

# User's Manual

## IEEE 802.11 b/g Outdoor AP/Bridge

(Support IEEE802.11a Client Backhaul)

### Models:

OWL800 v1.00

OWL2000 v1.00

HSG800 v1.00

## **Copyright & Disclaimer**

### **Copyright**

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.

# Regulatory Information

The device contains two radio modules inside. Although the model of the radio modules themselves has obtained the FCC modular approval, independently the whole system (with the antennas and power supplier installed) has been tested and evaluated again by a certified laboratory for the verification of FCC, CE and NCC compliances.

**This device requires professional installation.** Installers please refer to the caution statements under each regulatory section to make sure the final installation meet the regulation within you territory. If you are in the North America, please read the caution statements in FCC section. If you are in the Europe countries, please read the caution statements under CE. And if you are in Taiwan, please read the Chinese statements under NCC. In addition, it is important for all to read the following Safety Information first.

## Safety Information

All models of OWL800, OWL2000, and HSG800 have been evaluated to, and conforms to the product safety specifications of EN:60950:2001+A11:2004.

### Caution:

- This product was qualified under test conditions that included the use of the power supplying equipment. To ensure regulatory and safety compliance, use only the provided power supplying equipment and install them properly.
- To prevent electrical shock, this device may require a grounding conductor in the line cord. Connect the unit to a grounding type ac wall outlet using the power supplying equipment supplied with the unit.
- To avoid the risk of electric shock and for a safety outdoor installation, you may need other items, such as surge arrestors.
- To avoid the risk of electric shock from lightening, do not install or use this product during an electrical storm.
- Operate and install this product as described in this manual. This device must be installed and used in strict accordance with the manufacturer's instructions.
- Do not open the device casing. Do not perform any servicing other than that contained in the installation and troubleshooting instructions. Refer all servicing to qualified service personnel.



## FCC Regulatory Information (for US)

### FCC Certification

OWL800, HSG800 and OWL2000 use the same circuitry and housing except the billing and bandwidth management. The devices operate in the 2.4 GHz and 5.725 - 5.85 bands. They are evaluated and certified according to FCC Rules Part 15 subpart C under one granted FCC-ID: VZ9090001.

### FCC Compliance Information

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

### FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

For complying with the FCC radio frequency exposure requirements, the following antenna installation and device operating configurations must be satisfied:

- The device must be professionally installed on a fixed or permanent structure with a separation distance of at least 20cm from all persons.
- This device and its antennas must not be co-located or operating in conjunction with any other antenna or transmitter.
- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

### FCC Class B Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and uses radio frequency energy and, if not installed and used in accordance with the instructions, may cause interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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



## CE Regulatory Information (for Europe)

### **Declaration of Conformity with Regard to the 1999/5/EC (R&TTE Directive) for European Community, Switzerland, Norway, Iceland, and Liechtenstein**

#### **Models: OWL800, HSG800 and OWL2000**

All three models have been tested and passed the requirements of the following standards, and hence fulfills the EMC and safety requirements of R&TTE Directive within the CE marking requirement.

- Radio: EN 300.328:2006
- Radio: EN 50392:2004
- EMC: EN 301.489-1:2005, EN 301.489-17:2002,
- EMC: EN 55022:2006 Class B, EN 55024:1998 + A1:2001 + A2:2003 including the followings:
  - EN 61000-3-2, EN 61000-3-3.
  - EN 61000-4-2, EN 61000-4-3, EN 61000-4-4,
  - EN 61000-4-5, EN 61000-4-6, EN 61000-4-11
- Safety: EN 60950-1:2001 + A11:2004,

#### **Caution:**

- This declaration is only valid for configurations (combinations of software, firmware, and hardware) provided and supported by 4ipnet Inc. The use of software or firmware not provided and supported by 4ipnet Inc. may result in the equipment no longer being compliant with the regulatory requirements.
- European standards dictate maximum radiated transmit power of 100mW EIRP and frequency range 2.400-2.4835 GHz.
- This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact your local regulatory authority for compliance.



## NCC Regulatory Information (for Taiwan)

NCC 基本規定項目：

根據 NCC 低功率電波輻射性電機管理辦法 規定:

- |      |   |
|------|---|
| 第十二條 | 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。 |
| 第十四條 | 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時應立即停用，並改善至無干擾時方得繼續使用。  |
|      | 前項合法通信，指依電信法規定作業之無線電通信。                                   |
|      | 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。                     |

NCC 其他注意項目 (NCC Caution)：

一、本產品(OWL800, HSG800, OWL2000)及外接天線僅限於專業安裝，並限於固定式、點對點之操作。本產品是設計為專業用、防水、防風、防鏽、堅固之工業級產品；其銷售對象限於有發射器專業安裝技術之工程單位或無線系統之專業整合商。

二、本產品(OWL800, HSG800, OWL2000)內建兩個無線模組(型號CM9)，其最高輸出功率為19dBm。設定介面所提供的功率變更只能用於調降發射功率，也就是說，設定在最高時(Highest)，只會達19 dBm，設定的改變不會加大無線模組之發射功率。

三、本產品(OWL800, HSG800, OWL2000)雖然有介面可改設內建無線模組的發射頻道，以避免與其它鄰近無線設備衝突；但介面上所可選之頻道，是根據販售當地法令有所限制。例如，在台灣市場及在北美市場的產品，2.4G範圍只有11個頻道在介面上可選，使用者無法將發射頻道設為其他在歐、日可選而在台灣所不允許之頻道。

四、本產品(OWL800, HSG800, OWL2000)附有隨機所附手冊，包含以上所有繁體中文警告訊息。專業使用者與安裝者有責遵循NCC規定。專業使用者與安裝者若有自行變動產品，違規使用當地法規不允許頻率、功率，必須承擔法律責任並負責賠償受害用戶之一切損失。

## Table of Contents

Copyright & Disclaimer .....	i
Regulatory Information.....	ii
FCC Regulatory Information (for US) .....	iii
CE Regulatory Information (for Europe) .....	iv
NCC Regulatory Information (for Taiwan) .....	v
<b>1. Before You Start .....</b>	<b>3</b>
1.1 Preface .....	3
1.2 Document Convention .....	3
<b>2. System Overview .....</b>	<b>2</b>
2.1 Introduction of OWL800 .....	2
2.2 System Concept .....	2
<b>3. Base Installation .....</b>	<b>4</b>
3.1 Hardware Installation.....	4
3.1.1 Package Contents .....	4
3.1.2 Panel Function Descriptions .....	5
3.1.3 Hardware Installation.....	6
3.2 Software Configuration.....	7
3.2.1 Instruction of Web Management Interface .....	7
3.2.2 User Login Portal Page .....	10
3.2.3 Basic Configuration .....	12
3.2.4 Common Settings.....	16
<b>4. Menu Configuration (AP &amp; Gateway Mode).....</b>	<b>20</b>
4.1 System.....	24
4.1.1 General.....	24
4.1.2 Network Interface .....	27
4.1.3 Management.....	32
4.1.4 VLAN Overview.....	34
4.1.5 VLAN Configuration .....	36
4.1.6 Walled Garden.....	39
4.1.7 Mode .....	41
4.2 AP .....	42
4.2.1 Overview.....	42
4.2.2 General.....	45
4.2.3 VAP Configuration.....	46
4.2.4 Security .....	47
4.2.5 Advanced .....	51
4.2.6 Access Control.....	52

4.3	WDS.....	54
4.3.1	Overview.....	54
4.3.2	General.....	55
4.3.3	WDS Configuration .....	56
4.3.4	WDS Discovery .....	58
4.4	User.....	59
4.4.1	Local .....	59
4.4.2	RADIUS.....	62
4.4.3	On-demand.....	64
4.4.4	Policy .....	69
4.4.5	Firewall.....	71
4.4.6	Route.....	73
4.4.7	802.1X.....	74
4.5	Utilities.....	75
4.5.1	Change Password.....	75
4.5.2	Import & Export.....	76
4.5.3	Backup & Restore .....	77
4.5.4	System Upgrade .....	78
4.5.5	Reboot.....	79
4.5.6	Scan.....	80
4.5.7	Upload Certificate.....	81
4.6	Status.....	82
4.6.1	Overview.....	82
4.6.2	WDS List .....	85
4.6.3	Antennas .....	86
4.6.4	Associated Clients.....	87
4.6.5	Event Log.....	88
4.6.6	Online Users .....	89
4.6.7	User Log .....	90
<b>Appendix A.</b>	<b>Session Limit and Session Log .....</b>	<b>91</b>
<b>Appendix B.</b>	<b>802.1X Support.....</b>	<b>93</b>



# 1. Before You Start

## 1.1 Preface

This manual is intended for using by system integrators, professional field engineers and network administrators to help them set up OWL800 for their network deployment. It contains step by step procedures and pictures to guide users with basic network system knowledge to complete the installation.

The **IEEE 802.11 b/g Outdoor AP/Bridge (Support IEEE802.11a Client Backhaul)** is a rugged multi-mode dual-radio outdoor access point, specifically designed for building municipal or campus wide wireless networks in harsh outdoor environments. The entry model **OWL800** is deployed as a traditional multi-wireless Access Point (AP) or a backhaul. The second model **HSG800**, can be used as an Outdoor Wireless Gateway with built-in Hotspot Access Control and Billing features. The **OWL2000** is purely used for building point-to-point bridges. Some of the optional features (such as billing) are on or off depending on the model. Please refer to the optional feature lists provided separately. In this manual, all the optional featured are covered. In the following manual, we will refer the device as "OWL800" or "the system" for the convenience.

Model	Description
OWL800	This is the base model. Its firmware can be upgraded to be HSG800 or OWL2000 when optional software feature is purchase. The base firmware support AP/Bridge and Gateway operation mode.
HSG800	This model consists of all the features of OWL800, plus the Hotspot billing & payment function.
OWL2000	This model turn an OWL800 first radio card from an AP into another backhaul/bridge radio card. Traffic over multiple air links will be aggregated to achieve better throughput and reliability.

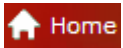
## 1.2 Document Convention

The following information provides the details of conventions used in this manual. In the following manual, we will refer the device as "OWL800" or "the system" for the convenience.

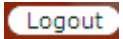
For cautionary statements or warning requiring special attention by readers, a text box with italic font will be used:

**Warning:** *For security purposes, you should immediately change the administrator's password.*

When any of the button and symbol shown below is selected, the following action will be executed accordingly:



Return to system **Home** page.



Logout the system.



Apply all configurations.



Clear all configurations and not to activate them.



Clear settings entered by clicking this button.

\* The red asterisk indicates information in this field is compulsory.

**Note:** Screen captures and pictures used in this manual may be displayed in part or in whole or **similar products**, and may vary or differ slightly from the actual product, depending on versioning and menu accessed.

## 2. System Overview

### 2.1 Introduction of OWL800

The **IEEE 802.11 b/g Outdoor AP/Bridge (Support IEEE802.11a Client Backhaul)** series (referred as OWL800 or the system in this manual) is a rugged multi-mode dual-radio outdoor access point, specifically designed for building municipal or campus wide wireless networks in harsh outdoor environments. There are two System Modes that can be used for dual purposes. First, it can be deployed as a traditional multi-wireless Access Point (AP) or a Relay. Secondly, it can be used as an Outdoor Wireless Gateway with Built-in Hotspot Access Control and Billing features (\* an optional feature).

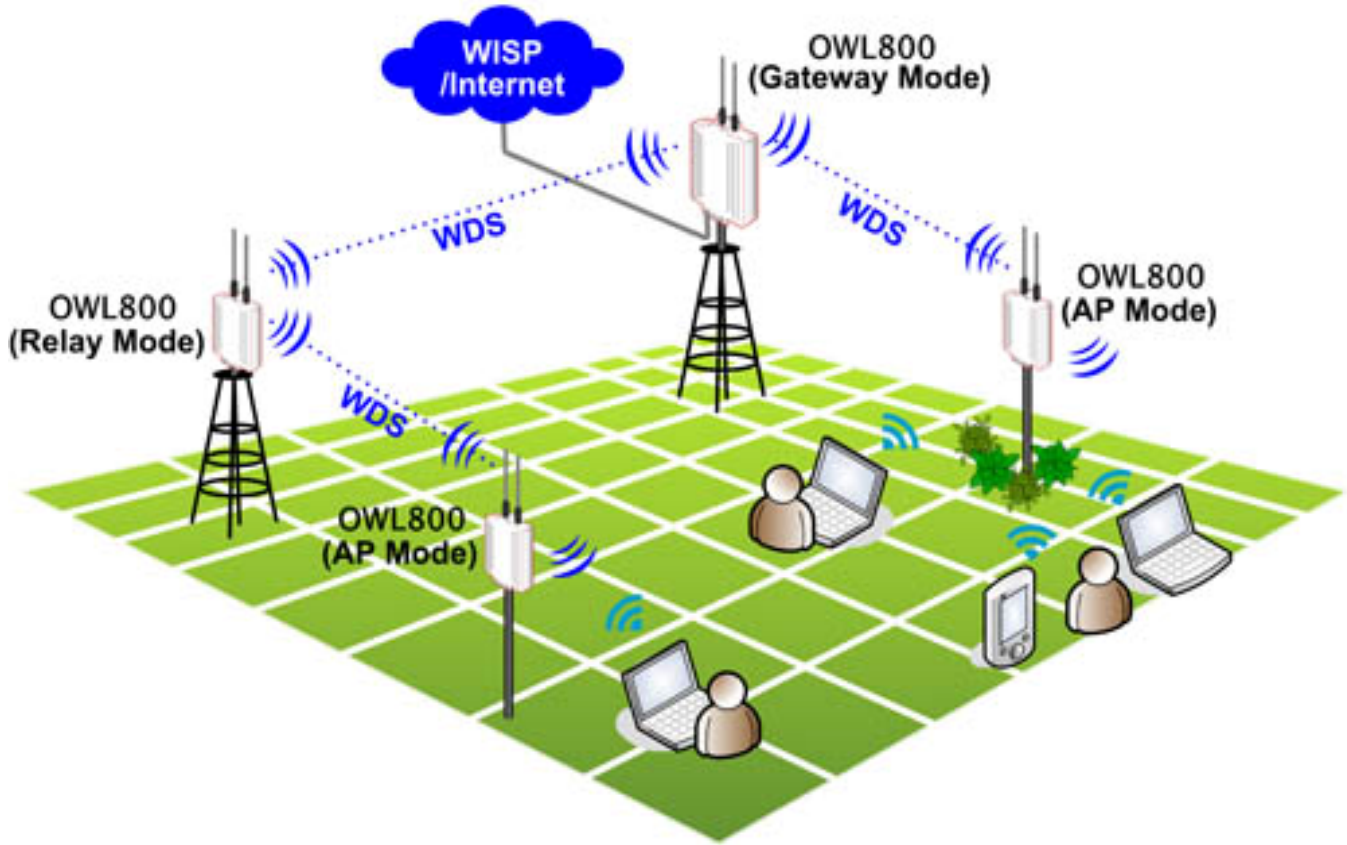
The metal sealed OWL800 is weatherproof. Coming with a mounting kit, it can be mounded on a pole or on wall. This Quick Installation Guide provides instructions and reference material for getting started with OWL800 (as well as the other two models).

OWL800's rust-free die-cast Aluminum housing is IP68 compliant and high wind load resilient. All the components are designed to operate in a wide range of temperature. The on-board surge protection provides the device up to 15KV surge immunity. The OWL800 delivers an excellent outdoor WLAN solution.

### 2.2 System Concept

The System contains two radio modules. Two 100mW modules are WNC's CM9, which are tested to be modular FCC and CE compliant. The first card is mainly used for serving clients at "b/g" mode. The second Radio module is used for building point-to-point or the back haul connection in "a" mode.

