

User's Manual

Enterprise Access Point

Indoor EAP Series /

Outdoor OWL Series

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.

Table of Contents

| | | |
|-------|---|----|
| 1. | Before You Start | 5 |
| 1.1 | Preface | 5 |
| 1.2 | Document Conventions | 5 |
| 1.3 | Package Content | 6 |
| 2. | System Overview and Getting Started | 8 |
| 2.1 | Introduction of 4ipnet Access Points | 8 |
| 2.2 | Hardware Description | 9 |
| 2.3 | Hardware Installation | 17 |
| 2.4 | Access Web Management Interface | 19 |
| 3. | Connect your AP to your Network | 22 |
| 4. | Adding Virtual Access Points | 29 |
| 5. | Securing the AP | 31 |
| 6. | Creating a WDS Bridge between two APs..... | 42 |
| 7. | Web Management Interface Configuration..... | 45 |
| 7.1 | System | 47 |
| 7.1.1 | General | 47 |
| 7.1.2 | Network Interface..... | 49 |
| 7.1.3 | Port..... | 51 |
| 7.1.4 | Management | 52 |
| 7.1.5 | CAPWAP | 55 |
| 7.1.6 | IPv6..... | 56 |
| 7.2 | Wireless | 57 |
| 7.2.1 | VAP Overview | 57 |
| 7.2.2 | General | 60 |
| 7.2.3 | VAP Configuration | 63 |
| 7.2.4 | Security..... | 65 |
| 7.2.5 | Repeater | 70 |
| 7.2.6 | Advanced..... | 72 |
| 7.2.7 | Access Control | 74 |
| 7.3 | Firewall..... | 78 |
| 7.3.1 | Firewall List | 78 |
| 7.3.2 | Service | 82 |
| 7.3.3 | Advanced | 83 |
| 7.4 | Utilities | 84 |
| 7.4.1 | Change Password..... | 84 |
| 7.4.2 | Backup & Restore..... | 85 |

| | |
|---|-----|
| 7.4.3 System Upgrade | 87 |
| 7.4.4 Reboot | 87 |
| 7.4.5 Upload Certificate | 88 |
| 7.4.6 Channel Analysis | 89 |
| 7.4.7 Background Scan | 90 |
| 7.5 Status | 91 |
| 7.5.1 Overview | 91 |
| 7.5.2 Interfaces | 93 |
| 7.5.3 Associated Clients | 95 |
| 7.5.4 WDS Link Status | 96 |
| 7.5.5 Event Log | 98 |
| 7.5.6 Monitor | 99 |
| 8. CPE Mode Configuration (OWL530/EAP210) | 100 |
| 8.1 System | 102 |
| 8.1.1 System Information | 102 |
| 8.1.2 Operating Mode | 104 |
| 8.1.3 Network Settings | 105 |
| 8.1.4 Management | 108 |
| 8.2 Wireless | 110 |
| 8.2.1 General Settings | 110 |
| 8.2.2 Advanced Wireless Settings | 111 |
| 8.2.3 Security Settings | 112 |
| 8.2.4 Site Survey | 114 |
| 8.3 Firewall | 116 |
| 8.3.1 IP/ Port Forwarding | 116 |
| 8.3.2 Demilitarized Zone | 117 |
| 8.4 Utilities | 118 |
| 8.4.1 Change Password | 118 |
| 8.4.2 Backup & Restore | 119 |
| 8.4.3 System Upgrade | 120 |
| 8.4.4 Reboot | 121 |
| 8.4.5 Upload Certificate | 122 |
| 8.5 Status | 123 |
| 8.5.1 System Overview | 123 |
| 8.5.2 Interfaces | 125 |
| 8.5.3 Event Log | 128 |
| 8.5.4 Monitor | 129 |
| 8.5.5 DHCP Leases | 130 |

| | |
|---|-----|
| 8.5.6 UPnP Status | 131 |
| 9. Console Interface Configuration..... | 132 |

1. Before You Start




1.1 Preface

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

Corresponding Software Versions for each Model

| | |
|--------|-----------------------------|
| EAP210 | Up to software version 1.10 |
| EAP220 | Up to software version 1.10 |
| EAP320 | Up to software version 2.10 |
| EAP747 | Up to software version 1.30 |
| EAP750 | Up to software version 2.10 |
| EAP757 | Up to software version 2.10 |
| OWL530 | Up to software version 1.10 |
| OWL610 | Up to software version 1.40 |
| OWL620 | Up to software version 1.40 |

1.2 Document Conventions

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

1.3 Package Content

The standard package of EAP210 includes:

- 4ipnet EAP210 x1
- Quick Installation Guide (QIG) x1
- CD-ROM (with User's Manual and QIG) x1
- Console Cable x1
- Power Adaptor (12V) x1
- Detachable Antenna x2

The standard package of EAP220 includes:

- 4ipnet EAP220 x1
- Quick Installation Guide (QIG) x1
- CD-ROM (with User's Manual and QIG) x1
- Console Cable x1
- Ethernet Cable x1
- Power Adaptor (12V) x1
- Detachable Antenna x4

The standard package of EAP320 includes:

- 4ipnet EAP320 x1
- Quick Installation Guide (QIG) x1
- CD-ROM (with User's Manual and QIG) x1
- Console Cable x1
- Ethernet Cable x1
- Power Adaptor (12V) x1
- Detachable Antenna x4

The standard package of EAP747 / EAP750 / EAP757 includes:

- 4ipnet EAP747 / EAP750 / EAP757 x1
- Quick Installation Guide (QIG) x1
- CD-ROM (with User's Manual and QIG) x1
- Ethernet Cable x1
- Power Adaptor (12V) (Optional) x1
- Mounting Kit x1
- Detachable Antenna (EAP750) x4

The standard package of OWL530 includes:

- 4ipnet OWL530 x1
- Quick Installation Guide (QIG) x1
- CD-ROM (with User's Manual and QIG) x1
- Power Sourcing Equipment (Optional) x1
- Ground Wire x1
- Mounting Kit x1

The standard package of OWL620 / OWL610 includes:

- 4ipnet OWL620 / OWL610 x1
- Quick Installation Guide (QIG) x1
- CD-ROM (with User's Manual and QIG) x1
- Power Sourcing Equipment (Optional) x1
- Mounting Kit x1



It is recommended to keep the original packing materials for possible future shipment when repair or maintenance is required. Any returned product should be packed in its original packaging to prevent damage during delivery.

2. System Overview and Getting Started

2.1 Introduction of 4ipnet Access Points

Indoor – EAP210 / EAP220 / EAP320 / EAP747 / EAP750 / EAP757

The 4ipnet's Enterprise Access Point EAP Series are embedded with 802.11 a/b/g/n MIMO technology, designed for seamless wireless connectivity in enterprise or industrial environments of all dimensions. EAP220 / EAP320 / EAP750 / EAP757 feature dual radio RF cards to offer flexible implementations needed for the growing wireless networking applications. The EAP Series make wireless communication fast, secure and easy. They support business grade security, namely 802.1X, and Wi-Fi Protected Access (WPA and WPA2). By pushing a purposely built button, the 4ipWES (Press-n-Connect) feature makes it easy to bridge wireless links of multiple access points for forming a wider wireless network coverage.

The EAP Series also features multiple ESSIDs with VLAN tags and multiple Virtual APs, great for enterprise applications, such as separating traffic from different departments using different ESSIDs. The PoE LAN port is able to receive power from Power over Ethernet (PoE) sourcing devices.

EAP210, EAP220 and EAP320's metal housing is IP50 anti-dust compliant, which means that these Access Points are well suited to WLAN deployment in industrial environments. EAP747 / EAP750 / EAP757 are packed in fire-retardant wall/ceiling mountable plastic enclosures, and are built perfectly to blend in with your décor.

Outdoor – OWL530 / OWL610 / OWL620

The 4ipnet OWL530 / OWL610 / OWL620 Outdoor Access Point is embedded with dual(OWL620) / single(OWL610 and OWL530) radio RF cards (802.11 a/b/g/n MIMO) in weatherproof housing, designed for building municipal or campus wide wireless networks in harsh outdoor environments. The OWL Series' 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 OWL Series Outdoor Access Point makes wireless communication fast, secure and easy. It supports business grade security, namely 802.1X, and Wi-Fi Protected Access (WPA and WPA2).

Combined with a variety of directional antennas (chosen by professionals), one OWL620 with dual radios is easy to serve clients located in different directions as well as to cover longer range. With all modules supporting a/b/g/n bands, more channels are available for better channel planning. For example, to reduce radio interferences, network planners may select channels in 5 GHz for backhaul or bridges while allocating non-overlapping channels in 2.4 GHz for serving clients.



- Please note that screenshots are taken from APs which feature dual RF cards. Single RF Card APs can be configured in the same manner from the User Interface.

2.2 Hardware Description

This section depicts the hardware information including all panel description.

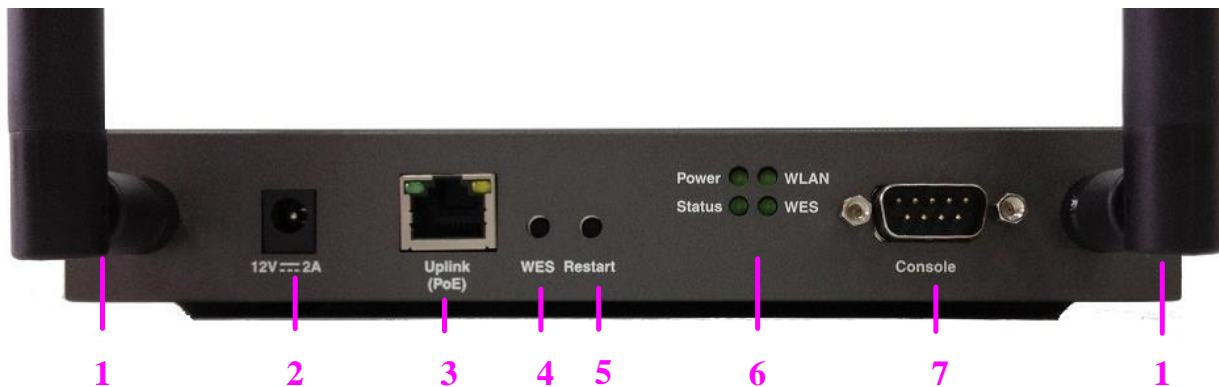
EAP210

Front Panel



EAP210 Front Panel

Rear Panel



EAP210 Rear Panel

| | | |
|---|--------------------------|---|
| 1 | Antenna Connector | Reverse SMA connectors for attaching antennas. |
| 2 | 12V 2A | Power Socket for the power adaptor. |
| 3 | Uplink Port | The port for uplink connection to another gateway or device. PoE (802.3af/at) is supported. |
| 4 | WES Button | WDS Easy Setup. Press the button to build up a WDS link with another peer. 4 WDS links can be set up. |
| 5 | Restart Button | Press to restart the system |

| | | | | | | |
|----------|-----------------------|--|---|--|--|--|
| 6 | LED Indicators | Power | On indicates power on. | | | |
| | | Status | On indicates the system is ready. | | | |
| | | WLAN | On indicates wireless network interface is ready for service. | | | |
| | | WES | For indicating WDS connection status. | | | |
| | | | | Master (Press for more than 3 seconds) | Slave (Press once and then release right away) | |
| | | | WES Start | LED (Green) OFF and then BLINKING SLOWLY | LED (Green) BLINKS SLOWLY | |
| | WES Negotiate | BLINKING SLOWLY (Green) | BLINKING RAPIDLY (Green) | | | |
| | WES Success | LED (Green) ON | LED (Green) ON | | | |
| | WES Fail/Timeout | LED (Green) OFF | LED (Green) OFF | | | |
| 7 | Console Port | To access EAP210 via the console interface | | | | |

EAP220

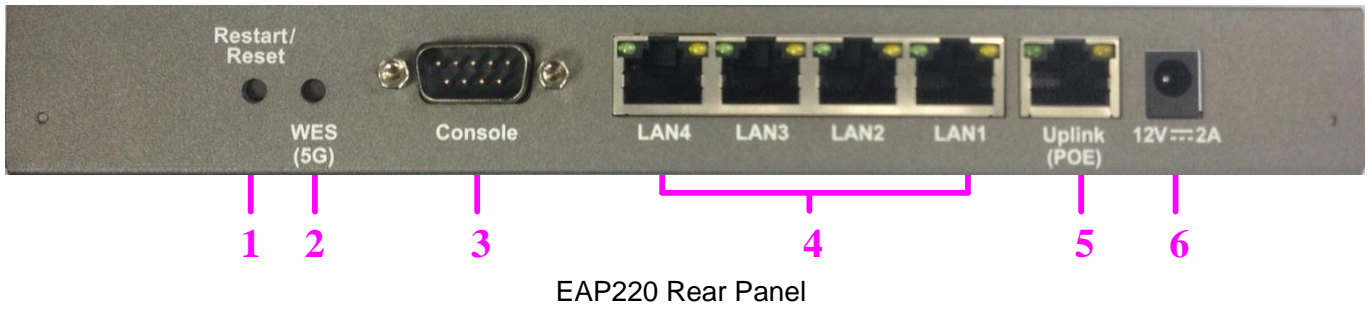
Front Panel



EAP220 Front Panel

| | | | | | |
|---|--|-----------------------------------|---|--|--|
| 1 | | Power LED | On indicates power on. | | |
| 2 | | Status LED | On indicates the system is ready. | | |
| 3 | | WES LED | For indicating WDS connection status. | | |
| | | | | Master (Press for more than 3 seconds) | Slave (Press once and then release right away) |
| | | | WES Negotiate | BLINKING SLOWLY (Green) | BLINKING RAPIDLY (Green) |
| | | | WES Success | LED (Green) ON | LED (Green) ON |
| | | WES Fail/Timeout | LED (Green) OFF | LED (Green) OFF | |
| 4 | | Wireless LED (2.4 / 5 GHz) | On indicates wireless network interface is ready for service. | | |

Rear Panel



EAP220 Rear Panel

| | | |
|---|--------------------------|--|
| 1 | Restart / Reset | Press once to restart the system; to reset the system to factory default settings, hold for more than 5 seconds. |
| 2 | WES Button (RF B) | WDS Easy Setup. Press the button to build up a WDS link with another peer. 4 WDS links can be set up per RF card. Note that the WES Button only runs on the 5 GHz RF Card B. |
| 3 | Console Port | To access EAP220 via the console interface. |
| 4 | LAN 1~4 Ports | The ports for connections with LAN side devices. |
| 5 | Uplink Port (PoE) | The port for uplink connection to another gateway or device. PoE (802.3at) is supported. |
| 6 | 12V 2A | Power Socket for the power adaptor |

EAP320

Front Panel



EAP320 Front Panel

Rear Panel

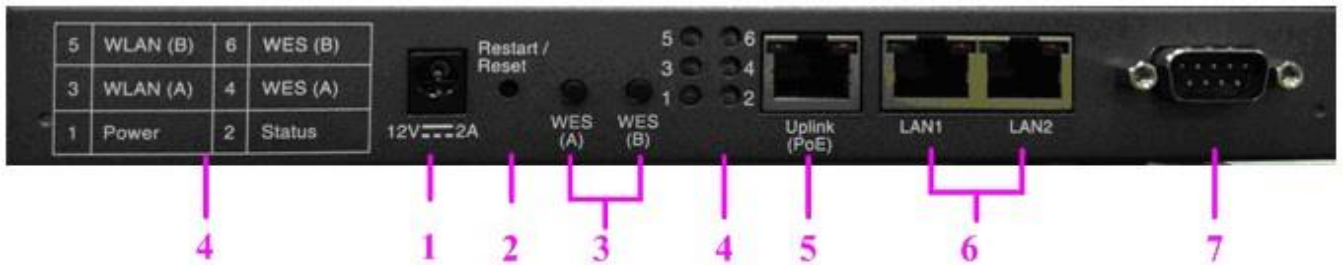


Figure 2 EAP320 Back Panel

| | | |
|---|--------------------|---|
| 1 | 12V 2A | Power Jack Socket |
| 2 | Restart / Reset | Press once to restart the system; to reset the system to factory default settings, hold for more than 5 seconds. |
| 3 | WES Button (A / B) | WDS Easy Setup. Press the button to build up a WDS link with another peer. 4 WDS links can be set up per RF card. |
| 4 | LED Indicators | 6 indicators that displays the states of 6 various functions or progresses. The numbers are explained on the leftmost side of the rear panel. |
| 5 | Uplink Port (PoE) | The port for uplink connection to another gateway or device. PoE is supported. |
| 6 | LAN Ports 1~2 | The ports for connections with LAN side devices. |
| 7 | Console Port | To access EAP320 via the console interface. |

EAP747 / EAP750 / EAP757

Rear Panel

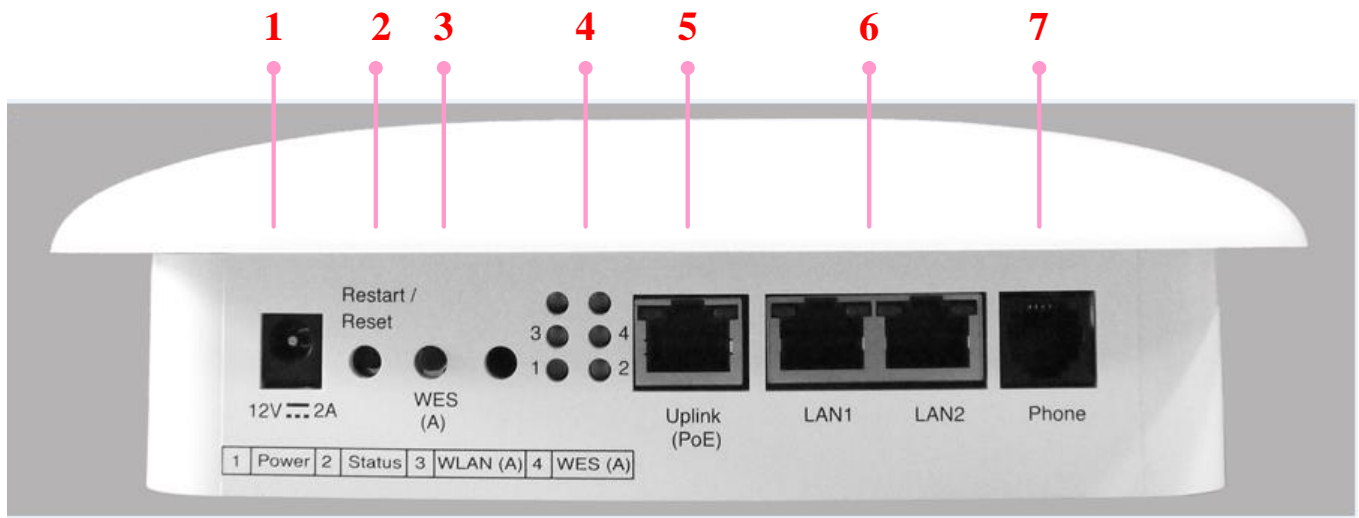


Figure 3 EAP747 / EAP750 / EAP757 Back Panel

| | | |
|---|---------------------------------|--|
| 1 | 12V $\overline{\text{---}}$ 2 A | Attach the power adaptor here. |
| 2 | Restart / Reset Button | Press once to restart the system; Press and hold for more than 5 seconds to reset to factory default. |
| 3 | WES Button | WDS Easy Setup. Press the button to build up a WDS link with another peer. |
| 4 | LED Indicators | 4 LED lights. Representation is listed at the bottom of the panel. (Top 2 reserved for RF Card B if applicable) |
| 5 | Uplink (PoE) Port | For Uplink connection. This port can be used to connect to a controller, gateway, or directly to the internet. PoE is supported. |
| 6 | LAN 1 – 2 Ports | Attach Ethernet cables here to connect to the wired local network. |
| 7 | Phone Jack (EAP747) | A telephone can bypass to a connected phone line in the back of the AP when connected to the socket. |

OWL530



| | | |
|---|-----------------------------|--|
| 1 | Ventilation Valve | Due to extreme weather conditions, water vapor in the OWL530 may condense. The valve allows ventilation to prevent moisture buildup within the OWL530. |
| 2 | Ground Connector | For connecting the ground wire. |
| 3 | PoE Connector | For connecting to the Power Sourcing Equipment (PSE). |
| 4 | N-type Connector x 2 | For connecting to an antenna |

OWL620 / OWL610



Figure 3 OWL620 / OWL610

| | | |
|---|-----------------------------|---|
| 1 | Console | The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's Hyper Terminal for troubleshooting purposes. |
| 2 | Ethernet LAN | Attach Ethernet cables here for connecting to the wired local network. |
| 3 | PoE Connector | For connecting to the Power Sourcing Equipment (PSE). |
| 4 | N-type Connector x 2 | For connecting to an antenna (OWL610). |
| 4 | N-type Connector x 4 | For connecting to an antenna (OWL620: RF Card A x 2, RF Card B x 2). |

2.3 Hardware Installation

Please follow the steps mentioned below to install the hardware of **EAP210 / EAP220 / EAP320**:

Step 1. Place the EAP210 / EAP220 / EAP320 at the best location. The best location is usually at the center of your intended wireless network.

Step 2. Connect the EAP210 / EAP220 / EAP 320 to your network device. Connect one end of the Ethernet cable to the Uplink port of EAP210 / EAP220 / EAP320 and the other end of the cable to a switch, a router, or a hub. EAP210 / EAP220 / EAP320 is then connected to your existing wired LAN network.

Step 3. There are two ways to supply power to EAP210 / EAP220 / EAP320

- a) Connect the DC power adaptor to the EAP210 / EAP220 / EAP320 power jack socket.
- b) The EAP210 / EAP220 / EAP320 Uplink port is capable of receiving DC currents. Connect a (IEEE 802.3at-compliant for EAP220 and 802.3af/at-compliant for EAP210 / EAP320) PSE device (e.g. a PoE-switch) to the Uplink port of EAP210 / EAP220 / EAP320 with the Ethernet cable.

Please follow the steps mentioned below to install the hardware of **EAP747 / EAP750 / EAP757**:

Step 1. Place the EAP747 / EAP750 / EAP757 at the best location. The best location is usually at the center of your intended wireless network. If admin would like to mount the AP on the wall (on a socket), the figure below indicates how the mounting kit can be used on the back of the device. Screw the metal panel to the wall, and then turn the EAP747 / EAP750 / EAP757 clockwise to fasten to the panel. For installation instructions on the Ceiling Mount Kit, please refer to the included Installation Guide.



Step 2. Connect one end of the Ethernet cable to the Uplink port and the other end of the cable to a switch, a router, or a hub. The EAP747 / EAP750 / EAP757 is now connected to your existing wired LAN network.

Step 3. There are two ways to supply power to EAP747 / EAP750 / EAP757

- a) Connect the DC power adaptor to the power jack socket.
- b) The Uplink port is capable of receiving PoE. Connect an IEEE 802.3af/at-compliant PSE device (e.g. a PoE-switch) to the Uplink port of EAP747 / EAP750 / EAP757 with the Ethernet cable.

Please follow the steps mentioned below to install the hardware of **OWL530 / OWL610 / OWL620**:

Step 1. Connect an antenna to the Access Point's antenna connector.

Step 2. Connect the Ethernet Port of OWL530 / OWL610 / OWL620 to the POWER & DATA OUT Port of a 802.3af PSE device.

Step 3. Connect one end of an Ethernet cable to the Data In Port of PSE and the other end to the computer.

Step 4. Power on the PSE in order to supply adequate power to the OWL530 / OWL610 / OWL620.

Now, the Hardware Installation is complete.



- *Please use only the power adapter supplied with the package. Using a different power adapter may damage this system.*
- *To verify the wired connection between the AP and your switch / router / hub, please also check the LED status indicator of the respective network devices.*

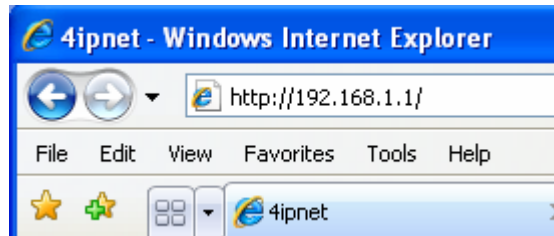
2.4 Access Web Management Interface

4ipnet Access Points support web-based configuration. When hardware installation is complete, the AP can be configured through a PC by using a web browser.

The default values of the AP's LAN IP Address and Subnet Mask are:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0



Example of entering the AP's default IP Address into a web browser

- To access the web management interface (WMI), connect the administrator PC to the LAN port of the AP via an Ethernet cable. Then, set a static IP Address on the same subnet mask as the AP in TCP/IP settings of your PC, such as the following example:

IP Address: 192.168.1.100

Subnet Mask: 255.255.255.0

- ▶ **Note:** Please note that the IP Address used should not overlap with the IP Addresses of any other device within the same network to avoid IP conflict.


- Launch the web browser on your PC and enter the IP Address of the AP (**192.168.1.1**) at the address field, and then press **Enter**. The following Administrator Login Page will appear. Enter "admin" for both the **Username** and **Password** fields, and then click **Login**.




Administrator Login Page

- After a successful login into AP, a **System Overview** page of the Web Management Interface (WMI) will appear.


