

OW-1000A

Outdoor Wireless Access Point

User's Manual

BEFORE INSTALLING THE UNIT, PLEASE READ THIS MANUAL THOROUGHLY, AND RETAIN IT FOR FUTURE REFERENCE.

Notice:

The unit must be used 12V, 1A power adaptor for PoE power supply!

The unit would be dead when using wrong power supply!

► Contents

Chapter 1.	Introduction	5
1.1	Introducing the OW-1000A.....	5
1.2	Product Features	5
1.3	Package Contents	5
1.4	System Requirements	6
1.5	Inline Power Injector (PoE)	6
Chapter 2.	Installation and Basic Configuration	7
2.1	Before You Start	7
2.2	Locate the OW-1000A and Inline Power Injector Ports.....	8
2.3	Preparing Installation.....	9
2.4	Basic Configuration	10
2.4.1	Basic Configuration Steps.....	10
2.4.2	Logging into the Web Interface	10
2.4.3	Set Operating Mode, IP Address, Subnet Mask, Default Route IP, DNS Server IP of OW-1000A.....	13
2.4.4	Set Wireless SSID for Wireless Interface	15
2.4.5	Set Wireless Encryption for Wireless Interface ..	16
2.4.6	Change Supervisor Account & Password.....	17
2.4.7	Upgrade the Firmware	18
Chapter 3.	Network Topologies.....	19
3.1	Wireless Client Bridge-to-Central Wireless Bridge.....	20
Chapter 4.	All function on Device.....	21
4.1	SYSTEM.....	21
4.1.1	Administrator	21
4.1.2	Firmware	22
4.1.3	Configuration Tools.....	23
4.1.4	Status	24
4.1.5	Log	25
4.1.6	System Time.....	26
4.1.7	Reboot.....	27
4.2	NETWORK	28
4.2.1	Network	28
4.2.2	HotSpot (Captive Portal)	31
4.3	WIRELESS.....	32
4.3.1	Wi-Fi 1.....	33
4.3.2	Wi-Fi 2.....	33
4.3.3	Wi-Fi 3.....	33
4.3.4	Wi-Fi 4.....	33
4.4	ACL	34
4.4.1	ACL for Wi-Fi 1.....	34
4.4.2	ACL for Wi-Fi 2.....	34
4.4.3	ACL for Wi-Fi 3.....	34

4.4.4	ACL for Wi-Fi 4	34
4.5	SNMP	35
4.5.1	Agent Settings	35
4.6	EXIT	35
Chapter 5.	Specifications	36
Chapter 6.	Default Settings	39
6.1	SYSTEM	39
6.1.1	Administrator	39
6.1.2	Firmware	39
6.1.3	Configuration Tools	39
6.1.4	Status	39
6.1.5	Log	40
6.1.6	System Time	40
6.1.7	Reboot	40
6.2	NETWORK	41
6.2.1	Network	41
6.2.2	Hotspot	41
6.3	WIRELESS	42
6.3.1	Wi-Fi 1	42
6.3.2	Wi-Fi 2	43
6.3.3	Wi-Fi 3	44
6.3.4	Wi-Fi 4	45
6.4	ACL	46
6.4.1	ACL for Wi-Fi	46
6.4.2	ACL for Wi-Fi 2	46
6.4.3	ACL for Wi-Fi 3	47
6.4.4	ACL for Wi-Fi 4	47
6.5	SNMP	48
6.6	EXIT	48
Chapter 7.	Regulatory Compliance Information	49

Chapter 1. Introduction

1.1 Introducing the OW-1000A

The OW-1000A is fully interoperable with IEEE 802.11b/g compliant Outdoor Wireless Last-mile product. The OW-1000A operates in AP mode or remote bridge mode, and connects to OW-1000A AP/CB to construct point-to-point as well as point-to-multipoint topologies, for maximum flexibility in configuring building-to-building networks and WISP functions.

1.2 Product Features

- Outdoor enclosure in compliance with versatile industrial IP (Ingress Protection) level covering IP65
- RF transmit power 802.11b mode @ 11Mbps data rate
- RF transmit power 802.11g mode @ 54Mbps data rate
- Embedded 9dBi patch directional antenna and one SMA connector for external antenna used.
- Support 12VDC 1A Power-over-Ethernet (PoE)
- MAC address based access control

Hint: IP (Ingress Protection)

1.3 Package Contents

The product package contains the following items.

1. One (1) OW-1000AA Outdoor Wireless Access Point / Client Bridge unit
2. One (1) 100~240VAC, 50~60Hz AC to 12V/1A DC switching adapter
3. One (1) Inline Power Injector (PoE)
4. One (1) User manual CD-disc
5. One (1) wall mounting kit
6. One (1) band clamp

1.4 System Requirements

Installation of the OW-1000A Outdoor Wireless Access Point/Client Bridge requires the following:

1. A Windows-based PC/AT compatible computer (PC system requirement : better than PIII 800 or other 100% compatible equipment , OS : windows 2000/XP) or Ethernet data device with an available RJ-45 Ethernet port to run the configuration program or with TCP/IP connection to the Ethernet network.
2. A 10/100Base-T Ethernet RJ-45 Ethernet cable is connected to Ethernet network.
3. An AC power outlet (100~240V, 50~60Hz) supplies the power.

1.5 Inline Power Injector (PoE)

The OW-1000A is equipped with an Inline Power Injector module. The Inline Power Injector (PoE) delivers both data and power to OW-1000A unit via a signal Ethernet cable, and gives the following benefits to improve the performance vs. installation cost ratio.

- This works great in areas where you may not have power , like house roof.
- This also allows you to place the OW-1000A unit closer to the antenna, to make installation easier more thus reducing signal loss over antenna cabling.
- Ethernet signal travels well over CAT 5 cable but 2.4GHz signal doesn't do as well over antenna cabling.
- Ethernet cabling is much cheaper than Antenna cabling.






Chapter 2. *Installation and Basic Configuration*

This chapter describes the procedures of installing the OW-1000A.

2.1 Before You Start

After unpacking the system, make sure the following items are present and in good condition. Refer to below pictures for product image.

- 1.** OW-1000A Outdoor Wireless Access Point/Client Bridge unit
- 2.** 100~240VAC, 50~60Hz AC to 12V/1A DC switching adapter
- 3.** Inline Power Injector (PoE) 12VDC, 1A
- 4.** User manual CD-disc
- 5.** Wall/mast mounting kit, including two (2) band clamp

1. Unit	2. Adapter	3. PoE	4. CD
			
5. Wall mount kit			
			

2.2 Locate the OW-1000A and Inline Power Injector Ports

► Interface on the OW-1000A Unit

- **Ethernet Port 1** : for connecting the 30m RJ-45 CAT-5 Ethernet cable.

► Interface on the Inline Power Injector

- **Data Input Port 2** : for connecting cross-over Ethernet Cable to PC or straight Ethernet cable to Hub Switch Router .
- **DC Input Port 3** : power adapter 12V, 1 DC input.
- **Power & Data Output Port 4** : for connecting the 30m RJ-45 CAT-5 Ethernet Cable.
- **Grounding Port 5** : for connecting grounding wire.

Device

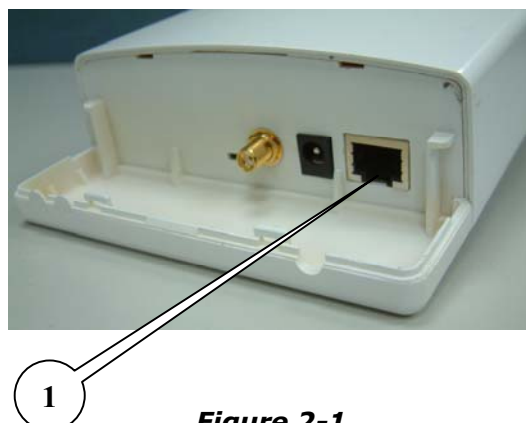
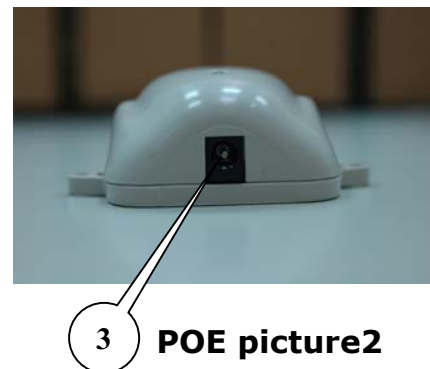
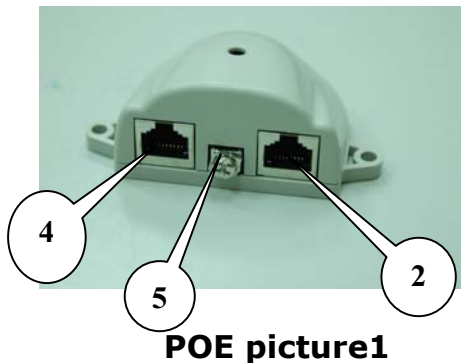


Figure 2-1
Power and Data Interface location on the PoE denoted by numbers 1-6.



