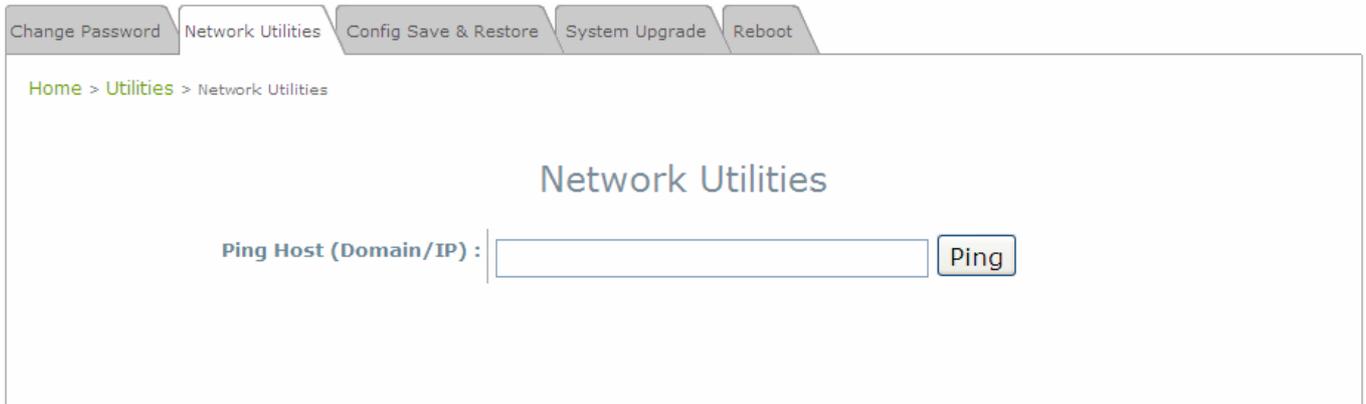
The screenshot shows a web interface with a navigation bar at the top containing tabs for 'Change Password', 'Network Utilities', 'Config Save & Restore', 'System Upgrade', and 'Reboot'. Below the navigation bar is a breadcrumb trail: 'Home > Utilities > Change Password'. The main content area is titled 'Change Password' and contains a form with the following fields:

Name :	root
Old Password :	<input type="password"/>
New Password :	<input type="password"/> *up to 32 characters
Re-enter New Password :	<input type="password"/>

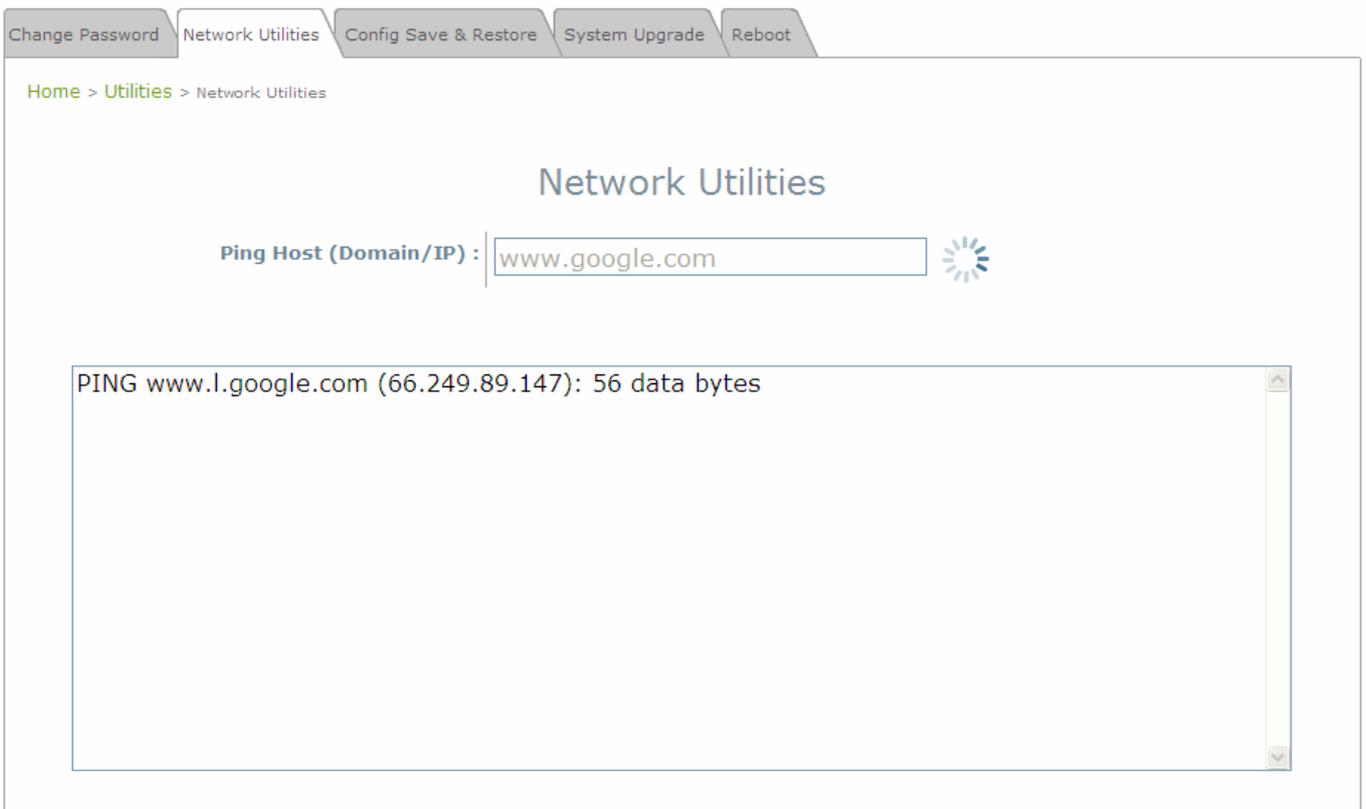
“root” account: Enter the original password (“admin”) and a new password, and then re-enter the new password in the Re-enter New Password field. Click **SAVE** to save the new password.

### 4.3.2 Network Utilities

The administrator can check the network connectivity via this function. The current provided network utility is Ping and the target host FQDN-compliant name or IP address can be provided to test network connection.

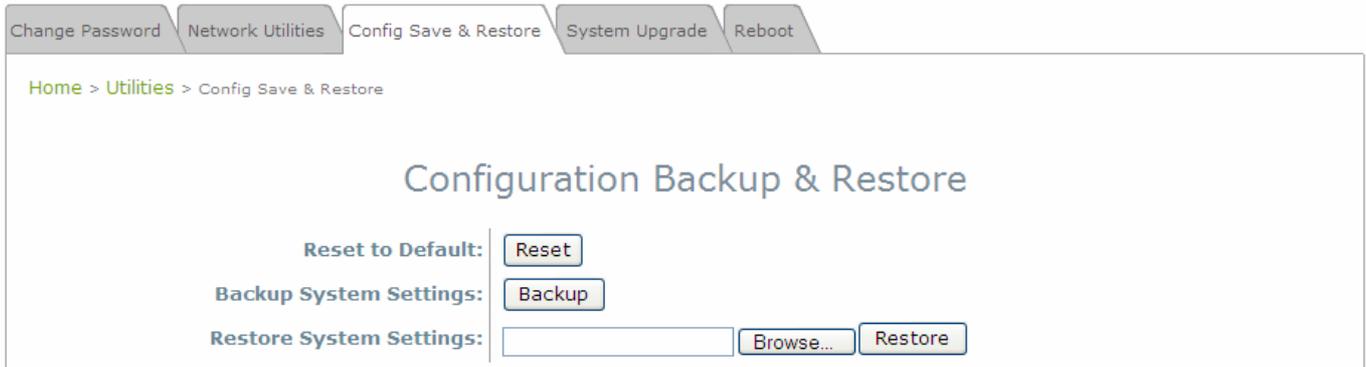


- **Ping Host (Domain/ IP):** Enter the domain name or IP address of a target device for diagnosis purpose, for example, www.4ipnet.com, and click **PING** to proceed. The ping result will be shown in the **Result** field.



### 4.3.3 Configuration Save & Restore

This function is used to backup or restore the current settings. The system can be restored to the default setting by clicking on Reset. The setting of the device can be backup to a file. It can be used to duplicate setting to the other OWL400/410 device.



- **Reset to Default:**

- Click **Reset** to load the factory default settings of OWL400/410. A pop-up screen will appear to reconfirm the request to restart the system. Click **OK** to proceed, or click **Cancel** to cancel the restart request.

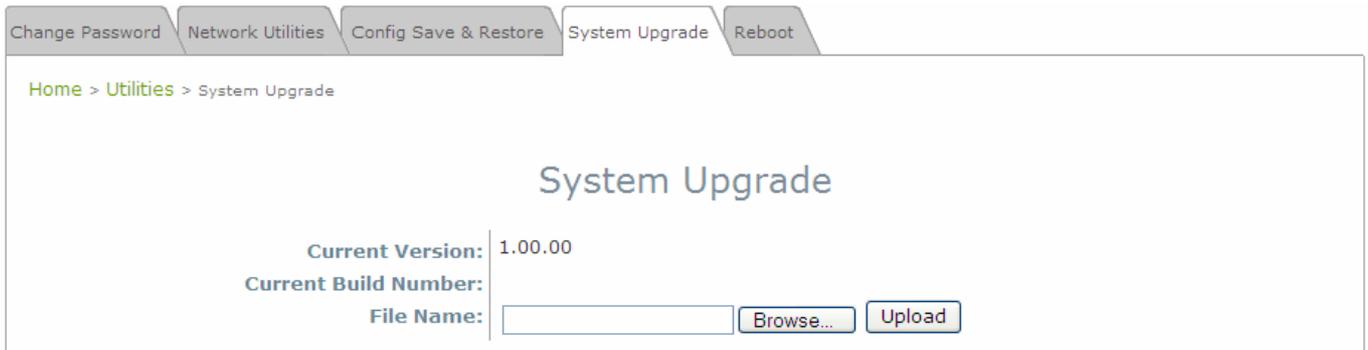


- A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.
- The **System Overview** page will appear upon the completion of reboot.