System Overview

 **System**


| | |
|------------------|--|
| System Name | felix - EAP220 |
| Firmware Version | 1.10.00 |
| Build Number | 1.20-1.6887 |
| Location | |
| Site | EN-A |
| Device Time | 2013/11/25 18:04:13 |
| System Up Time | 6 days, 5:11:27 |
| CPU/RAM Usage | 7.69% / 45.42% <input type="button" value="Plot"/> |

 **Radio Status**

| RF Card | MAC Address | Band | Channel | TX Power |
|-----------|-------------------|-----------|---------|----------|
| RF Card A | 00:1F:D4:94:19:3C | 802.11g+n | 9 | 27 dBm |
| RF Card B | 00:1F:D4:94:19:3D | 802.11a+n | 36 | 23 dBm |


 **LAN Interface**

| | |
|-------------|-------------------|
| MAC Address | 00:1F:D4:94:19:3B |
| IP Address | 10.1.121.21 |
| Subnet Mask | 255.255.0.0 |
| Gateway | 10.1.3.40 |

 **AP Status**

RF Card Name :

| Profile Name | BSSID | ESSID | Security Type | Online Clients | Tun |
|--------------|-------------------|-------------|---------------|----------------|----------------------------------|
| VAP-1 | 00:1F:D4:94:19:3C | 4ipnetAP-A1 | Open | 0 | <input type="button" value="✕"/> |
| VAP-3 | 02:1F:D4:94:19:3C | felix220-a3 | WPA-P... | 1 | <input type="button" value="✕"/> |

 **CAPWAP**

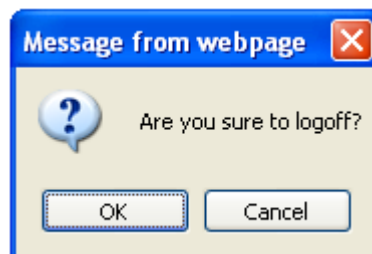
Status

IPv6


Status

The Web Management Interface - System Overview Page

- To logout, simply click on the **Logout** button at the upper right hand corner of the interface to return to the Administrator Login Page. Click **OK** to logout.



Logout Prompt

 For security reasons, it is strongly recommended to change the administrator's password upon the completion of all configuration settings

Please follow the following steps to change the administrator's password:

Home > Utilities > Change Password

Change Password

Name : admin

New Password : *up to 32 characters

Re-enter New Password :

Name : user

New Password : *up to 32 characters

Re-enter New Password :

SAVE **CLEAR**

Change Password Page

- Click on the **Utilities** icon on the main menu, and select the **Change Password** tab.
- Enter the old password and then a new password with a length of up to 32 characters, and retype it in the **Re-enter New Password** field.

Congratulation!

Now, the 4ipnet Access Point is installed and configured successfully.



- *It is strongly recommended to make a backup copy of your configuration settings.*
- *After the AP's network configuration is completed, please remember to change the IP Address of your PC Connection Properties back to its original settings in order to ensure that your PC functions properly in its real network environments.*

3. Connect your AP to your Network


The following instructions depict how to establish the wireless coverage of your network. The AP will connect to the network through its LAN port and provide wireless access to your network.


After having prepared the AP's hardware for configuration, set the TCP/IP settings of administrator's computer to have a static **IP Address** of 192.168.1.10 and **Subnet Mask** of 255.255.255.0.


Step 1: Configuring the AP's System Information


- Enter the AP's default IP Address (**192.168.1.1**) into the URL of a web browser.
- Log in using **Username: admin** and **Password: admin**.


The Web Management Interface will appear as shown below.


System


Wireless


Firewall


Utilities


Status

Overview

Interfaces

Associated Clients

WDS Link Status

Event Log

Monitor

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

System Overview

System

| | |
|------------------|-------------------------------------|
| System Name | felix - EAP220 |
| Firmware Version | 1.10.00 |
| Build Number | 1.20-1.6887 |
| Location | |
| Site | EN-A |
| Device Time | 2013/11/26 09:38:54 |
| System Up Time | 6 days, 20:46:08 |
| CPU/RAM Usage | 3.92% / 45.70% Plot |

Radio Status



| RF Card | MAC Address | Band | Channel | TX Power |
|-----------|-------------------|-----------|---------|----------|
| RF Card A | 00:1F:D4:94:19:3C | 802.11g+n | 9 | 27 dBm |
| RF Card B | 00:1F:D4:94:19:3D | 802.11a+n | 36 | 23 dBm |

LAN Interface

| | |
|-------------|-------------------|
| MAC Address | 00:1F:D4:94:19:3B |
| IP Address | 10.1.121.21 |
| Subnet Mask | 255.255.0.0 |
| Gateway | 10.1.3.40 |

AP Status

RF Card Name : RF Card A

| Profile Name | BSSID | ESSID | Security Type | Online Clients | Tun |
|--------------|-------------------|-------------|---------------|----------------|---|
| VAP-1 | 00:1F:D4:94:19:3C | 4ipnetAP-A1 | Open | 0 |  |
| VAP-3 | 02:1F:D4:94:19:3C | felix220-a3 | WPA-P... | 1 |  |

CAPWAP

Status Disabled

IPv6

Status Disabled

Web Management Interface Main Page (System Overview)

From here, click on the **System** icon to get to the following page. On this Page you can make entries to the **Name**, **Description**, and **Location** fields as well as set the device's time.

General Network Interface Port Management CAPWAP IPv6

Home > System > General

System Information

Name : 4ipnet - EAP220 *

Description :

Location :

Time

Device Time : 2013/11/26 10:12:19

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

NTP Server 1 : time.nist.gov *

NTP Server 2 : pool.ntp.org

System Information Page

There are two methods of setting up the time: Manual (indicated by the option **Set Date & Time**) and NTP.

The default is Manual and requires individual setup every time the system starts up. Simply choose a time zone and set the time accordingly. When it is finished, click **SAVE**.

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

Manually Time Setup

The alternative method is **NTP**. Upon selecting **NTP** under the **Time** field, the configuration changes to allow up to two **NTP** servers. Simply enter a local NTP server's IP Address (if available) or search online for an NTP server nearest to you. Set the time zone and click **SAVE**.

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

NTP Server 1 : *

NTP Server 2 :

NTP Setup

Step 2: Configuring the AP's Network Settings

While still on this Page, click on the **Network Interface** tab to begin configuration of the network settings.

The screenshot shows the 'Network Settings' page in the 4IPNET web interface. The breadcrumb trail is 'Home > System > Network Interface'. The page title is 'Network Settings'. The 'Mode' is set to 'Static' (selected with a radio button), with a 'Renew' button next to it. The 'DHCP' mode is unselected. The 'IP Address' is '192.168.1.1', 'Netmask' is '255.255.255.0', 'Default Gateway' is '192.168.1.254', and 'Primary DNS Server' is '192.168.1.254'. All these fields have a red asterisk next to them, indicating they are required. The 'Alternate DNS Server' field is empty. Below these fields, 'Ethernet IGMP Snooping' is set to 'Enable' (selected with a radio button), and 'Layer2 STP' is set to 'Disable' (selected in a dropdown menu).

Network Settings Page

If the deployment decides that the AP will be getting dynamic IP Addresses from the connected network, set **Mode** to *DHCP*; otherwise, set **Mode** to **Static** and fill in the required fields marked with a red asterisk (**IP Address**, **Netmask**, **Gateway**, and **Primary DNS Server**) with the appropriate values for the network. Click **SAVE** when you are finished to save changes that have been made.

Step 3: Configure the AP's Wireless General Settings

Click on the **Wireless** icon followed by the **General** tab. On this page we need to choose the **Band** and **Channel** that we wish to use.

Home > Wireless > General

General Settings

RF Card Name : RF Card A

Band : 802.11g+802.11n Pure 11n

Short Preamble : Disable Enable

Short Guard Interval : Disable Enable

Channel Width : 20 MHz

Channel : 6

Max Transmit Rate : Auto

Transmit Power : Level 1

ACK Timeout : 0 *(0 - 255, 0:Auto, Unit:4 micro seconds)

Beacon Interval : 100 *(100 - 500ms)

Airtime Fairness : Disable Fair Access Preferred Access

Packet Delay Threshold: 1000 millisecond(s) *(100 - 5000ms, 0:Disable)

Idle Timeout : 300 second(s) *(Larger than 15)

Band Steering : Disable Enable

Aggressive

Interference Detection : Adjacent Channel

Utilization Threshold 0 *(0 - 99, 0:Disable)

Latency 10 second(s) *

Co-Channel

Utilization Threshold 0 *(0 - 99, 0:Disable)

Invalid Packet Rate 90 *(0 - 99)

Latency 10 second(s) *

WME Configuration: [Configure](#)

Transmission Rate Threshold: 0 kbps *(0:Disable)

Wireless General Settings Page

On this page, choose the RF card you would like to set up and select the band in which the AP is to broadcast its signal. The rest of the fields are optional and can be configured at another time. Click **SAVE** if any changes have been made.

-
- **Note:**
- For EAP220, the RF Card A supports only 2.4GHz bands (b/g/n) and RF Card B supports only 5GHz bands (a/n).
 - EAP320 / EAP750 / EAP757 / OWL620 supports both 2.4GHz and 5GHz bands on both RF Cards A and B.
-

Step 4: Configuring Wireless Coverage (VAP-1)

To set up the AP's wireless access, refer to the following VAP-1 configuration (other VAP configuration can refer to the same setup steps as done for VAP-1). Click on the **Overview** tab to proceed.

VAP Overview

RF Card A

| VAP No. | ESSID | State | Security Type | MAC ACL | Advanced Settings |
|---------|--------------|--------------------------|------------------------------|--------------------------|----------------------|
| 1 | 4ipnetAP-A1 | Enabled | Open | Disabled | Edit |
| 2 | 4ipnetAP-A2 | Disabled | Open | Disabled | Edit |
| 3 | 4ipnetAP-A3 | Enabled | WPA-Personal | Disabled | Edit |
| 4 | 4ipnetAP-A4 | Disabled | Open | Disabled | Edit |
| 5 | 4ipnetAP-A5 | Disabled | Open | Disabled | Edit |
| 6 | 4ipnetAP-A6 | Disabled | Open | Disabled | Edit |
| 7 | 4ipnetAP-A7 | Disabled | Open | Disabled | Edit |
| 8 | 4ipnetAP-A8 | Disabled | Open | Disabled | Edit |
| 9 | 4ipnetAP-A9 | Disabled | Open | Disabled | Edit |
| 10 | 4ipnetAP-A10 | Disabled | Open | Disabled | Edit |
| 11 | 4ipnetAP-A11 | Disabled | Open | Disabled | Edit |
| 12 | 4ipnetAP-A12 | Disabled | Open | Disabled | Edit |
| 13 | 4ipnetAP-A13 | Disabled | Open | Disabled | Edit |
| 14 | 4ipnetAP-A14 | Disabled | Open | Disabled | Edit |
| 15 | 4ipnetAP-A15 | Disabled | Open | Disabled | Edit |
| 16 | 4ipnetAP-A16 | Disabled | Open | Disabled | Edit |

Virtual AP Overview Page

On this page click the hyperlink in the row and column that corresponds with VAP-1's *State*. This will bring up the following page.

The screenshot displays the configuration interface for an Enterprise Access Point. At the top, there are navigation buttons for System, Wireless, Firewall, Utilities, and Status. Below these are tabs for VAP Overview, General, VAP Config, Security, Repeater, Advanced, and Access Control. The main content area shows the 'VAP Configuration' page for 'RF Card A : VAP-1'. The configuration includes:

- Profile Name:** RF Card A : VAP-1 (selected from a dropdown menu)
- VAP:** Disable Enable
- Profile Name:** VAP-1 (text input field)
- ESSID:** 4ipnetAP-A1 (text input field)
- VLAN ID:** Disable Enable
- VLAN ID:** (text input field) *(1 - 4094)
- CAPWAP Tunnel Interface:**

At the bottom of the configuration area, there are two buttons: **SAVE** and **CLEAR**.

VAP Configuration Page (RF Card A : VAP-1 shown)

The desired VAP profile can be selected from the drop-down menu of Profile Name and VAP-1 configuration will serve as an example for all other VAPs. Before proceeding further, please make sure that the VAP field is marked *Enable*; afterwards, enter an ESSID to represent the WLAN associated with AP's VAP-1. It is suggested that Profile Name is used to describe what this particular VAP will be used for; otherwise, leave it as default. VLAN ID can be chosen at another time. Click *SAVE* to save all changes up to this point and *Reboot* the system to apply these revised settings.

Congratulations!

After reboot, the AP can start to operate with these revised settings.

4. Adding Virtual Access Points

The AP possesses the feature of multi-ESSID; namely, it can behave as multiple virtual access points, providing different levels of services from the same physical AP device.

Please click on the **Wireless** icon to review the **VAP Overview** page.

VAP Overview

RF Card A

| VAP No. | ESSID | State | Security Type | MAC ACL | Advanced Settings |
|---------|--------------|----------|---------------|----------|-------------------|
| 1 | 4ipnetAP-A1 | Enabled | Open | Disabled | Edit |
| 2 | 4ipnetAP-A2 | Disabled | Open | Disabled | Edit |
| 3 | 4ipnetAP-A3 | Enabled | WPA-Personal | Disabled | Edit |
| 4 | 4ipnetAP-A4 | Disabled | Open | Disabled | Edit |
| 5 | 4ipnetAP-A5 | Disabled | Open | Disabled | Edit |
| 6 | 4ipnetAP-A6 | Disabled | Open | Disabled | Edit |
| 7 | 4ipnetAP-A7 | Disabled | Open | Disabled | Edit |
| 8 | 4ipnetAP-A8 | Disabled | Open | Disabled | Edit |
| 9 | 4ipnetAP-A9 | Disabled | Open | Disabled | Edit |
| 10 | 4ipnetAP-A10 | Disabled | Open | Disabled | Edit |
| 11 | 4ipnetAP-A11 | Disabled | Open | Disabled | Edit |
| 12 | 4ipnetAP-A12 | Disabled | Open | Disabled | Edit |
| 13 | 4ipnetAP-A13 | Disabled | Open | Disabled | Edit |
| 14 | 4ipnetAP-A14 | Disabled | Open | Disabled | Edit |
| 15 | 4ipnetAP-A15 | Disabled | Open | Disabled | Edit |
| 16 | 4ipnetAP-A16 | Disabled | Open | Disabled | Edit |

VAP Overview Page

To proceed with specific VAP configuration, click on the corresponding cell in the **State** column and row of the VAP; the particular VAP's Configuration page will then appear for further configuration.

The screenshot displays the configuration interface for a VAP (Virtual Access Point). At the top, there are navigation tabs for System, Wireless, Firewall, Utilities, and Status. Below these are sub-tabs for VAP Overview, General, VAP Config, Security, Repeater, Advanced, and Access Control. The main content area is titled "VAP Configuration" and includes the following fields:

- Profile Name :** RF Card A : VAP-1 (dropdown menu)
- VAP :** Disable Enable
- Profile Name :** VAP-1 (text input)
- ESSID :** 4ipnetAP-A1 (text input)
- VLAN ID :** Disable Enable
- VLAN ID :** (text input) *(1 - 4094)
- CAPWAP Tunnel Interface :**

At the bottom of the configuration area, there are two buttons: **SAVE** and **CLEAR**.

VAP Configuration Page (VAP-1 shown)

Please select the desired RF card and VAP profile from the drop-down menu of Profile Name. Choose **Enable** for the **VAP** field. Pick a descriptive **Profile Name** and an appropriate **ESSID** for clients to associate to. A **VLAN ID** can be provided to indicate the traffic through this particular VAP. It may allow further management/control (e.g. access rights and Internet usage, etc) of each VAP with a management gateway. Click **SAVE** and then **Reboot** for the changes to take effect.

5. Securing the AP

Different VAP may require different levels of security. These instructions will guide the user through setting up different types of security for a particular VAP. Simply repeat the following steps for other VAP with security requirement.

Step 1: Ensure the intended VAP is Enabled

VAP Overview

RF Card A

| VAP No. | ESSID | State | Security Type | MAC ACL | Advanced Settings |
|---------|--------------|----------|---------------|----------|-------------------|
| 1 | 4ipnetAP-A1 | Enabled | Open | Disabled | Edit |
| 2 | 4ipnetAP-A2 | Disabled | Open | Disabled | Edit |
| 3 | 4ipnetAP-A3 | Enabled | WPA-Personal | Disabled | Edit |
| 4 | 4ipnetAP-A4 | Disabled | Open | Disabled | Edit |
| 5 | 4ipnetAP-A5 | Disabled | Open | Disabled | Edit |
| 6 | 4ipnetAP-A6 | Disabled | Open | Disabled | Edit |
| 7 | 4ipnetAP-A7 | Disabled | Open | Disabled | Edit |
| 8 | 4ipnetAP-A8 | Disabled | Open | Disabled | Edit |
| 9 | 4ipnetAP-A9 | Disabled | Open | Disabled | Edit |
| 10 | 4ipnetAP-A10 | Disabled | Open | Disabled | Edit |
| 11 | 4ipnetAP-A11 | Disabled | Open | Disabled | Edit |
| 12 | 4ipnetAP-A12 | Disabled | Open | Disabled | Edit |
| 13 | 4ipnetAP-A13 | Disabled | Open | Disabled | Edit |
| 14 | 4ipnetAP-A14 | Disabled | Open | Disabled | Edit |
| 15 | 4ipnetAP-A15 | Disabled | Open | Disabled | Edit |
| 16 | 4ipnetAP-A16 | Disabled | Open | Disabled | Edit |

VAP Overview Page

On the **VAP Overview** page, check the table to confirm the VAP State. If it is **Enabled**, skip to **Step 2**. If not, click on to proceed with **VAP Configuration** for that particular VAP.

Home > Wireless > VAP Config

VAP Configuration

Profile Name : RF Card A : VAP-1

VAP : Disable Enable

Profile Name : VAP-1

ESSID : 4ipnetAP-A1

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

SAVE CLEAR

VAP Configuration Page (RF Card A : VAP-1 as shown for example)

Select **Enable** for the **VAP** field and click **SAVE**. Click the **Overview** tab to return to the previous table to begin the next step.

Step 2: Configure Security Settings for your VAP

The following instructions will guide the user to set up wireless security with a specific VAP. If only restricted access of certain MAC addresses is desired, skip to Step3. MAC restriction can be coupled with wireless security to provide extra protection.

First, click on the corresponding cell in the column labeled **Security Type**. This hyperlink will direct the user to the following **Security Settings** page.

Home > Wireless > Security

Security Settings

Profile Name : RF Card A : VAP-1

Security Type :
Open
WEP
802.1X
WPA-Personal
WPA-Enterprise

CLEAR

Security Settings Page (RF Card A : VAP-1 shown)

Select the desired **Security Type** from the drop-down menu, which includes **Open**, **WEP**, **802.1X**, **WPA-Personal**, and **WPA-Enterprise**.



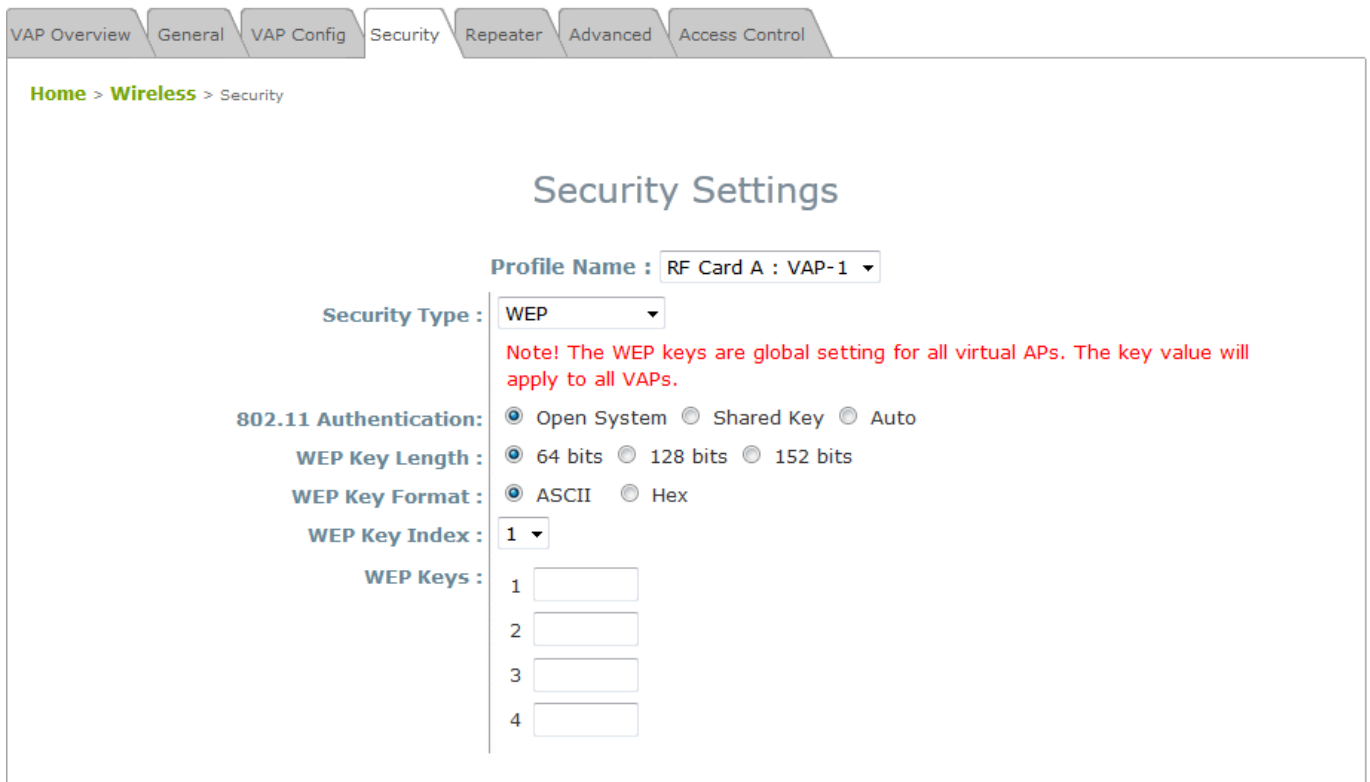
- 802.11n band does not support WEP nor WPA-PSK running TKIP. When the Security Type is set as such, the wireless link is only able to run at maximum 54Mbps.

- **Open:** Authentication is not required and data is not encrypted during transmission when this option is selected. This is the default setting as shown in the following figure.



Security Settings: None

- **WEP:** WEP (Wired Equivalent Privacy) is a data encryption mechanism with key length selected from 64-bit, 128-bit, or 152-bit.



Security Settings: WEP

- **802.11 Authentication:** Select from **Open System**, **Shared Key**, or **Auto**.

- **WEP Key Length:** Select a key length from **64-bit**, **128-bit**, **152-bit**.
 - **WEP Key Format:** Select from **ASCII** or **Hex** format for the WEP key.
 - **WEP Key Index:** Select a key index from 1 through 4. The WEP key index is a number that specifies which WEP key is used for the encryption of wireless frames during data transmission.
 - **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.
- **802.1X:** When **802.1X Authentication** is selected, RADIUS authentication and enhanced dynamic WEP are provided.

VAP Overview
General
VAP Config
Security
Repeater
Advanced
Access Control

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

Security Settings

Profile Name : RF Card A : VAP-1 ▼

Security Type : 802.1X ▼

Dynamic WEP : Disable Enable

WEP Key Length : 64 bits 128 bits

Rekeying Period : second(s)

Primary RADIUS Server :

Host : *(Domain Name / IP Address)

Authentication Port : *

Secret Key : *

Accounting Service : Disable Enable

Accounting Port : *

Accounting Interim Update Interval : second(s)*

Secondary RADIUS Server :

Host : (Domain Name / IP Address)

Authentication Port :

Secret Key :

Accounting Service : Disable Enable

Accounting Port :

Accounting Interim Update Interval : second(s)

Security Settings: 802.1X Authentication

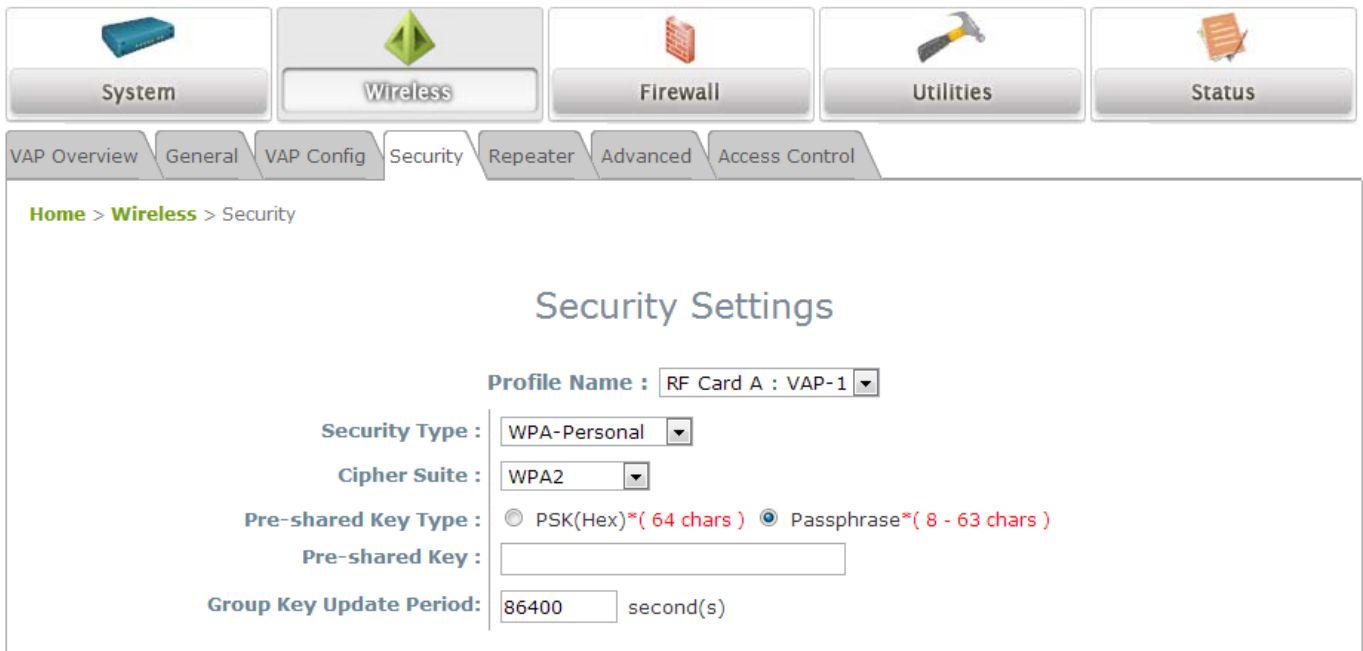
- **Dynamic WEP Settings:**
 - **Dynamic WEP:** For 802.1X security type, Dynamic WEP is always enabled to automatically generate WEP keys for encryption.
 - **WEP Key Length:** Select a key length from **64-bits** or **128-bits**.
 - **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in

seconds.