2.3 Preparing Installation

Before installing OW-1000A for outdoor application or hard-to-reach location, we recommend configuring and test all the devices first.

For configuring the OW-1000A, please follow the quick steps below to power up the OW-1000A. Refer to **Figure 2-2** for steps 1 through 5.

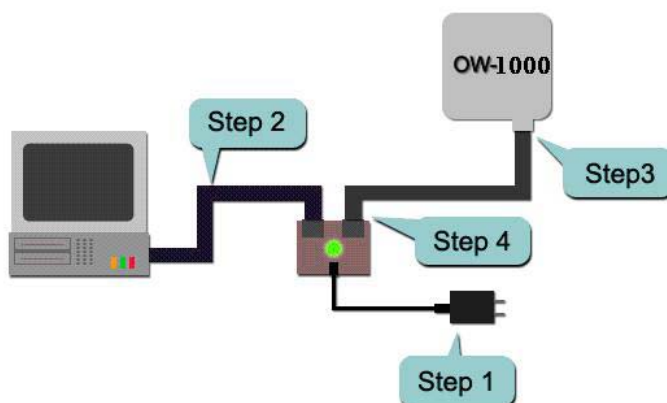


Figure 2-2

Step1 : Connect the DC plug of the AC/DC power adapter into the **DC Input Port** of Inline Power Injector and the wall-mount plug into a power outlet or power strip (refer to [page 6](#)). The Power LED on the Inline Power Injector will light up.

Step2 : Run the cross-over type uplink Ethernet cable from **Data Input Port** (refer to [page 6](#)) to the Ethernet port on a PC.

Step3 : Connect the 30m CAT 5 Ethernet cable into the OW-1000A unit. Hand tighten the connector.

Step4 : Connect the remaining end of the 30m CAT 5 cable into the PoE labeled AP/Bridge. This is the power side of the PoE that will power up the OW-1000A.

When the OW-1000A receives power over the Ethernet cable, the OW-1000A will start its boot up sequence and the **Active** LED on the Inline Power Injector will light up.

You can configure the OW-1000A via HTML browser, such as Microsoft Internet Explorer or Netscape Navigator from a remote host or PC.

2.4 Basic Configuration

2.4.1 Basic Configuration Steps

Note: All setting changing must **Reboot** the device after click **Apply**

This section describes a two-step SYSTEM configuration procedure to setup OW-1000A.

Step1 : Modify the factory-default parameters on the web page `"/Network/Network/"`, and click **APPLY** to save the changes.

Step2 : Modify the factory-default parameters on the web page `"/WIRELESS/Wi-Fi 1"`, and click **APPLY** to save the changes, than click `"/SYSTEM/Reboot/"` **Reboot** to take effect on the previous configuration changes.

2.4.2 Logging into the Web Interface

The OW-1000A supports access to the configuration system through the use of an HTTP Interface.

► Web Configuration

Before configuring OW-1000A, the user needs to know the IP Address assigned to the unit. When shipped from the factory, the IP Address **192.168.1.1** was assigned to the OW-1000A by default. **To start a web connection, use `http://192.168.1.1`**

► Web Access Procedures

Once you identify the IP Address assigned to OW-1000A, use web browser to configure OW-1000A through the HTTP Interface. The following procedure explains how to configure each item.

Step1 : Open your browser and enter the IP Address

Step2 : Press **<ENTER>** key and the OW-1000A **Login** screen appears as shown in **Figure 2-3**.



Figure 2-3

Step3 : Enter “**admin**” in the **Username** and **Password** fields, and click **LOGIN** to enter the web configuration user interface screen as shown below.

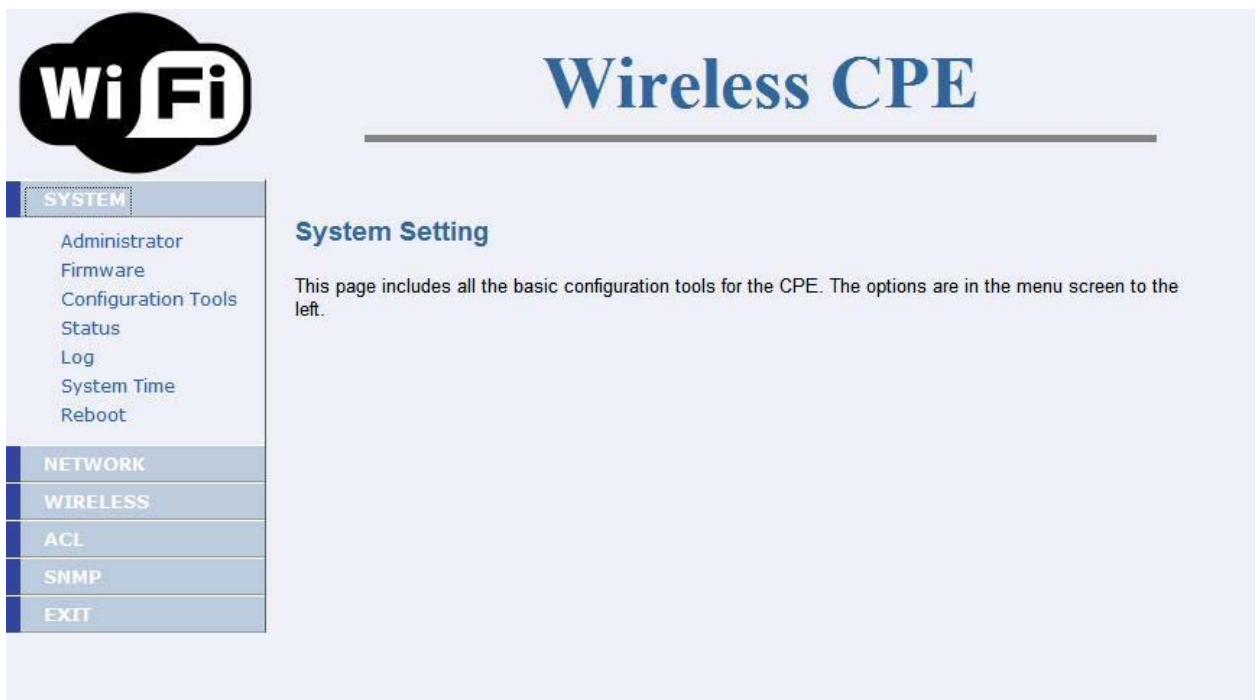


Figure 2-4

► **Web Configuration Structure**

The web configuration user interface shown above in **Figure 2-5** is grouped into a tree structure, and contains the following settings or information.

- ▽ SYSTEM
 - Administrator
 - Firmware
 - Configuration
 - Status
 - Log
 - System Time
 - Reboot
- ▽ NETWORK
 - Network
 - HotSpot
- ▽ WIRELESS
 - Wi-fi 1
 - Wi-fi 2
 - Wi-fi 3
 - Wi-fi 4
- ▽ ACL
 - ACL for Wi-fi 1
 - ACL for Wi-fi 2
 - ACL for Wi-fi 3
 - ACL for Wi-fi 4
- ▽ SNMP
 - Agent Settings
- ▽ EXIT

Move through the tree by clicking on an icon to expand or collapse the tree. The nodes on the tree represent web pages that allow viewing and modifying the parameters.

2.4.3 Set Operating Mode, IP Address, Subnet Mask, Default Route IP, DNS Server IP of OW-1000A

► LAN Settings

These are the settings of the LAN (Local Area Network) interface for the Access Point. The Access Point's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. This option is available in the "/**NETWORK/NETWORK** /" page as shown in **Figure 2-6**.

Wi-Fi

SYSTEM
NETWORK
Network
HotSpot
WIRELESS
ACL
SNMP
EXIT

Wireless CPE

Network Settings

Operational Mode

Operating Mode

☒ Access Point
☐ CB+AP
☐ AP Router Mode
☐ CB+AP Router Mode
☐ HotSpot AP
☐ VLAN enabled AP
☐ VLAN enabled CB+AP

LAN Interface

IP Assignment ☐ DHCP ☒ Manual ☐ PPPoE

IP Address

Subnet Mask

Gateway

DNS Server

Link Integrity

Link Integrity

HELP APPLY CANCEL

Figure 2-6

► Get LAN IP From

Choose "DHCP (Dynamic)" if your router supports DHCP and you want the router to assign an IP address to the AP. In this case, you do not need to fill in the following fields. Choose "Static IP (Manual)" if your router does not support DHCP or if for any other reason you need to assign a fixed address to the AP. In this case, you must also configure the following fields.

Note that you cannot choose "DHCP (Dynamic)" if you have enabled the "DHCP Server" option on the DHCP page; the AP cannot be both a DHCP client and a DHCP server.