- **Backup Settings:** Click **Save** to save the current system settings to a local disk such as the hard disk drive (HDD) of a local computer or a compact disc (CD).
- **Restore Settings:** Click **Browse** to search for a previously saved backup file, and then click **Upload** to restore the settings. The backup file will replace the active configuration file currently running on the system.

### 4.3.4 System Upgrade

To upgrade the system firmware, click **Browse** to search for the new firmware file, and then click **Upload** to execute the upgrade process. The first step is to acquire the correct firmware file and supply it in the UI field. During firmware update, please don't turn off the power to prevent from damaging the device permanently.



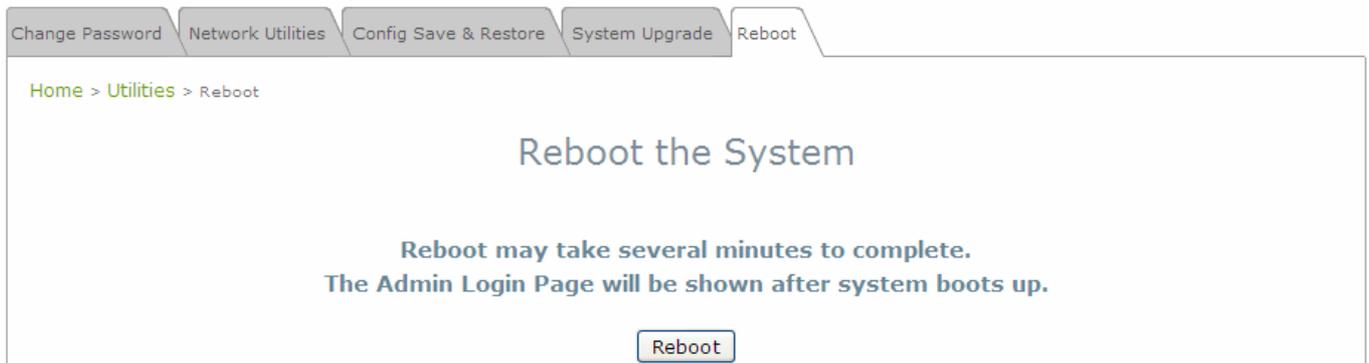
The screenshot shows a web interface for system upgrade. At the top, there are navigation tabs: Change Password, Network Utilities, Config Save & Restore, System Upgrade (selected), and Reboot. Below the tabs, the breadcrumb path is Home > Utilities > System Upgrade. The main heading is "System Upgrade". Below the heading, there are labels for "Current Version:" (1.00.00), "Current Build Number:", and "File Name:". To the right of the "File Name:" label is an input field, a "Browse..." button, and an "Upload" button.

▶▶ **Note:**

- To prevent data loss during firmware upgrade, please back up the current settings before proceeding further.
- Please restart the system after the upgrade. Do not interrupt the system, i.e. power on/off, during the upgrade or restart process since it may cause damage to the system.

### 4.3.5 Reboot

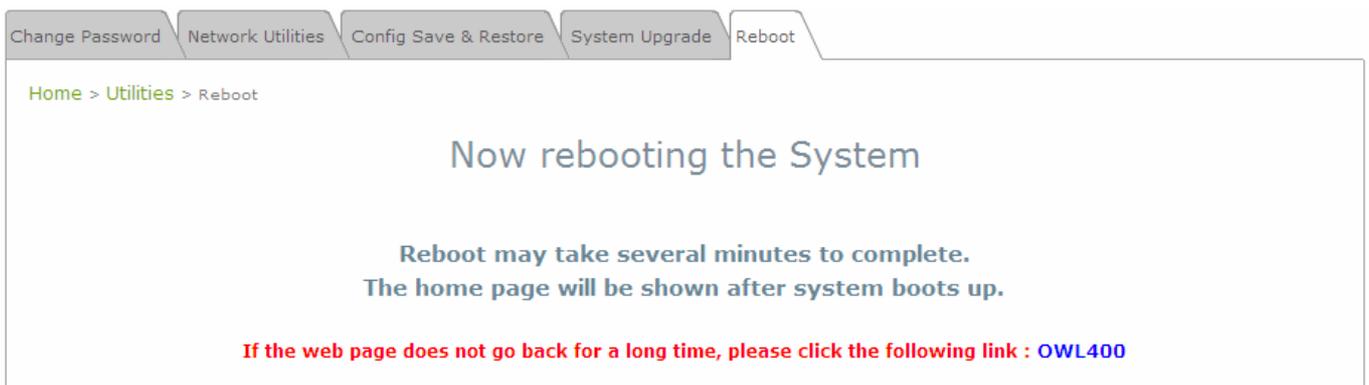
The administrator can reboot the device remotely. Click **Reboot** to restart the system immediately.



A pop-up screen will appear to confirm the request to restart the system. Click **OK** to proceed, or click **Cancel** to cancel the restart request.



A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.



The **System Overview** page will appear upon the completion of reboot.

## 4.4 Status

This section displays the status of **System Overview**, **Clients**, **Repeater**, and **Event Log**.

  
System

  
Wireless

  
Utilities

  
Status

Overview

Clients

Repeater

Event Log

[Home](#) > [Status](#) > System Overview

### System Overview

#### System

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.4-1.2536
Location	CA, US
Site	EN-A
Device Time	1999/12/31 16:28:59
System Up Time	0 days, 0:28:59
Operating Mode	AP

#### Radio Status

MAC Address	00:1F:D4:88:61:00
Band	802.11a
Channel	36
TX Power	Highest

#### LAN Interface

MAC Address	00:02:31:75:92:0A
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

#### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:88:61:00	OWL400-1	None	0

### 4.4.1 System Overview

The **System Overview** page provides an overview of the system status for the administrator.

Overview
Clients
Repeater
Event Log

[Home](#) > [Status](#) > System Overview

## System Overview

#### System

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.4-1.2536
Location	CA, US
Site	EN-A
Device Time	1999/12/31 17:38:12
System Up Time	0 days, 1:38:12
Operating Mode	AP

#### Radio Status

MAC Address	00:1F:D4:88:61:00
Band	802.11a
Channel	36
TX Power	Highest

#### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:88:61:00	OWL400-1	None	0

#### LAN Interface

MAC Address	00:02:31:75:92:0A
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

The description of the table is shown below:

ITEM		DESCRIPTION
System	<b>System Name</b>	The name provided in System Information.
	<b>Firmware Version</b>	The present firmware version of the system.
	<b>Build Number</b>	The Build Number of the firmware.
	<b>Location</b>	The location provided in System Information.
	<b>Site</b>	The firmware version for specific region.
	<b>Device Time</b>	The current time on the device.
	<b>System Up Time</b>	The system elapsing time since last reboot.
	<b>Operating Mode</b>	Either CPE or AP.
LAN Interface	<b>MAC Address</b>	The MAC address of LAN Interface.
	<b>IP Address</b>	The IP address of the LAN Interface.
	<b>Subnet Mask</b>	The Subnet Mask of the LAN Interface.
	<b>Gateway</b>	The gateway of LAN interface.
Radio Status	<b>MAC Address</b>	The MAC address of RF interface.
	<b>Band</b>	The operating band.
	<b>Channel</b>	The operating channel.
	<b>Tx Power</b>	The level of transmitted power.
AP Status	<b>BSSID</b>	The BSSID (MAC) of AP.
	<b>ESSID</b>	The assigned ESSID of AP.
	<b>Security Type</b>	The security type of AP.
	<b>Online Client</b>	The number of online clients associated with AP.

## 4.4.2 Associated Client Status

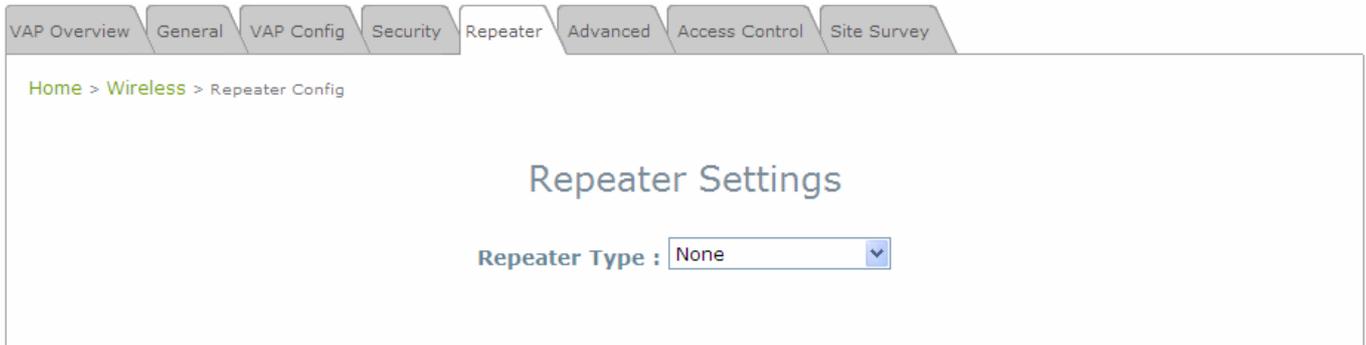
The administrator can remotely oversee the status of all associated clients on this page. Associated client's MAC, SNR and Idle Time are listed in the table.