OWL800 is a cost-effective choice as well as a flexible solution for constructing serviceable wireless network. Designed by the leading hotspot appliance provider, 4ipnet OWL800 behaves more than a wireless router when it is in Gateway mode. Not only it supports NAT, DHCP and firewall, it also has AAA features of a hotspot gateway, including UAM web login portal and billing plans. Standalone it has local user database for authentication, while at the same time it can play the role of RADIUS-NAS, authenticating users against ISP's RADIUS server in the data center.



*Multi-mode in Operation*

## 3. Base Installation

### 3.1 Hardware Installation

#### 3.1.1 Package Contents

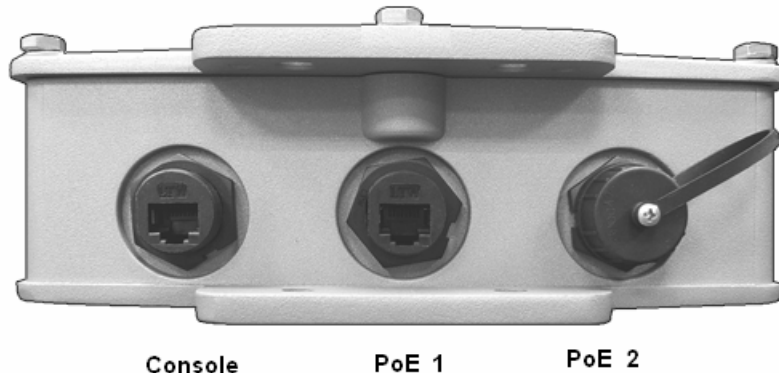
The standard package of OWL800 includes:

- OWL800 x 1
- Quick Installation Guide (with User's Manual and QIG) x 1
- CD-ROM x 1
- RJ45-RS232 Console Cable x 1
- PSE x 1
- Power cord x 1
- Mounting Kit x 1
- Waterproof Connector Pack x 2
- Rubber antenna x 4

**Note:** It is recommended to keep the original packing materials in case of product service requirements. Any returned product should be packed according to its original package content, together with its relevant packing materials used for protecting the equipment from damage during delivery.

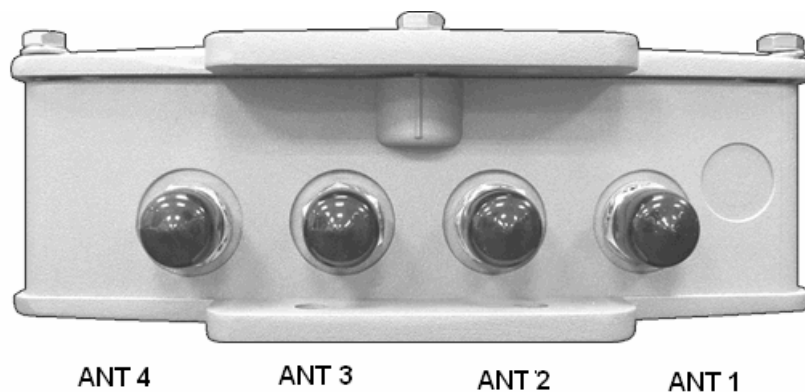
### 3.1.2 Panel Function Descriptions

#### Lower Panel



- **PoE1 / PoE2: For connecting to the PSE**
  - In AP/Relay mode, PoE1 and PoE2 work as LAN ports.
  - In Gateway mode, PoE1 works as a WAN port and PoE2 works as a LAN port.
- **Console:**
  - Attach the RJ45-RS232 console cable here.

#### Upper Panel



This picture represents ANT 1 ~ ANT 4 connectors from right to left when OWL800 chassis (with Mylar) is faced up. Each of the two radio module (CM9) inside has two antenna connectors for antenna diversity. **The required antenna is antenna ANT1 and antenna ANT2.** ANT1 is connected to the “Main” contact point of the first radio module. ANT2 is connected to the “Main” contact of the second module.

The other two antennas are optional for antenna diversity. The antenna ANT3 is connected to the “Aux” contact point of the first radio module, while ANT4 is connected to the “Aux” contact point of the second radio module. For further details on antenna, please refer to the section 4.6.3..

### 3.1.3 Hardware Installation

Please follow the steps mentioned below to complete the hardware of OWL800 for configuration.

1. Connect antennas to the required ANT1 and ANT3, which lead to the "Main" contacts of the two radio cards.
2. (Optional) Connect antennas to the required ANT3 and ANT4, which lead to the "Aux" contacts of the two radio cards.
3. Connect the PSE (POWER & DATA OUT) to the PoE 2 connector on the lower panel.
4. Connect one end of an Ethernet cable to the PSE (DATA IN) and the other end to a computer.
5. Connect the power cord to the PSE.
6. Power on the PSE in order to supply power to OWL800.
7. Note You must be professional to use a different replacement antenna, and you must following the code/regulation of your region/country for the installation.

Now, the Hardware Installation has been completed and ready for configuration. It is easier to following the Quick Installation Guild for the first time to configure the necessary network parameters, such as the IP address.

**Note:** *It is recommended to keep the original packing materials in case of product service requirements. Any returned product should be packed according to its original package content, together with its relevant packing materials used for protecting the equipment from damage during delivery.*

## 3.2 Software Configuration

### 3.2.1 Instruction of Web Management Interface

OWL800 provides the web management interface for configuration. OWL800 is a multi-mode system which can be configured as either an access point (**AP/Relay Mode with RF1 in AP**), a relay (**AP/Relay Mode with RF1 in WDS**), or a gateway that clients can associate on it based on your needs. It is required to follow the respective installation procedures provided to properly set up the desired mode of this system.

After completing hardware installation, the administrator can configure the OWL800 via web browsers.

The default IP address and Subnet Mask of different modes are as follows:

Mode	AP/Relay	Gateway
IP Address	192.168.2.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.2.254	192.168.1.254

Enter "**admin**" as the default **Username** and "**admin**" as the default **Password** and click **Login** to continue.

Username:

Password:

**Note:** If you are unable to get to the login screen, please check the IP address used. The IP address should be in the same subnet of the default gateway. For using static IP in TCP/IP setting, set a static IP address such as 192.168.1.x for your network interface and then open a new browser again.




- **Main Menu:** provides detailed configuration pages for administrators to configure the system manually. Please refer to **Section 4. - Main Menu** for more information.

Home > Status > System Overview


## System Overview

 **System**


System Name	OWL800
Firmware Version	1.00.00
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	0 days, 0:13:49
Operating Mode	GW

 **Radio Status**

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:A9:E7	802.11b+g	6	Highest
RF Card B	00:0B:6B:DB:A9:09	802.11b+g	9	Highest

 **AP Status**

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:A9:E7	OWL800-1	None	0
VAP-2	06:0B:6B:DB:A9:E7	OWL800-2	None	0
VAP-3	0A:0B:6B:DB:A9:E7	OWL800-3	None	0

 **Network Interfaces**

Interface	IP Address	Gateway	Type
WAN1	192.168.1.8	192.168.0.1	Static

Interface	IP Address	VLAN Tag	State
VLAN0	192.168.1.1	0	Enabled
VLAN1	192.168.11.1	1	Enabled
VLAN2	192.168.12.1	2	Enabled
VLAN3	192.168.13.1	3	Enabled
VLAN4	192.168.14.1	4	Enabled
VLAN5	192.168.15.1	5	Disabled
VLAN6	192.168.16.1	6	Disabled
VLAN7	192.168.17.1	7	Disabled
VLAN8	192.168.18.1	8	Disabled

### Gateway Mode

System    AP    WDS    Utilities    Status

Overview    WDS List    Antennas    Associated Clients    Event Log

Home > Status > System Overview

## System Overview

### System

System Name	OWL800
Firmware Version	1.00.00
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	2 days, 21:22:23
Operating Mode	AP

### Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:A9:E7	802.11b+g	6	Highest
RF Card B	00:0B:6B:DB:A9:09	802.11b+g	9	Highest

### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:A9:E7	OWL800-1	None	0
VAP-2	06:0B:6B:DB:A9:E7	OWL800-2	None	0
VAP-3	0A:0B:6B:DB:A9:E7	OWL800-3	None	0

### LAN Interface

MAC Address	00:08:00:00:01:09
IP Address	
Subnet Mask	255.255.0.0
Gateway	

**AP Mode**

### 3.2.2 User Login Portal Page

To be granted the network access via OWL800, clients have to be authenticated by the system first via entering the correct usernames and passwords in the User Login Portal Page as shown below. The local account generated previously in the Setup Wizard section is used as the example to illustrate this procedure.

#### Step 1:

Connect a client's PC to OWL800 via any one of the LAN Ports. The IP address will be assigned to the PC automatically via DHCP.

#### Step 2:

##### Verify New Local Account:

To verify whether the configuration with DHCP via the Setup Wizard is done properly, firstly, connect a client's PC from the system to LAN1 Port. The device will get an IP address automatically via DHCP.

Next, open a web browser and access any URL, and then the default **User Login Page** will appear.

Enter the username and password of the local user account generated by Setup Wizard previously (e.g. "**test@local**" as the **Username** and "**test**" as the **Password**), then click **Login**.

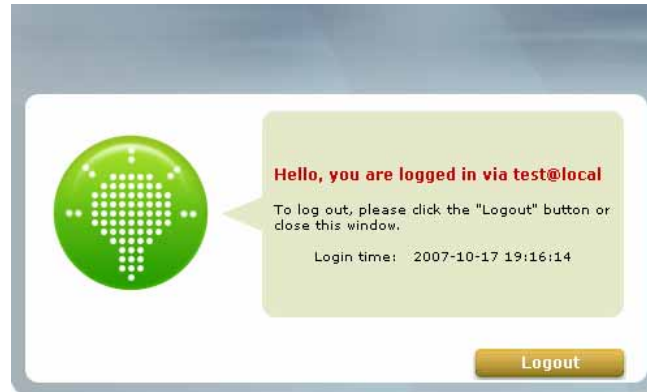


#### Note:

1. OWL800 supports both local built-in user database and external authentication database, such as RADIUS and LDAP. Thus, by entering the full username, the system will automatically identify which authentication server is used. *Exception: The postfix can be omitted only when the default authentication option is used; "local" is the default authentication option of the system. You may therefore enter either 'test', or 'test@local' in the username field for the previous example.*
2. The format of a valid Username is: **UserId@postfix**, where **UserId** is the User ID, and postfix is a name for the chosen authentication option.

**Step 3:**

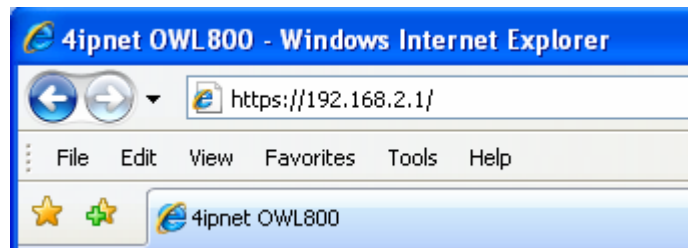
The Login Success Page will appear after a client is authenticated by the system and logs in successfully. In the meantime, successful login means OWL800 has been installed and configured properly.



### 3.2.3 Basic Configuration

#### <AP/Relay Mode>

After completing hardware installation, the administrator can configure the OWL800 via web browsers.



If the IP address of the administrator's PC is within the same subnet as OWL800's, then assigning a static IP address within the same subnet as OWL800's to the administrator's PC is needed in order to get Administrator Login Page.

The following IP address is listed as an example:

*IP Address: 192.168.2.10*

*Subnet Mask: 255.255.255.0*

*Default Gateway: 192.168.2.254*

Once OWL800 has been connected, the Administrator Login Page will appear. Enter "**admin**" for both the default user name and password in the *Username* and *Password* fields, and then click the **OK** button to log in.

*Username: admin*

*Password: admin*

Username:

Password:

After successfully logging into OWL800, the **System Overview** page of the web management interface will appear.

Home > Status > System Overview

### System Overview

#### System

System Name	OWL800
Firmware Version	
Build Number	
Location	Taipei, Taiwan
Site	EN-A
Device Time	2000/01/01 05:05:10
System Up Time	0 days, 0:01:10

#### Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:A9:B6	802.11b+g	2	highest
RF Card B	00:0B:6B:DB:A9:DB	N/A	N/A	N/A

#### LAN Interface

MAC Address	00:0B:6B:DB:A9:B6
IP Address	192.168.1.100
Subnet Mask	255.255.0.0
Gateway	192.168.1.10

#### AP Status

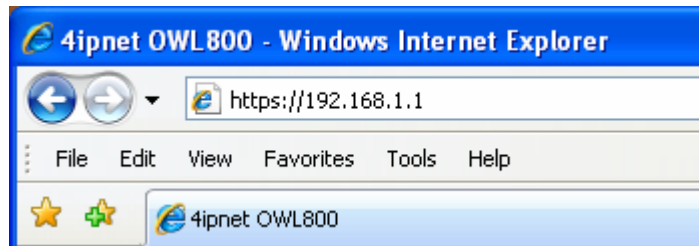
Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:A9:B6	OWL800-1	None	0
VAP-2	00:0B:6B:DB:A9:B7	OWL800-2	None	0
VAP-3	00:0B:6B:DB:A9:B8	OWL800-3	None	0
VAP-4	00:0B:6B:DB:A9:B9	OWL800-4	None	0
VAP-5	00:0B:6B:DB:A9:BA	OWL800-5	None	0
VAP-6	00:0B:6B:DB:A9:BB	OWL800-6	None	0
VAP-7	00:0B:6B:DB:A9:BC	OWL800-7	None	0
VAP-8	00:0B:6B:DB:A9:BD	OWL800-8	None	0

### AP Mode

To logout, simply click the **Logout** icon on the upper right corner of the web management interface to return to the Administrator Login Page.

**Note:** By default, the system is in AP/Relay mode. Therefore, the administrator must login to the system in AP/Relay mode at the first time and then be able to switch the system to the desired mode afterwards.

## &lt;Gateway Mode&gt;



If the IP address of the administrator's PC is not assigned via DHCP within the same subnet as OWL800's, then a static IP address assigned to the administrator's computer within the same subnet as OWL800's is needed. The following IP address is listed as an example:

*IP Address: 192.168.1.10*

*Subnet Mask: 255.255.255.0*

*Default Gateway: 192.168.1.254*

Once OWL800 has been connected, the Administrator Login Page will appear. Enter "**admin**" for both the default user name and password in the *User name* and *Password* fields, and then click the **OK** button to log in.


*User name: admin*


*Password: admin*


Username:


Password:


After successfully logging into OWL800, the **System Overview** page of the web management interface will appear.


  
System

  
AP

  
WDS

  
User

  
Utilities

  
Status

Overview

WDS List

Antennas

Associated Clients

Event Log

Online Users

User Log

Home > **Status** > System Overview

### System Overview

#### System

System Name	OWL800
Firmware Version	
Build Number	
Location	
Site	EN-A
Device Time	2000/01/02 05:50:46
System Up Time	0 days, 0:22:07
Operating Mode	GW

#### Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:AA:1E	802.11b+g	6	Highest
RF Card B	00:0B:6B:DB:A9:05	802.11b+g	9	Highest

#### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:AA:1E	OWL800-1	None	0
VAP-2	06:0B:6B:DB:AA:1E	OWL800-2	None	0
VAP-3	0A:0B:6B:DB:AA:1E	OWL800-3	None	0

#### Network Interfaces

Interface	IP Address	Gateway	Type
WAN1	192.168.1.198	10.30.1.254	Static

Interface	IP Address	VLAN Tag	State
VLAN0	192.168.1.1	0	Enabled
VLAN1	192.168.11.1	1	Enabled

### Gateway Mode

To logout, simply click the **Logout** icon on the upper right corner of the web management interface to return to the Administrator Login Page.



### 3.2.4 Common Settings

#### System Mode Configuration:

- 1) Change System Mode by clicking on the **System** menu item.
- 2) Select **Mode** from submenu item.
- 3) Select desired System mode - either AP/Relay or Gateway mode, and then click on **Apply** to confirm the change.