► **IP Address**

The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN.

For example, 192.168.1.1.

► **Subnet Mask**

The subnet mask of the local area network.

► **Gateway**

The IP address of the router on the local area network.

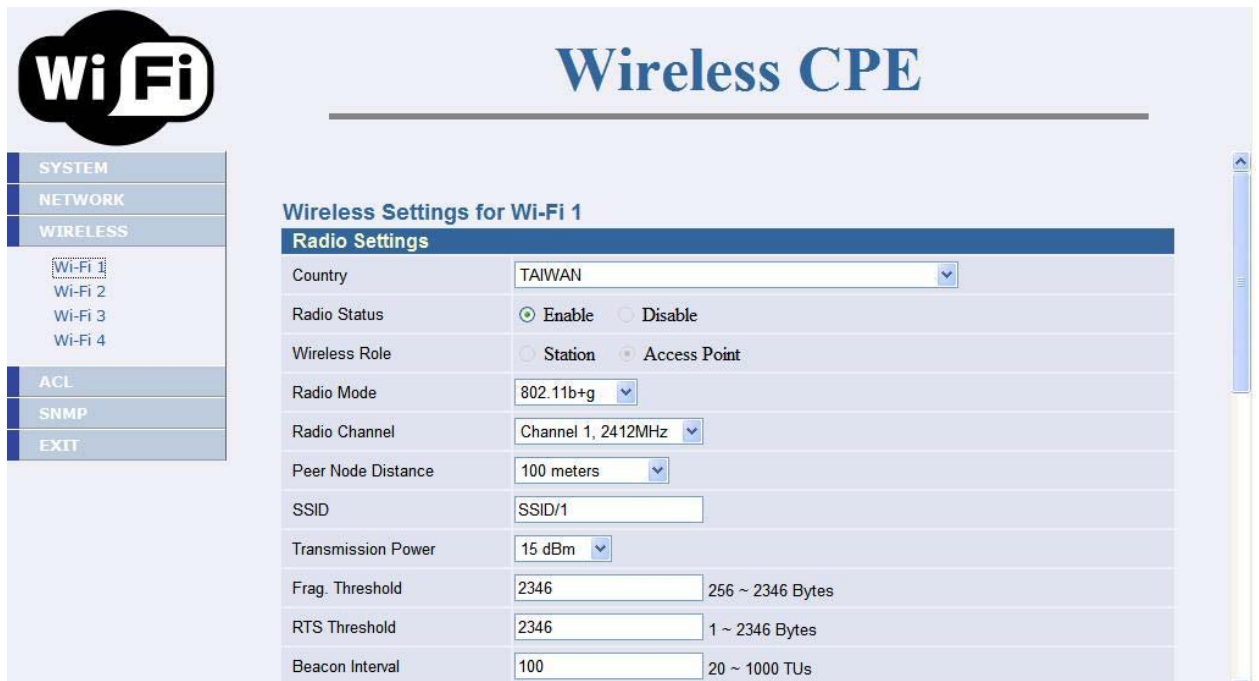
► **DNS Server**

This entry is optional. Enter a DNS Server for the local network.

2.4.4 Set Wireless SSID for Wireless Interface

► Wireless Network Name (Also called the SSID)

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. This option is available in the **"/WIRELESS/Wi-Fi 1/"** page as shown in **Figure 2-7**



Wi-Fi

Wireless CPE

SYSTEM

NETWORK

WIRELESS

Wi-Fi 1

Wi-Fi 2

Wi-Fi 3

Wi-Fi 4

ACL

SNMP

EXIT

Wireless Settings for Wi-Fi 1

Radio Settings	
Country	TAIWAN
Radio Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Role	<input type="radio"/> Station <input checked="" type="radio"/> Access Point
Radio Mode	802.11b+g
Radio Channel	Channel 1, 2412MHz
Peer Node Distance	100 meters
SSID	SSID/1
Transmission Power	15 dBm
Frag. Threshold	2346 256 ~ 2346 Bytes
RTS Threshold	2346 1 ~ 2346 Bytes
Beacon Interval	100 20 ~ 1000 TUs

Figure 2-7

2.4.5 Set Wireless Encryption for Wireless Interface

The OW-1000A supports 64-bit and 128-bit WEP encryption.

For **64-bit** WEP encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters.

For **128-bit** WEP encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.

Modify the WEP encryption parameters on the web page **"/WIRELESS/Wi-Fi 1 SECURITY "**. Choice "WEP" Enter 1~15 characters into the **WEP Key** field, than click **Apply** , **"/SYSTEM/Reboot "****Reboot**. page as shown in **Figure 2-8**

The screenshot displays the 'Wireless CPE' configuration interface. On the left is a navigation menu with categories: SYSTEM, NETWORK, WIRELESS (selected), ACL, SNMP, and EXIT. Under WIRELESS, there are sub-items: Wi-Fi 1, Wi-Fi 2, Wi-Fi 3, and Wi-Fi 4. The main content area is titled 'Wireless CPE' and contains several configuration fields:

- Radio Channel: Channel 1, 2412MHz
- Peer Node Distance: 100 meters
- SSID: SSID/1
- Transmission Power: 15 dBm
- Frag. Threshold: 2346 (range: 256 ~ 2346 Bytes)
- RTS Threshold: 2346 (range: 1 ~ 2346 Bytes)
- Beacon Interval: 100 (range: 20 ~ 1000 TUs)
- DTIM Interval: 1 (range: 1 ~ 15 Beacons)

Below these are two sections: 'Security Settings' and 'QoS Settings'.

Security Settings:

- Wireless Security: A dropdown menu is open, showing options: None, WEP, WPA-Personal, WPA/WPA2-Personal, WPA-Enterprise, and WPA/WPA2-Enterprise. The 'None' option is currently selected.
- VLAN Tagging ID: A field with a value of 1 and a range of ~ 4094.
- Layer2 Isolation: A checkbox that is currently checked, with the text 'Layer2 Isolation is enabled' next to it.

QoS Settings:

- Maximum Associated Stations: 32 (range: 1 ~ 2007)

Figure 2-8

2.4.6 Change Supervisor Account & Password

Enter the **SYSTEM > Administrator** page. **Figure 2-9** below shows the **SYSTEM / Administrator** page.

Wi-Fi

Wireless CPE

SYSTEM

- Administrator
- Firmware
- Configuration Tools
- Status
- Log
- System Time
- Reboot

NETWORK

WIRELESS

ACL

SNMP

EXIT

Administrator Settings

Hostname Settings

Hostname: wlan-cpe.lan

Password Settings

Current Password:

Password: (3-12 Characters)

Re-type Password:

Idle Time Out: 30 (minutes)

Remote Management

Enable: ☐ (If enabled, only the following PC can manage this AP.)

IP address: 0.0.0.0

HELP **APPLY** **CANCEL**

Figure 2-9

► ADMIN PASSWORD

Enter current password in the **SYSTEM / Administrator / Password Setting Current Password** field. Enter new password in the **"PASSWORD and Re-type Password"** field for changing new password. Then and click **APPLY** and **reboot** the device.

2.4.7 Upgrade the Firmware

► Update the Firmware

Enter the **SYSTEM > FIRMWARE** page as shown in **Figure 2-10** to upgrade OW-1000A. Here, user must select which file you want to upgrade it (**Program image**), then click **APPLY** button to start the upgrade process.

Hint: It takes about 10 min, to complete the restart process.

The screenshot shows the 'Wireless CPE' web interface. On the left is a navigation menu with a 'Wi-Fi' logo at the top. The menu categories are SYSTEM, NETWORK, WIRELESS, ACL, SNMP, and EXIT. Under the SYSTEM category, the following options are listed: Administrator, Firmware (which is highlighted with a dashed box), Configuration Tools, Status, Log, System Time, and Reboot. The main content area is titled 'Firmware Update'. It contains a table for 'Current Firmware Information' with the following data: Version: V 1.9.9 r1128, Date: 2008-05-05 07:18:28. Below this is a 'Method' section with two rows: 'Using TFTP' and 'Using FTP', each with a 'NEXT' button. A 'HELP' button is located at the bottom right of the main content area.

Current Firmware Information	
Version:	V 1.9.9 r1128
Date:	2008-05-05 07:18:28

Method	
Using TFTP	<input type="button" value="NEXT"/>
Using FTP	<input type="button" value="NEXT"/>

Figure 2-10



Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas. Any changes or modification to the product not expressly approved by Original Manufacture could void the user's authority to operate this device.



Caution To meet regulatory restrictions and the safety of the installation, this product **MUST** be **professionally installed**. End user can't install this device by themself

Chapter 3. *Network Topologies*

This chapter describes several common types of installations implemented by using the OW-1000A's line of Outdoor Wireless System. This is by no means intended to be an exhaustive list of all possible configurations, but rather shows examples of some of the more common implementations. The OW-1000A CB can be configured to function as a Wireless Client Router or Bridge to a central access point like the OW-1000A AP see Figure 3-1 below.