➤ **RADIUS Server Settings (A redundant server can also be added to the system):**

- **Host:** Enter the IP address or domain name of the RADIUS server.
- **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
- **Secret Key:** The secret key for the system to communicate with the RADIUS server.
- **Accounting Service:** Enabling this option allows accounting of login and logouts through the RADIUS server.
- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

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



Home > Wireless > Security

Security Settings

Profile Name : RF Card A : VAP-1

Security Type : WPA-Personal

Cipher Suite : WPA2

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


Pre-shared Key :


Group Key Update Period: second(s)


Security Settings: WPA-Personal


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


- **WPA-Enterprise:** Authenticates users by RADIUS and provides WPA data encryption.


System


Wireless


Firewall


Utilities


Status

VAP Overview
General
VAP Config
Security
Repeater
Advanced
Access Control

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

Security Settings

Profile Name : RF Card A : VAP-1 ▾

Security Type : WPA-Enterprise ▾

Cipher Suite : WPA2 ▾

Group Key Update Period: 86400 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: second(s)

Security Settings: WPA-Enterprise

➤ **WPA Settings:**

- **Cipher Suite:** Select an encryption method from **WPA2** or **WPA2/WPA**.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

➤ **RADIUS Server Settings:**

- **Host:** Enter the IP address or domain name of the RADIUS server.
- **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
- **Secret Key:** The secret key for the system to communicate with the RADIUS server.
- **Accounting Service:** Enabling this option allows accounting of login and logouts through the RADIUS server.
- **Accounting Port:** The port number used by the RADIUS server for accounting purposes.

Specify a port number or use the default, 1813.

- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

When these configurations are finished and MAC restriction is not needed, click **SAVE** and **Reboot** the system. Otherwise, click on the **Overview** tab and proceed to the next step.

Step 3: Configuring MAC ACL (Access Control List)

Clicking on the hyperlink corresponding with intended VAP in the **MAC ACL** column will bring the user to the **Access Control Settings** page.

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Access Control

Access Control Settings

Profile Name : RF Card A : VAP-1

Maximum Number of Clients : 32 *(Range: 1 ~ 256 per system)

Access Control Type : Disable Access Control

Access Control Settings Page

Please choose among **Disable**, **Allow**, **Deny**, and **RADIUS ACL** from the drop-down menu of **Access Control Type**.

- 1) **Disable Access Control:** This means that there is no restriction for client devices to access the system.
- 2) **MAC ACL Allow List:** This means that only the client devices (identified by their MAC addresses) listed in the **Allow List** (“allowed MAC addresses”) are granted with access to the system. The administrator can temporarily block any allowed MAC address by checking **Disable**, until the administrator renews the listed MAC.

Access Control Settings

Profile Name : RF Card A : VAP-1

Maximum Number of Clients : 32 *(Range: 1 ~ 256 per system)

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 |
| 4 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 5 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 6 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 7 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 8 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 9 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 10 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |

First Prev Next Last (total: 100)

MAC ACL Allow List



An empty Allow List means that there are no allowed MAC addresses. Make sure at least the MAC of the modifying system is included (e.g. network administrator's computer).

- MAC ACL Deny List:** This means that all client devices are granted with access to the system except those listed in the **Deny List** ("denied MAC addresses"). The administrator can allow any denied MAC address to connect to the system temporarily by checking **Enable**.

Access Control Settings

Profile Name : RF Card A : VAP-1 ▾

Maximum Number of Clients : *(Range: 1 ~ 256 per system)

Access Control Type : MAC ACL Deny List ▾

| No. | MAC Address | State |
|-----|----------------------|---|
| 1 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 2 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 3 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 4 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 5 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 6 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 7 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 8 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 9 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 10 | <input type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |

[First](#) [Prev](#) [Next](#) [Last](#) (total: 100)

MAC ACL Deny List

RADIUS ACL: Authenticate incoming MAC addresses by an external RADIUS server. When RADIUS ACL is selected, all incoming MAC addresses will be authenticated by an external RADIUS server. Please note that each VAP MAC ACL and its security type (shown on the **Security Settings** page) share the same RADIUS configuration.

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Access Control

Access Control Settings

Profile Name : RF Card A : VAP-1 ▼

Maximum Number of Clients : *(Range: 1 ~ 256 per system)

Access Control Type : RADIUS ACL ▼

Primary RADIUS Server : Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.

Host: *(Domain Name / IP Address)Authentication Port: *(1 - 65535)Secret Key: *

Secondary RADIUS Server :

Host: Authentication Port: Secret Key: **RADIUS ACL**Click **SAVE** and **Reboot** upon completing the related configurations to take effect.

6. Creating a WDS Bridge between two APs

WDS link creation is convenient for extending network coverage where running wires is not an option, effectively transferring the traffic to the other end of WLAN/LAN through the AP. Since this is a peer to peer connection, both APs will be configured the same way.

Step 1: Make sure the Band and Channel are matched between the WDS peers

In order to create a valid WDS link, the two APs must be configured to use the same channel and band for their wireless settings. Click the **Wireless** icon and then **General** tab to go to the following page.

VAP Overview
General
VAP Config
Security
Repeater
Advanced
Access Control

Home > Wireless > General

General Settings

RF Card Name : RF Card A

| | |
|--------------------------------------|--|
| Band : | 802.11g+802.11n <input type="checkbox"/> Pure 11n |
| Short Preamble : | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| Short Guard Interval : | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| Channel Width : | 20 MHz |
| Channel : | 6 |
| Max Transmit Rate : | Auto |
| Transmit Power : | Level 1 |
| ACK Timeout : | 0 <small>*(0 - 255, 0:Auto, Unit:4 micro seconds)</small> |
| Beacon Interval : | 100 <small>*(100 - 500ms)</small> |
| Airtime Fairness : | <input checked="" type="radio"/> Disable <input type="radio"/> Fair Access <input type="radio"/> Preferred Access |
| Packet Delay Threshold : | 1000 millisecond(s) <small>*(100 - 5000ms, 0:Disable)</small> |
| Idle Timeout : | 300 second(s) <small>*(Larger than 15)</small> |
| Band Steering : | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| | <input type="checkbox"/> Aggressive |
| Interference Detection : | Adjacent Channel |
| | Utilization Threshold 0 <small>*(0 - 99, 0:Disable)</small> |
| | Latency 10 second(s) * |
| | Co-Channel |
| | Utilization Threshold 0 <small>*(0 - 99, 0:Disable)</small> |
| | Invalid Packet Rate 90 <small>*(0 - 99)</small> |
| | Latency 10 second(s) * |
| WME Configuration : | Configure |
| Transmission Rate Threshold : | 0 kbps <small>*(0:Disable)</small> |

Wireless General Settings Page

Please make sure both APs are using the same **Band** and **Channel** in order to establish a successful WDS link. Click **SAVE** if any changes have been made.

Step 2: Prevent Loops when Connecting Multiple APs

When many APs are linked in this manner, undesired loops may form to lower overall WLAN performance. To prevent such occurrence, please make sure Layer 2 STP is enabled.

To turn on this feature, please click on the **System** icon and the **Network Interface** tab.

The screenshot shows the 'Network Settings' page with the following configuration:

- Mode:** Static DHCP
- IP Address:** 192.168.1.1 *
- Netmask:** 255.255.255.0 *
- Default Gateway:** 192.168.1.254 *
- Primary DNS Server:** 192.168.1.254 *
- Alternate DNS Server:** (empty)
- Ethernet IGMP Snooping:** Disable Enable
- Layer2 STP:** Disable

Network Settings Page

Please select **Enable** in the field labeled **Layer2 STP**. This will prevent data from looping or creating a broadcast storm. Click **SAVE** when completed, and then **Reboot** to allow updated settings to take effect.

Step 3: Building the WDS Link

To extend the wireless coverage, each RF card supports up to 8 WDS links for connecting wirelessly to other WDS-capable APs (peer APs). By default, all WDS profiles are disabled.

System Wireless Firewall Utilities Status

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Repeater Config

Repeater Settings

Repeater Type : WDS

WDS Profile : RF Card A : WDS Link 1

WDS : Disable

MAC Address :

Security type : None

CAPWAP Tunnel Interface :

1. Click on the **Wireless** button on the main menu.
2. Select the **Repeater Settings** tab.
3. Choose **WDS** as the **Repeater Type**.
4. Choose the desired WDS profile:
 - (a) Enable **WDS**.
 - (b) Enter the **MAC Address** (peer AP) and then Click **SAVE**.

If you are using another 4ipnet APs as the peer AP, simply repeat the above-mentioned steps to configure another peer AP(s).

►► **Note:**

- To support traffic with unlimited VLAN tags via WDS, EAP220 has to be set to Tag-Based Mode.
- Cross brand/model WES/WDS link performance may vary with different Access Points depending on hardware compatibility.

7. Web Management Interface Configuration

This chapter will guide the user through the AP's detailed settings. The following table shows all the User Interface (UI) functions of 4ipnet's Enterprise Access Points. The Web Management Interface (WMI) is the page where the status is displayed, control is issued and parameters are configured. In the Web Management Interface; there are two main interface areas: **Main Menu** and **Working Area**. The **Working Area** occupies the major area of the WMI, displayed in the center of the interface. It is also referred to as the configuration page. The **Main Menu**, on the top of the WMI, allows the administrator to traverse to various management functions of the system. The management functions are grouped into branches: **System**, **Wireless**, **Firewall**, **Utilities**, and **Status**.

Table 1 4ipnet Access Points' Function Organization

| OPTION | FUNCTION |
|------------------|--------------------|
| System | General |
| | Network Interface |
| | Port |
| | Management |
| | CAPWAP |
| | IPv6 |
| Wireless | VAP Overview |
| | General |
| | VAP Config |
| | Security |
| | Repeater |
| | Advanced |
| | Access Control |
| Firewall | Firewall List |
| | Service |
| | Advanced |
| Utilities | Change Password |
| | Backup & Restore |
| | System Upgrade |
| | Reboot |
| | Upload Certificate |
| | Channel Analysis |
| | Background Scan |

| | |
|---------------|--------------------|
| Status | Overview |
| | Interfaces |
| | Associated Clients |
| | WDS Link Status |
| | Event Log |
| | Monitor |

» Note:

On each configuration page, you may click **SAVE** to save the changes of your configured settings, but you must reboot the system for the changes to take effect. After clicking **SAVE**, the following message will appear: "**Some modification has been saved and will take effect after Reboot.**"

All online users will be disconnected during reboot or restart.

7.1 System

Upon clicking the **System** icon, users can utilize this section for general configurations of the devices (e.g. Time Setup, Network Configurations, and System Logs). This section includes the following functions:

General, Network Interface, Port, Management, CAPWAP and IPv6.

7.1.1 General

General Network Interface Port Management CAPWAP IPv6

Home > System > General

System Information

Name : OWL620

Description :

Location :

Time

Device Time : 2012/05/08 17:11:45

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

SAVE CLEAR

System Information Page

- **System Information**
 - For maintenance purposes, it is highly recommended to have the following information stated as clearly as possible:
 - **Name:** The system name used to identify this system.
 - **Description:** Further information about the system (e.g. device model, firmware version, and active date).
 - **Location:** The information on geographical location of the system for the administrator to locate the system easily.
- **Time**
 - **Device Time:** Display the current time of the system.
 - **Time Zone:** Select an appropriate time zone from the drop-down list box.
 - **Time:** Synchronize the system time by reachable NTP servers or manual setup.

1) Enable NTP:

By selecting **Enabled NTP**, the AP can synchronize its system time with the NTP server automatically. When this method is chosen, at least one NTP server's IP address or domain name must be provided.

Time

Device Time : 2000/01/03 04:32:49

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

NTP Server 1 : *

NTP Server 2 :

NTP Time Configuration Fields

Generally, networks should have a common NTP server (internal or external). If there isn't, locate a nearby NTP server on the web.

2) Manually set up:

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

Time

Device Time : 2000/01/03 04:32:49

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

Set Date : ---- Year -- Month -- Day

Set Time : -- Hour -- Min -- Sec

Manual Time Configuration Fields

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



Unless Internet connection or NTP becomes unavailable, it is recommended to use NTP server for time synchronization because system time needs to be reconfigured upon reboot.

7.1.2 Network Interface

On this page, the network settings of the device can be configured; fields with a red asterisk (i.e. **IP Address, Netmask, Default Gateway, and Primary DNS Server**) are mandatory.

Network Settings Page

- **Mode:** Determine the way to obtain the IP address, by **DHCP** or **Static**.
 - **Static:** The administrator can manually set up the static LAN IP address. All required fields are marked with a red asterisk.
 - **IP Address:** The IP address of the LAN port.
 - **Netmask:** The Subnet mask of the LAN port.
 - **Default Gateway:** The Gateway IP address of the LAN port.
 - **Primary DNS Server:** The IP address of the primary DNS (Domain Name System) server.
 - **Alternate DNS Server:** The IP address of the substitute DNS server.
 - **DHCP:** This configuration type is applicable when the system is connected to a network with the presence of a DHCP server; all related IP information required will be provided by the DHCP server automatically.
- **Ethernet IGMP Snooping:** When Enabled, the switch forwards traffic IGMP packets are transferred via the Access Point's network interface and the IP multicast host. Registration information is recorded and sorted into multicast groups. The internal switch forwards traffic only to those ports that request multicast traffic. Adversely, without IGMP snooping, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.
- **Layer 2 STP:** If the AP is set up to bridge other network components, this option can be enabled to

prevent undesired loops because a broadcasting storm may occur in a multi-switch environment where broadcast packets are forwarded in an endless loop between switches. Moreover, a broadcast storm may consume most of the available system resources in addition to available bandwidth. Thus, enabling the Layer 2 STP can lower such undesired occurrence and derive the best available data path for network communication. The AP also supports RSTP Operation. Configurable parameters include **Bridge Priority**, **Hello Time**, **Max Age**, and **Forward Delay**. Please refer to IEEE standards for recommended parameter values.

7.1.3 Port

The physical Ethernet ports of the AP can be configured to append a VLAN tag for upstream delivery.

Home > System > Port Config

Port Configuration

Switch Mode : Port-Based Tag-Based

Port : LAN1

VLAN ID : Disable Enable
 VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

TIP:
 *For tunneled LAN ports, Service Zones to VLAN ID Mappings are:
 Default Zone = 1000, SZ1 = 1001, SZ2 = 1002, SZ3 = 1003, SZ4 = 1004, SZ5 = 1005, SZ6 = 1006, SZ7 = 1007, SZ8 = 1008.
 *LAN port traffic tunneled back to a WHG Controller without a VLAN ID will be suspended from access to any network service.

- ***Switch Mode:** Select Port-Based to set VLAN IDs on physical LAN ports. Select Tag-Based for uplink traffic to recognize unlimited VLAN tags.
- **VLAN ID:** Enable selected implies that network traffic sent upstream from this LAN port will be tagged with the VLAN ID configured in the field below. Disable selected implies that traffic from this LAN port will not be tagged with a VLAN ID.
- **CAPWAP Tunnel Interface:** Select a LAN, VAP or WDS interface to designate its traffic to pass through the CAPWAP Tunnel established between the AP and the controller. For network interfaces that are unchecked, their traffic will be forwarded locally into the internet if this AP is deployed remotely on the WAN side of a controller.
- The '**TIP**' in red at the bottom of the page explains that each service zone, from default to Service Zone 8, has its fixed, pre-determined VLAN ID number when utilizing CAPWAP. Admin needs to enter one of the numbers in order to direct traffic back to a certain Service Zone.

**Applicable to EAP220 only. When Port-Based is selected and VLAN IDs are set on physical ports, the uplink traffic recognizes ONLY the VLANs set, all other VLAN tags will be dropped (such as traffic from an Access Point linked via WDS).*

7.1.4 Management

The management services (e.g. **VLAN for Management**, **SNMP**, and **System log**) can be configured here.

General
Network Interface
Port
Management
CAPWAP
IPv6

[Home](#) > [System](#) > Management Services

Management Services

VLAN for Management:

SNMP Configuration :

System Log :

Management IP List:

Disable
 Enable
 VLAN ID : *(1 - 4094)

Disable
 Enable
 Community String :
 Read :
 Write :

Trap : Disable
 Enable
 Server IP :

Disable
 Enable
 SYSLOG Server IP :
 Server Port :
 SYSLOG Level :

Management Services Page

- VLAN for Management:** When this is enabled, management traffic from the system will be tagged with a VLAN ID. In other words, administrator who wants to access the WMI must send management traffic with the same VLAN ID such as connecting to a specific VAP with the same VLAN ID. Enter a value between 1 and 4094 for the VLAN ID if the option is enabled.

► **Note:** Management is done without the utilization of VLAN IDs on selected AP models.

- **SNMP Configuration:** By enabling the SNMP function, the administrator can obtain the system information remotely.

SNMP Configuration :

Disable Enable

Community String :

Read :

Write :

Trap : Disable Enable

Server IP :

SNMP Configuration Fields

- **Enable/ Disable:** *Enable* or *Disable* this function.
- **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system.
 - **Read:** Enter the community string to access the MIB with Read privilege.
 - **Write:** Enter the community string to access the MIB with Write privilege.
- **SNMPv3 User List:** The system allows 5 SNMP Users with Read or Read & Write Access. Determine the Name and Authentication Password on the SNMP Account List.

SNMP Account List

| SNMP User List | | | |
|----------------------|------------------|---------------------|-------------------------|
| Name | Access Authority | Authentication Type | Authentication Password |
| <input type="text"/> | Read Only ▾ | MD5 ▾ | <input type="text"/> |
| <input type="text"/> | Read Only ▾ | MD5 ▾ | <input type="text"/> |
| <input type="text"/> | Read Only ▾ | MD5 ▾ | <input type="text"/> |
| <input type="text"/> | Read Only ▾ | MD5 ▾ | <input type="text"/> |
| <input type="text"/> | Read Only ▾ | MD5 ▾ | <input type="text"/> |

- **Trap:** When enabled, events on Cold Start, Interface UP & Down, and Association & Disassociation can be reported to an assigned server.
 - **Enable/ Disable:** *Enable* or *Disable* this function.
 - **Server IP Address:** Enter the IP address of the assigned server that will receive the trap report.

- **System Log:** When this function is enabled, specify an external SYSLOG server to accept SYSLOG messages from the system remotely.

System Log : Disable Enable

SYSLOG Server IP :

Server Port :

SYSLOG Level : ▼

System Log Fields

- **Enable/ Disable:** *Enable* or *Disable* this function.
- **SYSLOG Server IP:** The IP address of the Syslog server that will receive the reported events.
- **Server Port:** The port number of the Syslog server.
- **SYSLOG Level:** Select the desired level of received events from the drop-down menu.

7.1.5 CAPWAP

CAPWAP is a standard interoperable protocol that enables a controller to manage a collection of wireless access points. There are 5 methods of auto AP discovery, namely DNS SRV, DHCP option, Broadcast, Multicast, and Static. Please refer to the Web page at **System > CAPWAP**.

- **CAPWAP:** The CAPWAP feature can be turned on by selecting “Enable” or turned off by selecting “Disable”
- **Certificate Date Check:** To enable this item, select **Enable** and click **Manage Certificates** to enter the **Upload Certificate** page. Please refer to the section **7.4.4. Upload Certificate**.
- **DNS SRV Discovery:** Using DNS SRV to discover access controller.
 - **Domain Name Suffix:** Enter the suffix of the access controller, such as example.com.
- **DHCP Option Discovery:** Using DHCP option to discover access controller.
- **Broadcast Discovery:** Using Broadcast to discover access controller.
- **Multicast Discovery:** Using muticast to discover access controller.
- **Static Discovery:** Using Static approach to discover access controller.
 - **AC Address:** The IP address of the access controller. If it can not discover the first AC, it will try to discover the second AC.

7.1.6 IPv6

The 4ipnet Access Point supports IPv6 and IPv4 dual stack addressing capability. IPv6 by default is disabled but it can be enabled on this tab page.

General Network Interface Port Management CAPWAP IPv6

Home > System > IPv6 Configuration

IPv6 Configuration

Status : Disable Enable

Mode : Static DHCP

SAVE **CLEAR**

Mode: There are two options for acquiring an IPv6 address for this device.

- **Static:** Configuring IPv6 address manually via this option if you have already acquired a permanent IPv6 address for operation.
- **DHCP:** Acquire IPv6 address automatically from upstream server.

7.2 Wireless

This section includes the following functions: **VAP Overview**, **General**, **VAP Configuration**, **Security**, **Repeater**, **Advanced**, and **Access Control**. The 4ipnet Access Point supports up to eight Virtual Access Points (VAPs) per RF card. Each VAP can have its own settings (e.g. ESSID, VLAN ID, security settings, etc.). With such VAP capabilities, different levels of service can be configured to meet network requirements.

7.2.1 VAP Overview

An overall status is collected on this page, including **ESSID**, **State**, **Security Type**, **MAC ACL**, and **Advanced Settings**, where the AP features 16 VAPs per radio with respective settings. In this table, please click on the hyperlink to further configure each individual VAP.

VAP Overview

RF Card A

| VAP No. | ESSID | State | Security Type | MAC ACL | Advanced Settings |
|---------|--------------|--------------------------|------------------------------|--------------------------|----------------------|
| 1 | 4ipnetAP-A1 | Enabled | Open | Disabled | Edit |
| 2 | 4ipnetAP-A2 | Disabled | Open | Disabled | Edit |
| 3 | 4ipnetAP-A3 | Enabled | WPA-Personal | Disabled | Edit |
| 4 | 4ipnetAP-A4 | Disabled | Open | Disabled | Edit |
| 5 | 4ipnetAP-A5 | Disabled | Open | Disabled | Edit |
| 6 | 4ipnetAP-A6 | Disabled | Open | Disabled | Edit |
| 7 | 4ipnetAP-A7 | Disabled | Open | Disabled | Edit |
| 8 | 4ipnetAP-A8 | Disabled | Open | Disabled | Edit |
| 9 | 4ipnetAP-A9 | Disabled | Open | Disabled | Edit |
| 10 | 4ipnetAP-A10 | Disabled | Open | Disabled | Edit |
| 11 | 4ipnetAP-A11 | Disabled | Open | Disabled | Edit |
| 12 | 4ipnetAP-A12 | Disabled | Open | Disabled | Edit |
| 13 | 4ipnetAP-A13 | Disabled | Open | Disabled | Edit |
| 14 | 4ipnetAP-A14 | Disabled | Open | Disabled | Edit |
| 15 | 4ipnetAP-A15 | Disabled | Open | Disabled | Edit |
| 16 | 4ipnetAP-A16 | Disabled | Open | Disabled | Edit |

VAP Overview Page

- **State:** The hyperlink showing **Enable** or **Disable** links to the **VAP Configuration** page.

VAP – State Page

- **Security Type:** The hyperlink showing the security type links to the **Security Settings** Page.

VAP – Security Type Page

- **MAC ACL:** The hyperlink showing **Allow** or **Disable** links to the **Access Control Settings** Page.


VAP – MAC ACL Page


- **Advanced Settings:** The advanced settings hyperlink links to the **Advanced Wireless Settings** Page.


VAP – Advanced Settings Page


7.2.2 General


AP's general wireless settings can be configured here:


System


Wireless


Firewall


Utilities


Status

VAP Overview

General

VAP Config

Security

Repeater

Advanced

Access Control

Home > Wireless > General

General Settings

RF Card Name : RF Card A ▼

Band : 802.11g+802.11n ▼ Pure 11n

Short Preamble : Disable Enable

Short Guard Interval : Disable Enable

Channel Width : 20 MHz ▼

Channel : 6 ▼

Max Transmit Rate : Auto ▼

Transmit Power : Level 1 ▼

ACK Timeout : 0 *(0 - 255, 0:Auto, Unit:4 micro seconds)

Beacon Interval : 100 *(100 - 500ms)

Airtime Fairness : Disable Fair Access Preferred Access

Packet Delay Threshold: 1000 millisecond(s) *(100 - 5000ms, 0:Disable)

Idle Timeout : 300 second(s) *(Larger than 15)

Band Steering : Disable Enable

Aggressive

Interference Detection :

Adjacent Channel

Utilization Threshold 0 *(0 - 99, 0:Disable)

Latency 10 second(s) *

Co-Channel

Utilization Threshold 0 *(0 - 99, 0:Disable)

Invalid Packet Rate 90 *(0 - 99)

Latency 10 second(s) *

WME Configuration:

Transmission Rate Threshold: 0 kbps *(0:Disable)

AP General Settings Page

- **RF Card Name:** Select one RF card for further configuration.
- **Band:** Select an appropriate wireless band: **802.11a**, **802.11b**, **802.11g**, **802.11b+802.11g**, **802.11g+802.11n**, **802.11a+802.11n** or select **Disable** if the wireless function is not required.
 - **Pure 11n:** Enable 802.11n network only.