Home > System > Operation Mode



When OWL800 is set in AP/Relay mode, it is a layer2 IP device like a normal AP. No IP sharing (NAT) and routing feature are support.

When OWL is set in Gateway mode, it is a layer3 IP device. Like an AP router, OWL800 in the gateway mode support IP sharing (NAT). Its POE1 port is treated as the uplink.

Home > System > Operation Mode



#### Change Password:

- 1) Change administrator's password by clicking on the **Utilities** menu item.
- 2) Select **Change Password** from submenu item.
- 3) Enter new password. Supply new password with up to 32 characters, and then click on **Apply** to confirm the change.

Home > Utilities > Change Password

## Change Password

Name :	admin
Old Password :	<input type="text"/>
New Password :	<input type="text"/> *up to 32 characters
Re-enter New Password :	<input type="text"/>
Name :	manager
New Password :	<input type="text"/> *up to 32 characters
Re-enter New Password :	<input type="text"/>
Name :	operator
New Password :	<input type="text"/> *up to 32 characters
Re-enter New Password :	<input type="text"/>

### Gateway Mode

Home > Utilities > Change Password

## Change Password

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

### AP Mode

#### Check VAP Profile Settings

- 1) Click on the **AP** menu item.
- 2) Select **VAP Configuration** from submenu item.
- 3) Administrator can enable or disable specific VAP from the drop down list of "Profile Name".
- 4) Set desired ESSID.
- 5) Disable VLAN ID means untagged when this VAP is enabled. Set a VLAN ID if this VAP is tagged.

**Note:** To configure the rest of the profiles, please follow the same steps as illustrated for VAP-1.

Home > AP > VAP Config

## VAP Configuration

Profile Name :

VAP :  Disable  Enable

Profile Name :

ESSID :

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

### Gateway & AP Mode

#### Check AP Status

After finishing the settings, the enabled virtual AP should appear in the virtual AP list showing enabled state.

Home > AP > VAP Overview

## VAP Overview

VAP No.	State	Security Type	MAC ACL	Advanced Settings
1	Enabled	None	Disabled	Edit
2	Enabled	None	Disabled	Edit
3	Enabled	None	Disabled	Edit
4	Disabled	None	Disabled	Edit
5	Disabled	None	Disabled	Edit
6	Disabled	None	Disabled	Edit
7	Disabled	None	Disabled	Edit
8	Disabled	None	Disabled	Edit

### Gateway & AP Mode

#### Configure General WDS Settings

- 1) Click on the **WDS** menu item. Select **General** submenu.
- 2) WDS is used as bridge/backhaul. By default, 'a' mode is used for WDS. You must select a channel to Select preferred *Channel* for the wireless connection. For example, select channel code 149.

Note: Depending on your country, the list of allowed channels is different. For example, the OWL800 shipped to US market allow one to select the 5 channels for the WDS within the range of 5.725-5.850 only.

Home > WDS > RF Settings

### WDS Interface Settings

RF Card Name : RF Card B

Band : 802.11a

Channel : 149

Max Transmit Rate : Auto

Transmit Power : Highest

Shared Secret Key : 123456 (Optional: for WDS discovery)

Antenna Diversity :  Disable  Enable

Distance : 0 meter(s)  Advance

#### Gateway & AP Mode

#### Configure WDS Settings

- 1) Click on the **WDS** menu item.
- 2) Select **WDS Configuration** submenu item.
- 3) Setting WDS link parameters

By default, WDS profiles are disabled. First, choose the WDS Profile; enable WDS; supply peer's MAC address and security type.

Home > WDS > WDS Configuration

### WDS Link Settings

WDS Profile : RF Card B : WDS Link 1

WDS :  Disable  Enable

MAC Address of Remote AP : \*

Path Cost of STP : 100

Security Type : None

#### Gateway & AP Mode

**Note:** WDS profiles are able to be configured even when the respective Radio module is disabled which can be done in **General** submenu item of **WDS** menu.

Now, the system has been installed and configured successfully.

**Note:** It is strongly recommended to make a copy of configuration backup. (Local user database shall be saved separately.)

## 4. Menu Configuration (AP & Gateway Mode)

This chapter illustrates the detailed configurable settings of OWL800. The following table is the UI and functions supported by OWL800. In the web management interface, there are three main interface areas: **Main Menu**, **Submenu** and **Working Area**. The management functions are grouped into six branches: **System (Gateway/AP)**, **AP (Gateway/AP)**, **WDS (Gateway/AP)**, **User (AP)**, **Utilities (Gateway/AP)**, and **Status (Gateway/AP)**.

OPTION	FUNCTION
System	General(AP & Gateway)
	Network Interface (AP & Gateway)
	Management (AP & Gateway)
	VLAN Overview (Gateway)
	VLAN Configuration (Gateway)
	Walled Garden (Gateway)
	Mode (AP & Gateway)
	Overview (AP & Gateway)
	General (AP & Gateway)
	VAP Configuration (AP & Gateway)
AP	Security (AP & Gateway)
	Advanced (AP & Gateway)
	Access Control (AP & Gateway)
	Overview (AP & Gateway)
	General (AP & Gateway)
WDS	WDS Configuration (AP & Gateway)
	WDS Discovery (AP & Gateway)
User	Local (Gateway)
	Radius (Gateway)
	On-demand (Gateway)
	Policy (Gateway)
	Firewall (Gateway)
	Route (Gateway)
	802.1X(Gateway)

Utilities	Change Password (AP & Gateway)
	Import & Export (Gateway)
	Backup & Restore (AP & Gateway)
	System Upgrade (AP & Gateway)
	Reboot (AP & Gateway)
	Scan (AP & Gateway)
	Upload Certificate (AP & Gateway)
Status (AP & Gateway)	Overview (AP & Gateway)
	WDS List (AP & Gateway)
	Antennas (AP & Gateway)
	Associated Clients (AP & Gateway)
	Event Log (AP & Gateway)
	Online Users (Gateway)
	User Log (Gateway)

**Caution:** After finishing the configuration, please click **Apply** and pay attention to see if a restart message appears on screen. If the message appears, the system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.

## ■ Introduction:

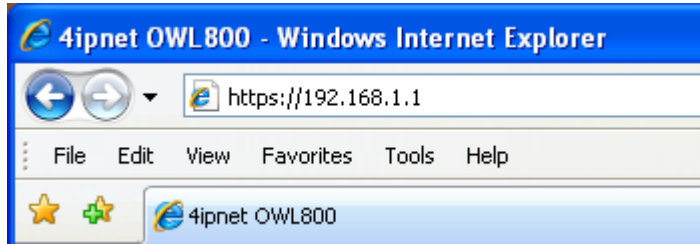
OWL800 has equipped a friendly Web graphical user interface for users and system administrators to configure parameters easily and remotely. The recommended web browsers are IE 6.0(TM), Firefox 2.0(TM) and the above. OWL800 provides the web management interface for easier configuration. After completing hardware installation, the administrator can configure the OWL800 through web browsers with JavaScript enabled, such as Mozilla Firefox 2.0 or Internet Explorer version 6.0 and the above.

Launch a web browser to access the web management interface of OWL800 by entering "<https://192.168.1.1>" in the URL. (Note: **https** is used for a secured connection.)

For configuring via web management interface, a computer with DHCP enabled in TCP/IP setting is needed. The default LAN IP address of OWL800 is listed as following:

*IP Address: 192.168.1.1*

*Subnet mask: 255.255.255.0*



Home > Status > System Overview

## System Overview

### System

System Name	OWL800
Firmware Version	1.00.00
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	2 days, 21:22:23
Operating Mode	AP

### Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:A9:E7	802.11b+g	6	Highest
RF Card B	00:0B:6B:DB:A9:09	802.11b+g	9	Highest

### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:A9:E7	OWL800-1	None	0
VAP-2	06:0B:6B:DB:A9:E7	OWL800-2	None	0
VAP-3	0A:0B:6B:DB:A9:E7	OWL800-3	None	0

### LAN Interface

MAC Address	00:08:00:00:01:09
IP Address	
Subnet Mask	255.255.0.0
Gateway	

**AP Mode**

Home > Status > System Overview

## System Overview

### System

System Name	OWL800
Firmware Version	1.00.00
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	0 days, 0:13:49
Operating Mode	GW

### Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:A9:E7	802.11b+g	6	Highest
RF Card B	00:0B:6B:DB:A9:09	802.11b+g	9	Highest

### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:A9:E7	OWL800-1	None	0
VAP-2	06:0B:6B:DB:A9:E7	OWL800-2	None	0
VAP-3	0A:0B:6B:DB:A9:E7	OWL800-3	None	0

### Network Interfaces

Interface	IP Address	Gateway	Type
WAN1	192.168.1.8	192.168.0.1	Static

Interface	IP Address	VLAN Tag	State
VLAN0	192.168.1.1	0	Enabled
VLAN1	192.168.11.1	1	Enabled
VLAN2	192.168.12.1	2	Enabled
VLAN3	192.168.13.1	3	Enabled
VLAN4	192.168.14.1	4	Enabled
VLAN5	192.168.15.1	5	Disabled
VLAN6	192.168.16.1	6	Disabled
VLAN7	192.168.17.1	7	Disabled
VLAN8	192.168.18.1	8	Disabled

### Gateway Mode



## 4.1 System

This section guides you through the following functions: **System Information**, **Network Interface**, **Management Service**, **VLAN Overview**, **VLAN Configuration**, **Walled Garden List**, and **Gateway/AP Mode Selection**.

### 4.1.1 General

[Home](#) > [System](#) > [General](#)

#### System Information

Name :	<input type="text" value="OWL800"/> *
Description :	<input type="text"/>
Location :	<input type="text"/>

#### Time

Device Time :	2000/01/23 07:49:19
Time Zone :	<input type="text" value="(GMT+08:00)Taipei"/>
Time :	<input type="radio"/> Enable NTP <input checked="" type="radio"/> Manually set up
Set Date :	<input type="text" value="----"/> Year <input type="text" value="--"/> Month <input type="text" value="--"/> Day
Set Time :	<input type="text" value="--"/> Hour <input type="text" value="--"/> Min <input type="text" value="--"/> Sec

#### AP Mode

[Home](#) > [System](#) > [General](#)

## System Information

Name :	<input type="text" value="OWL800"/> *
Description :	<input type="text"/>
Location :	<input type="text"/>
Internal Domain Name :	<input type="text" value="mygateway.mycompany.co"/> *( Domain Name )

## Time

Device Time :	2000/01/26 04:05:43
Time Zone :	<input type="text" value="(GMT+08:00)Taipei"/>
Time :	<input type="radio"/> Enable NTP <input checked="" type="radio"/> Manually set up
Set Date :	<input type="text" value="----"/> Year <input type="text" value="--"/> Month <input type="text" value="--"/> Day
Set Time :	<input type="text" value="--"/> Hour <input type="text" value="--"/> Min <input type="text" value="--"/> Sec

### Gateway Mode

#### System Information

For the purpose of maintenance, it is required to specify the system name, its location and corresponding basic parameters. Fields "Name", "Description" and "Location" are used for mnemonic purpose. It is recommended to have different values for each AP. Time settings allow you to set OWL800's system time manually or have it synchronized automatically with NTP server. When NTP server is used, NTP server1 must be filled. If FQDN (full qualified domain name) is used, the DNS server setting must also be activated.

- **Name:** System name used to identify this box
- **Description:** Give further information about this installation
- **Location:** The geographic location

## Time

- **Device time:** Current system time
- **Time zone:** Take UTC offset to set this field
- **Time:** There are two options of setting system time

### 1) NTP enabled:

By enabling NTP server, OWL800 can synchronize its system time with the NTP server automatically. While this method is selected, at least one NTP server's IP address should be provided. It is recommended to give both NTP servers' IP addresses to prevent occasionally NTP service unavailable.

### Time

<b>Device Time :</b>	2000/01/23 07:49:19
<b>Time Zone :</b>	(GMT+08:00)Taipei
<b>Time :</b>	<input checked="" type="radio"/> Enable NTP <input type="radio"/> Manually set up
<b>NTP Server 1 :</b>	<input type="text"/> *
<b>NTP Server 2 :</b>	<input type="text"/>

### Gateway & AP Mode

### 2) Set Date & Time manually:

Manually set the system time by giving date & time in this page underneath. If this method is chosen, the NTP server 1&2 settings will be closed. Note, unless Internet connection is unavailable, it is recommended to take NTP server for time synchronization.

### Time

<b>Device Time :</b>	2000/01/23 07:49:19
<b>Time Zone :</b>	(GMT+08:00)Taipei
<b>Time :</b>	<input type="radio"/> Enable NTP <input checked="" type="radio"/> Manually set up
<b>Set Date :</b>	---- Year    -- Month    -- Day
<b>Set Time :</b>	-- Hour    -- Min    -- Sec

### Gateway & AP Mode

## 4.1.2 Network Interface

There are 3 connection types supported on OWL800's WAN port: Static, DHCP or PPPoE.

[Home](#) > [System](#) > [Network Interface](#)

### Network Settings

**Mode :**  Static  DHCP

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

**Layer2 STP :**  Disable  Enable

### Dynamic DNS (DDNS)

**DDNS :**  Disable  Enable

**Provider :**

**Host Name :**

**User Name / E-mail :**

**Password / Key :**

**AP Mode**

Home > System > Network Interface

### WAN Configuration

**Mode :**  Static  DHCP  PPPoE

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

**Available Bandwidth on WAN Interface :**

Uplink :  ▼

Downlink :  ▼

### Dynamic DNS (DDNS)

**DDNS :**  Disable  Enable

**Provider :**

**Host Name :**

**User Name / E-mail :**

**Password / Key :**

### Gateway Mode

- **Mode:** Determine the way to obtain the IP address, by DHCP or Static.
  - **Static setting:** Static setting is to set these parameters manually. Basic parameters such as IP address, subnet mask, and gateway are needed.

Home > System > Network Interface

### Network Settings

**Mode :**  Static  DHCP

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

**Layer2 STP :**  Disable  Enable

#### AP Mode

Home > System > Network Interface

### WAN Configuration

**Mode :**  Static  DHCP  PPPoE

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

**Available Bandwidth on WAN Interface :**

Uplink :  ▼

Downlink :  ▼

#### Gateway Mode

- **DHCP client:** This option is provided when the users have a DHCP in the wired network, and make sure the network connection is correct.

Home > System > Network Interface

## Network Settings

Mode :  Static  DHCP  
Layer2 STP :  Disable  Enable

## Dynamic DNS (DDNS)

DDNS :  Disable  Enable  
Provider :   
Host Name :   
User Name / E-mail :   
Password / Key :

### AP Mode

Home > System > Network Interface

## WAN Configuration

Mode :  Static  DHCP  PPPoE  
Available Bandwidth on WAN Interface :  
Uplink :   
Downlink :

### Gateway Mode

- **PPPOE**: When selecting PPPoE to connect to the network, please set the “**Username**”, “**Password**”, “**MTU**” and “**CLAMP MSS**”. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

Home > System > Network Interface

## WAN Configuration

**Mode :**  Static  DHCP  PPPoE

Username :  \*

Password :  \*

MTU :  bytes \*(1000~1492)

Clamp MSS :  bytes \*(980~1400)

Dial on Demand :  Disable  Enable

Maximum Idle Time :  minutes

**Available Bandwidth on WAN Interface :**

Uplink :  ▼

Downlink :  ▼

### Gateway Mode

- **Primary and Alternate DNS Server:** If any other hosts address of management service are given in FQDN format (Full qualified domain name), ensure at least one of these DNS (Domain Name Service) server's IP is correct.
- **Layer 2 STP:** It depends on the configuration of the OWL800 including wired and wireless settings. When it is configured to bridge several networks, STP needs to be enabled.
- **Dynamic DNS (DDNS):** OWL800 provides a convenient DNS function to translate a domain name to the IP address of WAN port that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server.