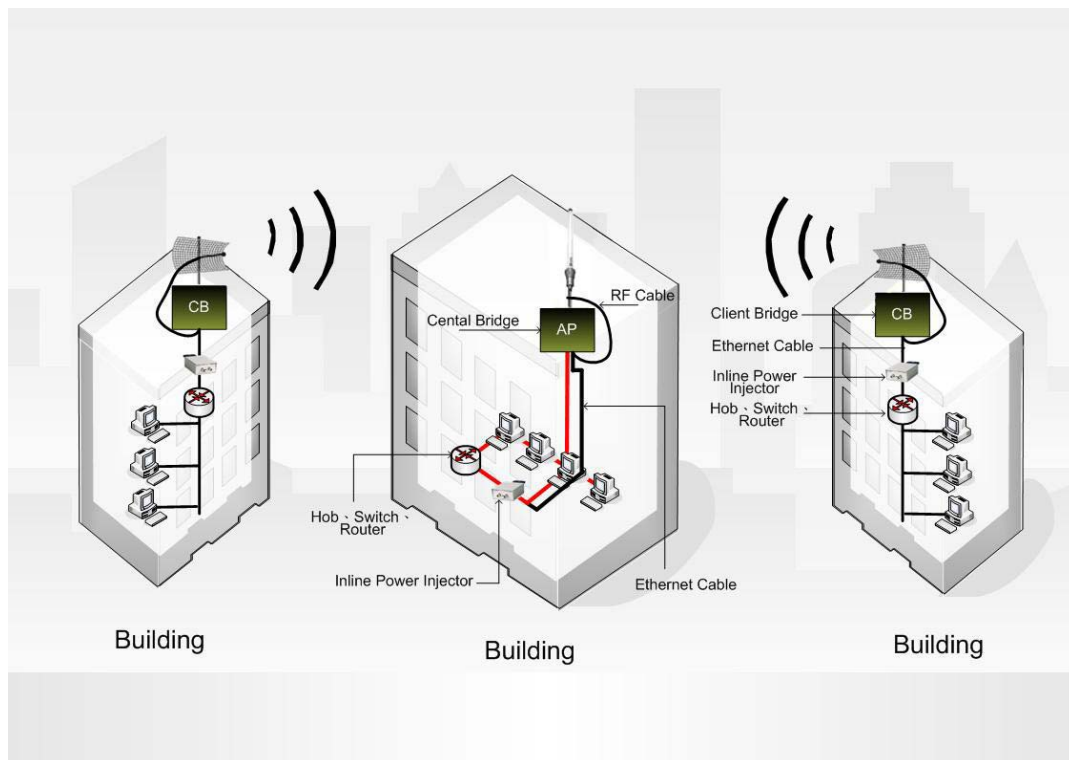


Figure 3-1

The OW-1000A CB performs in either router or bridge mode. In a Point-to-Multipoint topology, all communication between network systems is done through a centralized agent. Among the OW-1000A Outdoor Wireless Bridge products, the centralized agent is Central Bridge (OW-1000A AP) and the individual network nodes may be Bridge (OW-1000A CB).

To show the available Point-to-Multipoint topologies, the following examples are provided.

Wireless Client Bridge-to-Central Wireless Bridge

3.1 Wireless Client Bridge-to-Central Wireless Bridge

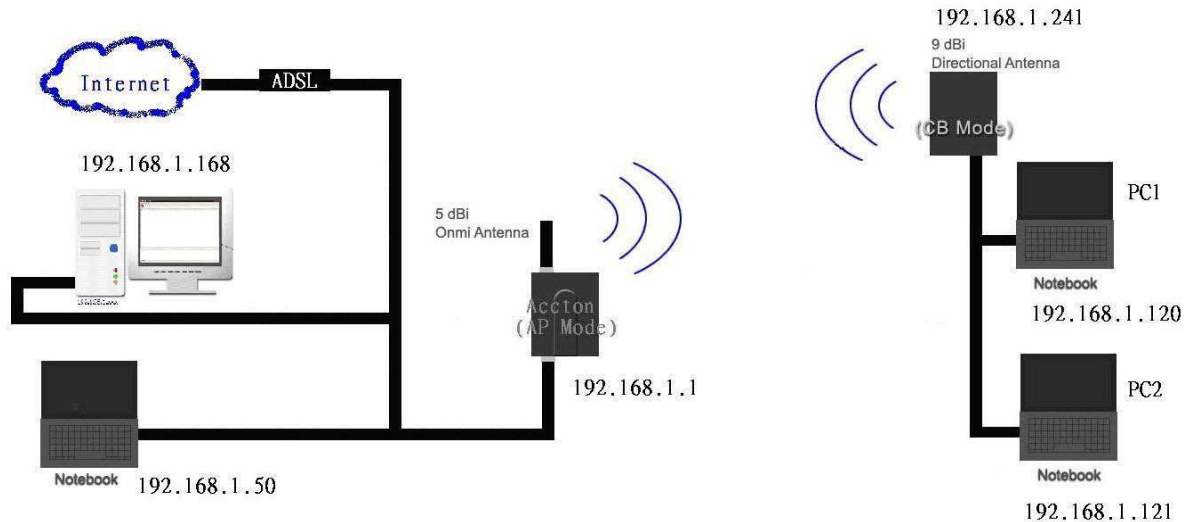


Figure 3-2

Refer to Figure 3-2 for the following setup.

Note: The OW-1000A AP is the Central Wireless Bridge and OW-1000A CB is the Wireless Client Bridge

Step 1 Set the OW-1000A AP to perform a bridge (**bridge IP address: 192.168.1.1**).

Step 2 Set Wireless parameters on the AP to: **Channel (1)** and **SSID (wireless)**

Step 3 Set the OW-1000A CB to function in the bridge mode (**bridge IP address: 192.168.1.241**).

Step 4 Set Wireless parameters on the OW-1000A CB to: **Channel (1)** and **SSID (wireless)**, and these parameters must be the same with COU.

Step 5 Left side subnet is transparent to the right side.

Step 6 DHCP server assign IP address to PC1 and PC2

Chapter 4. All function on Device

4.1 SYSTEM

4.1.1 Administrator

Administrator Settings

Use this menu to restrict management access based on a specific password. The default password comes with the installation guide. Please change this password as soon as possible, and store it in a safe place. Passwords can contain from 3-12 alphanumeric characters, and are case sensitive.

The screenshot shows the 'Wireless CPE' web interface. On the left is a sidebar menu with categories: SYSTEM (highlighted), NETWORK, WIRELESS, ACL, SNMP, and EXIT. Under SYSTEM, there are links for Administrator, Firmware, Configuration Tools, Status, Log, System Time, and Reboot. The main content area is titled 'Administrator Settings' and contains three sections: 'Hostname Settings' with a 'Hostname' field set to 'wlan-cpe-lan'; 'Password Settings' with fields for 'Current Password', 'Password' (with a '(3-12 Characters)' hint), and 'Re-type Password'; and 'Idle Time Out' set to '30 (minutes)'. Below these is the 'Remote Management' section with an 'Enable' checkbox (unchecked) and a note '(If enabled, only the following PC can manage this AP.)', and an 'IP address' field set to '0.0.0.0'. At the bottom right are 'HELP', 'APPLY', and 'CANCEL' buttons.

Figure 4-1

Administrator Time-out

The amount of time of inactivity allowed before the user proceeds next action. The user needs to re-login if the idle time passes timeout.

Remote Management

By default, management access is only available to users on your local network. However, you can also manage the Wireless CPE from a remote host. Just check the **Enable** box and enter the IP address of an administrator to this screen.

4.1.2 Firmware

The screenshot shows the 'Wireless CPE' web interface. On the left is a sidebar menu with categories: SYSTEM, NETWORK, WIRELESS, ACL, SNMP, and EXIT. The 'SYSTEM' category is expanded, showing sub-items: Administrator, Firmware, Configuration Tools, Status, Log, System Time, and Reboot. The main content area is titled 'Firmware Update - FTP'. It contains a table for 'Current Firmware Information' with fields for Version (V 1.9.9 r1128) and Date (2008-05-05 07:18:28). Below this is a section for 'Method: FTP to a FTP server' with input fields for FTP Server IP, Firmware Filename (pre-filled with 'firmware.tgz'), FTP Username, and FTP Password. A red note states: 'Note: The whole upgrade procedure takes about 10 mins.' At the bottom right are three buttons: HELP, BACK, and APPLY.

Current Firmware Information	
Version:	V 1.9.9 r1128
Date:	2008-05-05 07:18:28

Method: FTP to a FTP server	
FTP Server IP :	<input type="text"/>
Firmware Filename :	<input type="text" value="firmware.tgz"/>
FTP Username :	<input type="text"/>
FTP Password :	<input type="password"/>

Note: The whole upgrade procedure takes about 10 mins.