The screenshot shows a web interface with a navigation menu at the top containing 'Overview', 'Clients', 'Repeater', and 'Event Log'. Below the menu is a breadcrumb trail: 'Home > Status > Wireless Clients'. The main heading is 'Associated Client Status'. Underneath, there is a section titled 'Client List' which contains a table with the following headers: 'Associated VAP', 'ESSID', 'MAC Address', 'SNR (dB)', 'Idle Time (secs)', and 'Disconnect'.

- **ESSID:** The Extended Service Set ID which the client is associated with.
- **MAC Address:** The MAC address of associated clients.
- **SNR:** The Signal to Noise Ratio of respective client's association.
- **Idle Time:** Time period that the associated client is inactive; the time unit is in second.

### 4.4.3 Repeater Information

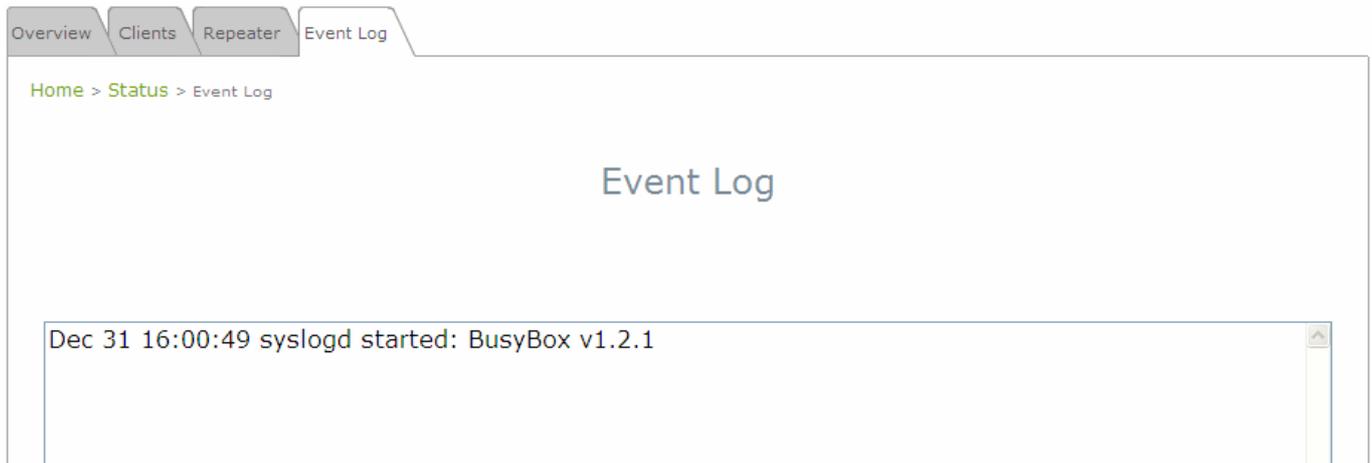
The administrator can review detailed information of the repeater function on this page. Information of repeater's status, mode and encryption is provided.



- **WDS Link Status:** The table will be displayed when WDS mode is selected. For more information on the repeater type, please refer to **Section 4.2.5 Repeater Settings**.
  - **Status:** Show the repeater status.
  - **MAC Address:** The MAC Address of the WDS peer.
  - **RSSI:** Received Signal Strength Indication, a measurement of received radio signal over WDS link.
  - **Tx Rate:** The transmit rate of the Repeater.
  - **Tx Error:** The accumulative number of transmission errors.
  - **Encryption:** The encryption method used for repeater connection.
- **Repeater Status:** The table will be displayed when Repeater mode is selected.
  - **SSID:** SSID of the upper-bound AP to be associated with.
  - **Status:** The status of the repeater function either *Enabled* or *Disabled*.
  - **Tx Rate:** The transmit rate of the Repeater.
  - **RSSI:** Received Signal Strength Indication, a measurement of received radio signal over wireless link with the upper-bound AP.
  - **Encryption:** The encryption type used: *None*, *WEP*, or *WPA-PSK*.

## 4.4.4 Event Log

Event log provides the records of the system activities. All the system events are shown here.



► **Note:** As the Event Log is stored in RAM, it will be refreshed after the system is restarted. The system also supports a Syslog reporting function of reporting the events to an external Syslog server.

- **Date/ Time:** The date and time when the event happened.
- **Hostname:** Indicate which Host records this event. Note that all events in this page are local events and this field of all events is the same. However, in remote Syslog service, this field will help the network administrator identify which event is from this system. For more information, please refer to **Section 4.1.4 Management Services**.
- **Process name (with square brackets):** Indicate which process with the specific event is associated.
- **Description:** Description of the event.

## 4.5 Online Help

The **Help** button is at the upper right hand corner of the display screen.

Click **Help** for the **Online Help** window, and then click the hyperlink of the desired topic for further information.



**Online Help (AP Mode)**

**Organization of the Configuration Web:**

<u><a href="#">System</a></u>	<u><a href="#">Wireless</a></u>	<u><a href="#">Utilities</a></u>	<u><a href="#">Status</a></u>
<u><a href="#">System Information</a></u>	<u><a href="#">VAP Overview</a></u>	<u><a href="#">Password</a></u>	<u><a href="#">System Overview</a></u>
<u><a href="#">Operating Mode</a></u>	<u><a href="#">General</a></u>	<u><a href="#">Network Utilities</a></u>	<u><a href="#">Clients</a></u>
<u><a href="#">Network</a></u>	<u><a href="#">VAP Config</a></u>	<u><a href="#">Config Save Restore</a></u>	<u><a href="#">Repeater</a></u>
<u><a href="#">Management Services</a></u>	<u><a href="#">Security</a></u>	<u><a href="#">System Upgrade</a></u>	<u><a href="#">Event Log</a></u>
	<u><a href="#">Repeater</a></u>	<u><a href="#">Reboot</a></u>	
	<u><a href="#">Advanced</a></u>		
	<u><a href="#">Access Control</a></u>		
	<u><a href="#">Site Survey</a></u>		

## 5. CPE Mode Configuration

When CPE mode is activated, the system acts as a gateway where it connects to the WAN wirelessly and provides Ethernet connection to users via wired LAN. This chapter will guide you through setting up the CPE mode with graphical illustrations. The following table shows all the functions of OWL400/410 in its CPE mode.

OPTION	System	Wireless	Firewall	Utilities	Status
<b>FUNCTION</b>	System Information	General Settings	IP/ Port Forwarding	Change Password	System Overview
	Operating Mode	Advanced Wireless Settings	Demilitarized Zone	Network Utilities	Event Log
	Network Settings	Security Settings		Configuration Save & Restore	DHCP Lease
	Management Services	Site Survey		System Upgrade	UPnP Status
				Reboot	

*Table of CPE Mode Functions*

System | Wireless | Firewall | Utilities | Status

System Overview | Event Log | DHCP Lease | UPnP

Home > Status > System Overview

## System Overview

### System

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.8-1.2628
Location	CA, US
Site	EN-A
Device Time	2000/01/01 13:29:24
System Up Time	0 days, 21:29:24
Operating Mode	CPE

### Radio Status

Status	Disable
SSID	N/A
MAC Address	N/A
Channel	56
Signal Strength	12
Security	None

### LAN Interface

MAC Address	00:1F:D4:00:30:F9
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

### WAN Interface

Mode	Static
MAC Address	00:1F:D4:00:31:40
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
Bandwidth	Down: Unlimited / UP: Unlimited

CPE Mode Main Page

## 5.1 System

This section provides information in configuring the following functions: **System Information**, **Operating Mode**, **Network Settings**, and **Management Services**.

System Information    Operating Mode    Network    Management

Home > System > General

### System Information

Name :  \*

Description :

Location :

### Time

Device Time : 2000/01/06 11:35:17

Time Zone :  ▼

Time :  Enable NTP     Manually set up

NTP Server 1 :  \*

NTP Server 2 :

►► **Note:** A system restart is required when a reminding message appears after clicking the **SAVE** button; all settings entered and saved will take effect only after a system restart.

## 5.1.1 System Information

For maintenance purpose, it is required to specify the system name, its location and corresponding basic parameters. Fields such as *Name*, *Description* and *Location* are used for mnemonic purpose. It is recommended to have different values in each AP.

The screenshot shows a web interface with a navigation bar at the top containing 'System Information', 'Operating Mode', 'Network', and 'Management'. Below the navigation bar, the breadcrumb path is 'Home > System > General'. The main content area is divided into two sections: 'System Information' and 'Time'.

**System Information Section:**

- Name :** OWL400 \*
- Description :** 4IPNET, INC.
- Location :** CA, US

**Time Section:**

- Device Time :** 2000/01/06 11:50:20
- Time Zone :** (GMT-08:00)Pacific Time(US&Canada),Tijuana
- Time :**  Enable NTP  Manually set up
- NTP Server 1 :** tock.stdtime.gov.tw \*
- NTP Server 2 :** (empty field)

- **System Information**

For maintenance purpose, it is recommended to have the following information stated as clearly as possible. Fields Name, Description, and Location are used for mnemonic purpose. It is recommended to have different values in each wireless device.

- *Name*: The system name used to identify this system.
- *Description*: Further information of the system.
- *Location*: Information about the geographical location of the system, which can help the administrator locate it easily.

- **Time**

Time settings allow the system time synchronized with NTP server or manually set.

- *Device Time*: Display the current time of the system.
- *Time Zone*: Select an appropriate time zone from the drop-down list box.

➤ *Synchronization*: Synchronize the system time either by NTP server or manual setup.

(1) **Enabled NTP:**

By selecting *Enabled NTP*, OWL400/410 can synchronize its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address or domain name must be provided. If FQDN (Full Qualified Domain Name) is used as the IP address of NTP server, the DNS server must also be activated (please refer to **5.1.3 Network Settings**).

Time

Device Time :	1999/12/31 16:05:36
Time Zone :	(GMT-08:00)Pacific Time(US&Canada),Tijuana
Time :	<input checked="" type="radio"/> Enable NTP <input type="radio"/> Manually set up
NTP Server 1 :	tock.stdtime.gov.tw *
NTP Server 2 :	

(2) **Manually set up:**

By selecting *Manually set up*, the administrator can manually set the system date and time.