### 4.1.3 Management

For easier maintenance, SNMP (Simple Network Management Protocol) and remote Syslog services are provided in OWL800. The OWL800 will be managed remotely in a centralized manner.

Home > System > Management Services

#### Management Services

**VLAN for Management:**  Disable  Enable  
 VLAN ID :  \*( 1 - 4094 )

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

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

#### AP Mode

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 :  ▼

#### Gateway Mode

- **SNMP Configuration:** By enabling this SNMP service, the remote SNMP manager could obtain OWL800's system status.
  - **Community String:** Specify the password for *Read* and *Write*.
  - **Read:** This string is for the SNMP managers to get the MIB information from the system. The example here indicates that the SNMP managers can read the MIB information from the system when the SNMP managers use the community **Public**.
  - **Write:** This string is for the SNMP managers to set the MIB information to the system. The example here indicates that the SNMP managers can write the MIB information to the system when the SNMP managers use the community **Private**.
  - **Trap:** Enable or Disable the feature. When enabled, its reported event will be sent to assigned management station with specified *Server IP Address*.
- **Syslog Configuration:** By enabling this service, specify a remote Syslog server which could accept system log messages from OWL800 remotely. By reading the Syslog message in the remote server, review activities of all installed OWL800s in the network.
  - **Server Port:** Port of the server.
  - **Log Level:** Select desired level of received events.

## 4.1.4 VLAN Overview

VLAN is to separate one physical network into different logical zones. VLAN overview is a summary table tells you each VLAN's current status. There are up to 9 tab-based VLANS to enable. Each VLAN is associated to one policy; authentication methods, encryption methods, traffic control, DHCP and etc.

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

### VLAN Overview

VLAN No.	VLAN Tag	Interface IP	DHCP	Start IP	End IP	State	Edit
Vlan 0	0	<a href="#">192.168.1.1</a>	Enabled	<a href="#">192.168.1.101</a>	<a href="#">192.168.1.200</a>	Enabled	<a href="#">Edit</a>
Vlan 1	1	<a href="#">192.168.11.1</a>	Enabled	<a href="#">192.168.11.101</a>	<a href="#">192.168.11.200</a>	Enabled	<a href="#">Edit</a>
Vlan 2	2	<a href="#">192.168.12.1</a>	Enabled	<a href="#">192.168.12.101</a>	<a href="#">192.168.12.200</a>	Enabled	<a href="#">Edit</a>
Vlan 3	3	<a href="#">192.168.13.1</a>	Enabled	<a href="#">192.168.13.101</a>	<a href="#">192.168.13.200</a>	Enabled	<a href="#">Edit</a>
Vlan 4	4	<a href="#">192.168.14.1</a>	Enabled	<a href="#">192.168.14.101</a>	<a href="#">192.168.14.200</a>	Enabled	<a href="#">Edit</a>
Vlan 5	5	<a href="#">192.168.15.1</a>	Enabled	<a href="#">192.168.15.101</a>	<a href="#">192.168.15.200</a>	Disabled	<a href="#">Edit</a>
Vlan 6	6	<a href="#">192.168.16.1</a>	Enabled	<a href="#">192.168.16.101</a>	<a href="#">192.168.16.200</a>	Disabled	<a href="#">Edit</a>
Vlan 7	7	<a href="#">192.168.17.1</a>	Enabled	<a href="#">192.168.17.101</a>	<a href="#">192.168.17.200</a>	Disabled	<a href="#">Edit</a>
Vlan 8	8	<a href="#">192.168.18.1</a>	Enabled	<a href="#">192.168.18.101</a>	<a href="#">192.168.18.200</a>	Disabled	<a href="#">Edit</a>

### Gateway Mode

- **VLAN Tag:** The VLAN tag for the respective VLAN. The hyperlink connects to **VLAN's Configuration Zone**.
- **Interface IP:** The hyperlink connects to **VLAN's Configuration Zone**.
- **DHCP:** Enable or Disable DHCP state shown here. The hyperlink connects to **VLAN's Configuration Zone**.
- **Start IP:** Show the Start IP Address here. The hyperlink connects to **VLAN's Configuration Zone**.
- **End IP:** Show the End IP Address here. The hyperlink connects to **VLAN's Configuration Zone**.
- **State:** Enable or Disable VLAN state shown here. The hyperlink connects to **VLAN's Configuration Zone**.
- **Edit:** Click "Edit" hyperlink takes you to each **VLAN's Configuration Zone**.

Home > System > VLAN Config

## VLAN Configuration

VLAN Name :

VLAN :  Disable  Enable

Remark :

VLAN Tag : VLAN ID :  \*( 1 - 4094 )

Operation Mode :  NAT  Router

Network Interface : IP Address :   
Subnet Mask :

DHCP Server :  Enable DHCP  Disable DHCP  DHCP Relay

Start IP Address :  \*

End IP Address :  \*

Primary DNS Server :  \*

Alternate DNS Server :

**Gateway Mode >> VLAN Configuration**

## 4.1.5 VLAN Configuration

Home > System > VLAN Config

### VLAN Configuration

**VLAN Name :**

**VLAN :**  Disable  Enable

**Remark :**

**VLAN Tag :** VLAN ID :  \*( 1 - 4094 )

**Operation Mode :**  NAT  Router

**Network Interface :** IP Address :   
Subnet Mask :

**DHCP Server :**  Enable DHCP  Disable DHCP  DHCP Relay

Start IP Address :  \*

End IP Address :  \*

Primary DNS Server :  \*

Alternate DNS Server :

DNS Suffix :  \*

WINS Server :

Lease time :  ▾

**Default Authentication Method :**  ▾

**Allowed Authentication Method and Applied Policy :** Local :  ▾

External Radius Server 1 :  ▾

External Radius Server 2 :  ▾

External Radius Server 3 :  ▾

External Radius Server 4 :  ▾

On-Demand :  ▾

### Gateway Mode

- **VLAN:** This section is where to configure each VLAN. There are 9 VLANs (VLAN0~8).
- **Remark:** Text remark about this VLAN.
- **VLAN Tag:** each VLAN is identified by different tags carried within message frames. The number that is mapped to the selected VLAN.

▪ **Operating Mode:**

- **NAT:** NAT stands for Network Address Translation that hides internal IP addresses. Like a two-way mirror (transparent mirror), NAT is like a protective wall that packets inside can pass through this wall and being transferred to the outside, but the outside can only see the IP Address of “the wall”.
- **Router:** Router mode is used when LAN client IPs are meant to be visible to WAN side for example if clients hold real IPs.

▪ **Network Interface:** IP address and Subnet Mask of this VLAN.

▪ **DHCP Server:**

- **Enable DHCP:** Make OWL800 your DHCP server.

**DHCP Server :**  Enable DHCP  Disable DHCP  DHCP Relay

Start IP Address :  \*

End IP Address :  \*

Primary DNS Server :  \*

Alternate DNS Server :

DNS Suffix :  \*

WINS Server :

Lease time :  ▾

- **Domain Name:** Domain Name looks like “domain.com” that is a better memorable term to IP address. Client looks up a website by entering its domain name or its IP address.
- **WINS Server:** WINS is short for windows internet name. WINS server translates Windows computer names to IP addresses. To see the full computer name: right click “My Computer” icon and scroll down to “Properties”.
- **Lease Time:** A Lease Time is the time period that DHCP server permits DHCP client to use a particular IP address. Shorter lease time is set for clients with the higher mobility. For example, clients in a commercial fair, exhibition, or around a hotel hotspot, come to this service zone for a quick internet surf and leave.
- **Disable DHCP:** Disable OWL800’s DHCP function.

**DHCP Server :**  Enable DHCP  Disable DHCP  DHCP Relay

**Default Authentication Method :**  ▾

**Allowed Authentication Method and Applied Policy :**

Local :  ▾

External Radius Server 1 :  ▾

External Radius Server 2 :  ▾

External Radius Server 3 :  ▾

External Radius Server 4 :  ▾

On-Demand :  ▾

- Reserved IP Address list: **Reserved IP Address** is a static IP address reserved for a special client by his MAC address.

**DHCP Server :**  Enable DHCP  Disable DHCP  DHCP Relay

Start IP Address :  \*

End IP Address :  \*

Primary DNS Server :  \*

Alternate DNS Server :

DNS Suffix :  \*

WINS Server :

Lease time :  ▾

**Reserved IP Address List**

Home > Firewall > VLAN Config > Reserved IP Address List

### Reserved IP Address List : VLAN 0

<b>IP Address</b>	<b>MAC Address</b>	<b>Remark</b>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

**Reserved IP Address List**

IP Address	MAC Address	Remark	Delete	Edit
192.168.1.1	00:00:00:00:00:00	test1	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>

- Allowed Authentication Method and Applied Policy:**
  - Local:** Select a policy and apply to local authentication.
  - External RADIUS server:** Select a policy and apply to RADIUS authentication.

## 4.1.6 Walled Garden

The **Walled Garden** supported by the system provides free surfing areas for clients to access before they are authenticated by the system. IP addresses or domain names of the websites can be defined in this list. Clients without network access right can still have a chance to experience the actual network service free of charge. This function allows clients to access specified websites before login and authentication. An example may be seen in hotels, where guests without network access right are allowed to utilize the network service free of charge such as accessing the Hotel's homepage. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can make use of the actual network service free of charge.

[Home](#) > [System](#) > Walled Garden

### Walled Garden List

No.	Domain Name/IP Address	No.	Domain Name/IP Address
1	<input type="text" value="www.google.com"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

#### Gateway Mode

Walled Garden List is a list of websites for all users to access before login or without being authenticated. Enter the **IP Address** or **Domain Name** of those websites and click **Apply**. **These websites can be for example menu, portal page, commercial advertisement, and etc.**



## Walled Garden List

No.	Domain Name/IP Address	No.	Domain Name/IP Address
1	<input type="text" value="www.advertisement.co"/>	2	<input type="text" value="www.new_stuff_post.c"/>
3	<input type="text" value="10.2.3.100"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>

### 4.1.7 Mode

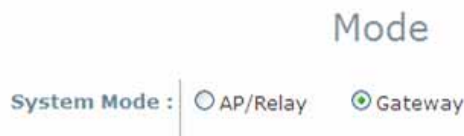
OWL800 supports 4 Radio modules; RF1 and RF2 are included in the original package. RF3 and RF4 are optional. From the software perspective, there are modes of two layers; "System Mode" and "Radio module Mode".

Home > System > Operation Mode



#### AP Mode

Home > System > Operation Mode



#### Gateway Mode

- **System Mode:**
  - **AP/Relay Mode:** Switching between AP mode and Relay mode is only for RF1.
    - **AP Mode:** RF1 acts like a regular Access Point' Radio module for other wireless clients to associate.
    - **Relay Mode:** Relay Mode is to create WDS link with other wireless devices.
  - **Gateway Mode:** Selecting Gateway Mode enhances OWL800 a new feature – user authentication gateway. Please see "Users" for configuration instruction.
- **Radio module Mode:**
  - **AP mode:** RF1 acts like a regular Access Point' Radio module for other wireless clients to associate.
  - **WDS mode:** WDS mode is for Radio modules to create WDS link with other wireless devices.
  - **Scan mode:** Scan mode is for system to search for available wireless devices.

▪ **Table for Radio modules and Modes supported:**

System Mode Radio module Mode	AP / Relay Mode		Gateway Mode
RF1	If select "AP"	AP mode (Default)	AP mode or WDS mode
	If select "WDS"	Relay mode	
RF2	WDS mode / Scan mode		WDS mode / Scan mode

## 4.2 AP

This section provides information on the following functions: **VPA Overview, General Settings, VAP Configuration, Security Settings, Advanced Wireless Settings** and **Access Control Settings**. The OWL800 supports up to 8 WLANs by Virtual Access Point (VAP). Each VAP can have its own settings including ESSID, VLAN ID, security settings, and etc. Therefore, these VAPs can bring different service level to clients depending on the ESSID connected to. Please click on the menu item AP to configure VAPs.

### 4.2.1 Overview

The overall status is collected in this page, including enable/disable state, security type, MAC state, and advanced settings. OWL800 has 8 VAPs; each has its own settings. In the table, please click on each setting item to have detailed configuration of these VAPs respectively.

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

#### VAP Overview

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

#### Gateway & AP Mode

- **State:** The hyperlink showing *enable* or *disable* connects to the screen of **VAP Configuration**.

[Home](#) > [AP](#) > VAP Config

## VAP Configuration

Profile Name : VAP-1 ▼

VAP :  Disable  Enable

Profile Name : VAP-1

ESSID : OWL800-1

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

### Gateway & AP Mode

- **Security Type:** The hyperlink showing security type connects to the screen of **Security Settings**.

[Home](#) > [AP](#) > Security

## Security Settings

Profile Name : VAP-1 ▼

Security Type : None ▼

### Gateway & AP Mode

- **MAC ACL:** The hyperlink showing status of MAC ACL connects to the screen of **Access Control Settings**.

[Home](#) > [AP](#) > Access Control

## Access Control Settings

Profile Name : VAP-1 ▼

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

Access Control Type : Disable Access Control ▼

### Gateway & AP Mode

- **Advanced Settings:** The hyperlink of advanced settings connects to the screen of **Advanced Wireless Settings**.

Home > AP > Advanced

## Advanced Wireless Settings

Profile Name :

Beacon Interval :  \*(100 - 500ms )

RTS Threshold :  \*(1 - 2346)

Fragment Threshold :  \*(256 - 2346)

Broadcast SSID :  Disable  Enable

Wireless Station Isolation :  Disable  Enable

WMM :  Disable  Enable

IAPP :  Disable  Enable

### Gateway & AP Mode

## 4.2.2 General

Home > AP > General

### General Settings

Band :	802.11b+802.11g ▼
Super Mode :	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Short Preamble :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Antenna Diversity :	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Channel :	6 ▼
Max Transmit Rate :	Auto ▼
Transmit Power :	Highest ▼

#### Gateway & AP Mode

- **Band:** The operating wireless frequency band of the device's AP module. Choose among frequency band **Disable**, **802.11b**, **802.11g** or mixed mode **802.11b+802.11g**. (Note: 802.11 a band is only allowed for the second radio, which serves as WDS for bridge/backhaul.)
- **Short Preamble:** Enable for using Short Preamble and disable for using the Long Preamble option.
- **Channel:** Choose from channel **1 ~ 11** in b/g mode, depending on the region or auto.
- **Max Transmit Rate:** Choose transmit rate from the drop-down list. The maximum transmit rate can be set as "auto" or specific available rate.
- **Transmit Power:** Choose from **Lowest** Power to **Highest** Power level or auto. (Note: The factory default setting is Highest ( ~ <19 dBm). Each level steps down around 3 dBm. That is, even the transmit power is adjustable; it can only be adjusted down from the radio card's limit. There is no power buster inside the product.)

**Note:** Depending on the region (US, EU, or JP) the product is built for shipping to, the number of selectable channels varies. For example, there are only 11 channels selectable in 2.4G band for the products made to ship to the US market, and there are 13 channels selectable in 2.4G for the product made to ship to the EU market. There are different firmware versions with different selectable channel-lists for different regions.

## 4.2.3 VAP Configuration

Home > AP > VAP Config

### VAP Configuration

Profile Name :

VAP :  Disable  Enable

Profile Name :

ESSID :

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

#### Gateway & AP Mode

To enable each VAP in the OWL800, the administrator has to configure each VAP individual manually. The settings of each VAP are collected as its profile.

- **VAP:** Enable or disabled virtual AP settings.
- **Profile Name:** Give the profile an identity for management purpose.
- **ESSID:** Extended Service Setting ID, indicate the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which assigned to the specified VAP.
- **VLAN ID:** Virtual LAN, the OWL800 supports tagged VLAN. To enable VLAN function, each VAP needs a unique VLAN ID; valid values are from 1 to 4094.