HELP BACK APPLY

Figure 4-2

Firmware Update - TFTP

You can use TFTP to upgrade the firmware. The "firmware information" displays current firmware version and firmware date. On the managed computer, run the TFTP Server utility. And specify the folder in which the firmware file resides. After running the TFTP server, enter the TFTP server IP and the filename. Click **APPLY** to complete your change. At the end of the upgrade, the Wireless CPE may not respond to commands for as long as ten minute. This is normal behavior and do not turn off the Wireless CPE during the time.

Firmware Update - FTP

You can use WEB to upgrade the firmware. The "firmware information" displays current firmware version and firmware date. Enter FTP Server IP , Type the correct firmware file path and file name on the File field. Enter the current FTP Username and Password. Click on **APPLY** to complete your change. At the end of the upgrade, the Wireless CPE may not respond to commands for as long as ten minute. This is normal behavior and do not turn off the Wireless CPE during the time.

4.1.3 Configuration Tools

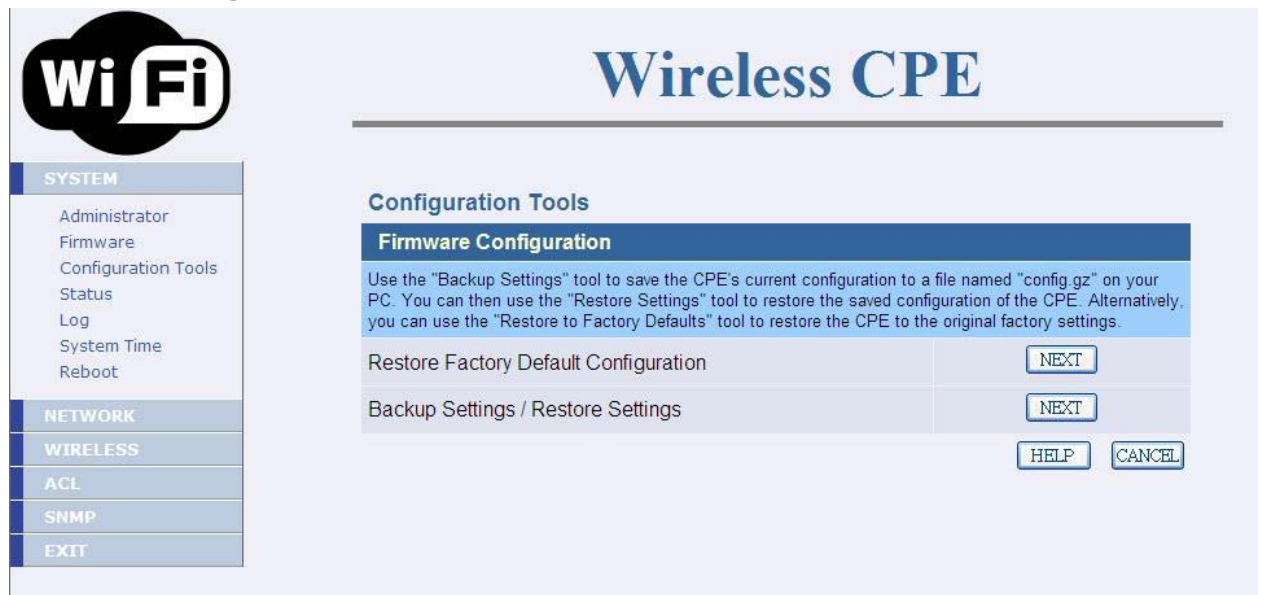


Figure 4-3

Restore Factory Defaults - Reset the CPE's configuration settings to the factory default values. Check the "Restore Factory Default Configuration" radio button then click on **APPLY** button.

Backup settings/Restore settings - Check the "Backup settings/Restore settings" radio button then click on **APPLY** button.

Backup Settings - Press the "Backup Settings" button to save the settings of this device to a file named "config.bin" on your PC.

Restore Settings - Restore the settings of this device to the backup settings. Enter the path and name of the backup file then press the "Restore Settings" button. You will be prompted to confirm the backup restoration.

4.1.1.4 Status

Wi-Fi

Wireless CPE

SYSTEM

- Administrator
- Firmware
- Configuration Tools
- Status
- Log
- System Time
- Reboot

NETWORK

WIRELESS

ACL

SNMP

EXIT

Status

System Information

MAC Address	00:40:C7:FA:01:F1
System Time	Sat Jan 1 14:47:40 2000
Current Firmware Version	v1.9.9 r1128
Operating Mode	Access Point

LAN Information

IP Address	192.168.1.220
Netmask	255.255.255.0
Gateway	0.0.0.0
DNS Server	0.0.0.0

Wi-Fi 1 Parameters

Status	Enabled
Mode	802.11b+g
SSID	SSID/1
Channel	Channel 1
Security	None
Wireless MAC Address	00:40:C7:FA:80:F9
Tx Packets	3002
Tx Bytes	338536
Rx Packets	0
Rx Bytes	0

Wireless Stations

AID	MAC Address	Tx Rate	Signal	Idle	Security	UAPSD
Wi-Fi 2 Disabled						
Wi-Fi 3 Disabled						
Wi-Fi 4 Disabled						

[HELP](#)

Figure 4-4

You can use the Status screen to see the connection status for the LAN and Wireless LAN interfaces. It also displays system up time and firmware version.

The following items are included in this screen:

SYSTEM INFORMATION - Displays MAC address, System time, Current firmware version and operation mode.

LAN INFORMATION - Displays IP settings of LAN port, including IP Address and Subnet Mask.

WIRELESS INFORMATION - Displays wireless information, including SSID, channel, Security status, and RF output power.

SYSTEM INFORMATION - Displays the system up time, the Wireless CPE's firmware version, and the serial number.

4.1.5 Log

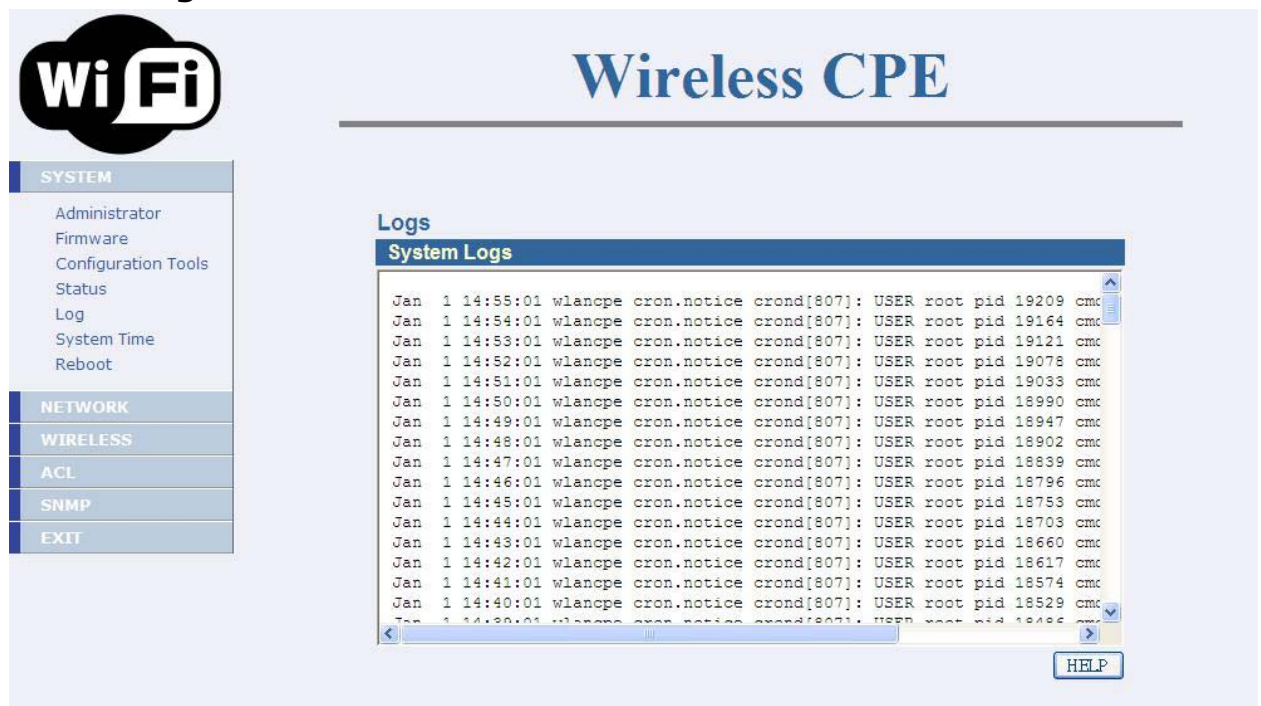


Figure 4-5

The Access Point automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the Access Point logs.