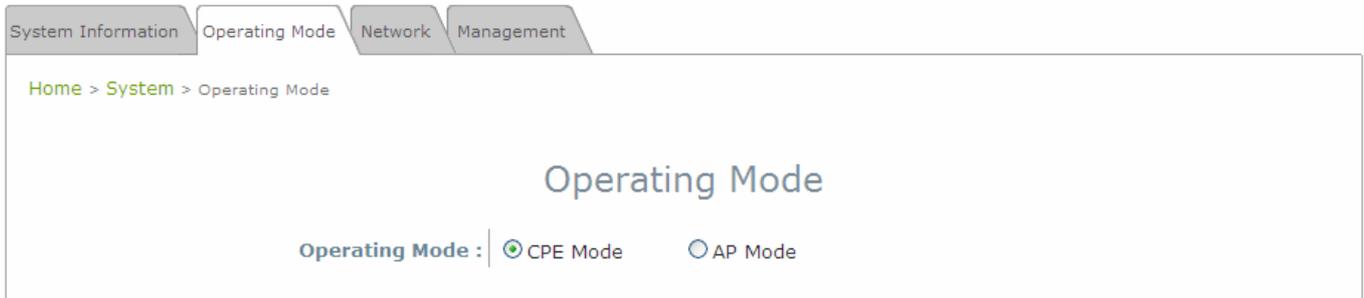
Time

Device Time :	1999/12/31 16:02:29
Time Zone :	(GMT-08:00)Pacific Time(US&Canada),Tijuana
Time :	<input type="radio"/> Enable NTP <input checked="" type="radio"/> Manually set up
Set Date :	---- Year -- Month -- Day
Set Time :	-- Hour -- Min -- Sec

- *Set Date*: Select the appropriate *Year*, *Month*, and *Day* from the drop-down list box.
- *Set Time*: Select the appropriate *Hour*, *Min*, and *Sec* from the drop-down list box.

## 5.1.2 Operating Mode

OWL400/410 supports two operation modes: CPE mode and AP mode. The administrator can set the desired mode on this page, and then configure the system according to deployment needs.



- **Operating Mode:** Select *CPE Mode* and then click **SAVE** to save the setting.

### 5.1.3 Network Settings

WAN and LAN settings can be configured on this page.

- **WAN Configuration:** Determine the way to obtain the IP address, by static or DHCP.
- **Mode:** Determine the way to obtain the IP address, by *DHCP* or *Static*.
  - **Static:** The administrator can manually set up the static WAN IP address.
    - **IP Address:** The IP address of the WAN port.
    - **Netmask:** The subnet mask of the WAN port.
    - **Default Gateway:** The gateway IP address of the WAN port.
    - **Primary DNS Server:** The IP address of the primary DNS (Domain Name System) server.
    - **Alternate DNS Server:** The IP address of the substitute DNS server.
  - **DHCP:** This connection type is applicable when the system is connected to a network with the presence of a DHCP server; all related IP information required will be provided by the DHCP server automatically.

- **Bandwidth Limit:**
  - **Download:** The maximum download bandwidth of WAN interface to be shared by clients.
  - **Upload:** The maximum upload bandwidth of the WAN interface to be shared by clients.

- **Dynamic DNS:** The option can be enabled to bind FQDN-compliant Host Name with this device. If enabled, the service Provider must be chosen from the drop-down list with provided Host Name, User Name, User Email and Password.

### Dynamic DNS (DDNS)

DDNS :	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Provider :	<input type="text"/>	
Host Name :	<input type="text"/>	
User Name / E-mail :	<input type="text"/>	
Password / Key :	<input type="text"/>	

- **DDNS:** Select *Enable* to activate this function or *Disable* to inactivate it.
- **Provider:** The name of the DDNS provider that the system is registered with. Select a DDNS provider from the drop-down list box.
- **Host Name:** The FQDN registered with the selected DDNS provider.
- **User name/ E-mail:** The account ID, user name or e-mail, registered with the DDNS provider.
- **Password/ Key:** The password of the account registered with the DDNS provider.

- **LAN Configuration:** Configure LAN and DHCP settings on this page. IP Address and Netmask are required fields to set up LAN interface.

## LAN Configuration

IP Address :	<input type="text" value="192.168.1.1"/>	*
Netmask :	<input type="text" value="255.255.255.0"/>	*
DHCP Server :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Start IP :	<input type="text" value="192.168.1.2"/>	*
End IP :	<input type="text" value="192.168.1.254"/>	*
Preferred DNS Server :	<input type="text" value="168.95.1.1"/>	*
Alternated DNS Server :	<input type="text"/>	
WINS Server IP :	<input type="text"/>	
Domain Name :	<input type="text"/>	
Lease Time :	<input type="text" value="1 Day"/>	

- **IP Address:** The IP address of the LAN port.
- **Netmask:** The Subnet mask of the LAN port.
- **DHCP Server:** If enabled, devices connected to this system can obtain an IP address automatically.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
  - **Start IP / End IP:** Specify the range of IP addresses to be distributed by the DHCP server to clients.
  - **Preferred DNS Server:** Enter the IP address of a preferred DNS server; this field is required.
  - **Alternate DNS Server:** Enter the IP address of a secondary DNS server; this is optional.
  - **WINS Server IP:** Enter the IP address of a WINS (Windows Internet Name Service) server; this is optional.
  - **Domain Name:** Enter the domain name for this network.
  - **Lease Time:** It can be chosen from the drop-down list to renew Leased LAN IP.

## 5.1.4 Management Services

The system supports **SNMP**, **Syslog**, **UPnP**, and **Auto Reboot** functions for easy management. These functions can be configured on this page.

System Information Operating Mode Network Management

Home > System > Management Services

### Management Services

**SNMP Configuration :**  Disable  Enable  
 Community String :  
 Read :   
 Write :   
 Trap :  Disable  Enable  
 Server IP :

**System Log :**  Disable  Enable  
 SYSLOG Server IP :   
 Server Port :   
 SYSLOG Level :

**UPnP Configuration :**  Disable  Enable

**Auto Reboot :**  Disable  Enable  
 Reboot Time :

- **SNMP Configuration:** By enabling SNMP function, the administrator can obtain the system information remotely.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
  - **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system.
    - **Read:** Enter the community string for accessing the MIB with Read privilege.
    - **Write:** Enter the community string for accessing the MIB with Write privilege.
  - **Trap:** When enabled, events on Cold Start, Interface UP & Down, and Association & Disassociation can be reported to an assigned server.
    - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
    - **Server IP Address:** Enter the IP address of the assigned server for receiving the trap report.

- **Remote Syslog:** By enabling this function, specify a remote Syslog server to accept system log messages from the system remotely.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
  - **Server IP:** The IP address of the Syslog server for receiving the reported events.
  - **Server Port:** The port number of the Syslog server.
  - **Syslog Level:** Select the desired level of received events from the drop-down list box.
  
- **UPnP Configuration:** This option can be enabled if UPnP service is required by LAN device.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
  
- **Auto Reboot:** The system can be functioning in a healthier state when this service is enabled.
  - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
  - **Reboot Time:** Select an appropriate time from the drop-down list box. Since all users on the network will be disconnected during reboot, it is suggested to set the reboot time during an off-peak period to reduce impacts on the online users.

## 5.2 Wireless

This section is for configuring wireless settings for this system to associate with its uplink access point.

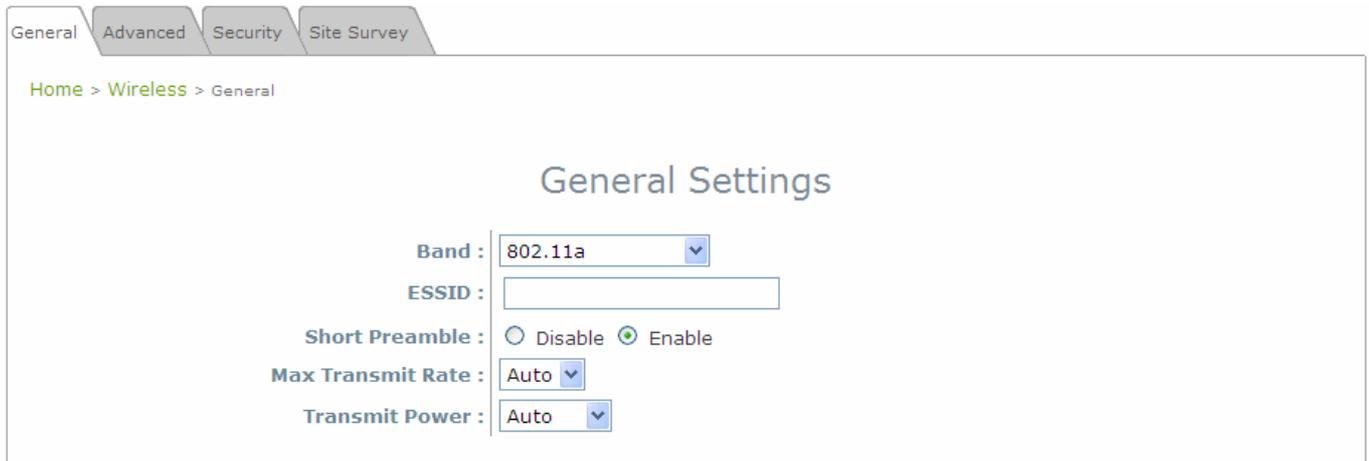
The screenshot shows the configuration interface for the 4IPNET device. At the top, there are five main menu buttons: System, Wireless, Firewall, Utilities, and Status. The 'Wireless' button is highlighted with a red border. Below these buttons are sub-menus for General, Advanced, Security, and Site Survey. The 'General' sub-menu is selected, and the breadcrumb path 'Home > Wireless > General' is displayed. The main content area is titled 'General Settings' and contains the following configuration options:

- Band :** 802.11a (dropdown menu)
- ESSID :** (text input field)
- Short Preamble :**  Disable  Enable
- Max Transmit Rate :** Auto (dropdown menu)
- Transmit Power :** Auto (dropdown menu)

At the bottom of the settings area, there are two yellow buttons: 'SAVE' and 'CLEAR'.