## 4.2.4 Security

The OWL800 supports various user authentication and data encryption in each VAP's profile. Thus the administrators can depend on the need to provide different service levels to clients. The security type includes the items on the drop-down menu of *security type*:

- **None:** No authentication required. This is the default setting as shown in the figure.

Home > AP > Security

Security Settings

Profile Name : VAP-1

Security Type : None

**Gateway & AP Mode**

- **WEP:** Supports key length of 64/128/152 bits.
  - **WEP Key Format:** Different format will affect the number of inputs to WEP keys.

Home > AP > Security

Security Settings

Profile Name : VAP-1

Security Type : WEP

Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.

**802.11 Authentication:**  Open System  Shared Key  Auto

**WEP Key Length :**  64 bits  128 bits  152 bits

**WEP Key Format :**  ASCII  Hex

**WEP Key Index :** 1

**WEP Keys :**

1

2

3

4

**Gateway & AP Mode**



- **802.1x:** Provides RADIUS authentication and enhanced WEP.

### 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)

### Gateway Mode

Home > AP > 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 :

Accounting Service :  Disable  Enable

Accounting Port : 1813

Accounting Interim Update Interval : 60 second(s)

**Secondary RADIUS Server :** Host:  ( Domain Name / IP Address )

Authentication Port:

Secret Key:

Accounting Service:  Disable  Enable

Accounting Port:

Accounting Interim Update Interval: 60 second(s)

### AP Mode

- **WPA-PSK:** Provides shared key authentication in WPA data encryption.

Home > AP > 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)

### Gateway & AP Mode

- **WPA-RADIUS:** Authenticate user by RADIUS in WPA data encryption.

Home > AP > Security

## Security Settings

Profile Name : VAP-1

Security Type : WPA-RADIUS

Cipher Suite : TKIP (WPA)

Group Key Update Period: 600 second(s)

### Gateway Mode

Home > AP > 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 :

Accounting Service :  Disable  Enable

Accounting Port : 1813

Accounting Interim Update Interval : 60 second(s)

Secondary RADIUS Server :

Host:  ( Domain Name / IP Address )

Authentication Port:

Secret Key:

Accounting Service:  Disable  Enable

Accounting Port:

Accounting Interim Update Interval: 60 second(s)

### AP Mode

## 4.2.5 Advanced

Virtual AP advanced settings should mostly meet general requirements. Take the following parameters for the purpose if occasionally it is necessary to tune or debug the wireless network.

[Home](#) > [AP](#) > [Advanced](#)

### Advanced Wireless Settings

Profile Name :

Beacon Interval :  \*(100 - 500ms )

RTS Threshold :  \*(1 - 2346)

Fragment Threshold :  \*(256 - 2346)

Broadcast SSID :  Disable  Enable

Wireless Station Isolation :  Disable  Enable

WMM :  Disable  Enable

IAPP :  Disable  Enable

#### Gateway & AP Mode

- **Beacon Interval:** This interval specifies the time interval, in milliseconds. Between each beacon frame is transmitted.
- **RTS Threshold:** To control station access to medium and to alleviate this effect of the hidden terminal problem, we can tune this RTS threshold value. It should have a value among 1-2346 and is default to 2346.
- **Fragmentation Threshold:** A unicast frame larger than this threshold will be fragmented before the transmission. If significant numbers of collisions are occurring, we can try to take a smaller value of the fragmentation threshold to see if it helps.
- **Broadcast SSID:** Disable this item will prevent the OWL800 from broadcasting its SSID publicly.
- **Wireless Station Isolation:** By enabling this item, all stations in the same OWL800's coverage area can only communicate with the OWL800 only.
- **WMM:** To decide which data streams are most important and assign them a higher traffic priority, we may enable this feature. It is default disabled.
- **IAPP:** To provide a better roaming capability for the stations among APs nearby the OWL800, we can enable this item. Its default disabled.

## 4.2.6 Access Control

The OWL800 supports various methods of authenticate clients from using wireless LAN. The default policy is unlimited connections without any authentication required. To restrict the station number of wireless connections, just change the **Maximum number of stations** to a desired number. For example, while the number of station is set to 20, only 20 stations are allowed to connect to this VAP.

For MAC ACL control, the supported methods include:

- **Disable Access Control:** No MAC address check required
- **MAC ACL Allow List:** Deny all except allowed ones in the list
- **MAC ACL Deny List:** Allow all except denied ones in the list

The one selected in the **Access Control Type** is the activated policy while the rest of the options are inactive.

- **Disable Access Control**

No MAC address check required.

[Home](#) > [AP](#) > [Access Control](#)

### Access Control Settings

Profile Name :

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

Access Control Type :

#### Gateway & AP Mode

▪ **MAC ACL Allow List**

When the policy is set to **Allow List**, all wireless connection to the VAP will be denied except for those allowed MAC addresses listed. For each allowed MAC address, the administrator can still enable or disabled the rule applied to the specified one. For example, 11:22:33:44:55:66 is in the allow list, to temporarily deny its access, we can **disable** the rule on it.

Home > AP > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( 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

**Gateway & AP Mode**

▪ **MAC ACL Deny List**

When the policy is set to **Deny List**, all wireless connection to the VAP will be allowed except those denied MAC addresses listed. When the users want to allow one listed MAC address temporary, **disable** the address from the deny lists.

Home > AP > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( 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

**Gateway & AP Mode**

## 4.3 WDS

OWL800 has equipped with Wireless Distribution System interfaces, and each interface can establish up to 4 WDS links to other WDS peers. In WDS configuration, each WDS-link setting is collected into one profile. This section provides information in the following functions: **WDS Link Overview**, **WDS Interface Settings**, **WDS Link Settings**, and **WDS Discovery**. The configurations under this category apply to all Virtual Access Point in this device.

### 4.3.1 Overview

WDS links are used as backhaul or bridges. The figure provides an overall status of all WDS links. Turn the WDS link by giving signal quality in the table.

[Home](#) > [WDS](#) > [WDS Link Overview](#)

#### WDS Link Overview

RF Card B

Link No.	State	MAC Address	Security	Delete	Edit
1	Disabled		None	<input type="checkbox"/>	<a href="#">Edit</a>
2	Disabled		None	<input type="checkbox"/>	<a href="#">Edit</a>
3	Disabled		None	<input type="checkbox"/>	<a href="#">Edit</a>
4	Disabled		None	<input type="checkbox"/>	<a href="#">Edit</a>

#### Gateway & AP Mode

- **Link No.:** corresponding profiles of each WDS interface
- **State:** Enabled or Disabled the plan.
- **MAC Address:** remote peer's MAC address.
- **Security:** Choose between *Disable* security and *WEP* type of security.
- **Delete:** Remove profiles by checkbox selection and click on **Delete** to remove them.
- **Edit:** To change the individual setting of each WDS profile, click on **Edit** to modify the settings. The hyperlink connects to the screen of **WDS Configuration**.

## 4.3.2 General

Home > WDS > RF Settings

### WDS Interface Settings

RF Card Name : RF Card B ▼

Band : 802.11b+802.11g ▼

Channel : 9 ▼

Max Transmit Rate : Auto ▼

Transmit Power : Highest ▼

Shared Secret Key : 123456 (Optional: for WDS discovery)

Antenna Diversity :  Disable  Enable

Distance : 0 meter(s)  Advance

#### Gateway & AP Mode

The shared secret is used to discover remote WDS peer. Both ends must share the same key; otherwise the remote peer will ignore the request. To use WDS discovery, both ends must be equipped with this feature containing shared secret. For example, the remote one is also an OWL800.

Each WDS interface has its own RF (Radio Frequency) settings; normally, valid combination of RF parameters configuration would be like the following table. However, the available values of each item will be affected by the RF regulation which is configured in AP's RF settings.

- **Band:** Select appropriate wireless band or disable if the service is not required; bands available for WDS links are 802.11a, 802.11b, 802.11g and 802.11b+802.11g.

**Note:** The second radio in the system is designed for building WDS links. WDS links are used as backhaul or point-to-point bridges. WDS links do not service AP clients. 11a (5.725~5.85GHz) is used by the 2<sup>nd</sup> radio module typically in order to avoid the channels of 11b/g (2.4GHz) used by the first radio module for serving clients. However, 11b and 11g are still available to the 2<sup>nd</sup> radio (WDS) in case the administrator determines to use 11b/g for building WDS links based on their deployment condition.

- **Channel:** Select an appropriate channel from the list to correspond with the network settings.

**Note:** Depending on the region (US, EU, or JP) the product is built for shipping to, the number of selectable channels varies. For example, there are only 11 channels selectable in 2.4G band for the products made to ship to the US market, and there are 13 channels selectable in 2.4G for the product made to ship to the EU market. There are different firmware versions with different selectable channel-lists for different regions.



### 4.3.3 WDS Configuration

For each WDS link profile, the administrators need to remote peer's MAC address and the authentication method for establishing connection to the peer.

Home > WDS > WDS Configuration

### WDS Link Settings

WDS Profile : RF Card B : WDS Link 1 ▾

WDS :  Disable  Enable

MAC Address of Remote AP :  \*

Path Cost of STP :

Security Type :  ▾

#### Gateway & AP Mode

- **WDS Profile:** Total 8 profiles included in the OWL800 device, pull the drop-down menu to select one WDS profile to configure.
- **WDS:** Enable or Disable the specified WDS link.
- **MAC Address of Remote AP:** For each link, type the MAC address of the remote peer here. The MAC address may also get by WDS Discovery. Please refer to *WDS discovery* in the following section for detail.
- **Path Cost of STP:** An assigned weighted metric here will determine the best path for data flow.
- **Security Type:** Set the encryption (WEP or None) of WDS link here.
  - **None:** No authentication is required to establish this WDS link.
  - **WEP:** Establish the WDS link in WEP authentication which must provides key length, format and the key itself respectively, recommended.

Home > WDS > WDS Configuration

### WDS Link Settings

WDS Profile : RF Card B : WDS Link 1 ▾

WDS :  Disable  Enable

MAC Address of Remote AP :  \*

Path Cost of STP :

Security Type :  ▾

WEP Key Length :  ▾

WEP Key Format :  ▾

WEP Key :

#### Gateway & AP Mode

o TKIP:

Home > WDS > WDS Configuration

## WDS Link Settings

WDS Profile : RF Card B : WDS Link 1

WDS :  Disable  Enable

MAC Address of Remote AP :

Path Cost of STP :

Security Type :

Cipher Suite :

Pre-shared Key Type :

Pre-shared Key :

### Gateway & AP Mode

### 4.3.4 WDS Discovery

Home > WDS > WDS Discovery

#### WDS Discovery

Wireless Interface :  RF Card B

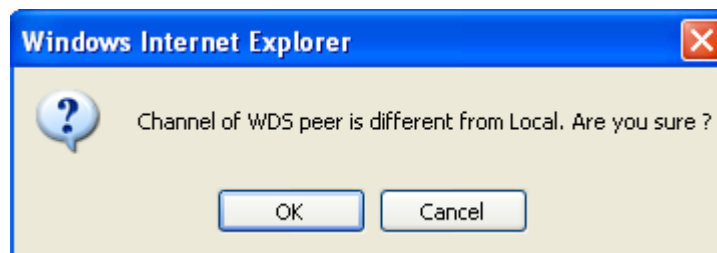
Discover Now !

Item	Status	Mac Address	Channel	SNR (dB)	
0	Ready	00:0B:6B:DB:A9:FC	9	18	Connect

#### Gateway & AP Mode

OWL800 provides easy-to-use peer discovery feature, the WDS discovery, which both ends must have the same 'shared secret'. Please refer to WDS *RF settings* for the shared secret. *The remote peer must also have the same 'Scan' feature equipped.* To start WDS discovery, select WDS interface and then click on the **Discover Now** button.

If the local WDS is in remote peer's coverage area, the information of remote peer will be listed. Click on the **Connect** button, the MAC address of remote peer will be retrieved locally for WDS connection.



## 4.4 User

When set to Gateway Mode, OWL800 is capable of dealing with user authentication, authorization and accounting. The user account information is stored in the local database or a specified external RADIUS server. This section provides information on the following functions: **Local User Authentication, RADIUS Authentication, On-demand Authentication, Policy Configuration, Policy Firewall, Policy Specific Route, and Roaming Out and 802.1X Client Device Settings.**

### 4.4.1 Local

Local user database is built locally in OWL800. To add new user accounts, enter specific information (User Name, Password, MAC Address, and Remark) and click **Add**. All created accounts are displayed in the **User List**.

Home > User > Authentication : Local User Setting

#### Authentication : Local User Setting

Postfix :  \*

Multiple Login :  Disable  Enable

802.1X Authentication :  Disable  Enable

Account Roaming Out :  Disable  Enable

Roaming Out & 802.1X Client Device Settings

Import/Export Local User :

User Name  Password  MAC Address  Remark

#### User List

User Name	Password	MAC Address	Remark	Delete all	Edit
admin01	admin01	00:00:00:00:00:01	tester 1	Delete	Edit
admin02	admin02	11:11:11:11:11:11	tester 2	Delete	Edit

First Prev current page : 1/1 Next Last

#### Gateway Mode

- Postfix:** It is a string used by the system to distinguish which database/server will be used for authentication when a user enters the user name to log in. For example, when the Postfix is configured as "local", user1@local will tell the system to use Local user database. A meaningful string will help administrators manage the authentication. It is only allowed to use numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters.

- **Multiple Login:** When enabled, the same Local user account can be used for login by multiple users at the same time.
- **802.1X Authentication:** When enabled, Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch. For more information, please see **Appendix B. 802.1X Support**.
- **Account Roaming Out:** When enabled, Local user database functions as an external RADIUS server for another gateway. Therefore, a user can roam out to the network under another gateway by using the same Local account. For more information, please see **Appendix B. 802.1X Support**. The button **Roaming Out & 802.1X Client Device Settings** connects to the screen of **802.1X**.

Home > User > Roaming Out and 802.1X Client Device Setting

## Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	
Roaming Out ▾	192.168.5.10	255.255.255.255 (/32) ▾	12345	<input type="button" value="Add"/>

### Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	Delete	Edit
------	------------	-------------	------------	--------	------

### Gateway Mode >> Add Roaming Out and 802.1X list

- **Import/Export Local User:** The button **Import/Export Local User** connects to the screen of **Import & Export User**.
- **User List:** When click **Edit**, change the content of **User Name**, **Password**, **Mac Address** and **Remark** above the List.

User Name	Password	MAC Address	Remark	
admin02	admin02	11:11:11:11:11:11	tester 2	<input type="button" value="Add"/>
				<input type="button" value="Search"/>

### User List

User Name	Password	MAC Address	Remark	Delete all	Edit
-----------	----------	-------------	--------	------------	------

First Prev current page : 1/1 Next Last

### Gateway Mode >> Add User List

User Name Password MAC Address Remark

User List

User Name	Password	MAC Address	Remark	Delete all	Edit
admin02	admin02	11:11:11:11:11:11	tester 2	Delete	Edit

First Prev current page : 1/1 Next Last

Gateway Mode >> Search User List

User Name Password MAC Address Remark

User List

User Name	Password	MAC Address	Remark	Delete all	Edit
8	1			Delete	Edit

Gateway Mode >> Edit User List

### 4.4.2 RADIUS

The system supports user authentication against external RADIUS servers. It functions as a RADIUS authenticator for external RADIUS servers.

To enable the RADIUS authentication, enter the related information for the primary RADIUS server and/or the secondary RADIUS server (not required). These settings will be effective immediately after clicking the **Apply** button.