4.1.6 System Time

The screenshot displays the 'Wireless CPE' configuration web interface. On the left is a sidebar menu with categories: SYSTEM, NETWORK, WIRELESS, ACL, SNMP, and EXIT. Under the SYSTEM category, the following options are listed: Administrator, Firmware, Configuration Tools, Status, Log, System Time (which is highlighted with a dotted border), and Reboot. The main content area is titled 'Time Setting' and shows the current system time as 'Sat Jan 1 14:57:48 2000'. Below this, there are two sections: 'Select Setting Type' and 'Manual Setting'. The 'Select Setting Type' section has two radio buttons: 'Manual Setting' (unselected) and 'Synchronize with an Internet Time Server' (selected). The 'Manual Setting' section contains three rows of input fields: 'Year / Month / Day' with values 20, 07, and 20; 'Hour : Minute : Second' with values 02, 26, and 06. Below these is another section titled 'Using Internet Time Server' with fields for 'Hours from UTC' (set to +8), 'Server IP' (pool.ntp.org), 'NTP Server for Reference' (pool.ntp.org or 129.132.2.21), and 'Time Update for Every' (0 days, 0 hours, 10 minutes). At the bottom right of this section are three buttons: HELP, APPLY, and CANCEL.

Figure 4-6

The Time Configuration option allows you to configure, update, and maintain the correct time on CPE's internal system clock. From this section you can set the time zone that you are in and set the Time Server.

Time Configuration- Set the Date and Time Manually. If you do not have the NTP Server option in effect, you can either manually set the time for your Access Point here.

Note: If the Access Point loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, you must enter the correct time after you restart the Access Point.

4.1.7 Reboot

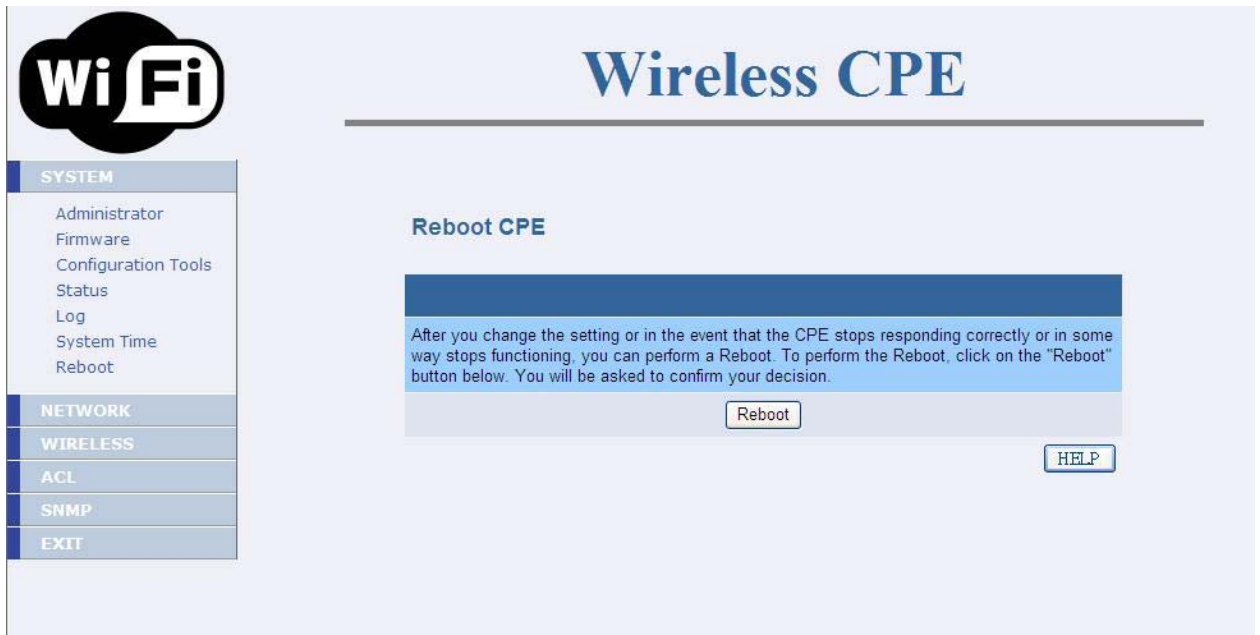


Figure 4-7

Reset Wireless CPE. In the event that the Wireless CPE stops responding correctly or in some way stops functioning, you can perform a reboot. Your existing settings will not be changed. To perform the reset, click on the **Reboot** button. You will be asked to confirm your decision.

4.2 NETWORK

4.2.1 Network

4.2.1.1 Operating Mode-Access Point IP Assignment

DHCP

Choose "DHCP (Dynamic)" if your router supports DHCP and you want the router to assign an IP address to the AP. In this case, you do not need to fill in the following fields.

The screenshot shows a web-based configuration interface for network settings. It is divided into three main sections: 'Operational Mode', 'LAN Interface', and 'Link Integrity'. In the 'Operational Mode' section, 'Access Point' is selected with a radio button. The 'LAN Interface' section shows 'DHCP' selected for IP Assignment. The 'Link Integrity' section shows a dropdown menu set to 'Disable'. At the bottom right, there are three buttons: 'HELP', 'APPLY', and 'CANCEL'.

Network Settings	
Operational Mode	
Operating Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> CB+AP <input type="radio"/> AP Router Mode <input type="radio"/> CB+AP Router Mode <input type="radio"/> HotSpot AP <input type="radio"/> VLAN enabled AP <input type="radio"/> VLAN enabled CB+AP
LAN Interface	
IP Assignment	<input checked="" type="radio"/> DHCP <input type="radio"/> Manual <input type="radio"/> PPPoE
Link Integrity	
Link Integrity	Disable ▼
<div>HELP APPLY CANCEL</div>	

Figure 4-8

Manual

Choose "Manual" if your router does not support DHCP or if for any other reason you need to assign a fixed address to the AP. In this case, you must also configure the following fields.

IP Address

The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.1.101.

Subnet Mask

The subnet mask of the local area network.

Gateway

The IP address of the router on the local area network.

DNS Server

DNS (Domain Name System) , Penetrates the DNS system, We may look up its IP by machine domain name, Also may instead look up its domain name by machine IP

This entry is optional. Enter a DNS Server for the local network.

The image shows a 'Network Settings' configuration window. It is divided into three main sections: 'Operational Mode', 'LAN Interface', and 'Link Integrity'. In the 'Operational Mode' section, 'Access Point' is selected. The 'LAN Interface' section shows 'IP Assignment' set to 'Manual', with 'IP Address' as 192.168.1.220, 'Subnet Mask' as 255.255.255.0, 'Gateway' as 0.0.0.0, and 'DNS Server' as 0.0.0.0. The 'Link Integrity' section shows 'Link Integrity' set to 'Disable'. At the bottom right are buttons for 'HELP', 'APPLY', and 'CANCEL'.

Network Settings	
Operational Mode	
Operating Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> CB+AP <input type="radio"/> AP Router Mode <input type="radio"/> CB+AP Router Mode <input type="radio"/> HotSpot AP <input type="radio"/> VLAN enabled AP <input type="radio"/> VLAN enabled CB+AP
LAN Interface	
IP Assignment	<input type="radio"/> DHCP <input checked="" type="radio"/> Manual <input type="radio"/> PPPoE
IP Address	192.168.1.220
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DNS Server	0.0.0.0
Link Integrity	
Link Integrity	Disable

HELP APPLY CANCEL

Figure 4-9

PPPoE

Choose "PPPoE" if your Internet support PPPoE Server .You need keyin **Username** and **Password** to login PPPoE Server.

The image shows a 'Network Settings' configuration window. It has three main sections: 'Operational Mode', 'LAN Interface', and 'Link Integrity'. In the 'Operational Mode' section, 'Access Point' is selected. In the 'LAN Interface' section, 'PPPoE' is selected for IP Assignment, and there are empty text boxes for 'PPPoE Username' and 'PPPoE Password'. In the 'Link Integrity' section, 'Disable' is selected from a dropdown menu. At the bottom right are buttons for 'HELP', 'APPLY', and 'CANCEL'.

Network Settings	
Operational Mode	
Operating Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> CB+AP <input type="radio"/> AP Router Mode <input type="radio"/> CB+AP Router Mode <input type="radio"/> HotSpot AP <input type="radio"/> VLAN enabled AP <input type="radio"/> VLAN enabled CB+AP
LAN Interface	
IP Assignment	<input type="radio"/> DHCP <input type="radio"/> Manual <input checked="" type="radio"/> PPPoE
PPPoE Username	<input type="text"/>
PPPoE Password	<input type="text"/>
Link Integrity	
Link Integrity	Disable ▼
<input type="button" value="HELP"/> <input type="button" value="APPLY"/> <input type="button" value="CANCEL"/>	

Figure 4-10

PPPoE

Choose "PPPoE" if your Internet support PPPoE Server .You need keyin **Username** and **Password** to login PPPoE Server.