- **Short Preamble:** The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select **Enable** to use Short Preamble or **Disable** to use Long Preamble with a 128-bit synchronization field.
- **Short Guard Interval (available when Band is 802.11g+802.11n or 802.11a+802.11n):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. In order to further boost throughput with **802.11n**, short guard interval is half of what it used to be; please select **Enable** to use Short Guard Interval or **Disable** to use normal Guard Interval.
- **Channel Width (available when Band is 802.11g+802.11n or 802.11a+802.11n):** Double channel bandwidth to 40 MHz to enhance throughput.
- **Channel:** Select the appropriate **channel** from the drop-down menu to correspond with your network settings, for example, Channel 1-11 is available in North American and Channel 1-13 in Europe, or choose the default **6**.
- **Max Transmit Rate:** The maximum wireless transmit rate can be selected from the drop-down menu. The system will use the highest possible rate when **Auto** is selected. Please note that MCS0 ~ MCS15 are transmit rates only for n bands.
- **Transmit Power:** The signal strength transmitted from the system can be selected by Levels. Each Level signifies a decrement of 1dBm from the highest power. **Level 1 is the actual highest power, Level 2 is the highest power minus 1dBm, so on and so forth.**
- **ACK Timeout:** It indicates a period of time when the system waits for an Acknowledgement frame sent back from a station without retransmission. In other words, upon timeout, if the Acknowledgement frame is still not received, the frames will be retransmitted. This option can be used to tune network performance for extended coverage. For regular indoor deployments, please keep the default setting.
- **Beacon Interval (ms):** The entered amount of time indicates how often the beacon signal will be sent from the access point.
- **Airtime Fairness:** Networks often are backward compatible, supporting 802.11b and/or 802.11g devices. But when these devices occupy airtime, throughput for 802.11n devices is affected. When enabled, this feature ensures all devices with different band compatibilities have the same air time. This feature is ideal for networks with devices supporting different bands. When set to "Preferred Access", N band clients are prioritized. This feature is ideal for networks with devices supporting different bands.
- **Packet Delay Threshold (ms):** An Access Point may be occupied trying to transmit a packet to a busy client or a client out of range, hence delaying transmission to other connected clients. When Enabled, this Tx queue flushing mechanism drops packets and immediately begins to process others if the queue has been processed for more than x milliseconds, where Default = 0 (disabled). This feature improves the performance of complex wireless networks but may require some packets to be resent.
- **Idle Timeout (s):** Client disconnects when inactivity reaches the configured amount of time in seconds, where default = 300s.

- Band Steering:** When enabled, clients with 5GHz connectivity will be steered towards the 5GHz band to reduce congestion in the 2.4GHz band. This is applicable only when the AP is set to 2.4GHz and 5GHz on the 2 RF Cards. When "Aggressive" is checked, clients with 5GHz connectivity are forced to connect to the 5GHz band.
- Interference Detection:** When Utilization, Latency (and Invalid Packet Rate) of the current channel or adjacent channel reaches the configured threshold (in %), the AP switches to a different Channel.
- WME Configuration:** Access priority can be configured using with different parameters. CW Min: Contention Window Minimum, CW Max: Contention Window Maximum, AIFS: Arbitration Inter Frame Spacing, TXOP Limit: Transmission Opportunity Limit.
- Transmission Rate Threshold:** The associated client will be kicked when transmission rate is lower than the configured threshold. This ensures high connection speed for all associated clients.

Table 2 RF Configurations (under normal circumstances in certain countries)

| Band | Channel | Rate | Power |
|------------------------|---|--|---|
| <i>Disable</i> | N/A | N/A | N/A |
| <i>802.11a</i> | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 | 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M | Auto |
| <i>802.11b</i> | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 | 1M, 2M, 5.5M, 11M | |
| <i>802.11g</i> | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 | 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M | |
| <i>802.11b+802.11g</i> | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 | 1M, 2M, 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M | |
| <i>802.11a+802.11n</i> | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 | 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~15 | Level 1 ~ Level 25 (model dependent) |
| <i>802.11n+802.11g</i> | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 | 1M, 2M, 5.5M, 11M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~15 | |

*Please note that available values above will vary depending on the regulation of different countries.

7.2.3 VAP Configuration

This section provides configuration of each Virtual Access Point with settings such as **Profile Name**, **ESSID**, and **VLAN ID**.

Home > Wireless > VAP Config

VAP Configuration

Profile Name : RF Card A : VAP-1

VAP : Disable Enable

Profile Name : VAP-1

ESSID : 4ipnetAP-A1

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

SAVE CLEAR

VAP Configuration Page

To enable specific VAP, select the VAP from the drop-down list of Profile Name. The basic settings of each VAP are collected in the profile as follows:

- **VAP: Enable** or **Disable** this VAP.
- **Profile Name:** The profile name of a specific RF card and its VAP for identity / management purposes.
- **ESSID:** ESSID (Extended Service Set ID) serves as an identifier for clients to associate with the specific VAP. It can be coupled with different service levels like a variety of wireless security types.
- **VLAN ID:** The 4ipnet Access Point supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP shall be given a unique VLAN ID with valid values ranging from 1 to 4094. Once VLAN is Enabled, QoS is supported on the VAP.

VAP Configuration

Profile Name : RF Card A : VAP-1 ▼

VAP : Disable Enable

Profile Name : VAP-1

ESSID : 4ipnetAP-A1

Uplink Bandwidth : 0 Kbits/s

Downlink Bandwidth : 0 Kbits/s

VLAN ID : Disable Enable

VLAN ID : * (1 - 4094)

Uplink 802.1p : Best Effort (BE) ▼

Downlink 802.1p AC Mapping:

Background (BK) : Best Effort ▼

Best Effort (BE) : Best Effort ▼

Excellent Effort (EE) : Best Effort ▼

Critical Applications (CA) : Best Effort ▼

Video (VI) : Best Effort ▼

Voice (VO) : Best Effort ▼

Internetwork Control (IC) : Best Effort ▼

Network Control (NC) : Best Effort ▼

CAPWAP Tunnel Interface :

- **Uplink/Downlink Bandwidth:** Bandwidth control is configurable on the VAP in Kbits per second. Set 0 for unlimited bandwidth control and the maximum allowed value for this field is 999999999.
- **Uplink 802.1P per VAP:** Priority levels for uplink traffic can be selected here. The options available are Background, Best Effort, Excellent Effort, Critical Applications, Video, Voice, Internetwork Control, Network Control. For more information, please refer to IEEE Standards 802.1P.
- **Downlink 802.1P AC Mapping:** Re-mapping options are available on 802.1P downlink traffic. The options available are Background, Best Effort, Video, and Voice.
- **CAPWAP Tunnel Interface:** Select Checkbox to designate traffic for the VAP to pass through CAPWAP Tunnel established between the AP and the controller.

▶▶ **Note:** 802.1P is supported when the Airtime Fairness function is Disabled

7.2.4 Security

The Access Point supports various wireless authentication and data encryption methods in each VAP profile. With this, the administrator can provide different service levels to clients. The security type includes **Open**, **WEP**, **802.1X**, **WPA-Personal**, and **WPA-Enterprise**.

- **Open:** Authentication is not required and data is not encrypted during transmission when this option is selected. This is the default setting as shown in the following figure.



Security Settings: Open

- **WEP:** WEP (Wired Equivalent Privacy) is a data encryption mechanism based on a 64-bit, 128-bit, or 152-bit shared key algorithm.

Home > Wireless > Security



Security Settings: WEP

- **802.11 Authentication:** Select from **Open System**, **Shared Key**, or **Auto**.
 - **WEP Key Length:** Select a key length from **64-bit**, **128-bit**, or **152-bit**.
 - **WEP Key Format:** Select a WEP key format from **ASCII** or **Hex**.
 - **WEP Key Index:** Select a key index from **1~4**. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
 - **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.
- **802.1X:** When **802.1X Authentication** is selected, RADIUS authentication and Dynamic WEP are provided.

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

Security Settings

Profile Name : RF Card A : 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: second(s)

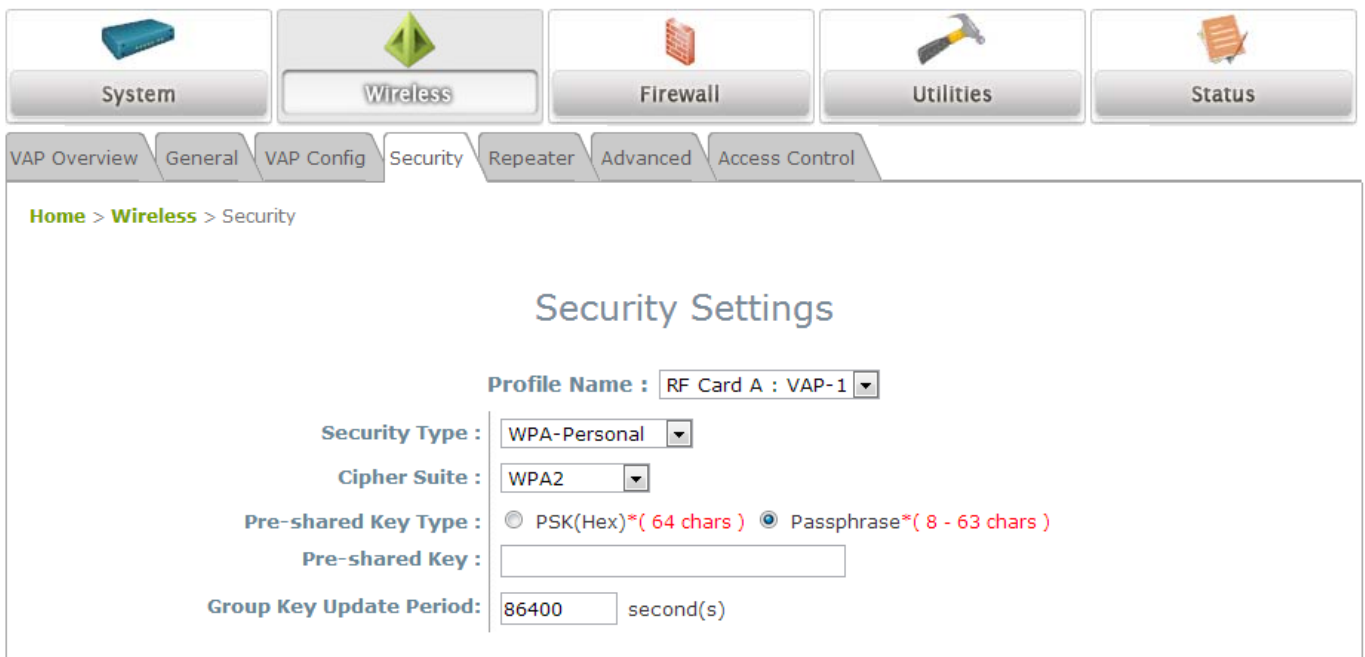
Security Settings: 802.1X Authentication

- **Dynamic WEP Settings:**
 - **Dynamic WEP:** For 802.1X security type, Dynamic WEP is always enabled to automatically generate WEP keys for encryption.
 - **WEP Key Length:** Select a key length from **64-bit** or **128-bit**.
 - **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in seconds.
- **RADIUS Server Settings (Primary/Secondary):**
 - **Host:** Enter the IP address or domain name of the RADIUS server.
 - **Authentication Port:** The port number used by the RADIUS server. Specify a port number or

use the default, 1812.

- **Secret Key:** The secret key for the system to communicate with the RADIUS server.
- **Accounting Service:** Enabling this option allows accounting of login and logouts through the RADIUS server.
- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

- **WPA-Personal:** WPA-Personal is a pre-shared key authentication method.



Home > Wireless > Security

Security Settings

Profile Name : RF Card A : VAP-1

Security Type : WPA-Personal

Cipher Suite : WPA2

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

Pre-shared Key :

Group Key Update Period: 86400 second(s)

Security Settings: WPA-Personal

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

- **WPA-Enterprise:** If this option is selected, the RADIUS authentication and data encryption will both be enabled.

Home > Wireless > Security

Security Settings

Profile Name : RF Card A : VAP-1

Security Type : WPA-Enterprise

Cipher Suite : WPA2

Group Key Update Period: 86400 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: second(s)

Security Settings: WPA-Enterprise

- **WPA Settings:**
 - **Cipher Suite:** Select an encryption method from **WPA2** or **WPA2/WPA**.
 - **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.
- **RADIUS Server Settings (Primary/Secondary):**
 - **Host:** Enter the IP address or domain name of the RADIUS server.
 - **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
 - **Secret Key:** The secret key for the system to communicate with the RADIUS server.
 - **Accounting Service:** *Enabling* this option allows accounting of login and logouts through the

RADIUS server.

- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

7.2.5 Repeater

4ipnet Access Points are capable of utilizing WDS or Universal Repeater (EAP210 and OWL530 only) to extend wireless network coverage.

If **WDS** is enabled, the AP can support up to 8 WDS links to its peer APs per radio. **Security Type** (**None**, **WEP**, or **WPA/PSK**) can be configured to decide which encryption is to be used for WDS connections respectively. Please fill in remote peer's MAC address and click **SAVE** to proceed; if setting revision is necessary, the **CLEAR** button can be used to clear the contents in the above WDS connection list.

Home > Wireless > Repeater Config

Repeater Settings

Repeater Type : WDS

WDS Profile : RF Card A : WDS Link 1

WDS : Disable

MAC Address :

Security type : None

CAPWAP Tunnel Interface :

SAVE CLEAR

Repeater Settings: WDS

- **WDS:** Select **Enable** to enable the respective WDS links; Select **Disable** to remove them.
- **MAC Address:** To input remote peer's MAC address.
- **Security Type:** None, WEP, or WPA-PSK.
- **CAPWAP Tunnel Interface:** Select Checkbox to designate WDS traffic to pass through CAPWAP Tunnel established between the AP and the controller.

- When the Repeater Type is set to **Universal Repeater** (EAP210 and OWL530 only), enter the SSID of upper-bound AP for uplink connection. Security Type (None, WEP, or WPA-PSK) can be configured for this Repeater connection, but note that the security type configured here needs to be the same as upper-bound AP.

Home > Wireless > Repeater Config

Repeater Settings

Repeater Type : Universal Repeater ▼

The SSID of Upper-Bound AP : *

Current wireless channel of the system is set at 6. Repeater connection may fail if the system is set to connect to upper AP with different channels

Security Type :
 None ▼
 None
 WEP
 WPA-PSK

Repeater Settings: Universal Repeater

7.2.6 Advanced

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

Home > Wireless > Advanced

Advanced Wireless Settings

Profile Name : RF Card A : VAP-1

RTS Threshold : 2346 *(1 - 2346)

DTIM period : 1 *(1 - 15)

Consecutive Dropped Packets: 5 *(2 - 50, 0:Disable)

Broadcast SSID : Disable Enable

Wireless Station Isolation : Disable Enable

WMM : Disable Enable

IAPP : Disable Enable

Multicast-to-Unicast Conversion : Disable Enable

Multicast/Broadcast Rate : 5.5M

Management Frame Rate : 5.5M

Receiving RSSI Threshold: 0 *(0 - 100, 0:Disable)

Advanced Wireless Settings Page

- RTS Threshold:** Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the fragment to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the AP or in areas where the clients are far apart and can detect only the AP but not each other.
- Fragmentation Threshold (802.11a, 802.11b and 802.11g Modes):** Enter a value between 256 and 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.
- DTIM Period:** Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will allow the wireless client to save more energy, but the throughput will be

lowered.

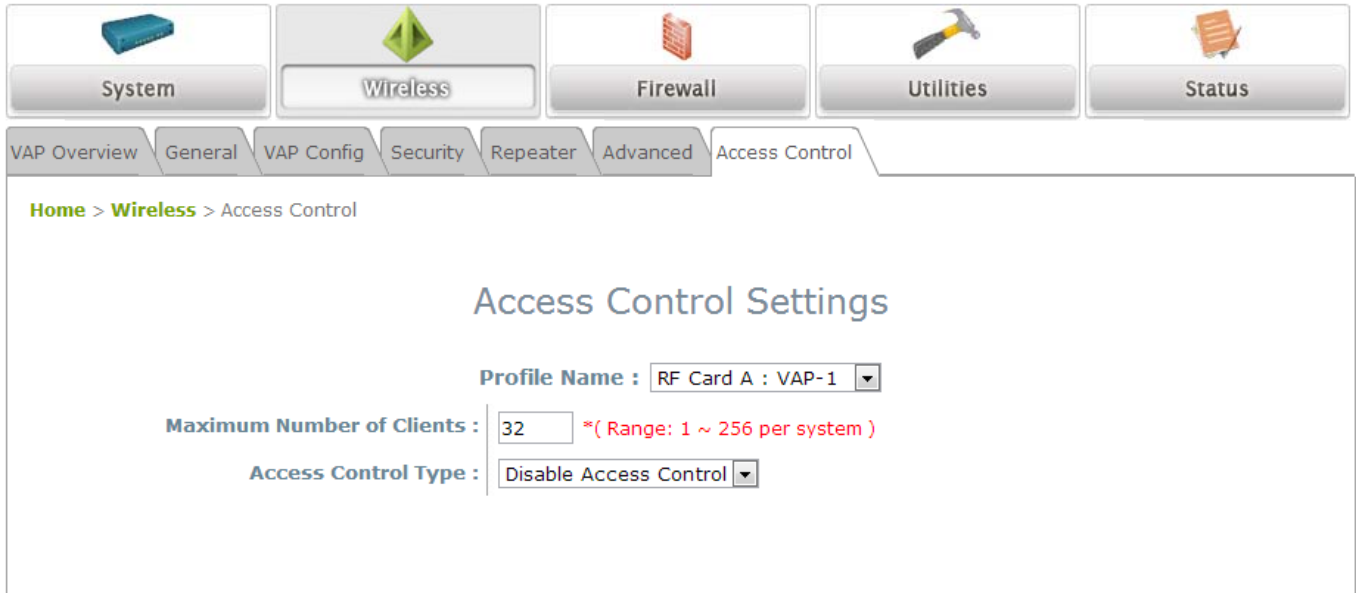
- **Consecutive Dropped Packets:** This is the maximum number of transmission retries the AP will attempt when packet transmission is dropped before deciding the client is out of transmission reach. When transmission retries fails for the set number of times, the Access Point kicks the client to optimize performance for other connected clients.
- **Broadcast SSID:** Disabling this function will stop the system from broadcasting its SSID. If broadcast of the SSID is disabled, only devices that have the correct SSID can connect to the system.
- **Wireless Station Isolation:** By enabling this function, all stations associated with the system are isolated and can only communicate with the system.
- **WMM:** The default is *Disable*. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

<To receive the benefits of WMM QoS>

- The application must support WMM.
- WMM shall be enabled on the Access Point.
- WMM shall be enabled in the wireless adapter on client's computer.
- **IAPP:** IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations connected to them. When this function is enabled, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.
- **Multicast-to-Unicast Conversion:** When Multicast-to-Unicast Conversion is enabled, the Access Point intelligently forwards traffic only to those ports that request multicast traffic. Adversely, when disabled, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.
- **Multicast/Broadcast Rate:** Bandwidth configuration for multicast/broadcast packets. If your wireless clients require a larger or smaller bandwidth for sending multicast/ broadcast packets, the administrator can customize the Access Point's multicast/ broadcast bandwidth here.
- **Management Frame Rate:** This feature controls the bandwidth for Management Frames. The higher the rate it, the shorter range the transmission covers
- **Receiving RSSI Threshold:** To keep connected stations with high connection speeds, the station is kicked out when its receiving sensitivity is lower than the threshold.

7.2.7 Access Control

On this page, the network administrator can restrict the total number of clients connected to the Access Point, as well as specify particular MAC addresses that can or cannot access the device.



System Wireless Firewall Utilities Status

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Access Control

Access Control Settings

Profile Name : RF Card A : VAP-1

Maximum Number of Clients : 32 *(Range: 1 ~ 256 per system)

Access Control Type : Disable Access Control

Access Control Settings Page

- **Maximum Number of Clients**

The 4ipnet Access Point supports various methods of authenticating clients for wireless LAN access. The default policy is unlimited access without any authentication requirement. To restrict the station number of wireless connections, simply change the **Maximum Number of Stations** to a desired number. For example, when the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

- **Access Control Type**

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

- **Disable Access Control:** When **Disable** is selected, there is no restriction for client devices to access the system.
- **MAC ACL Allow List:** When selecting **MAC ACL Allow List**, only the client devices (identified by their MAC addresses) listed in the Allow List (“allowed MAC addresses”) are granted access to the system. The administrator can temporarily block any allowed MAC address by checking **Disable**, until the administrator re-Enables the listed MAC.

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

Home > Wireless > Access Control

Access Control Settings

Profile Name : RF Card A : VAP-1

Maximum Number of Clients : *(Range: 1 ~ 256 per system)

Access Control Type : MAC ACL Allow List

| No. | MAC Address | State |
|-----|--|---|
| 1 | <input style="width: 90%;" type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 2 | <input style="width: 90%;" type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| 3 | <input style="width: 90%;" type="text"/> | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |

MAC Allow List

▶▶ **Note:** An empty Allow List means that there is no allowed MAC address. Make sure at least the MAC of the management system is included (e.g. network administrator's computer)

- **MAC ACL Deny List:** When selecting **MAC ACL Deny List**, all client devices are granted access to the system except those listed in the Deny List (“denied MAC addresses”). The administrator can allow any denied MAC address to connect to the system temporarily by checking **Disable**.

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

Home > Wireless > Access Control

Access Control Settings

Profile Name : RF Card A : VAP-1 ▾

Maximum Number of Clients : *(Range: 1 ~ 256 per system)

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 |

Deny List

- **RADIUS ACL:** Authenticate incoming MAC addresses by an external RADIUS. When **RADIUS ACL** is selected, all incoming MAC addresses will be authenticated by an external RADIUS. Please note that each VAP's MAC ACL and its security type (shown on the **Security Settings** page) share the same RADIUS configuration.

VAP Overview
General
VAP Config
Security
Repeater
Advanced
Access Control

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

Access Control Settings

Profile Name : RF Card A : VAP-1 ▼

Maximum Number of Clients : *(Range: 1 ~ 256 per system)

Access Control Type : RADIUS ACL ▼

Primary RADIUS Server :

Secondary RADIUS Server :

Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.

Host: *(Domain Name / IP Address)

Authentication Port: *(1 - 65535)

Secret Key: *

Host:

Authentication Port:

Secret Key:

RADIUS ACL

7.3 Firewall

The system provides an added security feature, Layer2 Firewall, in addition to the typical AP security. Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffic, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured on gateways, this extra security feature will assist to mitigate possible security breach. This section provides information in the following functions: **Firewall Lists**, **Service** and **Advanced Firewall Settings**.

7.3.1 Firewall List

It provides an overview of firewall rules in the system; 6 default rules with up to a total of 20 firewall rules are available for configuration.

Home > Firewall > Firewall List

Layer 2 Firewall Settings

Enable Layer 2 Firewall Disable Enable

| No. | State | Action | Name | EtherType | Remark | Setting |
|-----|--------------------------|--------|------|-----------|--------|--------------|
| 1 | <input type="checkbox"/> | DROP | CDP | IEEE_8023 | | Del Ed In Mv |
| 2 | <input type="checkbox"/> | DROP | STP | IEEE_8023 | | Del Ed In Mv |
| 3 | <input type="checkbox"/> | DROP | GARP | IEEE_8023 | | Del Ed In Mv |

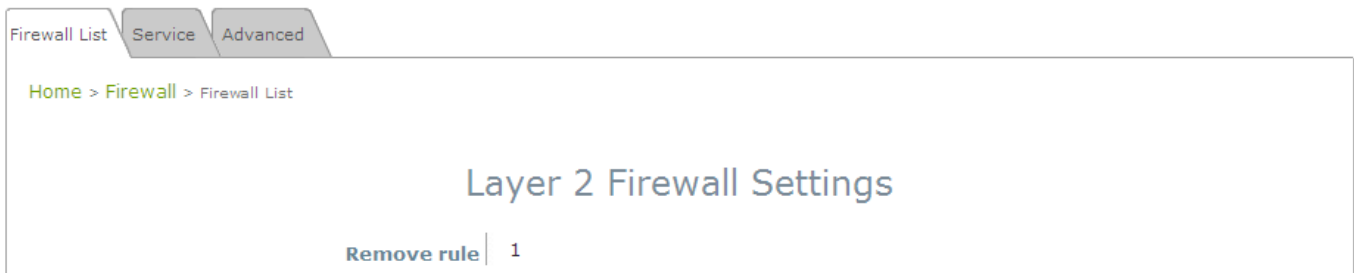
Firewall List Page

From the overview table, each rule is designated with the following field;

- **No.:** The numbering will decide the priority for the system to carry out the available firewall rules in the tables.
- **State:** The check marks will enable the respective rules.
- **Action:** **DROP** denotes a block rule; **ACCEPT** denotes a pass rule.
- **Name:** Shows the name of the rule.
- **EtherType:** Denotes the type of traffic subjected to this rule.
- **Remark:** Shows the note of this rule.
- **Setting:** 4 actions are available; **Del** denotes to delete the rule, **Ed** denotes to edit the rule, **In** denotes to insert a rule, and **Mv** denotes to move the rule.