[Home](#) > [User](#) > Authentication : RADIUS Setting

## Authentication : RADIUS Setting

External RADIUS Server : RADIUS 1 ▼

<p>Postfix :</p> <p>Extensible Authentication Protocol :</p> <p>Username Format to RADIUS Server :</p>	<div style="border: 1px solid #ccc; padding: 5px;"> <input style="width: 100%;" type="text" value="radius1"/> *         </div> <p> <input checked="" type="radio"/> Disable   <input type="radio"/> Enable         </p> <p> <input type="radio"/> ID Only   <input checked="" type="radio"/> Complete         </p> <div style="border: 1px solid #ccc; padding: 2px; text-align: center; font-weight: bold; margin: 5px 0;">802.1X Client Device Settings</div> <p>Primary RADIUS Server :</p> <p>Host: <input style="width: 150px;" type="text" value="192.168.130.1"/> *( Domain Name / IP Address )</p> <p>Authentication Port: <input style="width: 80px;" type="text" value="1812"/></p> <p>Secret Key: <input style="width: 150px;" type="text" value="12345678"/></p> <p>Accounting Service:   <input type="radio"/> Disable   <input checked="" type="radio"/> Enable</p> <p>Accounting Port: <input style="width: 80px;" type="text" value="1813"/></p> <p>Authentication Protocol: <span style="border: 1px solid #ccc; padding: 2px;">PAP</span> ▼</p> <p>Secondary RADIUS Server :</p> <p>Host: <input style="width: 150px;" type="text"/> ( Domain Name / IP Address )</p> <p>Authentication Port: <input style="width: 80px;" type="text"/></p> <p>Secret Key: <input style="width: 150px;" type="text"/></p> <p>Accounting Service:   <input checked="" type="radio"/> Disable   <input type="radio"/> Enable</p> <p>Accounting Port: <input style="width: 80px;" type="text"/></p> <p>Authentication Protocol: <span style="border: 1px solid #ccc; padding: 2px;">PAP</span> ▼</p>
--	---

**Gateway Mode**

- **Postfix:** It is a string used by the system to distinguish which database/server will be used for authentication when a user enters the user name to log in. For example, when the Postfix is configured as “radius1”, user1@radius1 will tell the system to use this RADIUS server. A meaningful string will help administrators manage the authentication. It is only allowed to use numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters.
- **Extensible Authentication Protocol:** When enabled, the system can accept 802.1X authentication request (EAP request) from 802.1X capable devices and relay the request to external RADIUS server. For more information, please see **Appendix B. 802.1X Support**.
- **802.1X Client Device Settings:** When **Extensible Authentication Protocol** is enabled, by clicking on this button, administrators can go to **Roaming Out and 802.1X Client Device Settings** page to further set up the 802.1X capable devices that are allowed to authenticate against the Local user database.

[Home](#) > [User](#) > [Roaming Out and 802.1X Client Device Setting](#)

## Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	
Disable <input type="button" value="v"/>	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>	<input type="button" value="Add"/>

- **Username Format to RADIUS Server:** When **ID Only** is selected, only the username will be sent to the external RADIUS server for authentication. On the other hand, when **Complete** option is selected, both the username and the postfix will be sent to the RADIUS server.
- **Primary RADIUS Server & Secondary RADIUS Server:**
  - Host:** Domain name or IP address of the external RADIUS server.
  - Authentication Port:** Port number of the external RADIUS server for authentication.
  - Security Key:** The Secret Key for RADIUS authentication.
  - Accounting Service:** RADIUS accounting can be enabled or disabled.
  - Accounting Port:** Port number of the external RADIUS server for accounting.
  - Authentication Protocol:** The authentication protocol configurations of the system must match with the configurations of the remote RADIUS server. **PAP** (Password Authentication Protocol) transmits password in plain text without encryption. **CHAP** (Challenge Handshake Authentication Protocol) is a more secured authentication protocol with hash encryption.



### 4.4.3 On-demand

There are some deployment scenarios (for example, at venues such as coffee shops, hotels, restaurants, etc.) where retail customers or casual visitors want to get wireless Internet access. To offer the Wi-Fi access (either for commercial use or for free), user accounts should be able to be created upon request and account tickets/receipts should also be provided. Therefore, **On-demand** is designed as the authentication option for this type of deployment scenarios.

Home > User > Ondemand : General Setting

#### Authentication : On-demand Setting

Postfix :	<input type="text" value="ondemand"/>
Ticket Customization :	<input type="button" value="Configure"/>
Currency :	<input type="radio"/> None <input checked="" type="radio"/> \$ USD <input type="radio"/> £ UK <input type="radio"/> € EURO <input type="radio"/> <input type="text" value=""/> (input other desired currency name e.g. AU)
Number of Tickets:	<input checked="" type="radio"/> 1 <input type="radio"/> 2
Terminal Servers :	<input type="button" value="Configure"/>
Billing Plans:	<input type="button" value="Configure"/>
On-demand Account Creation:	<input type="button" value="Create"/>
On-demand Account List:	<input type="button" value="View"/>

#### Gateway Mode

- **Postfix:** It is a string used by the system to distinguish which database/server will be used for authentication when a user enters the user name to log in. For example, when the Postfix is configured as “ondemand”, xrf6@ondemand will tell the system to use this authentication database. A meaningful string will help administrators manage the authentication. It is only allowed to use numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters.
- **Ticket Customization:** On-demand account ticket can be customized here.

Home > User > Ondemand : General Setting > Ondemand : Ticket Customization

#### On-demand : Ticket Customization

Receipt Header 1 :	<input type="text" value="Welcome1"/>
Receipt Header 2 :	<input type="text" value="welcome2"/>
Receipt Header 3 :	<input type="text" value="welcome3"/>
SSID :	<input type="text" value="OWL800-1"/>
Wireless Key :	<input type="text" value="key 121"/>
Remark :	<input type="text" value="ticket remark"/>
Receipt Footer 1 :	<input type="text" value="footer1"/>
Receipt Footer 2 :	<input type="text" value="footer2"/>
Receipt Footer 3 :	<input type="text" value="footer3"/>

#### Gateway Mode

- **Receipt Header:** There are two receipt headers supported by the system. The entered content will be printed on the receipt. These headers are optional.
  - **SSID:** The administrator can enter the defined wireless SSID in this field and it will be printed on the receipt for guest users' reference when accessing the Internet via wireless LAN service. The SSIDs given here should be those of the service zones enabled for guest users.
  - **Wireless Key:** The administrator can enter the defined wireless key such as WEP or WPA in the field. The Wireless Key will be printed on the receipt for the guest users' reference when accessing the Internet via wireless LAN service.
  - **Remark:** The administrator can enter extra information in this field for remark.
  - **Receipt Footer:** The entered content will be printed on the receipt. This footer is optional.
- **Currency:** The desired monetary unit or a unit specified by administrators for billing purpose.
  - **Number of Tickets:** Print one or duplicate receipts, when pressing the print button of the ticket printer which connected to serial port.
  - **Terminal Servers:**

On-demand Terminal Server Configuration

No.	Server IP Address	Port	Location	Remark
1	192.168.1.1	1800	floor1	rem
2				
3				
4				
5				
6				
7				
8				
9				
10				

**Gateway Mode**

- **Billing Plans:** Administrators can configure several billing plans.

On-demand : Billing Plan Configuration

Plan No.	Type	Quota	Price	Enable	Function
1	TIME	2hr(s):2min(s)	2	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>
2	TIME	3hr(s):32min(s)	3	<input type="checkbox"/>	<input type="button" value="Edit"/>
3	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
4	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
5	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
6	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
7	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
8	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
9	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
0	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>

Ondemand : Billing Plans

Plan No.: 1

Type: TIME

Quota: 2 hr(s) 2 min(s)  
\*( Range of min(s) : 0 ~ 59; they cannot both be zero )

Account Activation:  From the Ticket issue time  
 First time login must be done within 2 day(s) 2 hour(s)  
\*( Range of hour(s) : 0 ~ 23; they cannot both be zero )

Validity Period:  Account will be expired, even there is remaining quota, in 2 day(s) from its activation  
\*(should be > 1)

Price: 2  
\*( Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99 )

**Gateway Mode**

- **On-demand Account Creation:** When at least one plan is enabled, the administrator can generate On-demand user accounts here.

On-demand Account Creation

Plan No.	Type	Quota	Price	State	Function
1	TIME	2 Hr(s):2 Min(s)	2	Enabled	Create
2	TIME	3 Hr(s):32 Min(s)	3	Disabled	Create
3	N/A			Disabled	Create
4	N/A			Disabled	Create
5	N/A			Disabled	Create
6	N/A			Disabled	Create
7	N/A			Disabled	Create
8	N/A			Disabled	Create
9	N/A			Disabled	Create
0	N/A			Disabled	Create

Ondemand : Create an Account

Plan :Type : 1 :TIME  
 Quota : 2 Hr(s):2 Min(s)  
 Account Activation : Account will be activated from the First login.  
 Validity Period : Account will be expired in 2 days.  
 Unit Price : 2 US  
 Total Units :   
 Remark :

**Gateway Mode**

- **On-demand Account List:** All created On-demand accounts are listed and related information on is also provided.

On-demand Account List

Username	Password	Remaining Quota	State	Remark	
xrf6	998b2xt8	2Hr(s)2Min(s)	Alive		Delete

First Prev current page : 1 Next Last

**Gateway Mode**

- **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.
- **Username:** The login name of the instant account.
- **Password:** The login password of the instant account.
- **Remaining Quota:** The total time that the user can use currently.
- **Status:** The status of the account.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

### 4.4.4 Policy

The system supports multiple control Policies, including the **Global Policy** and individual **Policy** (1 ~ 16). Each Policy consists of access control profiles that can be configured respectively and applied to users.

- **Global Policy:**

Global is the system's universal policy including **Firewall Rules**, **Specific Routes Profile** which will be applied to all users unless the user has been regulated and applied to another policy.

[Home](#) > [User](#) > [Policy](#)

#### Policy Configuration

Policy Configuration	
Policy : Global ▼	
Firewall Profile	<input type="button" value="Setting"/>
Specific Route Profile	<input type="button" value="Setting"/>
User Session Control	Idle Timeout(minutes): <input type="text" value="10"/> *(1-1440)

**Gateway Mode >> Global Policy**

**Firewall Profile:** Global policy and each policy have a firewall service list and a set of firewall profile which is composed of firewall rules.

#### Policy : Firewall

Policy : Global ▼

Source IP / Subnet Mask	Destination IP / Subnet Mask	Protocol	Action	
<input type="text" value="255.255.255.255 (/32)"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text" value="ALL"/>	<input type="text" value="Pass"/>	<input type="button" value="Add"/>

#### Firewall

No.	Source IP / Subnet Mask	Destination IP / Subnet Mask	Protocol	Action	Delete	Edit
-----	-------------------------	------------------------------	----------	--------	--------	------

**Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.

### Policy : Specific Route

Policy :

Destination	Subnet Mask	Gateway	
<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="button" value="Add"/>

Specific Route				
Destination	Subnet Mask	Gateway	Delete	Edit

Policy 1 ~ Policy 16:

[Home](#) > [User](#) > [Policy](#)

### Policy Configuration

Policy Configuration	
Policy : <input type="text" value="Policy 1"/>	
Firewall Profile	<input type="button" value="Setting"/>
Specific Route Profile	<input type="button" value="Setting"/>
Total Uplink Bandwidth	<input type="text" value="Unlimited"/>
Total Downlink Bandwidth	<input type="text" value="Unlimited"/>
Maximum Concurrent Sessions	<input type="text" value="500"/> sessions per user

**Gateway Mode >> Individual Policy**

**Firewall Profile:** Each Policy has a firewall service list and a set of firewall profile consisting of firewall rules.

**Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.

**Schedule Profile:** The Schedule table in a 7x24 format is used to control the clients' login time. When Schedule is enabled, clients applied policies are only allowed to login the system at the time which is checked in the applied policy.

**Total Uplink Bandwidth:** Defines the maximum uplink bandwidth allowed to be shared by all clients.

**Total Downlink Bandwidth:** Defines the maximum downlink bandwidth allowed to be shared by all clients.

**Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

### 4.4.5 Firewall

Firewall rules in the Global Policy or individual Policy (1 ~ 16) can be defined to filter the traffic that travels through the system. When a packet matches the specified Source, Destination, and Protocol, the corresponding Action (Pass or Block) will be taken.

Home > User > Policy : Firewall

#### Policy : Firewall

Policy : Global

Source IP / Subnet Mask	Destination IP / Subnet Mask	Protocol	Action	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
255.255.255.255 (/32)	255.255.255.255 (/32)	ALL	Pass	

#### Firewall

No.	Source IP / Subnet Mask	Destination IP / Subnet Mask	Protocol	Action	Delete	Edit
1	192.168.10.10/255.255.255.255	192.168.9.20/255.255.255.255	all	pass	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>

#### Gateway Mode >> Global Firewall

Home > User > Policy : Firewall

#### Policy : Firewall

Policy : Policy 1

Source IP / Subnet Mask	Destination IP / Subnet Mask	Protocol	Action	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
255.255.255.255 (/32)	255.255.255.255 (/32)	ALL	Pass	

#### Firewall

No.	Source IP / Subnet Mask	Destination IP / Subnet Mask	Protocol	Action	Delete	Edit
1	192.168.10.1/255.255.255.255	192.168.9.1/255.255.255.255	all	pass	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>

#### Gateway Mode >> Policy Firewall

To add a rule to the **Firewall** list, specify the values of following fields and click the **Add** button. A rule in the list can be deleted (**Delete** button) from the list or edited (**Edit** button).

- **Source IP / Subnet Mask:** The combination of these two fields specifies either the IP address of a source host or the source network segment. For example, 192.168.1.101 with 255.255.255.255 (/32) stands for a single host - 192.168.1.101, while 192.168.1.0 with 255.255.255.0 (/24) indicates this is a Class C subnet - 192.168.1.xxx.
- **Destination IP / Subnet Mask:** The combination of these two fields specifies either the IP address of a destination host or the destination network segment. For example, 192.168.2.101 with 255.255.255.255 (/32) stands for a single host - 192.168.2.101, while 192.168.2.0 with 255.255.255.0 (/24) indicates this is a Class C



subnet - 192.168.2.xxx.

- **Protocol:** The specific service protocol for the filtering rule - ALL, TCP/UDP, TCP, UDP, ICMP, and IP.
- **Action:** **Pass** is to allow the packet to pass; **Block** is to block the packet from passing.

## 4.4.6 Route

Static routing rules in the Global Policy or individual Policy (1 ~ 24) can be defined to specifically route the traffic that travels through the system. When no rule is defined, all traffic will go through the system's default gateway (WAN interface).

[Home](#) > [User](#) > Policy : Specific Route

### Policy : Specific Route

Policy :

Destination

Subnet Mask

Gateway

Add

#### Specific Route

Destination	Subnet Mask	Gateway	Delete	Edit
-------------	-------------	---------	--------	------

#### Gateway Mode

To add a rule to the **Specific Route** list, specify the values of following fields and click the **Add** button. A rule in the list can be deleted (**Delete** button) from the list or edited (**Edit** button).

- **Destination / Subnet Mask:** The combination of these two fields specifies the IP address of a destination host or the destination network segment.
- **Gateway:** The IP address of the gateway for the destination host or network segment.

### 4.4.7 802.1X

OWL800 supports 802.1X authentication. In the Supplicant <-> Authenticator <-> Authentication Server architecture, The system will only allow 802.1X-enabled devices (Authenticator) to send 802.1X authentication request to internal or external RADIUS server. For more information, please see **Appendix B. 802.1X Support**.

Home > User > Roaming Out and 802.1X Client Device Setting

#### Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	
Disable ▾	<input type="text"/>	255.255.255.255 (/32) ▾	<input type="text"/>	<input type="button" value="Add"/>

Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	Delete	Edit
Roaming Out	192.168.5.10	255.255.255.255	12345	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>
802.1X	192.168.5.12	255.255.255.255	12340	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>

#### Gateway Mode

- Type

**Disable:** The 802.1X authentication request from the IP address or network segment of 802.1 X-enabled client devices or the remote gateway is not allowed.

**802.1X:** The client device is 802.1X-enabled, such as AP and switch.

**Roaming Out:** The device is the remote gateway to send authentication request of "Roaming Out User".

To add to the Device Setting List, configure *Type*, *IP Address*, *Subnet Mask* and *Secret Key* in the *Add* column; click **Add**.