## 5.2.1 General Settings

This section is for configuring the system RF settings.



General Settings

Band : 802.11a

ESSID :

Short Preamble :  Disable  Enable

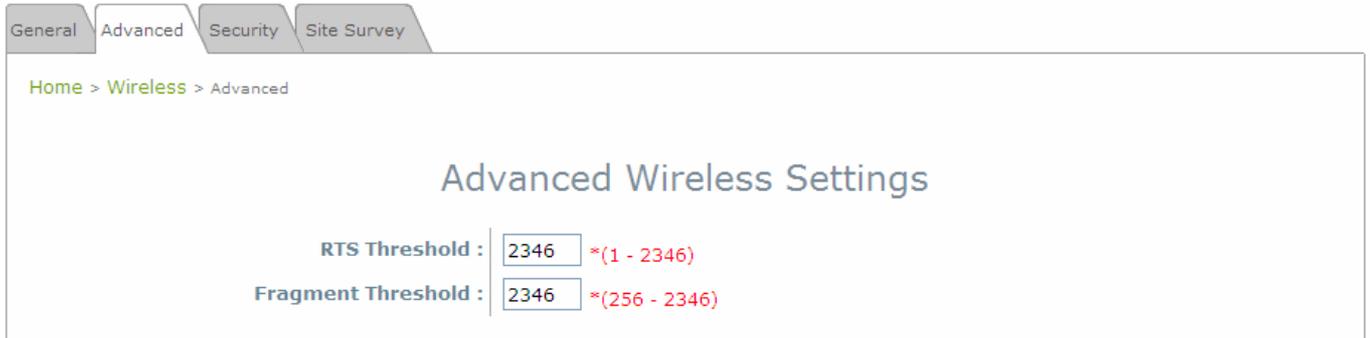
Max Transmit Rate : Auto

Transmit Power : Auto

- **Band:** Select an appropriate wireless band: *802.11a* or mixed mode *802.11a+802.11n*, or select *Disable* if the function is not required.
- **ESSID:** The ESSID (Service Set ID) of the client device that the system is to be associated with.
- **Short Preamble:** The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select *Enable* to use Short Preamble or *Disable* to use Long Preamble with a 128-bit synchronization field.
- **Max Transmit Rate:** The maximum wireless transmitting rate. Select the desired rate from the drop-down list box. The system uses the highest possible rate when *Auto* is selected.
- **Transmit Power:** The signal strength transmitted from the system. Select among *Auto*, *Lowest*, *Low*, *Medium*, *High*, and *Highest* from the drop-down list box.

## 5.2.2 Advanced Wireless Settings

The administrator can set the RTS threshold and fragmentation threshold on this page. In most circumstance, the default settings can meet general requirements. If occasionally wireless network needs to be tuned, the following parameters will assist with that purpose.



General Advanced Security Site Survey

Home > Wireless > Advanced

### Advanced Wireless Settings

RTS Threshold :  \*(1 - 2346)

Fragment Threshold :  \*(256 - 2346)

- **RTS Threshold:** To control station access to the medium and to alleviate this effect of the hidden terminal problem, the administrator can tune this RTS threshold value. A lower RTS Threshold setting can be useful in areas where many client devices are associating with OWL400/410 or in areas where the clients are far apart and can detect only OWL400/410 and not each other.
- **Fragmentation Threshold:** A unicast frame larger than this threshold will be fragmented before transmission. If a significant number of collisions are occurring, the administrator can try to set a smaller value of the threshold to see whether it helps. A smaller value results in smaller packets but allows a larger number of packets in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

## 5.2.3 Security Settings

The system supports various authentication and data encryption methods. The security type includes: None, WEP and WPA-PSK.

The screenshot shows the 'Security Settings' page in a web interface. At the top, there are four tabs: 'General', 'Advanced', 'Security', and 'Site Survey'. Below the tabs, a breadcrumb trail reads 'Home > Wireless > Security'. The main heading is 'Security Settings'. A single configuration item is visible: 'Security Type : None' with a dropdown arrow.

- **None:** No authentication is required.
- **WEP:** WEP (Wired Equivalent Privacy) supports key length of 64/128 bits.

The screenshot shows the 'Security Settings' page with 'WEP' selected in the 'Security Type' dropdown. Below this, there are several radio button options for '802.11 Authentication': 'Open System' (selected), 'Shared Key', and 'Auto'. Underneath are radio button options for 'WEP Key Length': '64 bits' (selected) and '128 bits'. Then, radio button options for 'WEP Key Format': 'ASCII' (selected) and 'Hex'. A 'WEP Key Index' dropdown is set to '1'. At the bottom, there are four input fields labeled 'WEP Keys : 1', '2', '3', and '4'.

- **802.11 Authentication:** Select from *Open System*, *Shared Key*, or *Auto*.
- **WEP Key Length:** Select from *64-bit* or *128-bit* key length.
- **WEP Key Format:** Select from *ASCII* or *Hex* format for the WEP key.
- **WEP Key Index:** Select a key index from 1 through 4. The WEP key index is a number that specifies which WEP key to use for the encryption of wireless frames during data transmission.
- **WEP Keys:** Provide WEP key value; the system supports up to 4 sets of WEP keys.

- **WPA-PSK:** WPA-PSK (WI-Fi Protected Access Pre-shared Key) supports pre-shared key authentication and WPA data encryption (TKIP/AES).

General Advanced Security Site Survey

Home > Wireless > Security

### Security Settings

Security Type : WPA-PSK

Cipher Suite : TKIP (WPA)

Pre-shared Key Type :  PSK(Hex)\*( 64 chars )  Passphrase\*( 8 - 63 chars )

Pre-shared Key :

Group Key Update Period: 600 second(s)

- **Cipher Suite:** Select an encryption method from *TKIP(WPA/WPA2)* and *AES (WPA/WPA2)*.
- **Pre-shared Key Type:** Select a pre-shared key type: *PSK (Hex)* or *Passphrase*.
- **Pre-shared Key:** Enter the key value for the pre-shared key; the format of the key value depends on the key type selected.
- **Group Key Update Period:** The time interval for the Group Key to be renewed. Enter the time length required; the time unit is in second.

## 5.2.4 Site Survey

The system can scan and display all surrounding available access points (APs). The administrator can then select an AP to be associated with the system on this page.

Site Survey is a useful tool to provide information about the surrounding wireless environment; available APs are shown with their respective SSID, MAC Address, Channel, Rate setting, Signal reading and Security type. The administrator can click Setup or Connect to configure the wireless connection according to the mentioned readings.

The screenshot shows the 'Site Survey' tab selected in the navigation menu. Below the menu, there is a breadcrumb trail: Home > Wireless > Site Survey. The main content area is titled 'Scan Result' and contains a 'Scan Again!' button. Below the button is a table with the following data:

SSID	MAC Address	Channel	Signal	Security	Setup / Connect
b0b24b	00:0B:6B:DD:A7:EE	36	20	WEP	Setup
9595d5	00:0B:6B:DD:27:A6	36	34	WEP	Setup
rh-OWL410-none	00:1F:D4:00:31:78	56	15	NONE	Connect
471f2a	00:0B:6B:DD:27:B9	56	10	WEP	Setup

AP Scan Result (example only)

- **SSID:** The SSID (Service Set ID) of the AP found in the system's coverage area.
- **MAC Address:** The MAC address of the respective AP.
- **Channel:** The channel number currently used by the respective AP.
- **Signal:** The signal strength of the respective AP.
- **Security:** The encryption type used by the respective AP.
- **Setup / Connect:**
  - **Connect:** Click **Connect** to associate with the respective AP directly; no further configuration is required.
  - **Setup:** Click **Setup** to configure security settings for associating with the respective AP or repeater.
    - **WEP:** Click **Setup** to configure the WEP setting for associating with the target AP.  
The following configuration box will then appear at the bottom of the screen. For more information on the WEP security settings, please refer to **Section 5.2.3 Security Settings**.
    - **WPA-PSK:** Click **Setup** to configure the WPA-PSK setting for associating with the target AP.  
The following configuration box will then appear at the bottom of the screen. For more information on the WPA-PSK security settings, please refer to **Section 5.2.3- Security Settings**.

## 5.3 Firewall

The system supports the following firewall functions: IP/ Port forwarding and DMZ (Demilitarized Zone). The administrator can allow a certain part of the network to be exposed to the Internet in limited and controlled ways for special purposes such as game and voice applications.

The screenshot displays the web management interface for the 4IPNET device. At the top, there are five navigation buttons: System, Wireless, Firewall (highlighted with a red box), Utilities, and Status. Below these, there are tabs for IP/Port Forwarding and DMZ. The main content area is titled 'IP/Port Forwarding' and contains a breadcrumb trail: Home > Firewall > IP/Port Forwarding. The configuration form includes fields for Service Name, External Port Range (with a dropdown menu set to 'User Define'), Internal IP Address, and Protocol (set to 'TCP/UDP'). An 'Add' button is located to the right of the form. Below the form is a table with the following columns: Item, Service Name, External Port Range, Internal IP Address, Protocol, State, Delete, and Edit. At the bottom of the page, there are two buttons: 'SAVE' and 'CLEAR'.