>>To delete a specific rule,

Del in the **Setting** column of firewall list will lead to the following page for removal confirmation. After the **SAVE** button is clicked and system is rebooted, the rule will be removed.



>>To edit a specific rule,

Ed in the **Setting** column of the firewall list will lead to the following page for detail configuration. From this page, the rule can be edited from scratch or from an existing rule for revision. The following fields will be displayed:

- **Rule ID:** The numbering of this specific rule will decide its priority among available firewall rules in the table.
- **Rule name:** The rule name can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffic subjected to this rule.
- **Interface:** It indicates inbound/outbound direction with desired interfaces.
- **Service** (when EtherType is **IPv4**): Select the available upper layer protocols/services from the drop-down list.
- **DSAP/SSAP** (when EtherType is **IEEE 802.3**): The value can be further specified for the fields in 802.2 LLC frame header.
- **Type** (when EtherType is **IEEE802.3**): The field can be used to indicate the type of encapsulated traffic.
- **VLAN ID** (when EtherType is **802.1 Q**): The VLAN ID is provided to associate with certain VLAN-tagging traffic.
- **Priority** (when EtherType is **802.1 Q**): It denotes the priority level with associated VLAN traffic.
- **Encapsulated Type** (when EtherType is **802.1 Q**): It can be used to indicate the type of encapsulated traffic.
- **Opcode** (when EtherType is **ARP/RARP**): This list can be used to specify the ARP Opcode in ARP header.
- **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.

- **Action:** The rule can be chosen to be **Block** or **Pass**.
- **Remark:** Any note of this rule can be specified here.

When the configuration for firewall rule is completed; please click **SAVE** and **Reboot** system to let the firewall rule take effect.

>>To insert a specific rule,

In in the **Setting** column of the firewall list will lead to the following page for detail configuration with rule ID for the current inserted rule.

From this page, a rule can be added or edited from an existing rule for revision.

>>To move a specific rule,

Mv in the **Setting** column of the firewall list will lead to the following page for reordering confirmation.

After the **SAVE** button is clicked and system is rebooted, the order of rules will be updated.

The screenshot shows a web interface with three tabs: 'Firewall List', 'Service', and 'Advanced'. The 'Firewall List' tab is active. Below the tabs, there is a breadcrumb trail: 'Home > Firewall > Move rule'. The main heading is 'Move Rule'. Below the heading, there is a form with the following fields:

- ID :** 1
- Move to :** Before After
- ID :** *(1 - 20)

Please make sure all desired rules (state of rule) are checked and saved in the overview page; the rules will be enforced upon system reboot.

Firewall List Service Advanced

Home > Firewall > Firewall List

Layer 2 Firewall Settings

Enable Layer 2 Firewall Disable Enable

| No. | State | Action | Name | EtherType | Remark | Setting |
|-----|-------------------------------------|--------|-------------|-----------|--------|--------------|
| 1 | <input checked="" type="checkbox"/> | DROP | CDP and VTP | IEEE_8023 | | Del Ed In Mv |
| 2 | <input type="checkbox"/> | DROP | STP/BPDU | IEEE_8023 | | Del Ed In Mv |
| 3 | <input type="checkbox"/> | DROP | GARP | IEEE_8023 | | Del Ed In Mv |
| 4 | <input type="checkbox"/> | DROP | RIP | IPv4 | | Del Ed In Mv |
| 5 | <input type="checkbox"/> | DROP | HSRP | IPv4 | | Del Ed In Mv |
| 6 | <input type="checkbox"/> | DROP | OSPF | IPv4 | | Del Ed In Mv |
| 7 | <input type="checkbox"/> | | | | | Del Ed In Mv |
| 8 | <input type="checkbox"/> | | | | | Del Ed In Mv |
| 9 | <input type="checkbox"/> | | | | | Del Ed In Mv |
| 10 | <input type="checkbox"/> | | | | | Del Ed In Mv |

First Prev Next Last (total: 20)

SAVE

CLEAR

7.3.2 Service

The administrator can add or delete firewall services here; the services in this list will become options to choose in firewall rule (when EtherType is IPv4).

The Access Point provides a list of rules to block or pass traffic of layer-3 or above protocols. These services are available to choose from a drop-down list of layer2 firewall rule edit page with Ether Type IPv4. The first 28 entries are default services and the administrator can add/delete any extra desired services.

There are 28 firewall services available in default settings; these default services cannot be deleted but can be disabled. If changes are made, please click **SAVE** to save the settings before leaving this page.

Firewall List
Service
Advanced

[Home](#) > [Firewall](#) > [Service Config](#)

Firewall Service

| No. | Name | Description | Delete |
|-----|----------|--|--------------------------|
| 1 | ALL | ALL | <input type="checkbox"/> |
| 2 | ALL TCP | TCP, Source Port: 0~65535, Destination Port: 0~65535 | <input type="checkbox"/> |
| 3 | ALL UDP | UDP, Source Port: 0~65535, Destination Port: 0~65535 | <input type="checkbox"/> |
| 4 | ALL ICMP | ICMP | <input type="checkbox"/> |
| 5 | FTP | TCP/UDP, Destination Port: 20~21 | <input type="checkbox"/> |
| 6 | HTTP | TCP/UDP, Destination Port: 80 | <input type="checkbox"/> |
| 7 | HTTPS | TCP/UDP, Destination Port: 443 | <input type="checkbox"/> |
| 8 | POP3 | TCP, Destination Port: 110 | <input type="checkbox"/> |
| 9 | SMTP | TCP, Destination Port: 25 | <input type="checkbox"/> |
| 10 | DHCP | UDP, Destination Port: 67~68 | <input type="checkbox"/> |

[First](#)
[Prev](#)
[Next](#)
[Last](#)
(total: 28)

Firewall Service Page

7.3.3 Advanced

At **Firewall > Advanced**, more advanced settings on firewall rules can be configured, providing extra security enhancement against DHCP and ARP traffic traversing the available interfaces of the system.

- **Trust Interface:** Each VAP interface can be checked individually to mark as trusted interfaces; security enforcements on DHCP/ARP like DHCP snooping and ARP inspection will be carried out on non-trusted interfaces.
- **DHCP Snooping:** When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the trusted DHCP server (IP/MAC) can be specified to prevent rouge DHCP server.
- **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing.
 - **Proxy ARP** option when enabled, AP will reply ARP requests on behalf of downlink stations. The ARP table maintained by the AP will be used as a look up table upon receipt of ARP request from AP uplink. Adversely, without Proxy ARP, ARP request is broadcasted down into the AP's wireless network causing network inefficiencies.
 - **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address does not send DHCP traffic, any clients with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static Trust List**.
 - **Trust List Broadcast** can be enabled to let other APs (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests.
 - **Static Trust List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears on the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

If any settings are changed, please click **SAVE** to save the configuration before leaving this page.

7.4 Utilities

The following utility features on this page allow the administrator to maintain the system: **Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, Channel Analysis, Background Scan.**

7.4.1 Change Password

To protect the Web Management Interface from unauthorized access, it is highly recommended to change the administrator's password to a secure password. Only alpha-numeric characters are allowed, and it is also recommended to make use of a combination of both numeric and alphabetic characters.

The screenshot shows the 'Change Password' page within the 'Utilities' section. At the top, there are navigation tabs for System, Wireless, Firewall, Utilities (selected), and Status. Below these are sub-tabs for Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, Channel Analysis, and Background Scan. The breadcrumb path is 'Home > Utilities > Change Password'. The main heading is 'Change Password'. There are two sections for password changes. The first section is for the 'admin' user, with fields for 'Name : admin', 'New Password :', and 'Re-enter New Password :'. A red note '*up to 32 characters' is next to the 'New Password' field. The second section is for the 'user' user, with fields for 'Name : user', 'New Password :', and 'Re-enter New Password :'. A red note '*up to 32 characters' is next to the 'New Password' field.

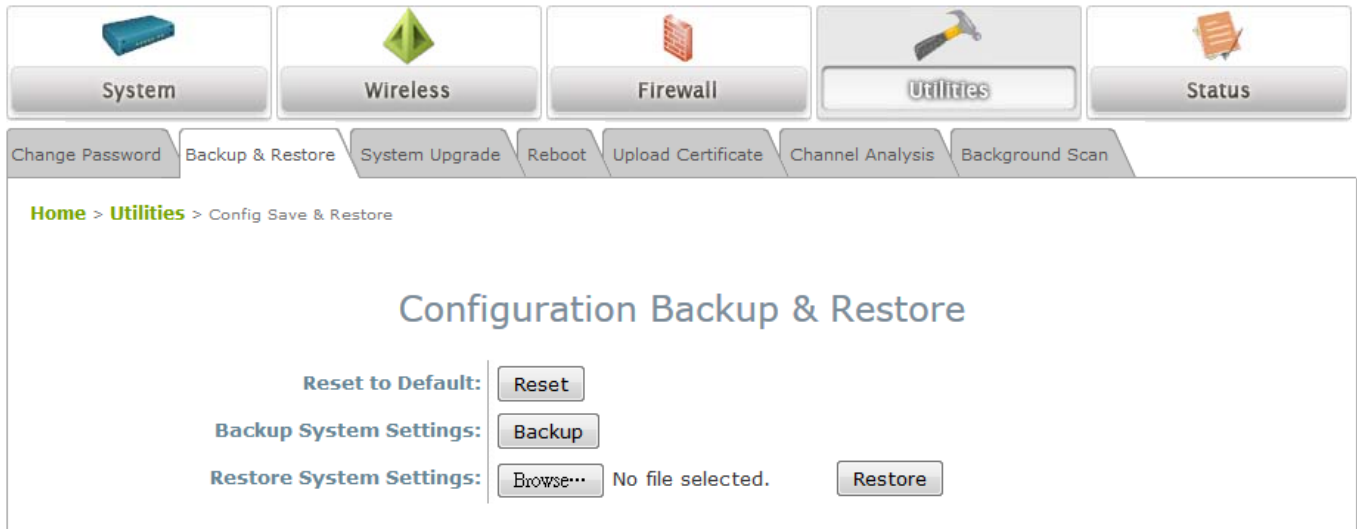
Change Password Page

The administrator can change password on this page. Enter the original password (“**admin**”) and new password, and then re-enter the new password in the **Re-enter New Password** field. Click **SAVE** to save the new password.

In addition to the admin account, there is a “**user**” account capable of accessing the web management interface with configuration limitations. The “user” account will not be able to reboot AP, change wireless settings or enable the Channel Analysis function. This account is typically issued by IT staff for employees to monitor AP statuses.

7.4.2 Backup & Restore

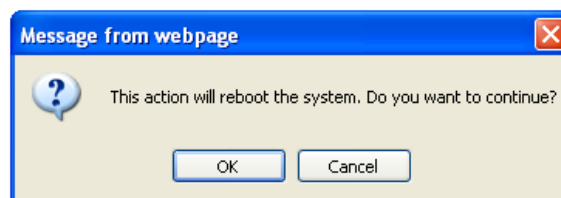
This function is used to backup and restore the Access Point's settings. The AP can also be restored to factory default using this function. It can be used to duplicate settings to other access points (backup settings of this system and then restore on another AP).



Backup & Restore Page

- **Reset to Default:**

- Click **Reset** to load the factory default settings of the Access Point. A pop-up Page will appear to re-confirm the request to reboot the system. Click **OK** to proceed, or click **Cancel** to cancel the reboot request.

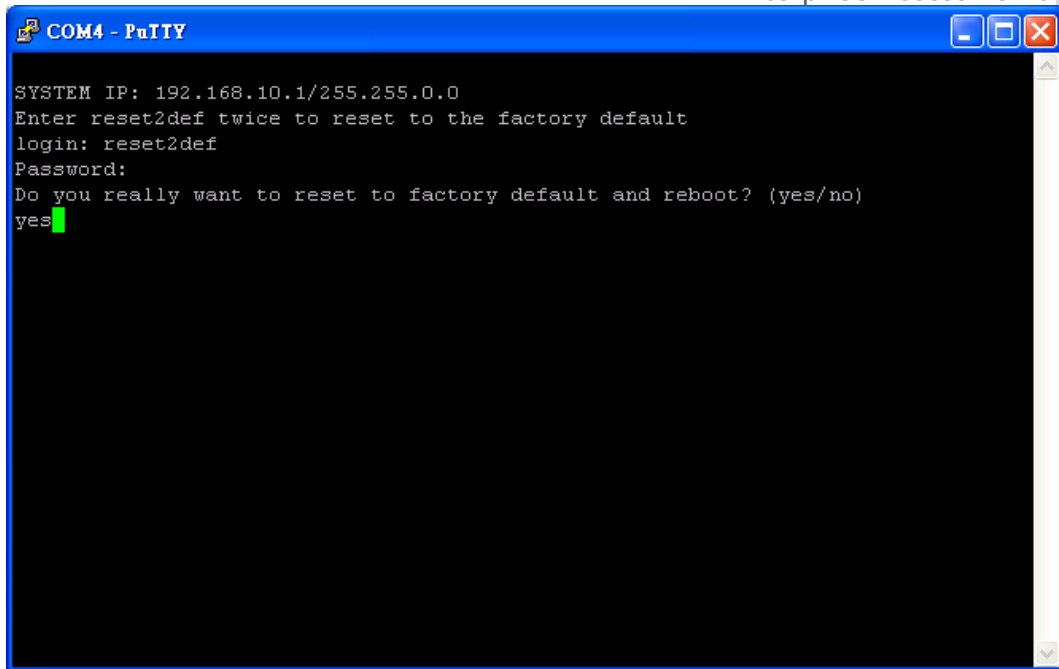


Reboot Confirmation Prompt

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

Additionally, there are two ways to reset the system to factory default settings from the console interface:

- 1) COM Port connection - Should the administrator forget the AP's IP address, with the right baud rate and a termination simulation program such as PuTTY or Hyper Terminal, a login prompt should be seen as such:



```
COM4 - PuTTY
SYSTEM IP: 192.168.10.1/255.255.0.0
Enter reset2def twice to reset to the factory default
login: reset2def
Password:
Do you really want to reset to factory default and reboot? (yes/no)
yes
```

Login as “reset2def” and enter “reset2def” as your password. Type “yes” to reset the AP to factory default.

- 2) Console connection via SSH - the IP address of the AP can be retrieved with an IP Discovery Utility provided by 4ipnet. Simply connect via an Ethernet cable and run the Discovery Utility. Note that the laptop/PC connecting to the AP must run in Windows XP compatible mode and a static IP must be set.

Login as “reset2def” and enter “reset2def” as your password. Type “yes” to reset the AP to factory default.

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



After network parameters have been reset / restored, the network settings of the administrator PC may need to be changed to ensure that the IP address of the administrator PC is on the same subnet mask as the AP.

7.4.3 System Upgrade

The EAP Access Point supports two methods of firmware upgrade: from the web management interface or through TFTP. The administrator can download the latest firmware from the 4ipnet Support Team and save it on the administrator's PC. To upgrade the system firmware, click **Browse** to choose the new firmware file you downloaded onto your PC and then click **Upload** to execute the process. There will be a prompt confirmation message to notify the administrator to restart the system after a successful firmware upgrade. To upgrade by TFTP, enter the designated IP address, Port, and File Name, then click "Apply". Please restart the system after upgrading the firmware.

The screenshot shows the 'System Upgrade' page. At the top, there are navigation tabs: System, Wireless, Firewall, Utilities (selected), and Status. Below these are sub-tabs: Change Password, Backup & Restore, System Upgrade (selected), Reboot, Upload Certificate, Channel Analysis, and Background Scan. The main content area has a breadcrumb 'Home > Utilities > System Upgrade' and a title 'System Upgrade'. It displays the following information:

- Current Version:** 1.10.00
- Current Build Number:** 1.20-1.6887
- File Name:** No file selected.
- Upgrade by TFTP:**
 - IP Address:
 - Port:
 - File Name:

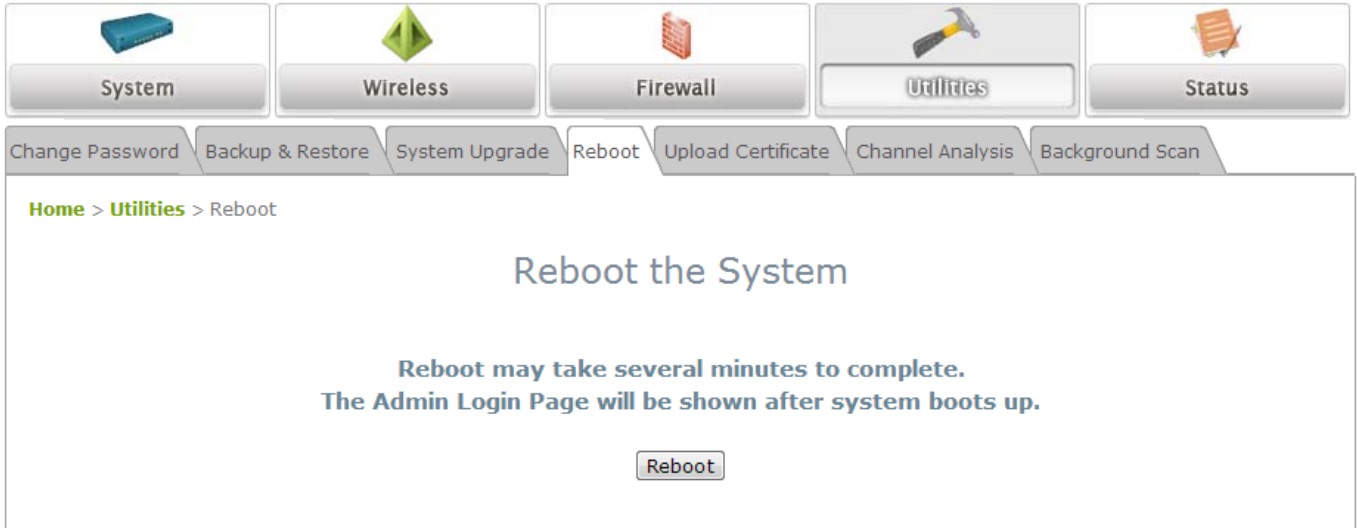
System Upgrade Page

- It is recommended to check the firmware version number before proceeding further. Please make sure you have the correct firmware file.
- » **Note:**
 - Firmware upgrade may sometimes result in the loss of data. Please ensure that all necessary settings are written down before upgrading the firmware.
 - During firmware upgrade, please do not turn off the power. This may permanently damage the system.

7.4.4 Reboot

This function allows the administrator to restart the AP safely. The process takes approximately three minutes. Click **Reboot** to restart the system. Please wait for the blinking timer to complete its countdown before accessing the system's Web Management Interface again. The System Overview page will appear after a successful reboot.

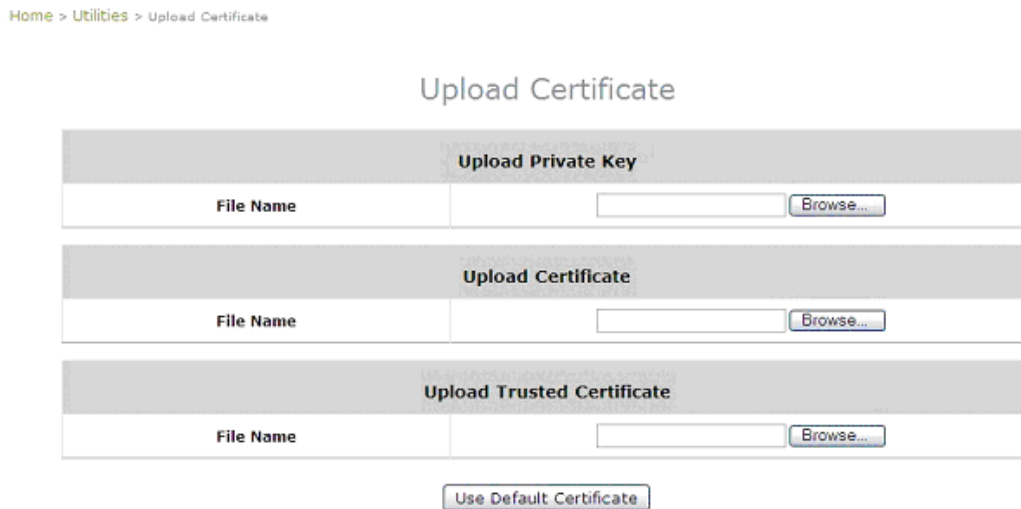
Occasionally, it is necessary to reboot the AP to ensure that parameter changes are submitted.



Reboot Page

7.4.5 Upload Certificate

This function is used to configure a valid certificate for security validation required in CAPWAP.



- **Upload Certificate:** It provides flexibility to support customer's own Certificate, Private Key, or Trusted Certificate for a means of security verification for CAPWAP or other security needs to ensure the authenticity of this AP to other network entities.
- **Use Default Certificate:** Click **Use Default Certificate** to use the default certificate and key.

7.4.6 Channel Analysis

The Channel Analysis is an excellent tool for IT staff to quickly grasp an idea of what the channel dynamics are. Included for channel analysis is a spectrogram, density graph and other charts to detect interference from Bluetooth devices, Microwave devices, Cordless phones, and etc.

The screenshot shows the web interface for Channel Analysis. At the top, there are navigation buttons for System, Wireless, Firewall, Utilities, and Status. Below these are utility buttons: Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, Channel Analysis, and Background Scan. The breadcrumb trail is Home > Utilities > Channel Analysis. The main heading is 'Channel Analysis'. Under 'Analyzer Configuration', there are radio buttons for 'Disable' and 'Enable', with 'Enable' selected. Under 'RF Card Name', there is a radio button for 'RF Card A', which is selected.

-
- **Note:**
- Please be reminded that when Channel Analysis is in progress, the RF card loses its capability to serve clients and kicks off current users.
 - The browser used to implement Channel Analysis must have Java Runtime Environment installed or it would not display correctly.
 - The system allows only 1 operator to use this function at one time.
 - Channel Analysis only runs on 2.4GHz Band.
-

7.4.7 Background Scan

The Access Point is capable of doing background scanning without affecting service. This works in complement with Channel Analysis so administrators have a complete overview of the wireless environment.

Home > Utilities > Background Scan

Background Scan

RF Card Name :

| SSID | MAC | Signal Strength | Channel |
|-----------------|-------------------|-----------------|---------|
| OWL410-1 | 00:1F:D4:02:87:58 | -71 | 36 |
| OWL400-1 | 00:1F:D4:02:87:58 | -75 | 36 |
| OWL410-1 | 00:1F:D4:02:87:E0 | -83 | 36 |
| OWL400-1 | 00:1F:D4:02:87:E0 | -80 | 36 |
| 4ipnetAP-B1 | 00:C0:CA:5F:8B:35 | -88 | 36 |
| OWL410-1 | 00:1F:D4:02:87:78 | -61 | 36 |
| OWL400-1 | 00:1F:D4:02:87:78 | -86 | 36 |
| OWL410-1 | 00:1F:D4:02:86:A0 | -55 | 36 |
| JamesIWF2220-B1 | 00:1F:D4:02:B4:88 | -90 | 36 |
| 4ipnetAP-B1 | 00:1F:D4:02:BE:F4 | -89 | 36 |
| CAP320-B1 | 00:C0:CA:5F:89:B0 | -87 | 36 |
| GONZO-A1 | 00:C0:CA:5F:8B:49 | -83 | 36 |
| SEB-B1 | 00:C0:CA:5F:89:9E | -86 | 36 |
| OWL410-1 | 00:1F:D4:02:86:C0 | -64 | 36 |


The Scan Whole Channel button triggers the AP to scan all channels in the configured band. Note that the Radio is only capable of scanning in its configured band.

7.5 Status


This page is used to view the current condition and state of the system and it includes the following functions: **Overview**, **Interfaces**, **Associated Clients**, **WDS Link Status**, **Event Log** and **Monitor**.