Home > User > Roaming Out and 802.1X Client Device Setting

#### Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	
Roaming Out ▾	<input type="text" value="192.168.5.10"/>	255.255.255.255 (/32) ▾	<input type="text" value="12345"/>	<input type="button" value="Add"/>

Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	Delete	Edit
------	------------	-------------	------------	--------	------

#### Gateway Mode >> Add Roaming Out and 802.1X list

- IP Address / Subnet Mask:** The combination of these two fields specifies the IP address or network segment of 802.1 X-enabled client devices or the remote gateway.
- Security Key:** Security key for the authentication.

## 4.5 Utilities

This section provides information on four utilities used for customizing and maintaining the system, including **Change Password, Import & Export, Backup & Restore, System Upgrade, Reboot, Scan and Upload Certificate.**

### 4.5.1 Change Password

To protect the administration web site from unauthorized access, it is strongly recommended to change the default administrator's password to your own one. Only alpha-numeric characters pattern is allowed and it is strongly recommended to take a combination of both numeric and alphabetic characters.

[Home](#) > [Utilities](#) > [Change Password](#)

### Change Password

<b>Name :</b>	<b>admin</b>	
<b>Old Password :</b>	<input type="text"/>	
<b>New Password :</b>	<input type="text"/>	*up to 32 characters
<b>Re-enter New Password :</b>	<input type="text"/>	
<b>Name :</b>	<b>manager</b>	
<b>New Password :</b>	<input type="text"/>	*up to 32 characters
<b>Re-enter New Password :</b>	<input type="text"/>	
<b>Name :</b>	<b>operator</b>	
<b>New Password :</b>	<input type="text"/>	*up to 32 characters
<b>Re-enter New Password :</b>	<input type="text"/>	

#### **Gateway Mode**

[Home](#) > [Utilities](#) > [Change Password](#)

### Change Password

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

#### **AP Mode**

The administrator/manager/operator can change the passwords of the system. The login account for the administrator is "admin". The admin password of the system can be changed here by entering the new password. The default admin password of the system is "admin". Click **Apply** to activate the new passwords.

## 4.5.2 Import & Export

Home > Utilities > Import & Export User

### Import & Export User

Note : The format of each line in the file is "Username, Password, MAC Address, Remark" without quotes. There must be no space between the fields and commas. The MAC Address field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.

Import Local User

Export Local User

#### Gateway Mode

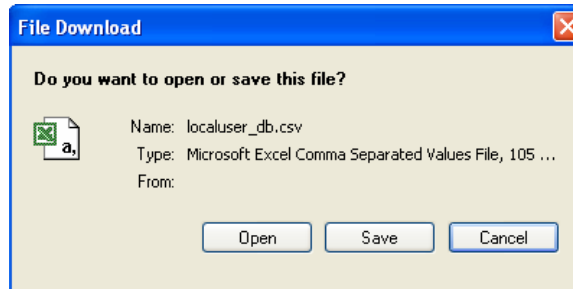
- **Import Local User:** Click **Browser** button to select the file for uploaded user account and then click **Import** to execute the process.

Home > Utilities > Import Result

### Import Result

User duplicated in line 1!

- **Export Local User:** Click **Export** button to create all build-in user account information and click **Open** or **Save** to view or save the user's file.



### 4.5.3 Backup & Restore

This function is used to backup and to restore the OWL800 settings. The OWL800 can also be restored to the factory default settings using this function. It can be used to duplicate settings to other access points (backup settings and then restore in another AP).

[Home](#) > [Utilities](#) > [Config Save & Restore](#)

#### Configuration Backup & Restore

Reset to Default:	<input type="button" value="Reset"/>
Backup System Settings:	<input type="button" value="Backup"/>
Restore System Settings:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Restore"/>

#### Gateway & AP Mode

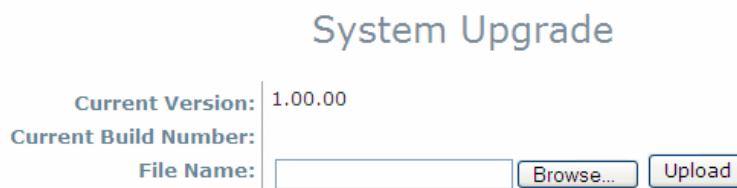
- **Reset to Default:** Click **Reset** to load the factory default settings of the OWL800. After confirming this action, the system will reset all parameters. Reboot to let the default settings takes effect.
- **Backup System Settings:** Click **Backup** button to save the current system configurations to a backup file on a local disk of the management console. A backup file for OWL800 keeps the current system settings as well as the local user accounts. Before any configuration changed, it is recommended to backup the system before you proceed with any changes; thus, it can be recovered soon if occasionally something wrong happened.
- **Restore System Settings:** Click on the **Browse** button to select configuration file to restore, and then, press **Upload** to proceed. After confirming the action, the system will start to replace the existing settings with this newly upload one; reboot the system as required to ensure the parameter changes take effect.

Since network parameters have been reset/restored, the administrator may need to change PC's network settings in order to match OWL800's default settings.

## 4.5.4 System Upgrade

OWL800 provides Web firmware upload/upgrade feature. While the new firmware is obtained, it has to put locally in the administrator's computer. The users can easily download the latest firmware from the website and upgrade the system. To upgrade the system firmware, click **Browse** button to choose the new firmware file and then click **Apply** button to execute the process. There will be a prompt confirmation message appearing to notify the administrator to restart the system after successful firmware upgrade.

[Home](#) > [Utilities](#) > System Upgrade



System Upgrade

Current Version: 1.00.00  
Current Build Number: |  
File Name:

### Gateway & AP Mode

Although the system will check the firmware's contents to ensure its integrity, it is still recommended to check the version number before action proceeded.

*Please note that firmware upgrade may sometime result in loss of some data. Please ensure that you read the release notes to understand the limitations before upgrading the firmware. Please restart the system after upgrading the firmware.*

**Do not power on/off the system during the upgrade or the restart process as it may damage the system.**

*For further information of available firmware version, please contact local dealers.*

## 4.5.5 Reboot

This function allows the administrator to restart the OWL800 safely. The process should take about three minutes. Click **Reboot** button to restart the system. Please wait for the blinking timer to finish before accessing the system web management interface again.

Occasionally, it is necessary to reboot OWL800 to ensure parameter changes being submitted. Take this page for the purpose.

[Home](#) > [Utilities](#) > [Reboot](#)

### Reboot the System

**Reboot may take several minutes to complete.  
The Admin Login Page will be shown after system boots up.**

Reboot

**Gateway & AP Mode**



## 4.5.6 Scan

OWL800 provides this **Scan** feature for users to figure out the wireless status from the view of VAPs. It probes the WLAN and retrieves the information from clients. Thus, while compare scan result to the VAPs settings, it can avoid unexpected conflict in settings and tune the corresponding parameters.

[Home](#) > [Utilities](#) > [Scan](#)

### Scan Settings

Scan :  Disable  Enable

Scan Interval : sec(s)

## Not Found Anything.

**Gateway & AP Mode**

- **Scan:** Enable or Disable scan settings.
- **Scan Interval:** The time interval used to trigger the scanning, it takes 86400 seconds as the default setting.

The result table records the latest AP scanning result. Still, the user could click the **Scan Now** button again to renew the result immediately. Take the result to compare with the AP's setting and status and tune necessary AP settings.

## 4.5.7 Upload Certificate

Home > Utilities > Upload Certificate

### Upload Certificate

Upload Private Key	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Upload Certificate	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

### Gateway & AP Mode

The administrator can upload new private key and customer certification, external certificate issued by public or private authority.

Click the first **Browse** button to select the **Private Key** or **Certificate**. Click the second **Browse** button to select the file for the certificate upload. Next, click **Save** to complete the upload process. Click **Use Default Certificate** button to restore the default certificate automatically.

## 4.6 Status

This section provides information on the following functions: **System Overview**, **WDS List**, **Antennas**, **Associated Clients**, **Event Log**, **Online Users** and **User Log**.

### 4.6.1 Overview


The section provides an overview of the system status for the administrator. System's overall status, for individual setting and status, please check them in each configuration page.

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


### System Overview

 **System**


System Name	OWL800
Firmware Version	1.00.00
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	0 days, 0:13:49
Operating Mode	GW

 **Radio Status**

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:A9:E7	802.11b+g	6	Highest
RF Card B	00:0B:6B:DB:A9:09	802.11b+g	9	Highest

 **AP Status**

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:A9:E7	OWL800-1	None	0
VAP-2	06:0B:6B:DB:A9:E7	OWL800-2	None	0
VAP-3	0A:0B:6B:DB:A9:E7	OWL800-3	None	0

 **Network Interfaces**

Interface	IP Address	Gateway	Type
WAN1	192.168.1.8	192.168.0.1	Static

Interface	IP Address	VLAN Tag	State
VLAN0	192.168.1.1	0	Enabled
VLAN1	192.168.11.1	1	Enabled
VLAN2	192.168.12.1	2	Enabled
VLAN3	192.168.13.1	3	Enabled
VLAN4	192.168.14.1	4	Enabled
VLAN5	192.168.15.1	5	Disabled
VLAN6	192.168.16.1	6	Disabled
VLAN7	192.168.17.1	7	Disabled
VLAN8	192.168.18.1	8	Disabled

**Gateway Mode**

System    AP    WDS    Utilities    Status

Overview    WDS List    Antennas    Associated Clients    Event Log

Home > Status > System Overview

## System Overview

### System

System Name	OWL800
Firmware Version	1.00.00
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	2 days, 21:22:23
Operating Mode	AP

### Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:0B:6B:DB:A9:E7	802.11b+g	6	Highest
RF Card B	00:0B:6B:DB:A9:09	802.11b+g	9	Highest

### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:0B:6B:DB:A9:E7	OWL800-1	None	0
VAP-2	06:0B:6B:DB:A9:E7	OWL800-2	None	0
VAP-3	0A:0B:6B:DB:A9:E7	OWL800-3	None	0

### LAN Interface

MAC Address	00:08:00:00:01:09
IP Address	
Subnet Mask	255.255.0.0
Gateway	

**AP Mode**

The description of the table is as the following:

<b><u>Item</u></b>		<b><u>Description</u></b>
<b>Firmware Version</b>		The present firmware version of OWL800
<b>System Name</b>		The system name. The default is OWL800
<b>Device Time</b>		The network time server that the system is set to align.
<b>System Up Time</b>		The system time is shown as the local time.
<b>Network Interface</b>	<b>MAC Address</b>	The MAC address of Network Interface
	<b>IP Address</b>	The IP address of the Network Interface
<b>LAN Interface</b>	<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>Radio Status</b>	<b>MAC Address</b>	The MAC address of Radio module
	<b>Band</b>	The RF band(a/b/g) used
	<b>Channel</b>	The channel specified
	<b>Radio module</b>	The RF module used for AP
<b>AP Status</b>	<b>BSSID</b>	Basic Service Setting ID
	<b>ESSID</b>	Extended Service Setting ID

## 4.6.2 WDS List

WDS lists indicate the link status of each RF interface including status of Mac Address, SNR dB, rate, count and errors.

[Home](#) > [WDS](#) > WDS Link Overview

### WDS Link Overview

#### RF Card B

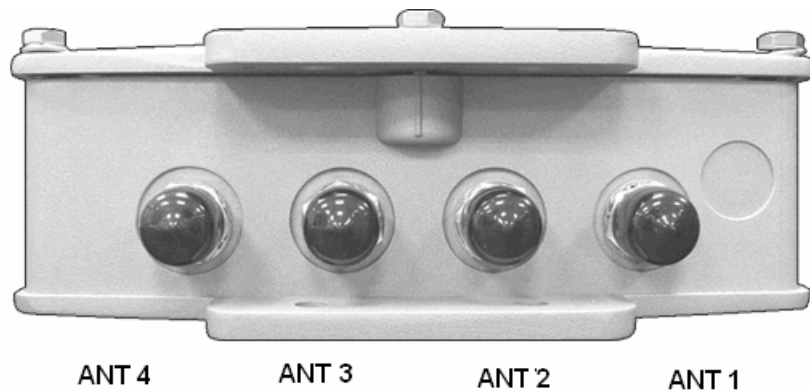
Link No.	State	MAC Address	Security	Delete	Edit
1	Disabled		None		<a href="#">Edit</a>
2	Disabled		None		<a href="#">Edit</a>
3	Disabled		None		<a href="#">Edit</a>
4	Disabled		None		<a href="#">Edit</a>

#### Gateway & AP Mode

### 4.6.3 Antennas

Antenna Diversity is an important feature of the 802.11 specification. The two radio modules (CM9) inside the system support the feature of Antenna Diversity. Each of them comes with two antenna connectors for connecting up to two antennas. When the feature of antenna diversity is turned on, the module uses two receiving antennas to eliminate multipath signal distortion. That is, the signal from the antenna with the least noise (best SNR) is chosen, and the other antenna is ignored. For more explanation please refer to the wiki page on [Antenna Diversity](#).

To support the Antenna Diversity, each radio module (CM9) inside has two antenna connectors - one "Main" connector and the other as "Auxiliary" connector. The "Main" connector must be connected with an antenna. The "Auxiliary" is optionally connected to an antenna.



The above picture represents ANT 1 ~ ANT 4 connectors from right to left when OWL800 chassis (with Mylar) is faced up.

ANT1: The "Main" connector of 1<sup>st</sup> radio module. Antenna at this connector is required.

ANT2: The "Main" connector of 2<sup>nd</sup> radio module. Antenna at this connector is required.

ANT3: The "Auxiliary" connector of 1<sup>st</sup> radio module. Antenna at this connector is optional.

ANT4: The "Auxiliary" connector of 2<sup>nd</sup> radio module. Antenna at this connector is optional.

Each of the two radio module (CM9) inside has two antenna connectors for antenna diversity. **The required antenna is antenna ANT1 and antenna ANT3.** ANT1 is connected to the "Main" contact point of the first radio module. ANT3 is connected to the "Main" contact of the second module.

### 4.6.4 Associated Clients

List all associated clients from all the VAPs. Please take this table to manage the clients and take the signal strength for debug purpose.

[Home](#) > [Status](#) > [Wireless Clients](#)

#### Associated Client Status

##### Client List

Associated VAP	ESSID	MAC Address	SNR (dB)	Idle Time (secs)	Disconnect
----------------	-------	-------------	----------	------------------	------------

#### Gateway & AP Mode



## 4.6.5 Event Log

[Home](#) > [Status](#) > Event Log

### Event Log

```
Jan 20 10:39:42 syslogd started: BusyBox v1.2.1
```

#### **Gateway & AP Mode**

Event log provides the system activities records and monitor the system status by checking this log.

In the log, normally, each line represent an event record; And in each line, there are fields such as Date, Time, Name or Status.

- **Date/Time** : The time & date when the event happened
- **Hostname**: Indicate which host records this event. Note that all events in this page are local event, so events of this field are all the same. However in remote syslog service, this field will help us to identify which event are from this OWL800.
- **Process name** (with square brackets): Indicate the event generated by this running instance

To save the file locally or clear all the records, press **Save Log** or **Clear** button respectively.

### 4.6.6 Online Users

All online users' information can be obtained by using this function. These include **User name**, **IP Address**, **MAC Address**, **Idle Time**, and **Action**. The administrator can use this function to force a specific online user to log out, or terminate any user session by clicking the hyperlink of **Action**.



**Gateway & AP Mode**

### 4.6.7 User Log

This function is used to check the history of the system and it will be kept up to 3 days. All records are sorted by date and listed accordingly. Please note that these records are stored on the volatile memory and will be lost if the system is powered off.