### 5.3.1 IP/ Port Forwarding

A certain part of the network can be exposed to the Internet in a limited and controlled way for special-purpose Internet services such as on-line game or video conferencing on this page. Please ensure that the internal port to be used is not occupied by other applications.

- **Service Name:** The administrator can provide an easy remembered alias for the specific forwarding.
- **External Port Range:** The external port for forwarding traffic can be selected from the drop-down list or specified by choosing *User Define* to set the range manually.

#### External Port Range

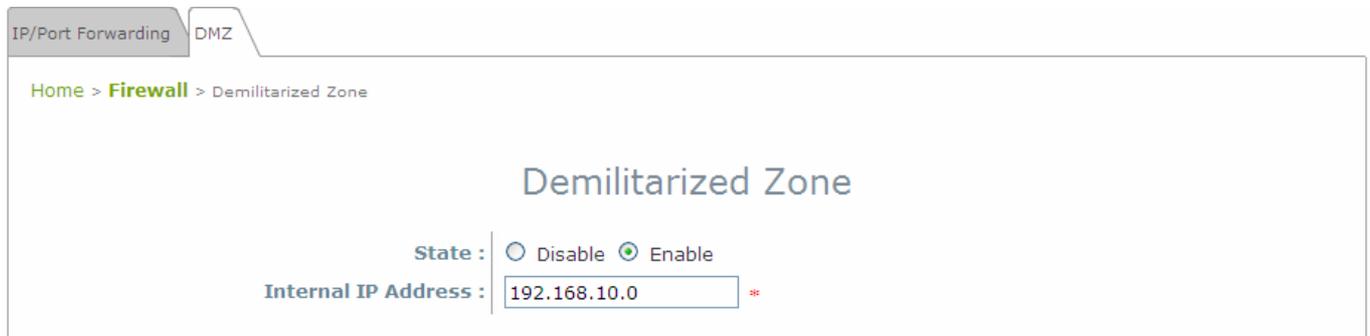
- **Internal IP Address:** Enter the LAN IP address to receive the forwarding traffic.
- **Protocol:** Forwarding traffic protocol can be selected from drop-down list to be *TCP/UCP*, *TCP* or *UDP*.
- **Add:** Click **Add** to activate the new service.
- **IP/ Port Forwarding:** Details of current services available. Click **Delete** to remove the specified service. Click **Edit** to configure the current setting.

### IP/Port Forwarding

Item	Service Name	External Port Range	Internal IP Address	Protocol	State	Delete	Edit
1	GAME	6112	10.30.5.112	TCP/UDP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Delete	Edit
2	Phone	6670	10.30.5.250	TCP/UDP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Delete	Edit

## 5.3.2 Demilitarized Zone

The DMZ (Demilitarized Zone) allows one local computer or server (used as a DMZ host) to be exposed to the Internet for special-purpose Internet services such as functioning as a web server. External users can access the DMZ host without authentication.



The screenshot shows a web interface for configuring the DMZ. At the top, there are two tabs: "IP/Port Forwarding" and "DMZ". Below the tabs, a breadcrumb trail reads "Home > Firewall > Demilitarized Zone". The main heading is "Demilitarized Zone". There are two configuration fields: "State" with radio buttons for "Disable" and "Enable" (the "Enable" option is selected), and "Internal IP Address" with a text input field containing "192.168.10.0" and a red asterisk indicating a required field.

- **State:** Select *Enable* to activate this function or *Disable* to deactivate it.
- **Internal IP Address:** Fill in the internal IP address to allow system forwarding traffic other than those specifically listed in IP/Port Forwarding.

## 5.4 Utilities

The system provides **Change Password**, **Network Utilities**, **Configuration Save & Restore**, **System Upgrade**, and **Reboot** functions for maintenance.

The screenshot shows the 4IPNET web interface. At the top, there is a navigation bar with five main menu items: System, Wireless, Firewall, Utilities, and Status. The Utilities menu item is highlighted with a red border. Below this bar, there are five sub-menu items: Change Password, Network Utilities, Config Save & Restore, System Upgrade, and Reboot. The main content area displays the breadcrumb path: Home > Utilities > Change Password. The title of the page is "Change Password". There are two sections for password changes. The first section is for the "root" user, with fields for "Old Password", "New Password", and "Re-enter New Password". The "New Password" field has a red asterisk and the text "\*up to 32 characters". The second section is for the "admin" user, with fields for "New Password" and "Re-enter New Password". The "New Password" field also has a red asterisk and the text "\*up to 32 characters". At the bottom of the form, there are two yellow buttons: "SAVE" and "CLEAR".

## 5.4.1 Change Password

The administrator can update or change password. The system provides two management accounts for CPE mode, **root** and **admin**. The **root** account is empowered with full privileges while the **admin** account is with partial. For more information on the respective privileges of these two management accounts, please refer to **Appendix A**.

### System Management Privileges.

- **“root” account management:** The **root** administrator is entitled to changing passwords for both the **root** and **admin** account.

Change Password | Network Utilities | Config Save & Restore | System Upgrade | Reboot

Home > Utilities > Change Password

### Change Password

**Name :** root

**Old Password :**

**New Password :**  \*up to 32 characters

**Re-enter New Password :**

**Name :** admin

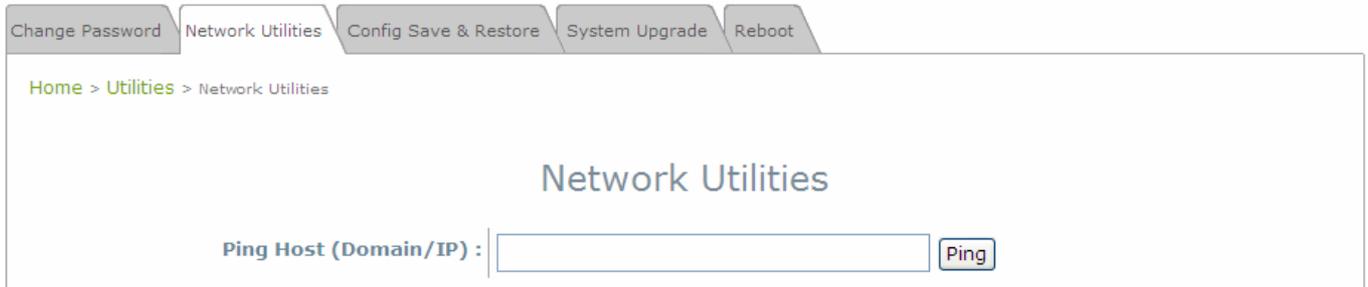
**New Password :**  \*up to 32 characters

**Re-enter New Password :**

- **“root” account:** Enter the original password (“**admin**”) and a new password, and then re-enter the new password in the *Re-enter New Password* field. Click **SAVE** to save the new password.
- **“admin” account:** Enter a new password, and then re-enter it in the *Re-enter New Password* field. The **root** administrator is acting as a superintendent here; thus, entering the old password is not required. Click **SAVE** to save the new password.

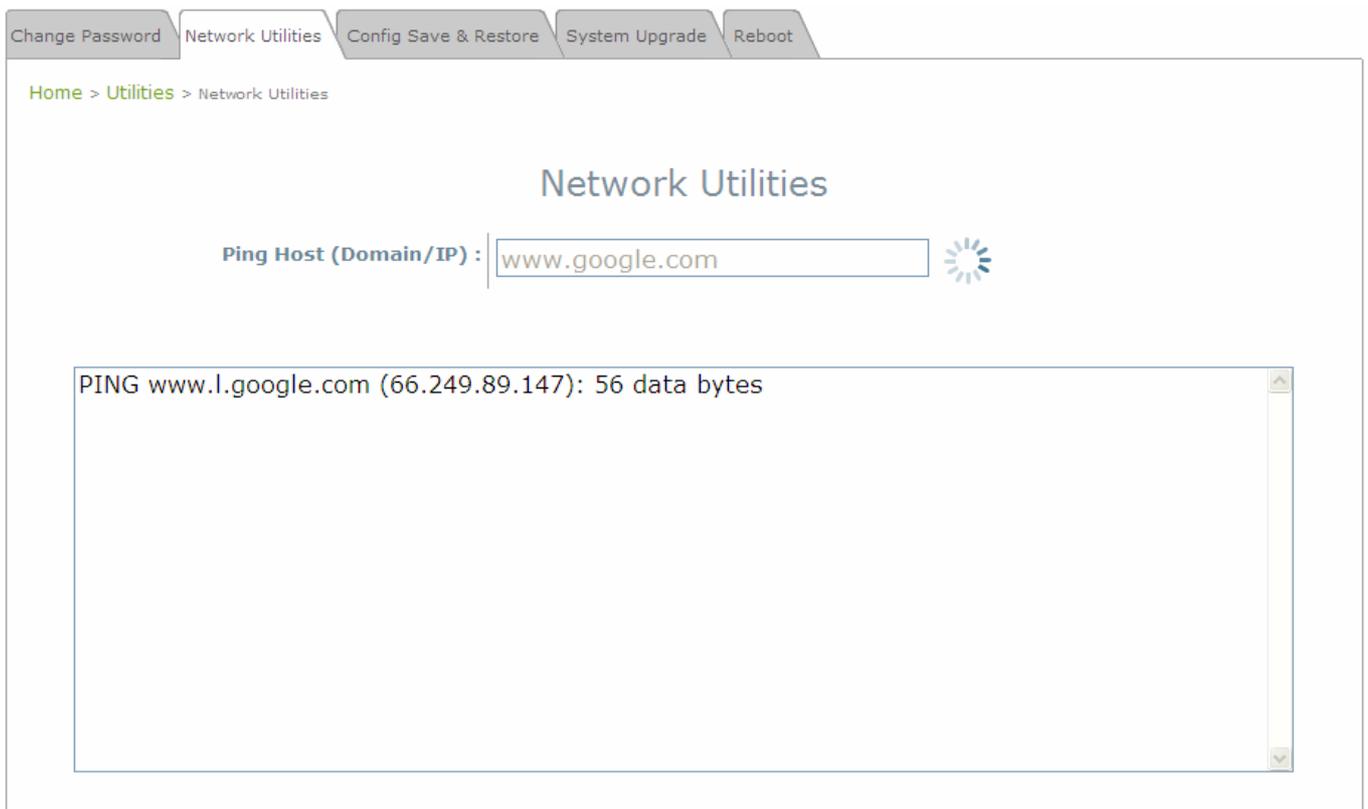
## 5.4.2 Network Utilities

The administrator can check the WAN and LAN connectivity via this function. The current provided network utility is Ping and the target host FQDN-compliant name or IP address can be provided to test network connection.