4.2.1.2 Operating Mode-Access Point

4.2.1.3 Operating Mode-CB+AP

4.2.1.4 Operating Mode-AP Router

4.2.1.5 Operating Mode- CB+AP Router

4.2.1.6 Operating Mode- Hot Spot

4.2.1.7 Operating Mode- VLAN enable AP

4.2.1.8 Operating Mode- VLAN enable CB+AP

HotSpot (Captive Portal)

HotSpot: Enable/Disable captive portal function. Note, the CPE will become router mode and ALL ssid in Access Point role after HotSpot enabled.

Domain: Set domain name for hotspot.

Primary Radius: Set primary radius server for hotspot user authentication.

Secondary Radius: Set backup radius server for hotspot user authentication.

NAS ID: Set CPE's NAS ID in RADIUS frames.

Called Station Name: Set CPE's station name in RADIUS frames.

NAS Location: Set CPE's location name in RADIUS frames.

NAS Location ID: Set CPE's location ID in RADIUS frames.

UAM Server: The URL for hotspot user login.

UAM Secret: The encryption key between UAM server and CPE.

UAM Allowed List: IPs/Hostnames that hotspot can visit before login.

HotSpot Settings

HotSpot Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Domain	<input type="text"/>	
Primary Radius	Server <input type="text" value="192.168.10.80"/>	Auth Port <input type="text" value="1812"/>
Secondary Radius	Server <input type="text" value="192.168.10.80"/>	Acct Port <input type="text" value="1813"/>
Radius Shared Secret	<input type="text" value="TypeYourRadiusSecretHere"/>	
NAS ID	<input type="text"/>	
Called Station Name	<input type="text"/>	
NAS Location	<input type="text"/>	
NAS Location ID	<input type="text" value="isocc=tw,cc=886,ac=4,ne"/>	
UAM URL	<input type="text"/>	
UAM Secret	<input type="text" value="TypeYourUamSecretHere"/>	
UAM Allowed List	<input type="text" value="www.paypal.com,www.google.com"/>	

HELP APPLY CANCEL

Figure 4-11

4.3 WIRELESS

You can set the wireless related setting here

The screenshot displays the 'Wireless CPE' configuration page. On the left is a navigation menu with 'SYSTEM', 'NETWORK', 'WIRELESS', 'ACL', 'SNMP', and 'EXIT'. The 'WIRELESS' section is expanded, showing 'Wi-Fi 1' as the selected interface. The main area is titled 'Wireless Settings for Wi-Fi 1' and is divided into three sections: 'Radio Settings', 'Security Settings', and 'QoS Settings'. The 'Radio Settings' section includes fields for Country (TAIWAN), Radio Status (Enable), Wireless Role (Access Point), Radio Mode (802.11b+g), Radio Channel (Channel 1, 2412MHz), Peer Node Distance (100 meters), SSID (SSID/1), Transmission Power (15 dBm), Frag. Threshold (2346), RTS Threshold (2346), Beacon Interval (100), and DTIM Interval (1). The 'Security Settings' section includes Wireless Security (None), VLAN Tagging ID (1), and Layer2 Isolation (Enable). The 'QoS Settings' section includes Maximum Associated Stations (32) and a table of WMM settings for different traffic types (Tx and Station) and priorities (Best Effort, Background, Video, Voice). At the bottom right are buttons for HELP, APPLY, and CANCEL.

Wireless Settings for Wi-Fi 1									
Radio Settings									
Country	TAIWAN								
Radio Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable								
Wireless Role	<input type="radio"/> Station <input checked="" type="radio"/> Access Point								
Radio Mode	802.11b+g								
Radio Channel	Channel 1, 2412MHz								
Peer Node Distance	100 meters								
SSID	SSID/1								
Transmission Power	15 dBm								
Frag. Threshold	2346		256 ~ 2346 Bytes						
RTS Threshold	2346		1 ~ 2346 Bytes						
Beacon Interval	100		20 ~ 1000 TUs						
DTIM Interval	1		1 ~ 15 Beacons						
Security Settings									
Wireless Security	None								
VLAN Tagging ID	1		1 ~ 4094 <i>only effect when VLAN tagging is enabled</i>						
Layer2 Isolation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable								
QoS Settings									
Maximum Associated Stations	32		1 ~ 2007						
WMM Tx - Best Effort	CWmin	7	CWmax	1023	AIFS	2	Burst	0.0	
WMM Tx - Background	CWmin	15	CWmax	1023	AIFS	7	Burst	0.0	
WMM Tx - Video	CWmin	3	CWmax	7	AIFS	1	Burst	1.5	
WMM Tx - Voice	CWmin	7	CWmax	15	AIFS	1	Burst	3.0	
WMM Station - Best Effort	CWmin	7	CWmax	1023	AIFS	2	TXOP Limit	2048	ACM Optional
WMM Station - Background	CWmin	15	CWmax	1023	AIFS	7	TXOP Limit	32	ACM Optional
WMM Station - Video	CWmin	3	CWmax	7	AIFS	1	TXOP Limit	1504	ACM Optional
WMM Station - Voice	CWmin	7	CWmax	15	AIFS	1	TXOP Limit	3008	ACM Optional

HELP APPLY CANCEL

Figure 4-12

4.3.1 Wi-Fi 1

Wireless Settings

Radio Status: Enable/Disable SSID.

Wireless Role: This SSID will act as Station or Access Point. Note: only first SSID can act as station.

Radio Mode: Set 11g, 11b or 11b+g mode.

Radio Channel: Select radio channel or use auto.

Peer Node Distance: Set distance between this CPE and it's adjacent.

SSID: Set (extended) service set ID, a.k.a. network name.

Transmission Power: Set transmission power in dBm, Note: H/W may not xmit power as high as you set, depends on H/W faculty.

VLAN Tagging ID: Set this SSID's VLAN tag when VLAN tagging enabled.

Maximum Associated Stations: Restrict maximum number of associated stations.

Layer 2 Isolation: Prevent packets exchange between associated stations.

Frag. Threshold: Fragmentation threshold.

RTS Threshold: RTS threshold.

Beacon Interval: Beacon interval in TUs.

WMM Tx: Set WMM parameters for packet transmission.

WMM Station: Set WMM parameters that provide for station.

Security:

WEP: Set WEP key in hexadecimal

WPA-Personal: WPA with pre-shared key.

WPA/WPA2-Personal: WPA and WPA2 co-existence with pre-shared key.

WPA-Enterprise: WPA, key provided by RADIUS server.

WPA/WPA2-Enterprise: WPA and WPA2 co-existence, key provided by RADIUS server.

4.3.2 Wi-Fi 2

4.3.3 Wi-Fi 3

4.3.4 Wi-Fi 4

4.4 ACL

You can set the access control related setting here

The screenshot displays the 'Wireless CPE' configuration page. On the left is a sidebar menu with options: SYSTEM, NETWORK, WIRELESS, ACL, and EXIT. Under the 'ACL' menu, there are sub-links: 'ACL for Wi-Fi 1', 'ACL for Wi-Fi 2', 'ACL for Wi-Fi 3', and 'ACL for Wi-Fi 4'. The main content area is titled 'Wireless Access Control Settings'. It contains two sections: 'Wireless MAC ACL Settings' and 'Wireless On/Off Scheduling Settings'. In the 'Wireless MAC ACL Settings' section, the 'Wireless MAC ACL Status' is set to 'Disabled' via a dropdown menu. Below it is a text input field for 'Add New MAC Address' containing '00:00:00:00:00:00' and an 'Add MAC' button. The 'Wireless On/Off Scheduling Settings' section has a status set to 'Disabled' (selected with a radio button). Below this, there is a table for scheduling settings for each day of the week, with 'Turn on at' and 'Turn off at' dropdown menus set to 0 and 24 respectively. At the bottom right of the main area are 'HELP', 'APPLY', and 'CANCEL' buttons.

Wireless On/Off Scheduling Settings		
Wireless On/Off Scheduling Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Scheduling on Sunday	Turn on at 0	Turn off at 24
Scheduling on Monday	Turn on at 0	Turn off at 24
Scheduling on Tuesday	Turn on at 0	Turn off at 24
Scheduling on Wednesday	Turn on at 0	Turn off at 24
Scheduling on Thursday	Turn on at 0	Turn off at 24
Scheduling on Friday	Turn on at 0	Turn off at 24
Scheduling on Saturday	Turn on at 0	Turn off at 24

Figure 4-13

4.4.1 ACL for Wi-Fi 1

Wireless MAC ACL

Wireless MAC ACL Status: Enable/Disable ACL by MAC address.

Add New MAC Address: Add a new MAC address to MAC table and in active status.

MAC Table: Active, this MAC will be checked. Inactive, this MAC will ignore for checking. Remove, remove this MAC from MAC table.