7.5.1 Overview


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


System


Wireless


Firewall


Utilities


Status

Overview

Interfaces

Associated Clients

WDS Link Status

Event Log

Monitor

Home > Status > System Overview

System Overview

System

| | |
|------------------|--|
| System Name | Enterprise Access Point - EA... |
| Firmware Version | 1.10.00 |
| Build Number | 1.20-1.6887 |
| Location | |
| Site | EN-A |
| Device Time | 2013/11/29 17:01:59 |
| System Up Time | 1 days, 2:46:29 |
| CPU/RAM Usage | 100.00% / 45.10% Plot |

Radio Status

| RF Card | MAC Address | Band | Channel | TX Power |
|-----------|-------------------|-----------|---------|----------|
| RF Card A | 00:1F:D4:94:19:3C | 802.11g+n | 9 | 27 dBm |
| RF Card B | 00:1F:D4:94:19:3D | 802.11a+n | 36 | 23 dBm |

LAN Interface

| | |
|-------------|-------------------|
| MAC Address | 00:1F:D4:94:19:3B |
| IP Address | 10.1.121.21 |
| Subnet Mask | 255.255.0.0 |
| Gateway | 10.1.3.40 |

AP Status

RF Card Name : RF Card A

| Profile Name | BSSID | ESSID | Security Type | Online Clients | Tun |
|--------------|-------------------|-------------|---------------|----------------|--|
| VAP-3 | 00:1F:D4:94:19:3C | felix220-a3 | WPA-P... | 0 | ✕ |

CAPWAP

Status Disabled

IPv6

Status Disabled

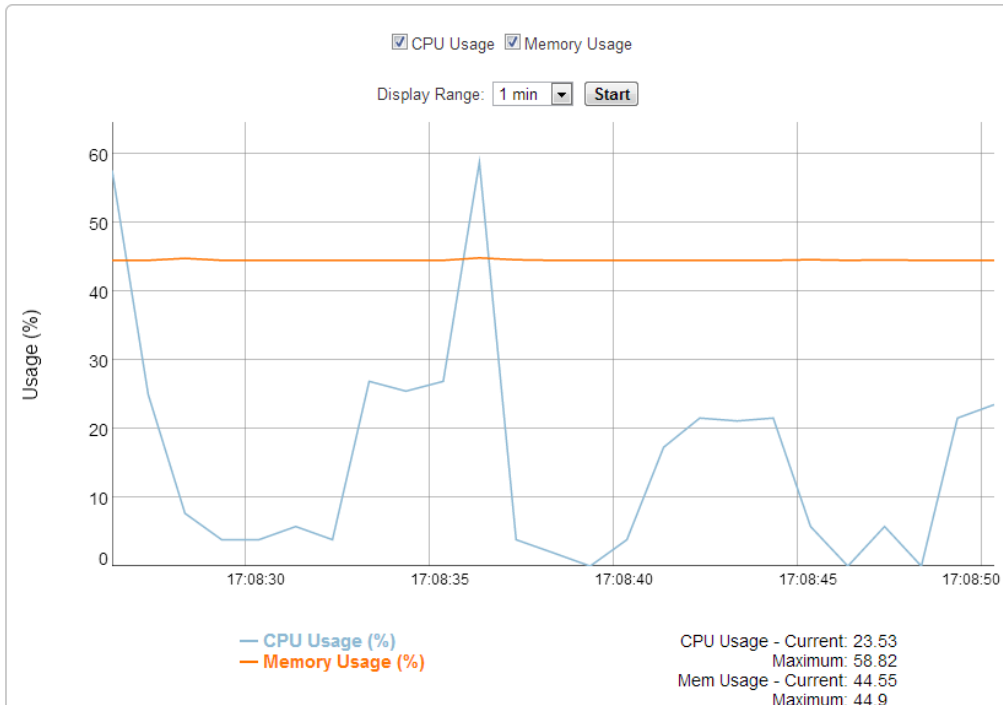
System Overview Page

Table 3 Status Page's Organizational Layout

| Item | | Description |
|---------------|------------------|--|
| System | System Name | The system name of the Access Point. |
| | Firmware Version | The current firmware version of the Access Point. |
| | Build Number | The current firmware build number of the Access Point. |
| | Location | The location of the Access Point. |
| | Site | The site of the Access Point. |
| | Device Time | The system time of the Access Point. |
| | System Up Time | The time that the system has been in operation. |
| | CPU/RAM Usage | Displays the current CPU/RAM utilization. |
| LAN Interface | MAC Address | The MAC address of the LAN Interface. |
| | IP Address | The IP address of the LAN Interface. |
| | Subnet Mask | The Subnet Mask of the LAN Interface. |
| | Gateway | The Gateway of the LAN Interface. |
| Radio Status | MAC Address | The MAC address of the RF Card. |
| | Band | The RF band in use. |
| | Channel | The channel specified. |
| | Tx Power | Transmit Power level of RF card. |
| AP Status | Profile Name | The profile name of AP. |
| | BSSID | Basic Service Set ID. |
| | ESSID | Extended Service Set ID. |
| | Security Type | Security type of the Virtual AP. |
| | Online Clients | The number of online clients. |
| | Tunnel | The status of the used Tunnel. |
| IPv6 | Status | Enabled/ Disabled. |
| CAPWAP | Status | Enabled/ Disabled. |

The system is able to plot a dynamic graph for CPU/RAM usage with the time Axis.

CPU / Memory Usage



The Time Axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

7.5.2 Interfaces

Traffic information is available per interface. Recorded data includes **Packets In**, **Packets Out**, **Traffic In (kb)**, and **Traffic Out (kb)**.

System Wireless Firewall Utilities Status

Overview Interfaces Associated Clients WDS Link Status Event Log Monitor

Home > Status > Interface

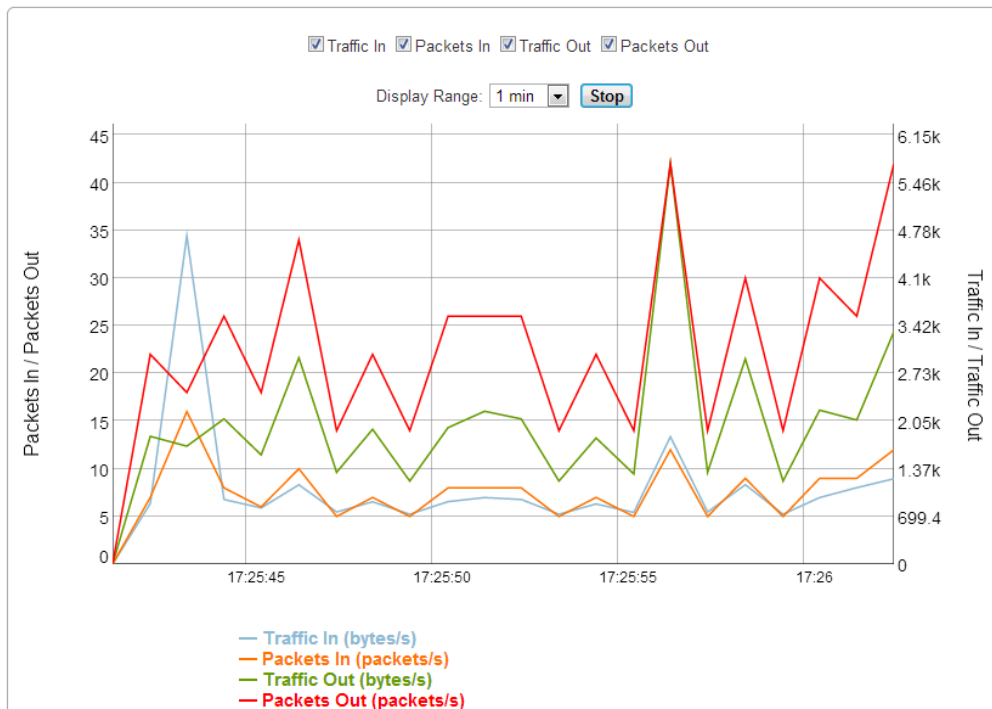
Interface Traffic

Interface List

| Interface | Traffic Out (KB) | Packets Out | Traffic In (KB) | Packets In | Real Time |
|------------------|------------------|-------------|-----------------|------------|----------------------|
| Uplink | 354627 | 5267468 | 294976 | 1474959 | Plot |
| RF Card A : VAP3 | 57180 | 186780 | 4121 | 32498 | Plot |
| RF Card B : VAP3 | 4268 | 16794 | 9 | 221 | Plot |

A real time plot is also available for each interface as such:

Uplink Traffic



The Time Axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

7.5.3 Associated Clients

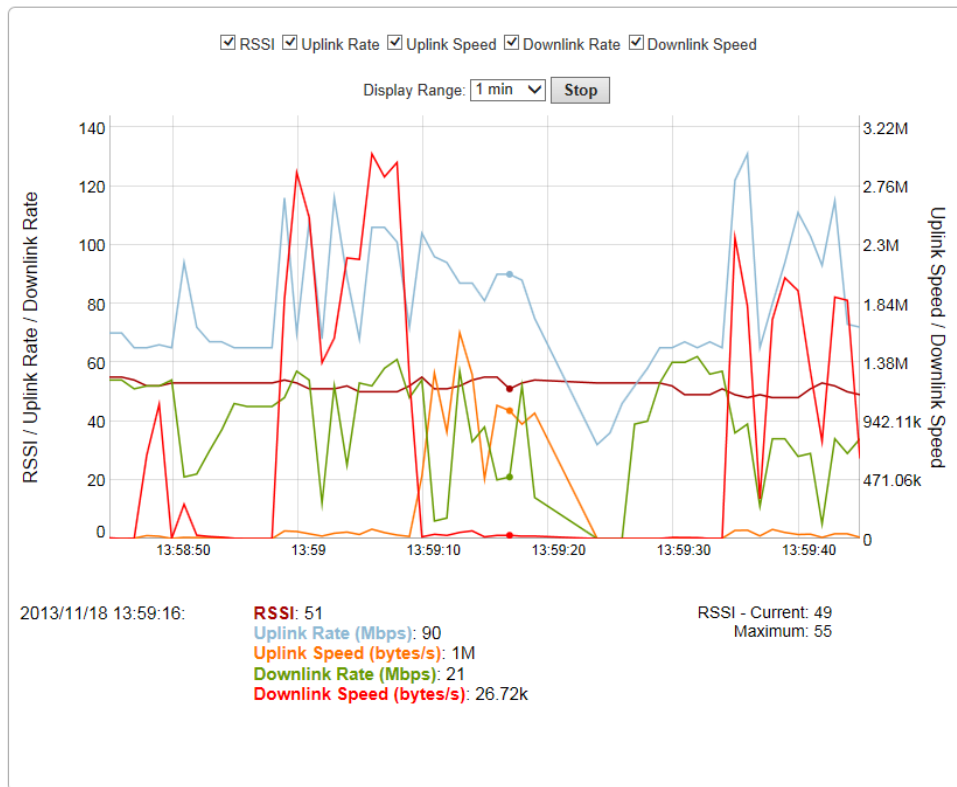
The administrator can remotely oversee the status of all associated clients on this page. When a low SNR is found here, the administrator can tune the corresponding parameters or investigate the settings of associated clients to improve network communication performance.

| Associated VAP | ESSID | MAC Address | RSSI | Packet Error Ratio (%) | Idle Time (secs) | Up Time (secs) | Real Time | Disconnect |
|-------------------|-------------|-------------------|------|------------------------|------------------|----------------|-------------------------------------|-------------------------------------|
| RF Card A : VAP-3 | felix220-a3 | 0c:74:c2:3d:23:c7 | 24 | 16 | 30 | 780 | <input type="button" value="Plot"/> | <input type="button" value="Kick"/> |
| RF Card A : VAP-3 | felix220-a3 | 00:1f:d4:02:c9:f4 | 71 | 0 | 0 | 1073 | <input type="button" value="Plot"/> | <input type="button" value="Kick"/> |

Associated Client Status Page

- **Associated VAP:** The name of a VAP (Virtual Access Point) that the client is associated with.
- **ESSID:** The Extended Service Set ID which the client is associated with.
- **MAC Address:** The MAC address of associated clients.
- **RSSI:** The Received Signal Sensitivity Index of respective client's association.
- **Packet Error Ratio:** Indication of the associated client's service quality to see if packets are not received.
- **Idle Time:** Time period that the associated client is inactive for; the time unit is in seconds.
- **Up time:** Time period that the client is associated for; the time unit is in seconds.
- **Real Time:** A real time plot of each associated client's traffic information including Packets In/Out, Traffic In/Out in Kb, RSSI, Uplink/Downlink Rates, and etc.

Client 0c:74:c2:3d:23:c7 Status



The Time Axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

- **Disconnect:** Upon clicking **Kick**, the client will be disconnected from the system.

7.5.4 WDS Link Status

The administrator can review detailed information of the repeater function at **Status > WDS Link Status**. Information of WDS status, traffic statistics, encryption and other details are provided.

System | Wireless | Firewall | Utilities | Status

Overview | Interfaces | Associated Clients | WDS Link Status | Event Log | Monitor

Home > Status > Repeater Status

Repeater Status

WDS Link List

RF Card A

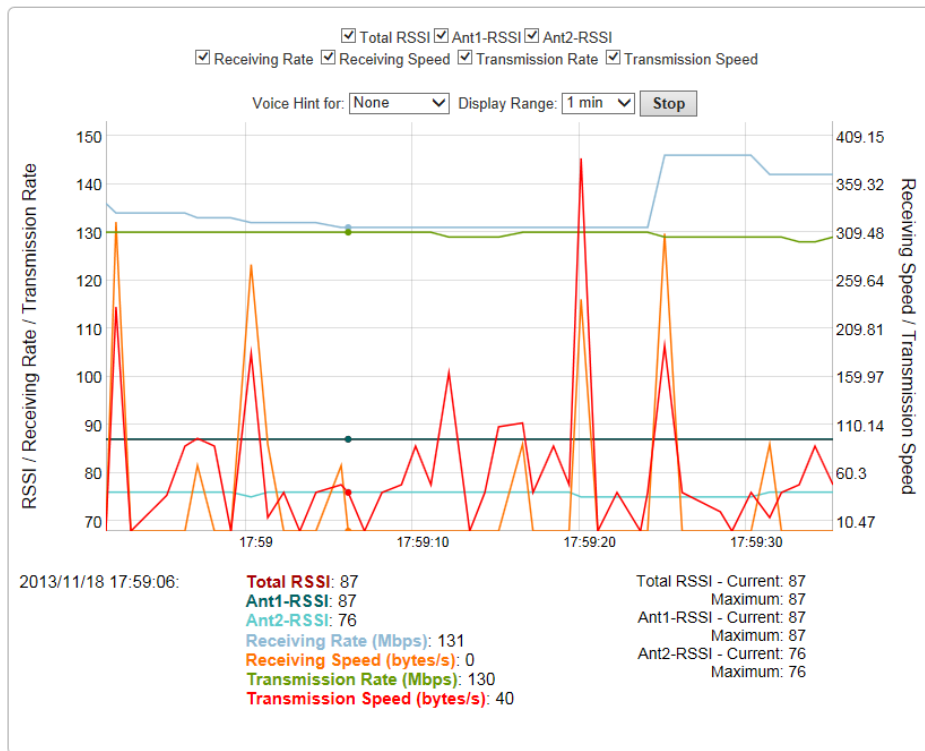
| Item | Status | MAC Address | RSSI | TX Rate | TX Count | TX Error | Encryption Tunnel | Real Time |
|------|----------|-------------|------|---------|----------|----------|-------------------|-------------------------------------|
| 1 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 2 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 3 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 4 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 5 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 6 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 7 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 8 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |

RF Card B

| Item | Status | MAC Address | RSSI | TX Rate | TX Count | TX Error | Encryption Tunnel | Real Time |
|------|----------|-------------|------|---------|----------|----------|-------------------|-------------------------------------|
| 1 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 2 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 3 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 4 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 5 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 6 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 7 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |
| 8 | Disabled | | N/A | N/A | N/A | N/A | N/A | <input type="button" value="Plot"/> |

By clicking plot, a dynamic graph for WDS link status is displayed. Information on the plot includes Total RSSI, Ant1 RSSI, Ant2 RSSI, Transmission Rate, Receiving Rate, Transmission Speed, and Receiving Speed.

RF Card B : WDS Link 1 Status



The Time Axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

Voice hint may also be enabled for convenience during antenna adjustment.

7.5.5 Event Log

The Event Log provides a record of system activities. The administrator can monitor the system status by checking this log.

Overview Interfaces Associated Clients WDS Link Status **Event Log** Monitor

Home > Status > Event Log

Event Log

```

Nov 29 13:18:16 logd@localhost hostapd: ath0ap2: STA 00:18:de:c9:18:e1 IEEE 802.11:
deauthenticated due to local death request
Nov 29 13:18:16 logd@localhost hostapd: ath0ap2: STA 00:18:de:c9:18:e1 IEEE 802.11:
disassociated
    
```

Event Log Page

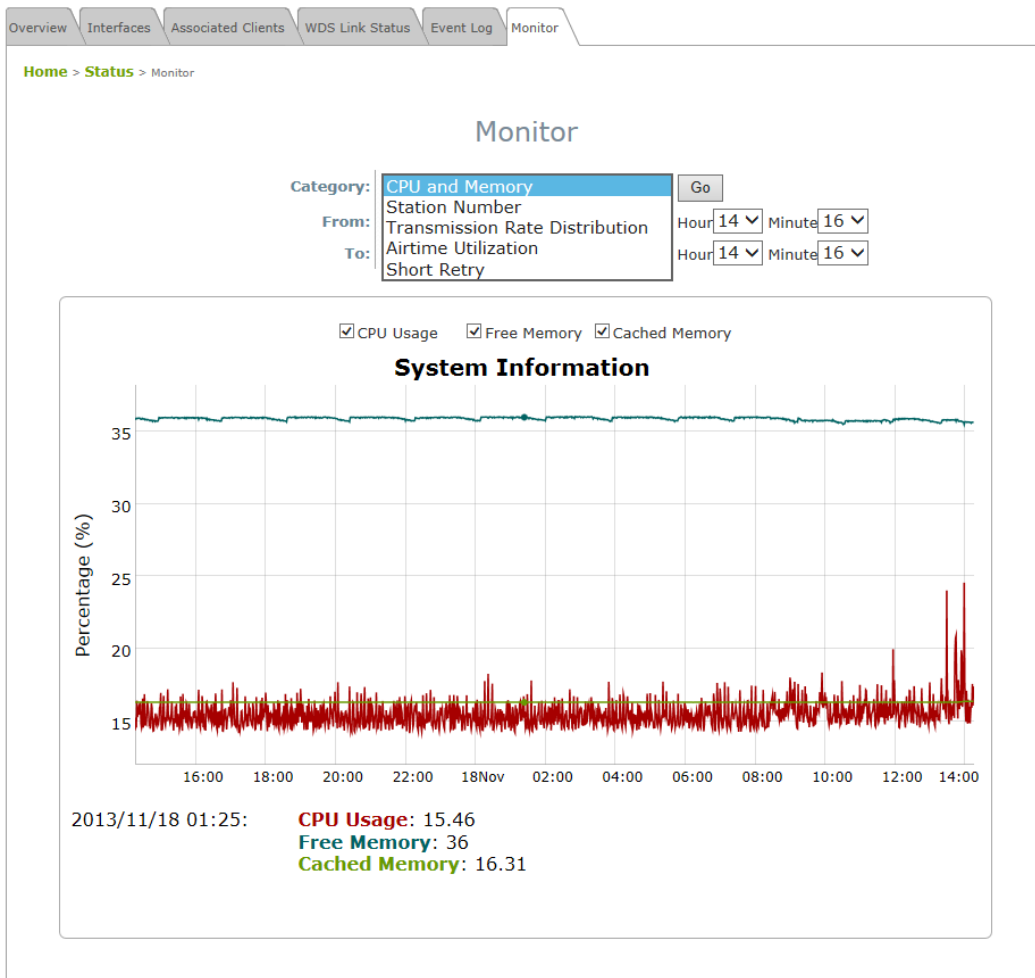
Each line in the log represents an event record; in each line, there are 4 fields:

- **Date / Time:** The time & date when the event happened.
- **Hostname:** Indicates which host recorded this event. Note that all events on this page are local events, so the hostname in this field is always the same. In remote SYSLOG service however, this field will help the administrator identify which event is from this Access Point.
- **Process name:** Indicate the event generated by the running instance.
- **Description:** Description of the event.

To save the file locally, click **SAVE LOG**; to clear all of the records, click **CLEAR**.

7.5.6 Monitor

For a quick overview on the AP's performance, the 'Monitor' feature displays an RRD graph recording CPU utilization, memory usage, associated station numbers, TX rate distribution, airtime utilization, and short retries.



The begin and end time for the RRD graph can be selected for filtering data. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

8. CPE Mode Configuration (OWL530/EAP210)

The OWL530 and EAP210 support CPE mode, which acts as a gateway where it connects to the WAN wirelessly and provides Ethernet connection to users via wired LAN. This chapter will guide you through setting up the CPE mode with graphical illustrations. The following table shows all the functions of the Access Point in CPE mode.

| OPTION | System | Wireless | Firewall | Utilities | Status |
|-----------------|--------------------|----------------------------|---------------------|--------------------|-----------------|
| FUNCTION | System Information | General Setting | IP/ Port Forwarding | Change Password | System Overview |
| | Operating Mode | Advanced Wireless Settings | Demilitarized Zone | Backup & Restore | Event Log |
| | Network | Security Settings | | System Upgrade | DHCP Lease |
| | Management | Site Survey | | Reboot | UPnP Status |
| | | | | Upload Certificate | |

Table of CPE Mode Functions

| | | | | |
|---|---|---|--|---|
|  System |  Wireless |  Firewall |  Utilities |  Status |
|---|---|---|--|---|

System Overview | Interfaces | Event Log | Monitor | DHCP Lease | UPnP

Home > Status > System Overview

System Overview

System

| | |
|-------------------------|-------------------------------------|
| System Name | Enterprise Access Point - OWL5... |
| Firmware Version | 1.10.00 |
| Build Number | 1.13-1.6891 |
| Location | |
| Site | EN-A |
| Device Time | 2013/12/02 07:48:20 |
| System Up Time | 0 days, 5:32:07 |
| CPU/RAM Usage | 1.92% / 30.70% Plot |
| Operating Mode | CPE |

Radio Status

| | |
|------------------------|-------------------------|
| Status | Connected |
| SSID | felix220-a3 |
| MAC Address | 00:1F:D4:94:19:3C |
| Channel | 9 |
| Signal Strength | 94 Plot |
| Security | WPA-PSK |

LAN Interface

| | |
|--------------------|-------------------|
| MAC Address | 00:1F:D4:02:C9:F3 |
| IP Address | 192.168.21.1 |
| Subnet Mask | 255.255.255.0 |
| DHCP Server | Enabled |

WAN Interface

| | |
|--------------------|---------------------------------|
| Mode | DHCP |
| MAC Address | 00:1F:D4:02:C9:F4 |
| IP Address | 10.1.121.10 |
| Subnet Mask | 255.255.0.0 |
| Gateway | 10.1.3.40 |
| Bandwidth | Down: Unlimited / UP: Unlimited |

CPE Mode Main Page

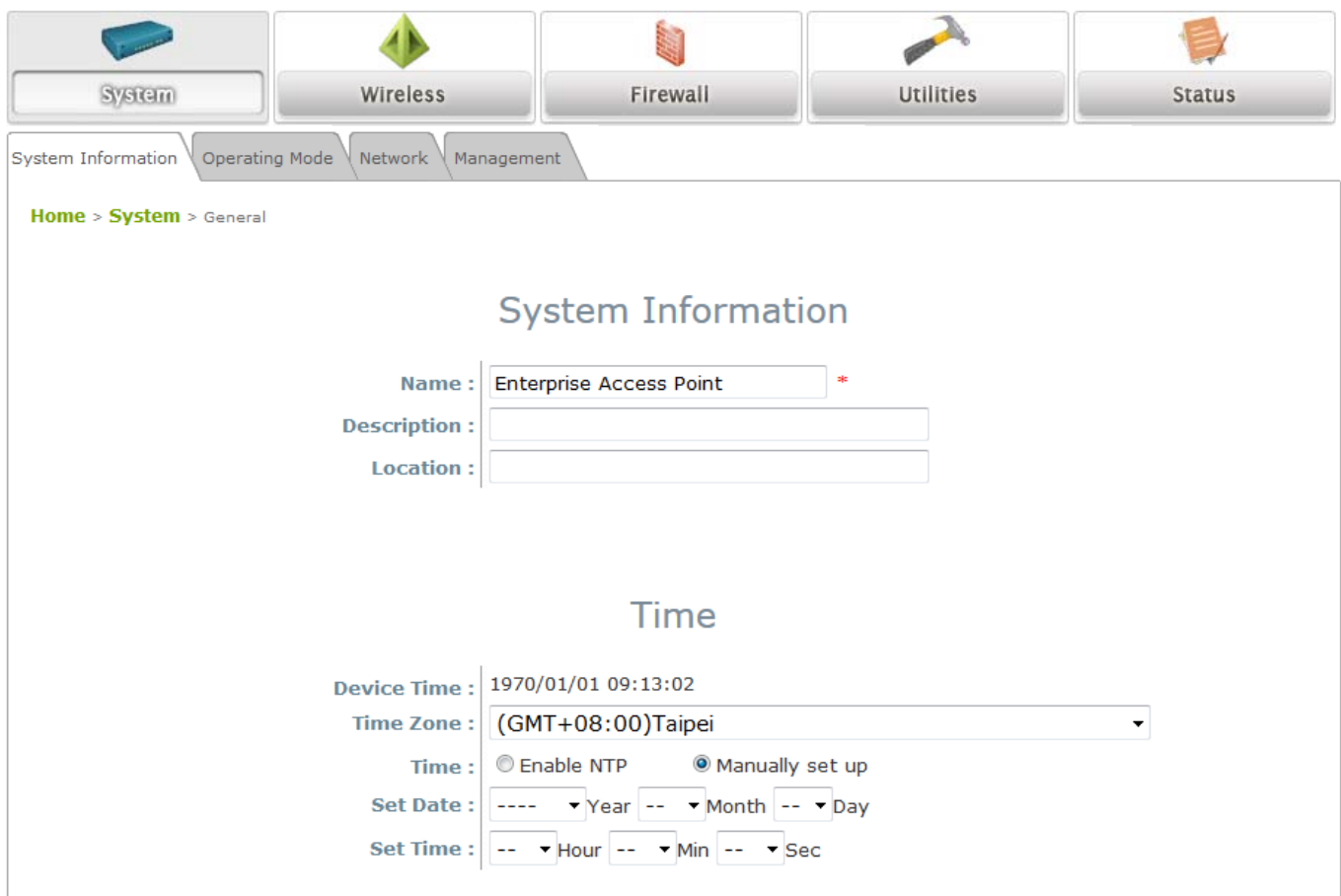
8.1 System

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

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

8.1.1 System Information

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



System Information

Operating Mode Network Management

Home > System > General

System Information

Name : Enterprise Access Point *

Description :

Location :

Time

Device Time : 1970/01/01 09:13:02

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

- **System Information**

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

- *Name*: The system name used to identify this system

- *Description*: Further information of the system.
- *Location*: Information about the geographical location of the system, which can help the administrator locate it easily.