Home > Status > User Log

#### User Log

SYSLOG Server Settings			
<b>User Log</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	IP Address: <input type="text"/>	Port : <input type="text" value="514"/>
<b>Session Log</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	IP Address: <input type="text"/>	Port : <input type="text" value="514"/>

#### Gateway & AP Mode

- **Users Log:** The **Users Log** provides information of all users' login and logout activities except guest users, RADIUS roaming in/out users, and SIP clients.
- **Session Log:** Log each connection created by clients and tracking the source IP and destination IP. Session Log can be sent to the SYSLOG server or via email automatically. In addition, it can be uploaded to a FTP server periodically.

## Appendix A. Session Limit and Session Log

### ■ Session Limit

To prevent ill-behaved clients or malicious software from using up system's connection resources, administrators will have to restrict the number of concurrent sessions that a client can establish.

- The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the policy setting, which can be chosen to apply to all users including authenticated users, users on non-authenticated ports, privileged users, and clients in virtual server and DMZ zones.
- When the number of a user's sessions reaches the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350, and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to the SYSLOG server specified in the *Policy Configuration*.
- Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in the network deployment to protect the network in daily operation.

### ■ Session Log

The system can record connection details of each client while accessing the Internet. In addition, the log data can be sent out to a specified SYSLOG Server, Email Box or FTP Server based on pre-defined time interval.

- The following table shows the fields of a session log record.

Field	Description
Date and Time	The date and time that the session is established
Session Type	[New]: This is the newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user; It shows "N.A." if the user or device does not need to log in with a username. For example, the user or device is on a non-authenticated port or on the privileged MAC/IP list.  Note: Only 31 characters are available for the combination of Session Type plus Username. Please change the account name accordingly, if the name is not identifiable in the record.
Protocol	The communication protocol of session: TCP or UDP
MAC	The MAC address of the client
SIP	The source IP address of the client
SPort	The source port number of the client
DIP	The destination IP address of the client
DPort	The destination port number of the client

- The following table shows an example of the session log data.

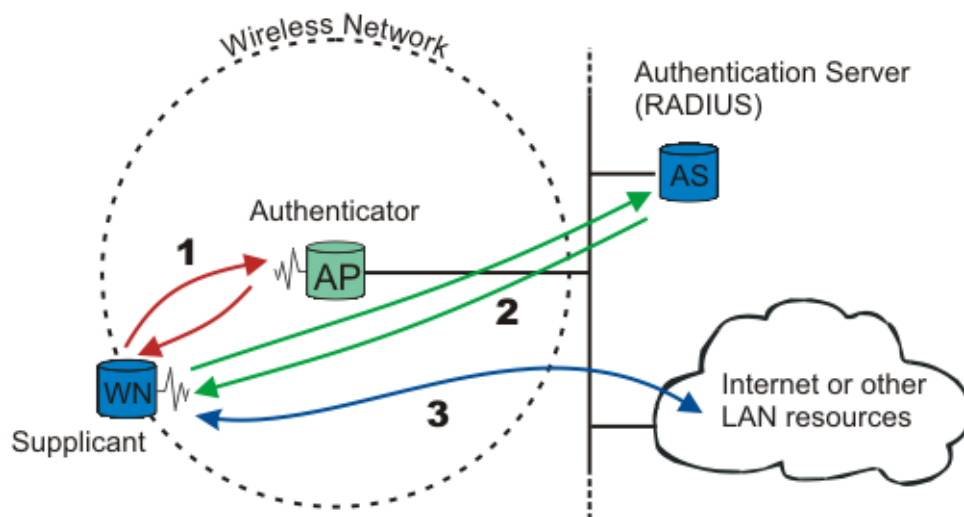
Aug 30 12:35:05 2007	[New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1626 DIP=203.125.164.132 DPort=80
Aug 30 12:35:05 2007	[New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1627 DIP=203.125.164.132 DPort=80
Aug 30 12:35:06 2007	[New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1628 DIP=203.125.164.142 DPort=80
Aug 30 12:35:06 2007	[New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1629 DIP=203.125.164.142 DPort=80
Aug 30 12:35:07 2007	[New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1630 DIP=67.18.163.154 DPort=80
Aug 30 12:35:09 2007	[New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1631 DIP=202.43.195.52 DPort=80
Aug 30 12:35:10 2007	[New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1632 DIP=203.84.196.242 DPort=80

## Appendix B. 802.1X Support

### ▪ What is IEEE 802.1X ?

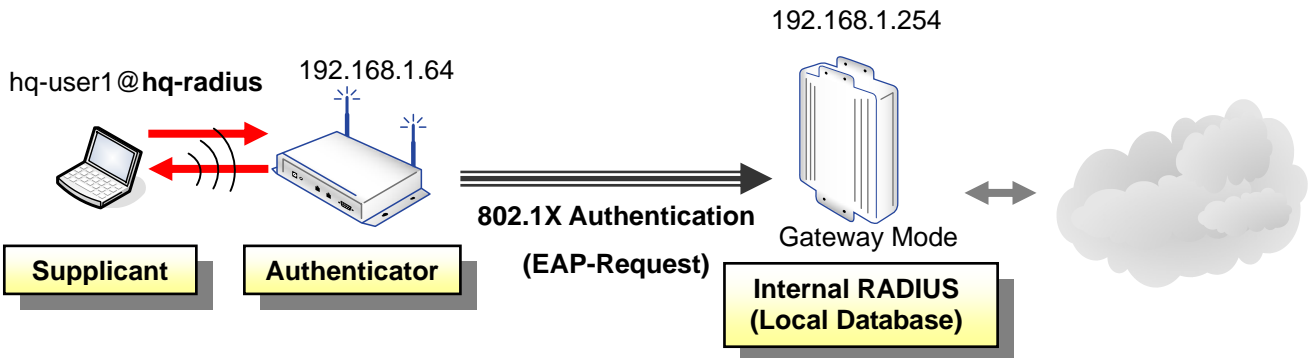
The 802.1X-2001 standard states:

"Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases which the authentication and authorization fails. A port in this context is a single point of attachment to the LAN infrastructure." --- 802.1X-2001, page 1.



**802.1X Authentication Architecture**

- **Example #1:** OWL800 is configured in the way that Local user database acts like an internal RADIUS server.



• **Configuration Steps:**

- **Step 1:** Enable Local database as internal RADIUS server

When **802.1X Authentication** in Local User Setting is enabled, Local database will act like an internal RADIUS server.

Home > User > Authentication : Local User Setting

### Authentication : Local User Setting

Postfix :

Multiple Login :  Disable  Enable

**802.1X Authentication** :  Disable  Enable

Account Roaming Out :  Disable  Enable

Import/Export Local User :

- **Step 2:** Specify the 802.1X Client Device (Authenticator)

The system will only allow this 802.1X-enabled client device (AP) to send 802.1X authentication request to internal or external RADIUS server.

Click the **Roaming Out & 802.1X Client Device Settings** button above or the **802.1X** tab to go to the configuration page. Set the Type to **802.1X** and enter the IP address of the authenticator.

Home > User > Roaming Out and 802.1X Client Device Setting

### Roaming Out and 802.1X Client Device Setting

Type:  | IP Address:  | Subnet Mask:  | Secret Key:  |

#### Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	Delete	Edit
Roaming Out	192.168.5.10	255.255.255.255	12345	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>
<b>802.1X</b>	192.168.1.64	255.255.255.255	12340	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>

- **Step 3:** Configure the RADIUS server setting of the AP (Authenticator)

### Security Settings

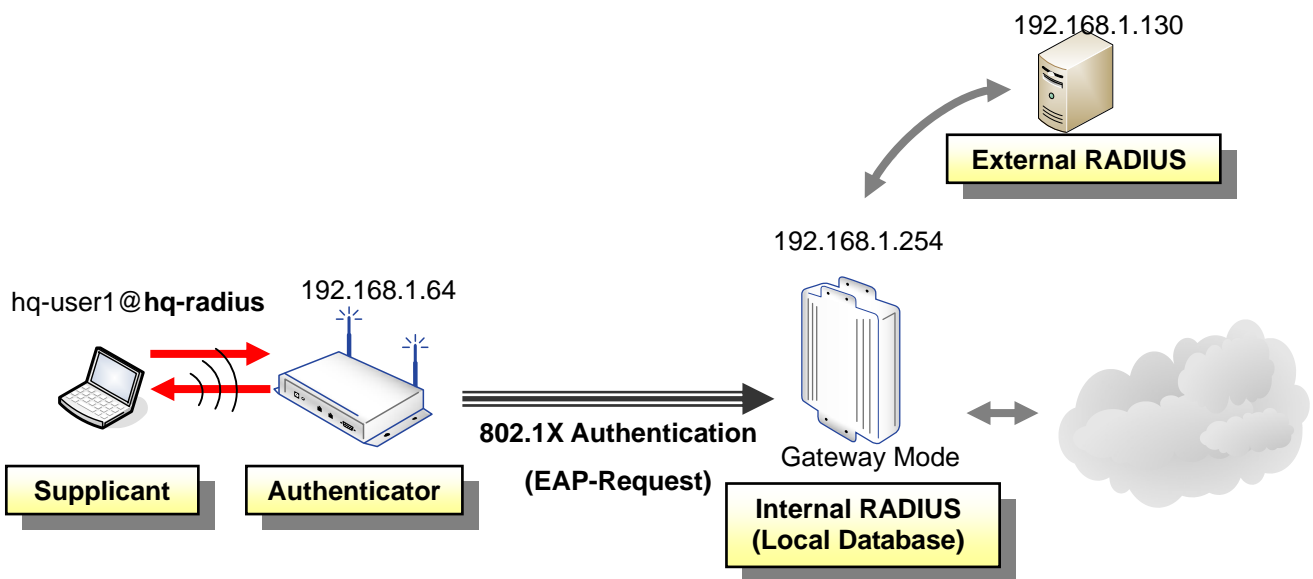
Profile Name :

Security Type :

Cipher Suite :

Group Key Update Period:  second(s)

- **Example #2:** OWL800 is configured to use external RADIUS server for 802.1X authentication.





• **Configuration Steps:**

- **Step 1:** Configure the external RADIUS server

Enable the **Extensible Authentication Protocol** and enter the information of the RADIUS server in the RADIUS page.

Home > User > Authentication : RADIUS Setting

### Authentication : RADIUS Setting

External RADIUS Server : RADIUS 1

Postfix : radius1\*

Extensible Authentication Protocol :  Disable  Enable

Username Format to RADIUS Server :  ID Only  Complete

802.1X Client Device Settings

Primary RADIUS Server :

Host: 192.168.1.130\* (Domain Name / IP Address)

Authentication Port: 1812

Secret Key: abcd1234

- **Step 2:** Specify the 802.1X Client Device (Authenticator)

The system will only allow this 802.1X-enabled client device (AP) to send 802.1X authentication request to internal or external RADIUS server.

Click the **Roaming Out & 802.1X Client Device Settings** button above or the **802.1X** tab to go to the configuration page. Set the Type to **802.1X** and enter the IP address of the authenticator.

Home > User > Roaming Out and 802.1X Client Device Setting

### Roaming Out and 802.1X Client Device Setting

Type: Disable

IP Address: [ ]

Subnet Mask: 255.255.255.255 (/32)

Secret Key: [ ]

Add

#### Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	Delete	Edit
Roaming Out	192.168.5.10	255.255.255.255	12345	Delete	Edit
802.1X	192.168.1.64	255.255.255.255	abcd1234	Delete	Edit

- **Step 3:** Configure the RADIUS server setting of the AP (Authenticator)

Home > AP > Security

### Security Settings

Profile Name :

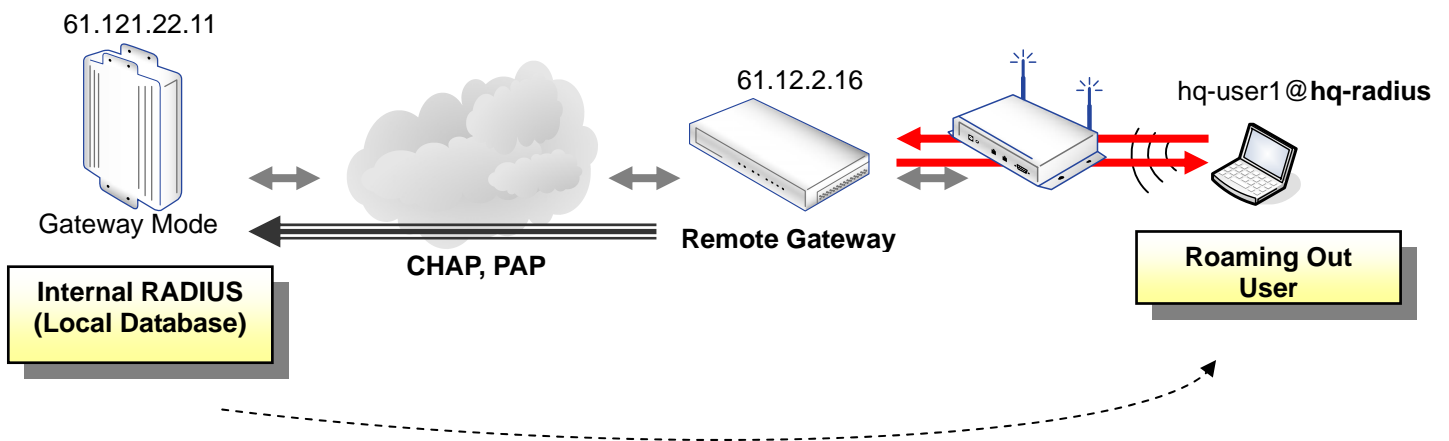
Security Type :

Cipher Suite :

Group Key Update Period:  second(s)

**Example #3:** Local Database of OWL800 acts like an external RADIUS server for remote gateway to service “Roaming Out” users.

**Note:** In this example, the AP is not enabled as 802.1X Authenticator; therefore, the “Roaming Out User” will be authenticated via web-based login page, instead of 802.1X client window.



• **Configuration Steps:**

- **Step 1:** Enable Local database for use of Roaming Out User

When **Account Roaming Out** in Local User Setting is enabled, Local database will act like an internal RADIUS server.

Home > User > Authentication : Local User Setting

### Authentication : Local User Setting

Postfix :  \*

Multiple Login :  Disable  Enable

802.1X Authentication :  Disable  Enable

**Account Roaming Out :**  Disable  Enable

Import/Export Local User :

- **Step 2:** Specify the remote gateway (Authenticator)

The system will only allow this 802.1X-enabled client device (remote gateway) to send 802.1X authentication request to internal or external RADIUS server.

Click the **Roaming Out & 802.1X Client Device Settings** button above or the **802.1X** tab to go to the configuration page. Set the Type to **Roaming Out** and enter the IP address of the remote gateway.

Home > User > Roaming Out and 802.1X Client Device Setting

### Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	
<input type="button" value="Disable"/> ▾	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> ▾	<input type="text"/>	<input type="button" value="Add"/>

Roaming Out and 802.1X Client Device Setting

Type	IP Address	Subnet Mask	Secret Key	Delete	Edit
Roaming Out	61.12.2.16	255.255.255.255	abcd1234	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>
802.1X	192.168.1.64	255.255.255.255	abcd1234	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>

- **Step 3:** Configure the RADIUS server setting of the remote gateway (Authenticator)

Home > User > Authentication : RADIUS Setting

## Authentication : RADIUS Setting

External RADIUS Server : RADIUS 1

Postfix :	<input type="text" value="radius1"/> *
Extensible Authentication Protocol :	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Username Format to RADIUS Server :	<input type="radio"/> ID Only <input checked="" type="radio"/> Complete
<b>802.1X Client Device Settings</b>	
Primary RADIUS Server :	Host: <input type="text" value="192.168.22.11"/> *( Domain Name / IP Address )
	Authentication Port: <input type="text" value="1812"/>
	Secret Key: <input type="text" value="abcd1234"/>
	Accounting Service: <input type="radio"/> Disable <input checked="" type="radio"/> Enable
	Accounting Port: <input type="text" value="1813"/>
	Authentication Protocol: <input type="text" value="PAP"/>

P/N:100200904071