The screenshot shows the 'Network Utilities' page with a navigation menu at the top containing 'Change Password', 'Network Utilities', 'Config Save & Restore', 'System Upgrade', and 'Reboot'. Below the menu is a breadcrumb trail: 'Home > Utilities > Network Utilities'. The main heading is 'Network Utilities'. There is a text input field labeled 'Ping Host (Domain/IP):' and a 'Ping' button to its right.

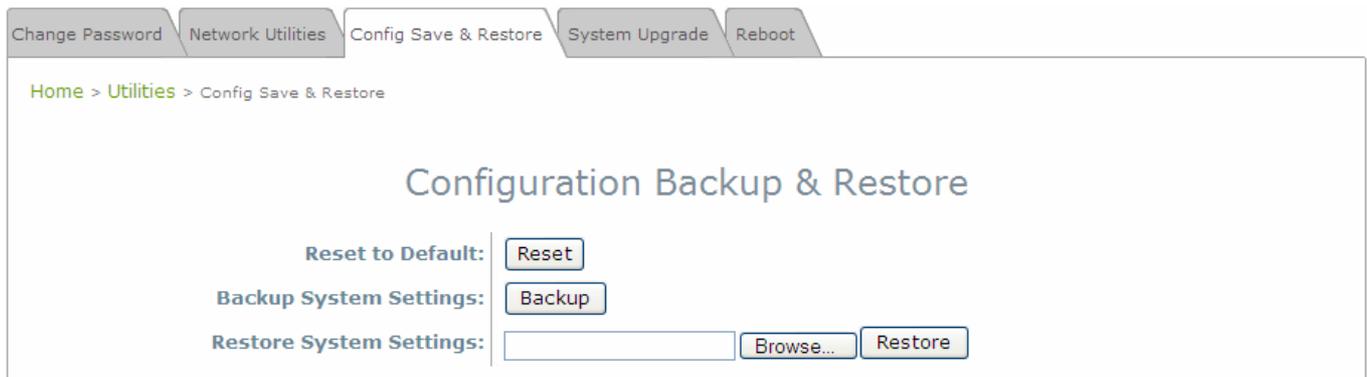
- **Ping Host (Domain/ IP):** Enter the domain name or IP address of a target device for diagnosis purpose, for example, www.4ipnet.com, and click **PING** to proceed. The ping result will be shown in the **Result** field.



The screenshot shows the 'Network Utilities' page after a ping operation. The 'Ping Host (Domain/IP):' field now contains 'www.google.com' and a loading spinner is visible to its right. Below the input field is a scrollable text area containing the following output: 'PING www.l.google.com (66.249.89.147): 56 data bytes'.

### 5.4.3 Configuration Save & Restore

This function is used to backup or restore the current settings. The system can be restored to the default setting by clicking on Reset. The setting of the device can be backup to a file. It can be used to duplicate setting to the other OWL400/410 device.



- **Reset to Default:**

- Click **Reset** to load the factory default settings of OWL400/410. A pop-up screen will appear to reconfirm the request to restart the system. Click **OK** to proceed, or click **Cancel** to cancel the restart request.



- A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.
  - The **System Overview** page will appear upon the completion of reboot.
- **Backup Settings:** Click **Save** to save the current system settings to a local disk such as the hard disk drive (HDD) of a local computer or a compact disc (CD).
  - **Restore Settings:** Click **Browse** to search for a previously saved backup file, and then click **Upload** to restore the settings. The backup file will replace the active configuration file currently running on the system.

## 5.4.4 System Upgrade

To upgrade the system firmware, click **Browse** to search for the new firmware file, and then click **Upload** to execute the upgrade process. The first step is to acquire the correct firmware file and supply it in the UI field. During firmware update, please don't turn off the power to prevent from damaging the device permanently.

The screenshot shows a web interface for system upgrade. At the top, there is a navigation bar with tabs: Change Password, Network Utilities, Config Save & Restore, System Upgrade (selected), and Reboot. Below the navigation bar, the breadcrumb path is Home > Utilities > System Upgrade. The main heading is "System Upgrade". The interface displays the following information:

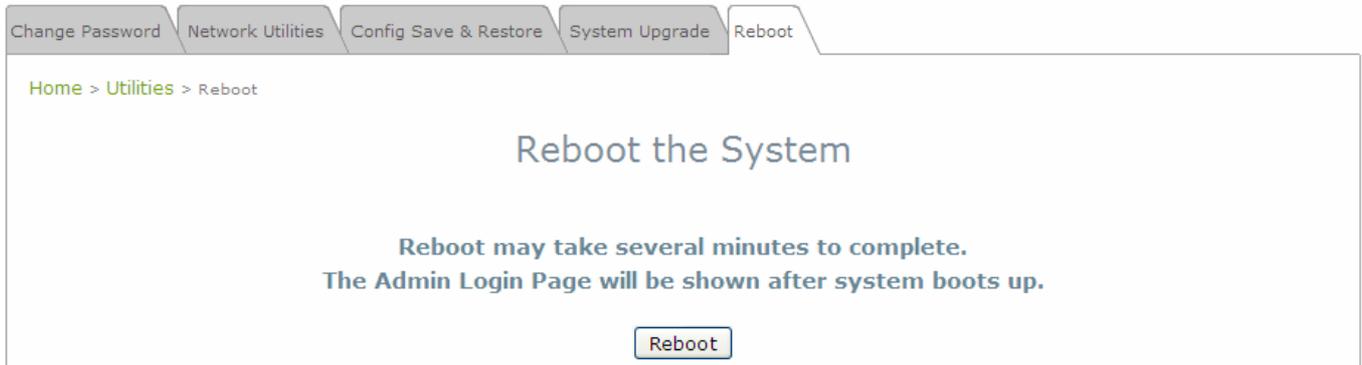
Current Version:	1.00.00
Current Build Number:	
File Name:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>

►► **Note:**

- To prevent data loss during firmware upgrade, please back up the current settings before proceeding further.
- Please restart the system after the upgrade. Do not interrupt the system, i.e. power on/off, during the upgrade or restart process as this may damage the system.

## 5.4.5 Reboot

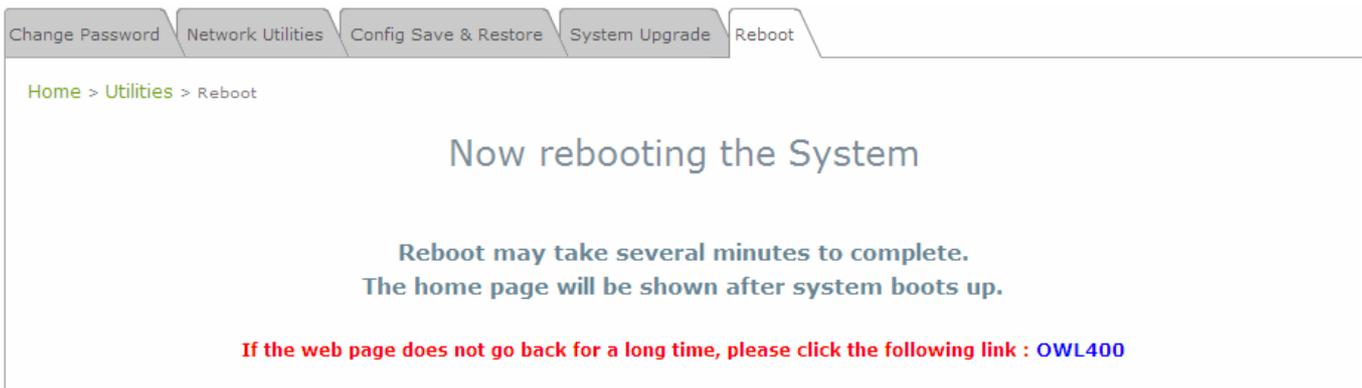
The administrator can reboot the device remotely. Click **Reboot** to restart the system immediately.



A pop-up screen will appear to confirm the request to restart the system. Click **OK** to proceed, or click **Cancel** to cancel the restart request.



A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.



The **system Overview** page will appear upon the completion of reboot.

## 5.5 Status

This section displays the status of **System Overview**, **Event Log**, **DHCP Lease** and **UPnP**.

  
System

  
Wireless

  
Firewall

  
Utilities

  
Status

System Overview

Event Log

DHCP Lease

UPnP

Home > Status > System Overview

### System Overview



#### System

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.4-1.2536
Location	CA, US
Site	EN-A
Device Time	2000/01/06 11:44:31
System Up Time	5 days, 19:44:31
Operating Mode	CPE



#### Radio Status

Status	Connected
SSID	VAP-1
MAC Address	00:1F:D4:00:31:40
Channel	60
Signal Strength	98
Security	None



#### LAN Interface

MAC Address	00:02:31:75:92:0A
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled



#### WAN Interface

Mode	Static
MAC Address	00:1F:D4:88:61:00
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
Bandwidth	Down: Unlimited UP: Unlimited

## 5.5.1 System Overview

The **System Overview** page provides an overview of the system status for the administrator.