- **Time**

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

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

(1) **Enabled NTP:**

By selecting *Enabled NTP*, the Access Point synchronizes its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address or domain name must be provided. If FQDN (Full Qualified Domain Name) is used as the IP address of NTP server, the DNS server must also be activated (please refer to **8.1.3 Network Settings**).

Time

Device Time : 1999/12/31 16:05:36

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

Time : Enable NTP Manually set up

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

NTP Server 2 :

(2) **Manually set up:**

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

Time

Device Time : 1999/12/31 16:02:29

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

Time : Enable NTP Manually set up

Set Date : ---- Year -- Month -- Day

Set Time : -- Hour -- Min -- Sec

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

8.1.2 Operating Mode

OWL530 / EAP210 supports two operation modes: CPE mode and AP mode. The administrator can set the desired mode on this page, and then configure the system according to deployment needs.

The screenshot shows the web interface for configuring the Operating Mode. At the top, there are four tabs: 'System Information', 'Operating Mode', 'Network', and 'Management'. Below the tabs, a breadcrumb trail reads 'Home > System > Operating Mode'. The main heading is 'Operating Mode'. Underneath, the 'Operating Mode' is set to 'CPE Mode', indicated by a selected radio button. The 'AP Mode' radio button is unselected. At the bottom, there are two yellow buttons: 'SAVE' and 'CLEAR'.

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

8.1.3 Network Settings

WAN and LAN settings can be configured on this page.

System Information
Operating Mode
Network
Management

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

WAN Configuration

Mode : Static DHCP

IP Address : *

Netmask : *

Default Gateway : *

Primary DNS Server : *

Alternate DNS Server :

Bandwidth Limit : Download : Mbps
 Upload : Mbps

* (0~999 for Kbps, 0~300 for Mbps, 0:unlimited)

Dynamic DNS (DDNS)

DDNS : Disable Enable

Provider : v

Host Name :

User Name / E-mail :

Password / Key :

LAN Configuration

IP Address : *

Netmask : *

DHCP Server : Disable Enable

Start IP : *

End IP : *

Preferred DNS Server : *

Alternated DNS Server :

WINS Server IP :

Domain Name :

Lease Time : v

- **WAN Configuration:** Determine the way to obtain the IP address, by static or DHCP.
- **Mode:** Determine the way to obtain the IP address, by *DHCP* or *Static*.
 - **Static:** The administrator can manually set up the static WAN IP address.
 - **IP Address:** The IP address of the WAN port.
 - **Netmask:** The subnet mask of the WAN port.
 - **Gateway:** The gateway IP address of the WAN port.
 - **Primary DNS Server:** The IP address of the primary DNS (Domain Name System) server.
 - **Secondary DNS Server:** The IP address of the substitute DNS server.
 - **DHCP:** This connection type is applicable when the system is connected to a network with the presence of a DHCP server; all related IP information required will be provided by the DHCP server automatically.
- **Bandwidth Limit:**
 - **Download:** The maximum download bandwidth of WAN interface to be shared by clients.
 - **Upload:** The maximum upload bandwidth of the WAN interface to be shared by clients.
- **Dynamic DNS:** The option can be enabled to bind FQDN-compliant Host Name with this device. If enabled, the service Provider must be chosen from the drop-down list with provided Host Name, User Name, User Email and Password.
- **DDNS:** Select *Enable* to activate this function or *Disable* to inactivate it.
- **Provider:** The name of the DDNS provider that the system is registered with. Select a DDNS provider from the drop-down list box.
- **Host Name:** The FQDN registered with the selected DDNS provider.
- **User name/ E-mail:** The account ID, user name or e-mail, registered with the DDNS provider.
- **Password/ Key:** The password of the account registered with the DDNS provider.
- **LAN Configuration:** Configure LAN and DHCP settings on this page. IP Address and Netmask are required fields to set up LAN interface.
 - **IP Address:** The IP address of the LAN port.
 - **Netmask:** The Subnet mask of the LAN port.
 - **DHCP Server:** If enabled, devices connected to this system can obtain an IP address automatically.
 - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
 - **Start IP / End IP:** Specify the range of IP addresses to be distributed by the DHCP server to clients.
 - **Preferred DNS Server:** Enter the IP address of a preferred DNS server; this field is required.
 - **Alternate DNS Server:** Enter the IP address of a secondary DNS server; this is optional.
 - **WINS Server IP:** Enter the IP address of a WINS (Windows Internet Name Service) server; this is optional.
 - **Domain Name:** Enter the domain name for this network.

- **Lease Time:** It can be chosen from the drop-down list to renew Leased LAN IP.

8.1.4 Management

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

System Information Operating Mode Network Management

Home > System > Management Services

Management Services

SNMP Configuration : Disable Enable

Community String :

Read :

Write :

Trap : Disable Enable

Server IP :

System Log : Disable Enable

SYSLOG Server IP :

Server Port :

SYSLOG Level :

UPnP Configuration : Disable Enable

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

- **Remote Syslog:** By enabling this function, specify a remote Syslog server to accept system log messages from the system remotely.
 - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
 - **Server IP:** The IP address of the Syslog server for receiving the reported events.
 - **Server Port:** The port number of the Syslog server.
 - **Syslog Level:** Select the desired level of received events from the drop-down list box.

- **UPnP Configuration:** This option can be enabled if UPnP service is required by LAN device.
 - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.

8.2 Wireless

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

8.2.1 General Settings

This section is for manual configuration of the system RF settings. Manually enter the uplink ESSID to associate with on this page. Security can be set on the “Security” tab to be discussed in section 8.2.3. For automatic configuration, use the ‘Site Survey’ tab (discussed in section 8.2.4) to search for the desired SSID.

The screenshot shows the configuration interface for the Wireless section. At the top, there are five main tabs: System, Wireless (selected), Firewall, Utilities, and Status. Below these are sub-tabs for General, Advanced, Security, and Site Survey. The current page is titled 'General Settings' and contains the following fields:

- ESSID:** A text input field containing '4ipnetAP-A1' with a red asterisk to its right.
- Transmit Power:** A dropdown menu currently set to 'Level 1'.
- ACK Timeout:** A text input field containing '0' with a red asterisk and the text '(0 - 255, 0:Auto, Unit:4 micro seconds)' to its right.

- **ESSID:** The ESSID (Service Set ID) of the client device that the system is to be associated with.
- **Transmit Power:** The signal strength transmitted from the system. Select the Transmit Power Level from the drop-down list box. *Level 1 is the actual highest power, Level 2 is the highest power minus 1dBm, so on and so forth.*
- **ACK Timeout:** When packet loss is increasing over longer distance, ACK Timeout can be used to alleviate this issue.

8.2.2 Advanced Wireless Settings

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

System Wireless Firewall Utilities Status

General Advanced Security Site Survey

Home > Wireless > Advanced

Advanced Wireless Settings

RTS Threshold : *(1 - 2346)

Roaming : Disable Enable

Background Scanning Period : *(10 - 600 seconds)

Roaming Check RSSI Threshold : *(15 - 85)

- **RTS Threshold:** To control station access to the medium and to alleviate this effect of the hidden terminal problem, the administrator can tune this RTS threshold value. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the Access Point or in areas where the clients are far apart and can detect only Access Point and not each other.
- **Roaming:** When the Access Point is mobile and is operating in CPE mode, Enable the Roaming feature to determine:
 - **Background Scanning Period:** The AP scans in the background for a signal with a higher RSSI at each configured time interval (in seconds).
 - **Roaming Check RSSI Threshold:** When the signal falls below the configured RSSI threshold, the AP begins scanning for higher RSSI signals to associate to.

8.2.3 Security Settings

The system supports various authentication and data encryption methods when wireless settings are manually configured. The security type includes: None, WEP and WPA-PSK.

The screenshot shows the 'Security Settings' page in a web interface. At the top, there are tabs for 'General', 'Advanced', 'Security', and 'Site Survey'. Below the tabs is a breadcrumb trail: 'Home > Wireless > Security'. The main heading is 'Security Settings'. A single configuration item is visible: 'Security Type : Open' with a dropdown arrow.

- **Open:** No authentication is required.
- **WEP:** WEP (Wired Equivalent Privacy) supports key length of 64/128/152 bits.

The screenshot shows the 'Security Settings' page with 'WEP' selected in the 'Security Type' dropdown. Below this, several options are available:

- 802.11 Authentication:** Radio buttons for 'Open System' (selected), 'Shared Key', and 'Auto'.
- WEP Key Length:** Radio buttons for '64 bits' (selected), '128 bits', and '152 bits'.
- WEP Key Format:** Radio buttons for 'ASCII' (selected) and 'Hex'.
- WEP Key Index:** A dropdown menu set to '1'.
- WEP Keys:** Four input fields for keys. The first field contains '11111', and the others are empty.

- **802.11 Authentication:** Select from *Open System*, *Shared Key*, or *Auto*.
- **WEP Key Length:** Select from *64-bit*, *128-bit* or *152-bit* key length.
- **WEP Key Format:** Select from *ASCII* or *Hex* format for the WEP key.
- **WEP Key Index:** Select a key index from 1 through 4. The WEP key index is a number that specifies which WEP key to use for the encryption of wireless frames during data transmission.
- **WEP Keys:** Provide WEP key value; the system supports up to 4 sets of WEP keys.

- **WPA-Personal:** WPA-Personal supports pre-shared key authentication and WPA2 data encryption.

General Advanced Security Site Survey

Home > Wireless > Security

Security Settings

Security Type : WPA-Personal ▾

Cipher Suite : WPA2 ▾

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

Pre-shared Key :

Group Key Update Period: second(s)

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

8.2.4 Site Survey

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

Site Survey is a useful tool to provide information on the surrounding wireless environment; available APs are shown with their respective SSID, MAC Address, Channel, Rate setting, Signal reading and Security type.

The administrator can click Setup or Connect to configure the wireless connection according to the mentioned readings.

The screenshot shows the 'Site Survey' tab selected in the navigation menu. Below the menu, there is a breadcrumb trail: Home > Wireless > Site Survey. The main heading is 'Scan Result', followed by a 'Scan Again!' button. A table displays the scan results for three APs. Below the table, there is a configuration panel for the selected AP (Cip-Cherry), including a dropdown for 'Pre-shared Cipher' (TKIP), radio buttons for 'Pre-shared Key Type' (PSK(Hex) and Passphrase), a text input for 'Pre-shared Key', and a 'Connect' button.

| SSID | MAC Address | Channel | Rate | Signal | Security | Setup / Connect |
|------------|-------------------|---------|------|--------|----------|-----------------|
| Cip-AP | 0A:11:A3:08:09:56 | 6 | 54 | 38 | None | Connect |
| Cip-Cherry | 06:11:A3:08:09:56 | 6 | 54 | 37 | WPA-PSK | Setup |
| Cip-wep | 00:11:A3:08:09:56 | 6 | 54 | 37 | WEP | Setup |

Pre-shared Cipher : TKIP

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

Pre-shared Key :

Connect

AP Scan Result (example)

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

| | | | | | | |
|--------|-------------------|---|----|----|------|---------|
| Cip-AP | 0A:11:A3:08:09:56 | 6 | 54 | 38 | None | Connect |
|--------|-------------------|---|----|----|------|---------|

- **Setup:** Click **Setup** to configure security settings for associating with the respective AP or repeater.
 - **WEP:** Click **Setup** to configure the WEP setting for associating with the target AP.

| | | | | | | |
|---------|-------------------|----|----|----|-----|-------|
| Cip-wep | 06:1F:D4:39:10:74 | 11 | 54 | 50 | WEP | Setup |
|---------|-------------------|----|----|----|-----|-------|

The following configuration box will then appear at the bottom of the screen. For more information on the WEP security settings, please refer to **Section 8.2.3 Security Settings**.

WEP Key Type : Open Shared Auto

WEP Key Length : 64 bits 128 bits 152 bits

WEP Key Format : ASCII Hex

WEP Key Index : ▼

WEP Keys :

1

2

3

4

- **WPA-PSK:** Click **Setup** to configure the WPA-PSK setting for associating with the target AP.

| | | | | | | |
|------------|-------------------|---|----|----|---------|-------|
| Cip-Cherry | 06:11:A3:08:09:56 | 6 | 54 | 37 | WPA-PSK | Setup |
|------------|-------------------|---|----|----|---------|-------|

The following configuration box will then appear at the bottom of the screen. For more information on the WPA-PSK security settings, please refer to **Section 8.2.3 Security Settings**.

Pre-shared Cipher : ▼

Pre-shared Key Type : PSK(Hex) *(64 chars)

Passphrase *(8 - 63 chars)

Pre-shared Key :

8.3 Firewall

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

8.3.1 IP/ Port Forwarding

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

The screenshot shows the 'IP/Port Forwarding' configuration page. At the top, there are navigation tabs for 'System', 'Wireless', 'Firewall', 'Utilities', and 'Status'. Below these, there are sub-tabs for 'IP/Port Forwarding' and 'DMZ'. The main content area is titled 'IP/Port Forwarding' and contains a breadcrumb trail: 'Home > Firewall > IP/Port Forwarding'. Below the title, there are four input fields: 'Service Name', 'External Port Range' (with a tilde symbol between two boxes), 'Internal IP Address', and 'Protocol' (a dropdown menu set to 'TCP/UDP'). An 'Add' button is located to the right of the 'Protocol' dropdown. Below this form is a table titled 'IP/Port Forwarding' with the following columns: 'Item', 'Service Name', 'External Port Range', 'Internal IP Address', 'Protocol', 'State', 'Delete', and 'Edit'.

- **Service Name:** The administrator can provide an easy remembered alias for the specific forwarding.
- **External Port Range:** The range of external port for forwarding traffic can be defined manually by the administrator.
- **Internal IP Address:** Enter the LAN IP address to receive the forwarding traffic.
- **Protocol:** Forwarding traffic protocol can be selected from drop-down list to be *TCP/UCP*, *TCP* or *UDP*.
- **Add:** Click **Add** to activate the new service.
- **IP/ Port Forwarding:** Details of current services available. Click **Delete** to remove the specified service. Click **Edit** to configure the current setting.

IP/Port Forwarding

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

8.3.2 Demilitarized Zone

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

IP/Port Forwarding
DMZ

[Home](#) > [Firewall](#) > Demilitarized Zone

Demilitarized Zone

State : Disable Enable

Internal IP Address : *

SAVE

CLEAR

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

8.4 Utilities

The system provides **Change Password**, **Backup & Restore**, **System Upgrade**, **Reboot**, and **Upload Certificate** functions for system maintenance.

8.4.1 Change Password

The administrator can update or change password.

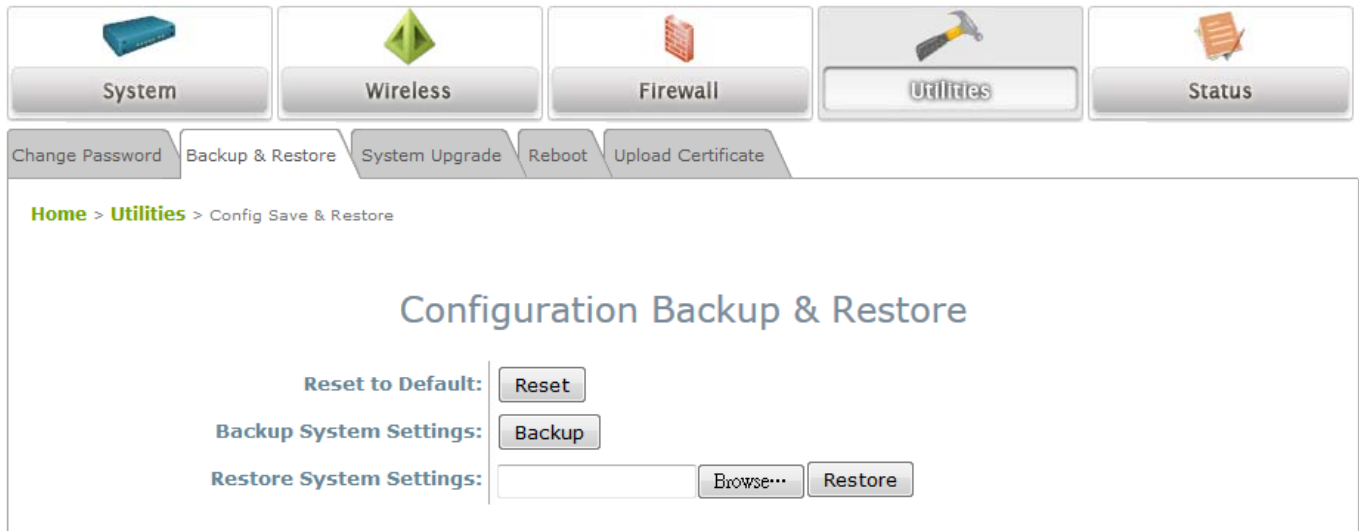
The screenshot displays the web management interface for the 4IPNET Enterprise Access Point. At the top, there are five main navigation buttons: System, Wireless, Firewall, Utilities (which is highlighted), and Status. Below these, there are five sub-navigation tabs: Change Password, Backup & Restore, System Upgrade, Reboot, and Upload Certificate. The main content area shows the breadcrumb path: Home > Utilities > Change Password. The title of the page is "Change Password". There are two sections for password changes. The first section is for the "admin" account, with fields for Name (admin), New Password (with a note "*up to 32 characters"), and Re-enter New Password. The second section is for the "user" account, with fields for Name (user), New Password (with a note "*up to 32 characters"), and Re-enter New Password.

- **“admin” account:** Enter a new password, and then re-enter it in the *Re-enter New Password* field. Click **SAVE** to activate the new password.
- **“user” account:** Enter a new password, and then re-enter it in the *Re-enter New Password* field. Click **SAVE** to activate the new password.

In addition to the admin account, there is a **“user”** account capable of accessing the web management interface with configuration limitations. The “user” account will not be able to reboot AP or change wireless settings. This account is typically issued by IT staff for employees to monitor AP statuses.

8.4.2 Backup & Restore

This function is used to backup or restore the current settings. The system can be restored to the default setting by clicking on Reset. The setting of the device can be backup to a file. It can be used to duplicate setting to the other OWL530 devices.



- **Reset to Default:**

- Click **Reset** to load the factory default settings of OWL530. A pop-up will appear to re-confirm the request to restart the system. Click **OK** to proceed, or click **Cancel** to cancel the restart request.



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

8.4.3 System Upgrade

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

The screenshot shows the 'System Upgrade' utility interface. At the top, there are five main menu buttons: System, Wireless, Firewall, Utilities (highlighted), and Status. Below these are sub-menu buttons: Change Password, Backup & Restore, System Upgrade (highlighted), Reboot, and Upload Certificate. The breadcrumb path is 'Home > Utilities > System Upgrade'. The main title is 'System Upgrade'. The interface displays the following information and controls:

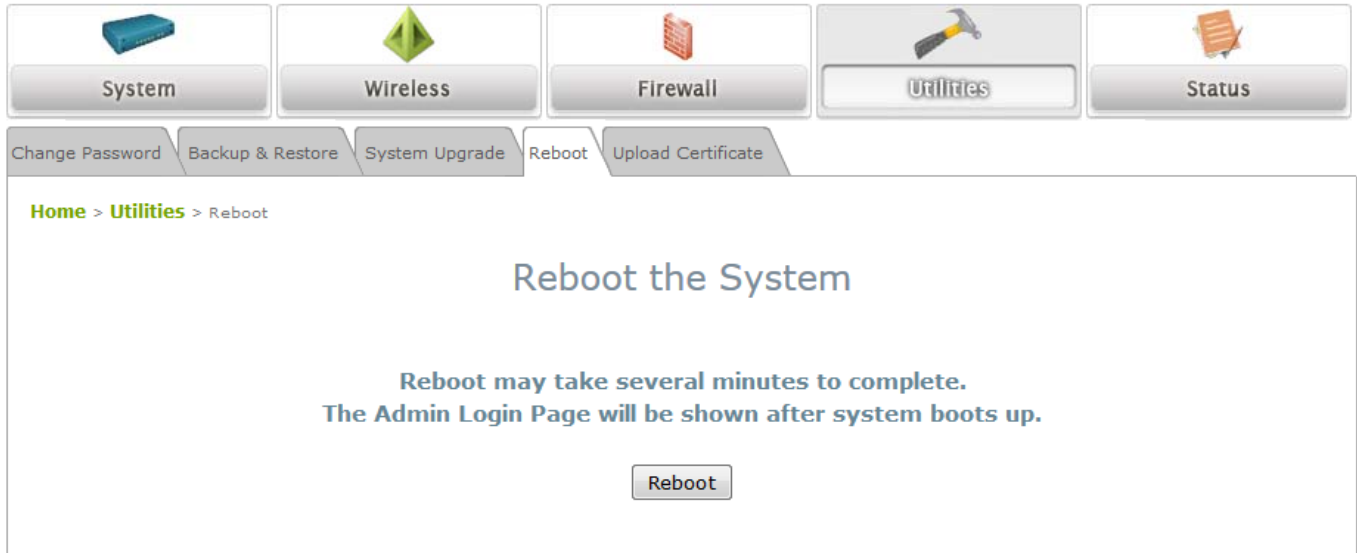
| | |
|------------------------------|--|
| Current Version: | 1.10.00 |
| Current Build Number: | 1.13-1.6891 |
| File Name: | <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/> |
| Upgrade by TFTP: | IP Address: <input type="text"/> Port: <input type="text"/> |
| | File Name: <input type="text"/> <input type="button" value="Apply"/> |

▶▶ **Note:**

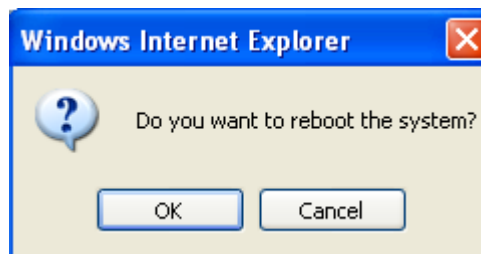
- To prevent data loss during firmware upgrade, please back up the current settings before proceeding further.
- Please restart the system after the upgrade. Do not interrupt the system, i.e. power on/off, during the upgrade or restart process as this may damage the system.

8.4.4 Reboot

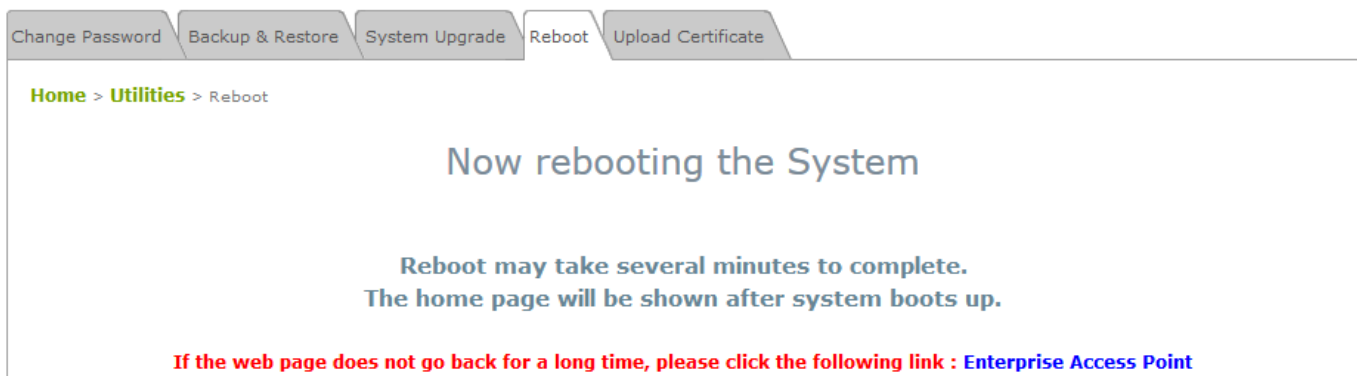
The administrator can reboot the device remotely. Click **Reboot** to restart the system immediately.



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



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



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

8.4.5 Upload Certificate

In CPE mode, a certificate can be uploaded for HTTPS protected login. Click **Browse** to select the desired certificate and the matching Private Key. Uploading a certificate allows encrypted content transfer.