System Overview | Event Log | DHCP Lease | UPnP

Home > Status > System Overview

### System Overview

#### System

System Name	OWL400
Firmware Version	1.00.00
Build Number	1.4-1.2536
Location	CA, US
Site	EN-A
Device Time	2000/01/06 12:32:01
System Up Time	5 days, 20:32:01
Operating Mode	CPE

#### Radio Status

Status	Connected
SSID	A600-1-aiX
MAC Address	00:1F:D4:00:2E:54
Channel	60
Signal Strength	82
Security	None

#### LAN Interface

MAC Address	00:02:31:75:92:0A
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

#### WAN Interface

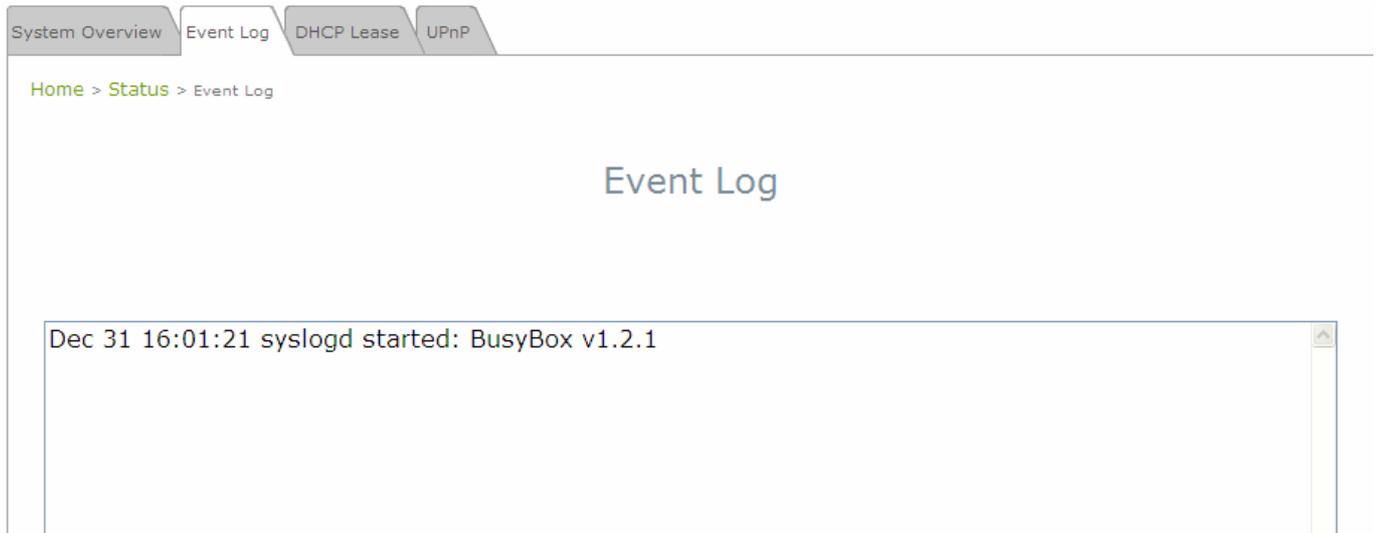
Mode	Static
MAC Address	00:1F:D4:88:61:00
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
Bandwidth	Down: Unlimited UP: Unlimited

The description of the table is shown below:

ITEM		DESCRIPTION
System	System Name	The name provided in System Information.
	Firmware Version	The present firmware version of the system.
	Build Number	The Build Number of the firmware.
	Location	The location provided in System Information.
	Site	The firmware version for specific region.
	Device Time	The current time on the device.
	System Up Time	The system elapsing time since last reboot.
	Operating Mode	Either CPE or AP.
LAN Interface	MAC Address	The MAC address of LAN Interface.
	IP Address	The IP address of the LAN Interface.
	Subnet Mask	The Subnet Mask of the LAN Interface.
	DHCP Server	DHCP server status.
Radio Status	Status	The RF status.
	SSID	The SSID of the associated AP.
	MAC Address	The MAC address of the associated AP.
	Channel	The operating channel.
	Signal Strength	The signal strength reading of the wireless connection.
	Security	The security type used for wireless connection.
WAN Status	Mode	The method to obtain IP for the WAN interface.
	MAC Address	The MAC address of the WAN (RF) Interface.
	IP Address	The IP address of the WAN interface.
	Subnet Mask	The Subnet Mask of the WAN interface.
	Gateway	The gateway IP address.
	Bandwidth	The bandwidth setting of the WAN interface.

## 5.5.2 Event Log

Event log provides the records of the system activities. All the system events are shown here.



► **Note:** As the Event Log is stored in RAM, it will be refreshed after the system is restarted. The system also supports a Syslog reporting function of reporting the events to an external Syslog server.

- **Date/ Time:** The date and time of the record when the event happened.
- **Hostname:** Indicate which Host records this event. Note that all events in this page are local events and this field of all events is the same. However, in remote syslog service, this field will help the network administrator identify which event is from this system. For more information, please refer to **Section 5.1.4 Management Services**.
- **Process name (with square brackets):** Indicate which process with the specific event is associated.
- **Description:** Description of the event.

### 5.5.3 DHCP Leases

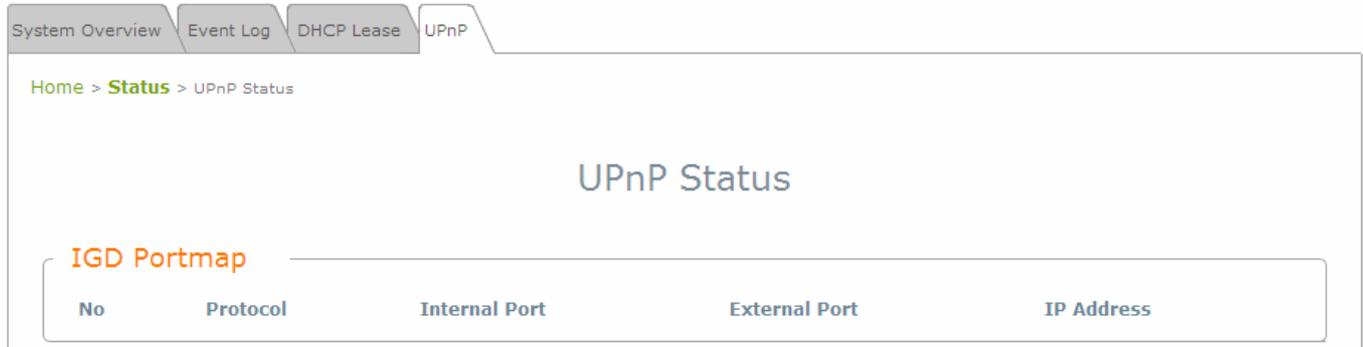
The table provides information about the leased LAN IP address with binding MAC address and expiration time.

No	IP	MAC Address	Expires in
1	192.168.1.2	00:0d:60:cb:76:82	22hours,15minutes,20seconds

- **No:** The item number of the LAN IP leased.
- **IP:** The IP address assigned by DHCP server to a specific LAN device.
- **MAC Address:** The MAC address of the LAN device.
- **Expires in:** The expiration time of the leased IP address.

## 5.5.4 UPnP Status

The table provides information about the UPnP overview such as Protocol, Internal Port, External Port, and IP Address.



No	Protocol	Internal Port	External Port	IP Address
----	----------	---------------	---------------	------------

- **IGD Portmap:**
  - **No:** The item number of an UPnP device.
  - **Protocol:** The Protocol used by the UPnP device.
  - **Internal Port:** The internal port number of the UPnP device.
  - **External Port:** The mapped external port number of the system.
  - **IP Address:** The IP address of the UPnP device.

## 5.6 Online Help

The **Help** button is at the upper right hand corner of the display screen.

Click **Help** for the **Online Help** window, and then click the hyperlink of the desired topic for further information.



### Online Help (CPE Mode)

#### Organization of the Configuration Web:

<u>System</u>	<u>Wireless</u>	<u>Firewall</u>	<u>Utilities</u>	<u>Status</u>
<a href="#">System Information</a>	<a href="#">General</a>	<a href="#">IP/Port Forwarding</a>	<a href="#">Password</a>	<a href="#">System Overview</a>
<a href="#">Operating Mode</a>	<a href="#">Advanced</a>	<a href="#">DMZ</a>	<a href="#">Network Utilities</a>	<a href="#">Event Log</a>
<a href="#">Network</a>	<a href="#">Security</a>		<a href="#">Config Save &amp; Restore</a>	<a href="#">DHCP Lease</a>
<a href="#">Management Services</a>	<a href="#">Site Survey</a>		<a href="#">System Upgrade</a>	<a href="#">UPnP</a>
			<a href="#">Reboot</a>	

## Appendix A. System Management Account Privileges

The system provides two system management accounts for AP & CPE mode, **root** and **admin**. The **root** account is empowered with full privileges while the **admin** account is with partial.

The management privileges of the admin account are shown in the following table.

Main Menu	Sub Menu	Group	Admin Privilege
System	System Information	System Information	Read
		Time	Read
	Operating Mode	Operating Mode	Read
	Network	WAN Configuration	Read
		Dynamic DNS	Read & Write
		LAN Configuration	Read & Write
	Management Services	SNMP Configuration	Read
		Syslog Configuration	Read
		UPnP Configuration	Read & Write
		Auto Reboot	Read
Wireless	General	General Settings	Read
	Advanced	Advanced Wireless Settings	Read
	Security	Security Settings	Read
	Site Survey		Read
Firewall	IP/Port Forwarding		Read & Write
	DMZ		Read & Write
Utilities	Password	Admin Password	Read & Write
	Network Utilities		Read & Write
	Config Save & Restore	Reset to Default	Read
		Backup Settings	Read & Write
		Restore Settings	Read
	System Upgrade		Read
Reboot		Read & Write	

P/N: V10020110307