Change Password Backup & Restore System Upgrade Reboot Upload Certificate

Home > Utilities > Upload Certificate

Upload Certificate

| Upload Private Key | |
|--------------------|--------------------------------|
| File Name | <input type="text"/> Browse... |

| Upload Certificate | |
|--------------------|--------------------------------|
| File Name | <input type="text"/> Browse... |


Use Default Certificate


8.5 Status


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


8.5.1 System Overview


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


System


Wireless


Firewall


Utilities


Status

System Overview

Interfaces

Event Log


Monitor

DHCP Lease

UPnP


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

System Overview




System

| | |
|-------------------------|--|
| System Name | Enterprise Access Point - OWL5... |
| Firmware Version | 1.10.00 |
| Build Number | 1.13-1.6891 |
| Location | |
| Site | EN-A |
| Device Time | 2013/12/02 07:48:20 |
| System Up Time | 0 days, 5:32:07 |
| CPU/RAM Usage | 1.92% / 30.70% Plot |
| Operating Mode | CPE |




Radio Status

| | |
|------------------------|--|
| Status | Connected |
| SSID | felix220-a3 |
| MAC Address | 00:1F:D4:94:19:3C |
| Channel | 9 |
| Signal Strength | 94 Plot |
| Security | WPA-PSK |



LAN Interface

| | |
|--------------------|-------------------|
| MAC Address | 00:1F:D4:02:C9:F3 |
| IP Address | 192.168.21.1 |
| Subnet Mask | 255.255.255.0 |
| DHCP Server | Enabled |



WAN Interface

| | |
|--------------------|---------------------------------|
| Mode | DHCP |
| MAC Address | 00:1F:D4:02:C9:F4 |
| IP Address | 10.1.121.10 |
| Subnet Mask | 255.255.0.0 |
| Gateway | 10.1.3.40 |
| Bandwidth | Down: Unlimited / UP: Unlimited |

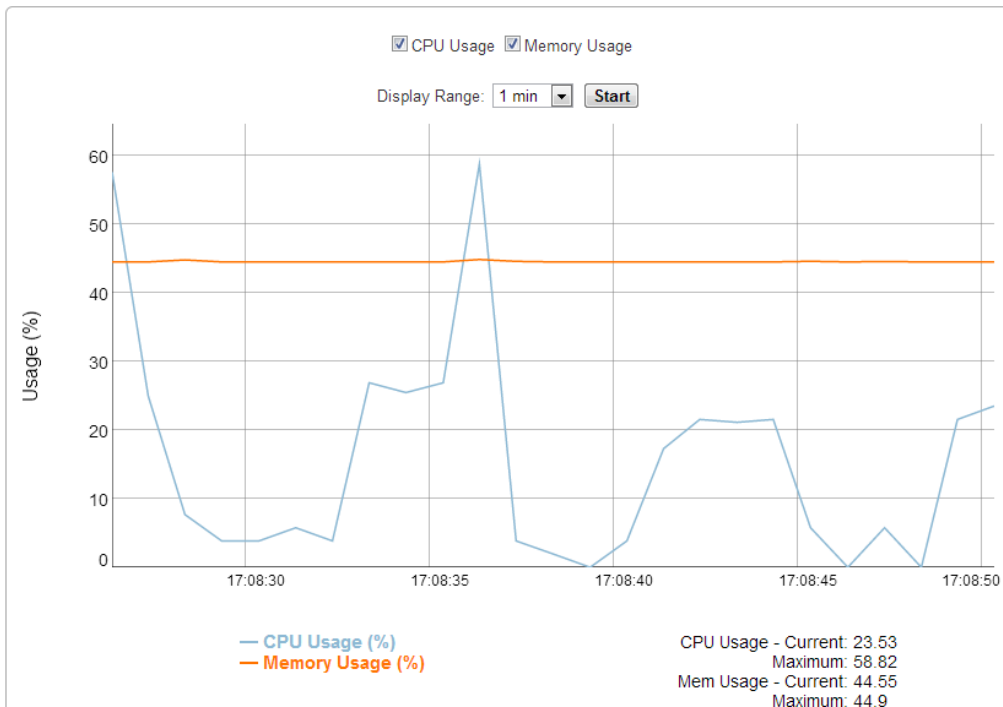
The description of the table is shown below:

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

The system supports graph displays of CPU/RAM usage and Signal Strength RSSI on the status page.

The Time Axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

CPU / Memory Usage



8.5.2 Interfaces

Traffic information is available per interface. Recorded data includes **Packets In**, **Packets Out**, **Traffic In (kb)**, and **Traffic Out (kb)**. The Time Axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

System | Wireless | Firewall | Utilities | Status

System Overview | Interfaces | Event Log | Monitor | DHCP Lease | UPnP

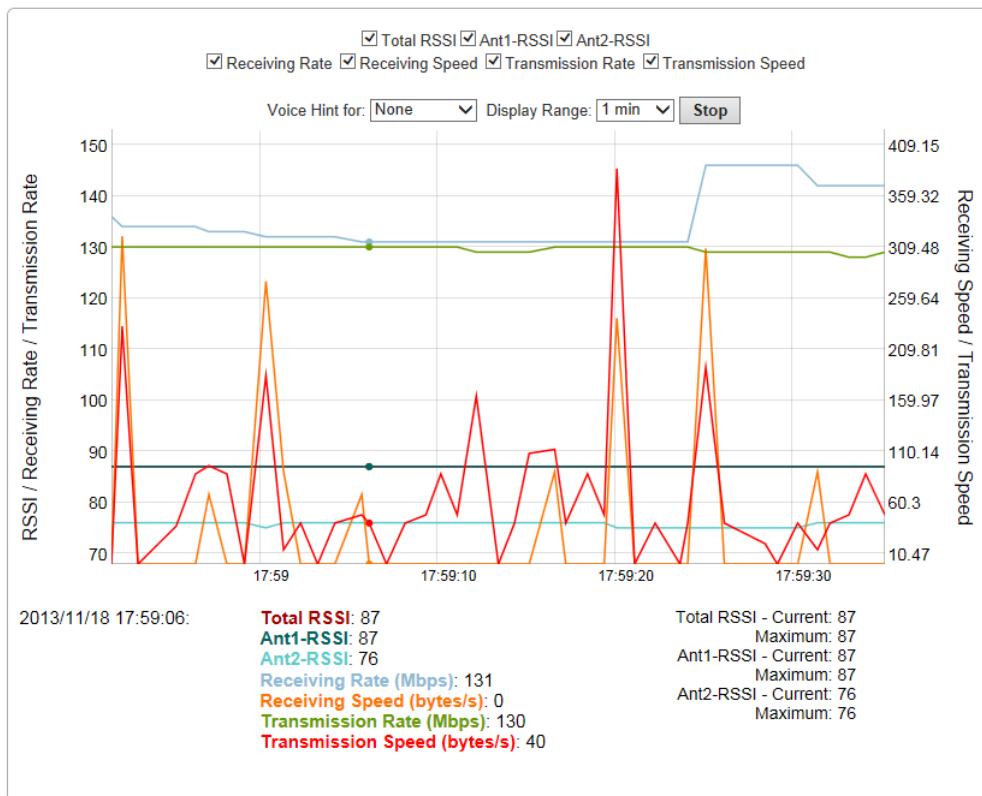
Home > Status > Interface

Interface Traffic

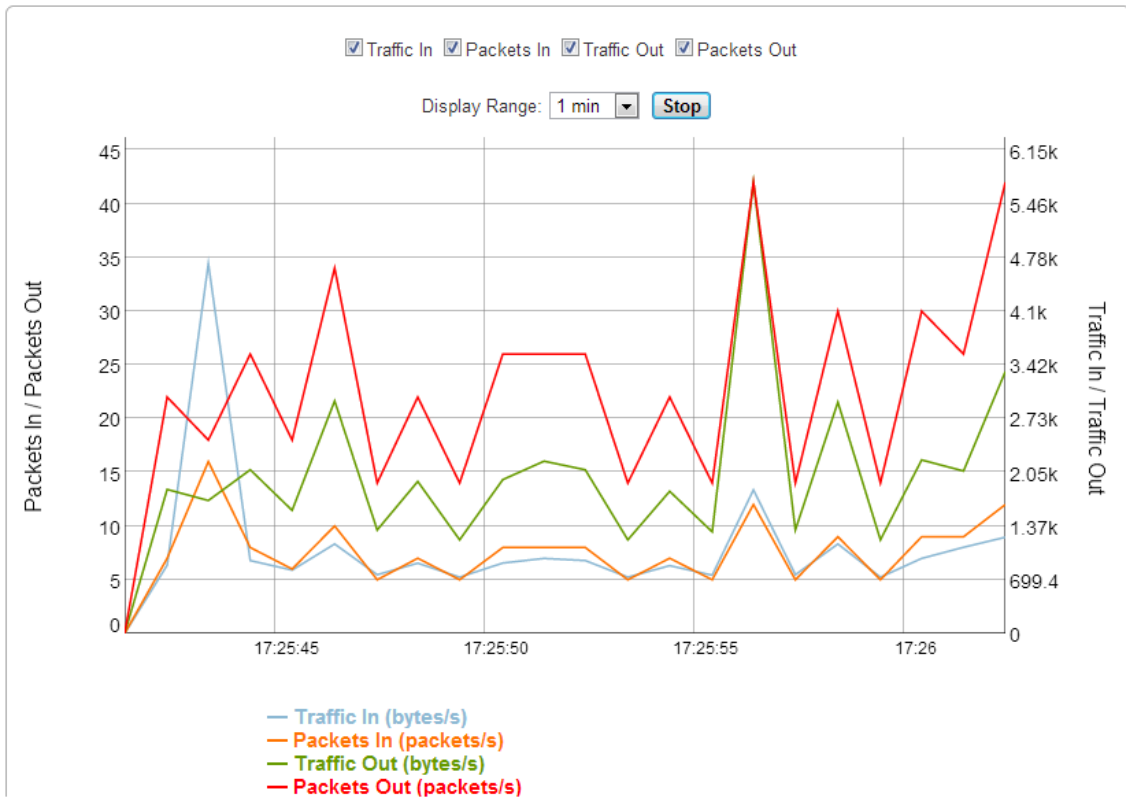
Interface List

| Interface | Traffic Out (KB) | Packets Out | Traffic In (KB) | Packets In | Real Time |
|-----------|------------------|-------------|-----------------|------------|----------------------|
| WAN | 6827 | 17515 | 7127 | 47853 | Plot |
| LAN | 17 | 39 | 46 | 293 | Plot |

WAN Status



LAN Traffic



8.5.3 Event Log

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

System Overview Interfaces **Event Log** Monitor DHCP Lease UPnP

Home > Status > Event Log

Event Log

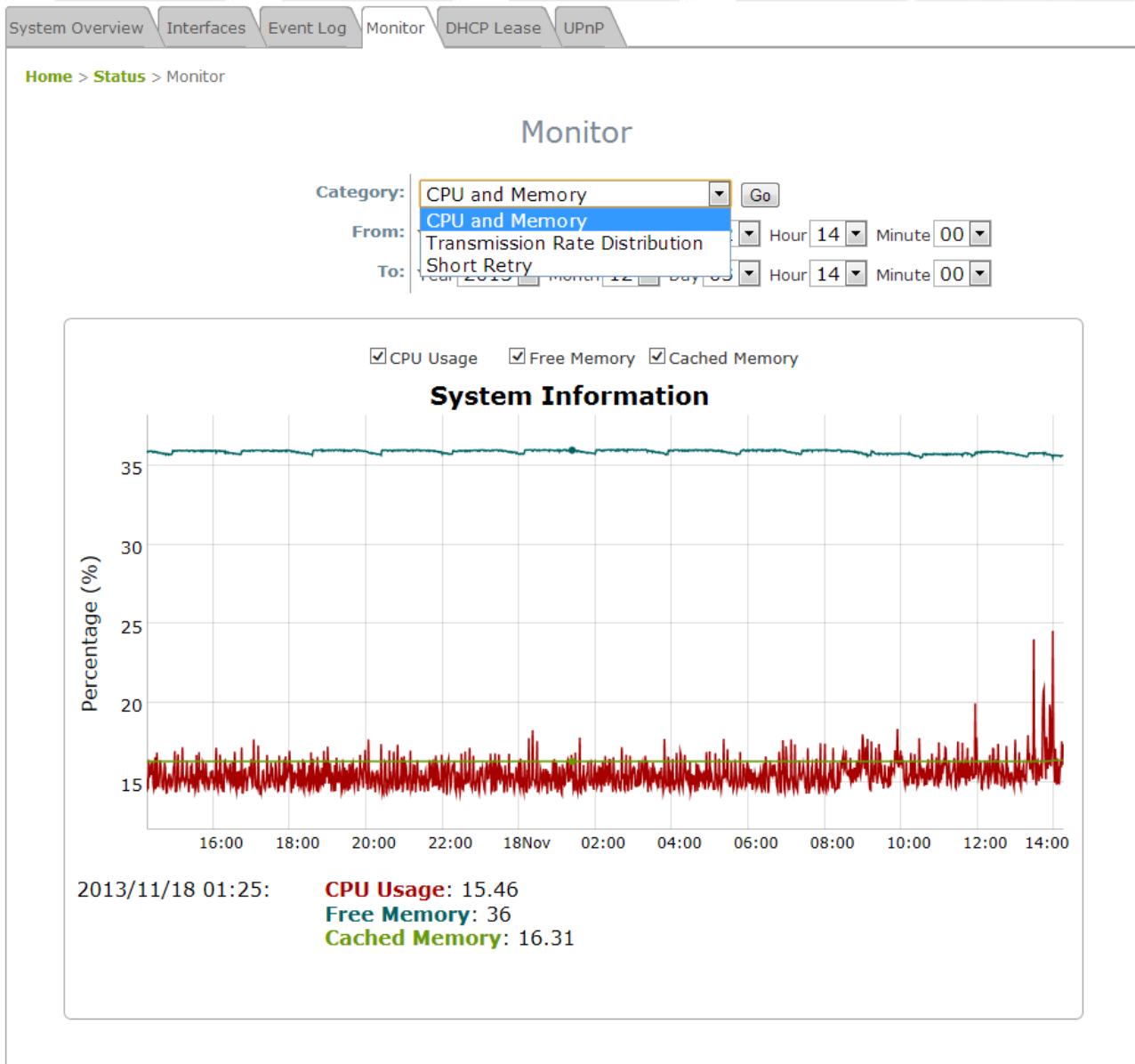
```
Jan 1 00:00:01 syslogd started: BusyBox v1.12.4
Jan 1 00:00:01 logd@localhost crond[1835]: crond (busybox 1.12.4) started, log level 8
Jan 1 00:02:01 logd@localhost crond[1835]: USER root pid 2241 cmd /etc/rc.d/rc.systemtime sync_ntp
```

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

- **Date/ Time:** The date and time of the record when the event happened.
- **Hostname:** Indicate which Host records this event. Note that all events in this page are local events and this field of all events is the same. However, in remote syslog service, this field will help the network administrator identify which event is from this system. For more information, please refer to **Section 8.1.4 Management Services**.
- **Process name (with square brackets):** Indicate which process with the specific event is associated.
- **Description:** Description of the event.

8.5.4 Monitor

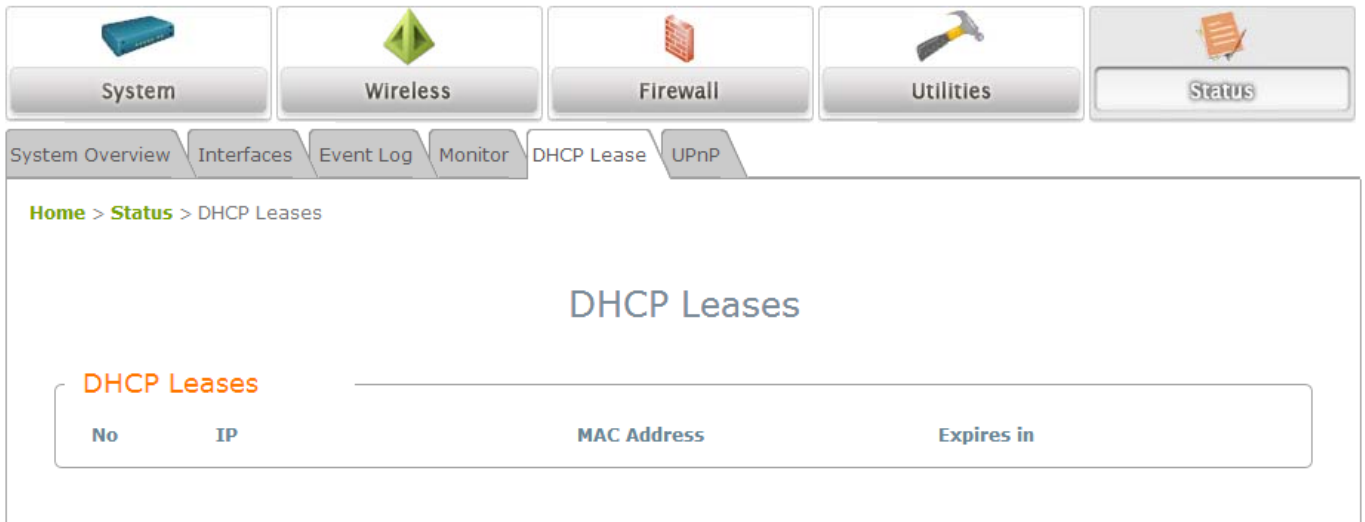
For a quick overview on the AP's performance, the 'Monitor' feature displays an RRD graph recording CPU utilization, memory usage, associated station numbers, TX rate distribution, airtime utilization, and short retries.



The begin and end time for the RRD graph can be selected for filtering data. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

8.5.5 DHCP Leases

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



Home > Status > DHCP Leases

DHCP Leases

DHCP Leases

| No | IP | MAC Address | Expires in |
|----|----|-------------|------------|
|----|----|-------------|------------|

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

8.5.6 UPnP Status

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

System Overview Interfaces Event Log Monitor DHCP Lease UPnP

Home > Status > UPnP Status

UPnP Status

IGD Portmap

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

- **IGD Portmap:**

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

9. Console Interface Configuration

Via the console port, administrators are able to enter the console interface to reset the access point to its factory default settings. In order to connect to the console port of a 4ipnet access point, a console, modem cable, and a terminal simulation program, such as PuTTY are needed. There are 2 ways to access the console interface:

1. Direct Connection

Notebook > USB-to-RS232 with DB9 connector > Console Cable > Console Port

The USB-to-RS232 cable is not supplied with standard packaging. It is recommended to use only the console cable provided with the packaging.



USB-RS232



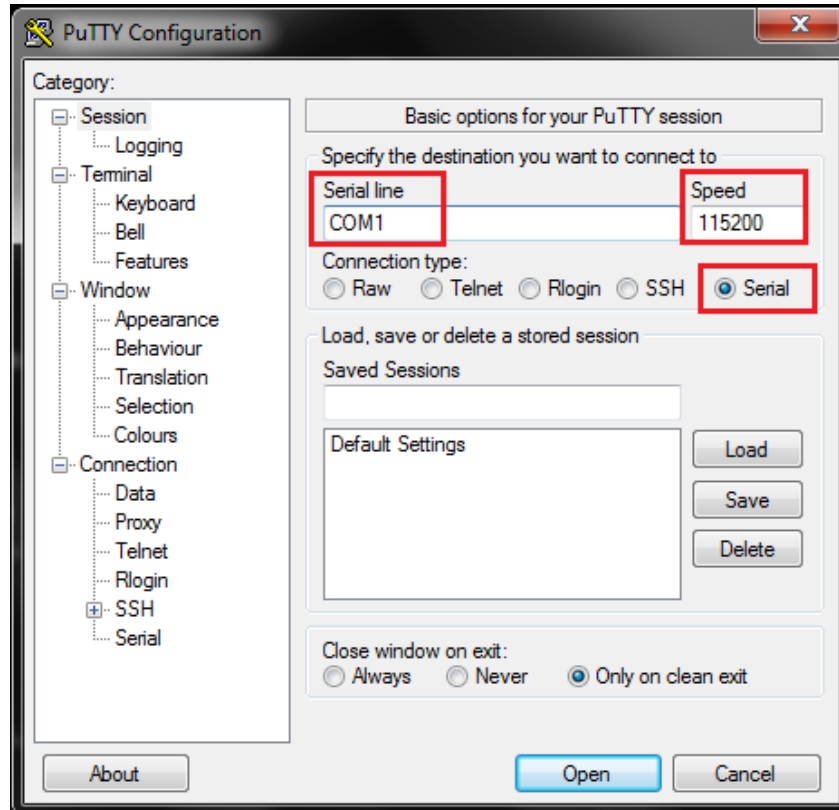
Console Cable-RS232



Console Cable – RJ45

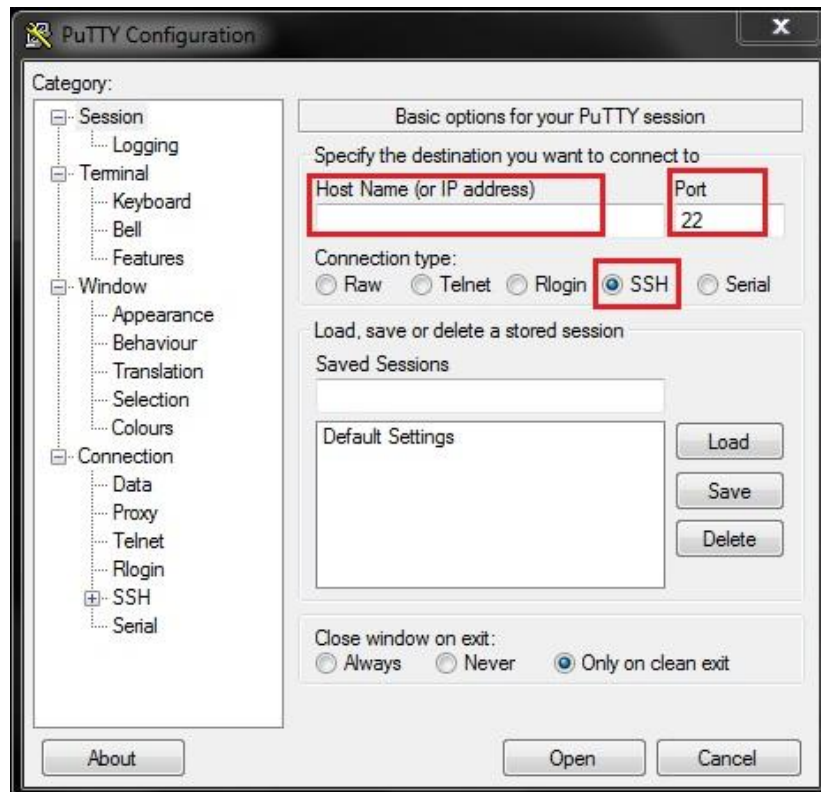
The speed (baud rate) needs to be selected for direct connections and the baud rate is summarized as follows:

| Model | Baud Rate (bps) |
|--------|-----------------|
| EAP210 | 115200 |
| EAP220 | 115200 |
| EAP320 | 115200 |
| EAP747 | 115200 |
| EAP750 | 115200 |
| EAP757 | 115200 |
| OWL530 | 115200 |
| OWL610 | 115200 |
| OWL620 | 115200 |

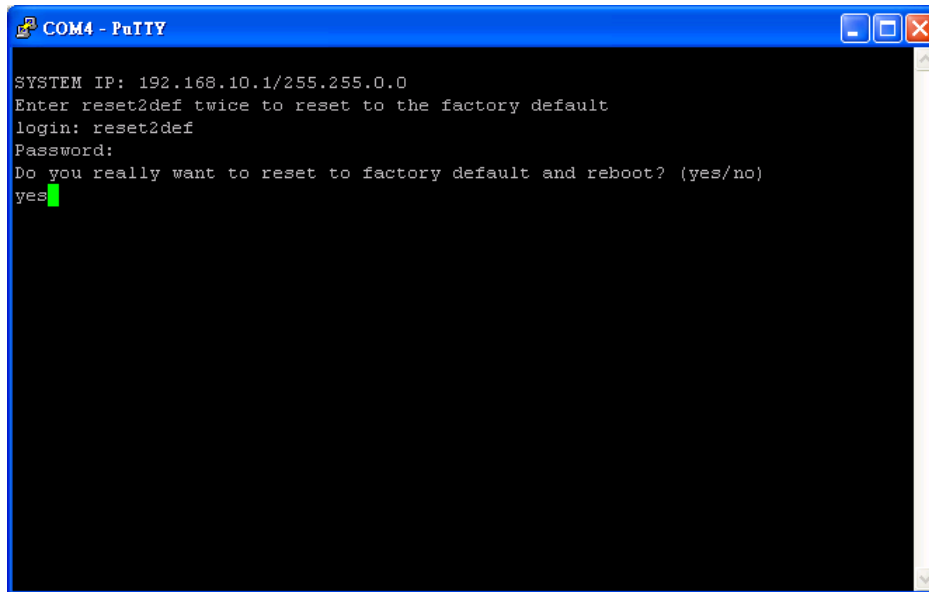


2. Remote Connection

The system supports access to the console interface via SSH. Typically SSH utilizes Port 22 and would require the WAN IP address for access.



To reset the system to factory default through the console interface, Login as “reset2def” and enter “reset2def” as your password.



```
COM4 - PuTTY
SYSTEM IP: 192.168.10.1/255.255.0.0
Enter reset2def twice to reset to the factory default
login: reset2def
Password:
Do you really want to reset to factory default and reboot? (yes/no)
yes
```

If the console connection is not readily available, the IP address of the AP can be retrieved with an IP Discovery Utility provided by 4ipnet. Simply connect via an Ethernet cable and run the Discovery Utility. Note that the laptop/PC connecting to the AP must run in Windows XP compatible mode and a static IP must be set.

P/N: V10020140326