4.4.2 ACL for Wi-Fi 2

4.4.3 ACL for Wi-Fi 3

4.4.4 ACL for Wi-Fi 4

4.5 SNMP

You can set the SNMP Community and SNMP Trap setting here

4.5.1 Agent Settings

SNMP Agent provides a simple protection. Access to the SNMP device is controlled through community names. The community name can be thought of as a password. If you don't have the correct community name, you can't retrieve any data (get) or make any change (set). Multiple SNMP managers may be organized in a specified community. You can change your SNMP community settings on this screen. Check the "Enable" check box to turn on SNMP daemon. Click APPLY to complete your change.

Read Only Community: Specify the name of community for read only access.

Read Write Community: Specify the name of community for read and write access.

The screenshot displays the 'Wireless CPE' configuration page. On the left is a sidebar menu with options: SYSTEM, NETWORK, WIRELESS, ACL, SNMP, Agent Settings (highlighted), and EXIT. The main content area is titled 'Wireless CPE' and contains the 'SNMP Agent' configuration section. This section is divided into two parts: 'System Information' and 'Community Name'. In the 'System Information' part, 'Agent Status' is set to 'Enable' (radio button selected), 'System Location' is 'You know where it is.', 'System Contact' is 'That is you.', 'System Name' is 'Wireless CPE', and 'System Description' is 'This is a wireless CPE'. The 'Community Name' part shows 'Read Only Community' as 'public' and 'Read Write Community' as 'private'. At the bottom right of the form are three buttons: HELP, APPLY, and CANCEL.

SNMP Agent	
System Information	
Agent Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
System Location	<input type="text" value="You know where it is."/>
System Contact	<input type="text" value="That is you."/>
System Name	<input type="text" value="Wireless CPE"/>
System Description	<input type="text" value="This is a wireless CPE"/>
Community Name	
Read Only Community	<input type="text" value="public"/>
Read Write Community	<input type="text" value="private"/>

HELP APPLY CANCEL

Figure 4-14

4.6 EXIT

Chapter 5. *Specifications*

The OW1000APP Outdoor Wireless Multi-Client Bridge/Access Point/WDS (wireless distribution system) operates seamlessly in the 2.4 GHz frequency supporting the IEEE 802.11b/802.11g wireless standards. It's the best way to add wireless capability to your existing wired network, or to add bandwidth to your existing wireless installation.

To secure your wireless connectivity, it can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA/WPA2 (Personal/Enterprise). A MAC address filter lets you select exactly which stations should have access to your network. With the Wireless Multi-Client Bridge/Access Point, you'll experience the best wireless connectivity available today.

Features

- High Speed Data Rate Up to 54Mbps
- Output Power up to 26dBm±2dBm
- IEEE 802.11b/g Compliant
- Access Point / CB+AP / AP Router / CB+AP Router / HotSpot AP / VLAN AP / VLAN CB+AP
- WEP/WPA/WPA2/ IEEE 802.1x Authenticator support
- Dust tight and Watertight and Weatherproof (IP65)
- Wide temperature range and robust mechanical design
- Power-over-Ethernet (12V-24V)

Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Standards	IEEE802.11b/g, IEEE802.1x, IEEE802.3, IEEE802.3u
Compatibility	IEEE 802.11g/ IEEE 802.11b
Power Requirements	Active Ethernet – 12 VDC/1A
Regulation Certifications	FCC Part 15/UL, ETSI 300/328/CE
RF Information	Atheros BB/MAC/RF
Frequency Band	2.400~2.483.5 MHz
Media Access Protocol	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Modulation Technology	Orthogonal Frequency Division Multiplexing (OFDM), DBPSK @ 1Mbps, DQPSK @2Mbps, CCK @ 5.5 & 11Mbps, BPSK @ 6 and 9 Mbps, QPSK @ 12 and 18 Mbps, 16-QAM @ 24 and 36 Mbps, 64-QAM @ 48 and 54 Mbps
Operating Channels	11 for North America, 14 for Japan, 13 for Europe
Receive Sensitivity (Typical)	-72dBm @ 54Mbps
Available transmit power(Typical)	802.11b: 15dBm 802.11g : 16dBm

RF Connector	1 SMA female connector for external antenna using
Networking Topology	Ad-Hoc, Infrastructure
Operation Mode	Access Point / CB+AP / AP Router / CB+AP Router / HotSpot AP / VLAN AP / VLAN CB+AP
Interface	One 10/100Mbps RJ-45 LAN Port , RS-232 Console
Security	IEEE802.1x authenticator /RADIUS client (EAPMD5/TLS/TTLS) support in AP mode WPA / Pre Share KEY (PSK)/TKIP MAC address filtering Hide SSID in beacons Layer 2 Isolation
IP Auto-configuration	DHCP client/server/PPPoE
Management Configuration	Web-based configuration (HTTP)
Firmware Upgrade	Upgrade firmware via web browser
Physical Dimensions	190(L)mm * 116(W)mm * 65H)mm
Weight	300g
Environmental Temperature Range	-Operating: -10°C to 60°C (14°F to 140°F) -Storage: -20°C to 70°C (-4°F to 158°F)
Humidity (non-condensing)	5%~95% Typical
Package Contents	EW-7301APG unit 12V, 1A AC/DC adapter with wall-plug power code Inline Power Injector (PoE) User's manual CD-ROM Wall mounting kit

Chapter 6. *Default Settings*

6.1 SYSTEM

6.1.1 Administrator

Parameter	Description	Default Value
Hostname		Wlancpe.lan
Current Password		
Password		
Re-type Password		
Idle Time Out		30
Enable		
IP address		0.0.0.0

6.1.2 Firmware

Parameter	Description	Default Value
Using TFTP		
Using FTP		

6.1.3 Configuration Tools

Parameter	Description	Default Value
Restore Factory Default Configuration		
Backup Settings / Restore Settings		

6.1.4 Status

6.1.5 Log

6.1.6 System Time

Parameter	Description	Default Value
Setting by		Synchronize with an Internet Time Server
Year / Month / Day		07/8/20
Hour : Minute : Second		02:26:06
Hours from UTC		+8
Server IP		pool.ntp.org
NTP Server for Reference		pool.ntp.org or 129.132.2.21
Time Update for Every		0/0/0

6.1.7 Reboot

6.2 NETWORK

6.2.1 Network

Parameter	Description	Default Value
Operating		Access Point
IP Assignment		Manual
IP Address		192.168.1.1
Subnet Mask		255.255.255.0
Gateway		0.0.0.0
DNS Server		0.0.0.0
Link Integrity		Disable
PPPoE Username		
PPPoE Password		

6.2.2 Hotspot

Parameter	Description	Default Value
Domain		Access Point
Primary Radius		192.168.10.80 1812
Secondary Radius		192.168.10.80 1813
Radius Shared Secret		TypeYourRadiusSecretHere
NAS ID		
Called Station Name		
NAS Location		
NAS Location ID		isocc=tw,cc=886,ac=4,network=hotspot
UAM URL		
UAM Secret		TypeYourUamSecretHere
UAM Allowed List		www.paypal.com,www.google.com

6.3 WIRELESS

6.3.1 Wi-Fi 1

Parameter	Description	Default Value					
Country		TAIWAN					
Radio Status		Enable					
Wireless Role		Access Point					
Radio Mode		802.11b+g					
Radio Channel		Channel 1, 2412MHz					
Peer Node Distance		100 meters					
SSID		SSID/1					
Transmission Power		15dBm					
Frag. Threshold		2346					
RTS Threshold		2346					
Beacon Interval		100					
DTIM Interval		1					
Wireless Security		None					
VLAN Tagging ID		1					
Layer2 Isolation		Enable					
Maximum Associated Stations		32					
WMM Tx - Best Effort		7	1023	2	0.0		
WMM Tx - Background		15	1023	7	0.0		
WMM Tx - Video		3	7	1	1.5		
WMM Tx - Voice		7	15	1	3.0		
WMM Station - Best Effort		7	1023	2	2048	Optional	
WMM Station - Background		15	1023	7	32	Optional	
WMM Station - Video		3	7	1	1504	Optional	
WMM Station - Voice		7	15	1	3008	Optional	

6.3.2 Wi-Fi 2

Parameter	Description	Default Value				
Country		TAIWAN				
Radio Status		Enable				
Wireless Role		Access Point				
Radio Mode		802.11b+g				
Radio Channel		Channel 1, 2412MHz				
Peer Node Distance		100 meters				
SSID		SSID/2				
Transmission Power		15dBm				
Frag. Threshold		2346				
RTS Threshold		2346				
Beacon Interval		100				
DTIM Interval		1				
Wireless Security		None				
VLAN Tagging ID		2				
Layer2 Isolation		Enable				
Maximum Associated Stations		32				
WMM Tx - Best Effort		7	1023	2	0.0	
WMM Tx - Background		15	1023	7	0.0	
WMM Tx - Video		3	7	1	1.5	
WMM Tx - Voice		7	15	1	3.0	
WMM Station - Best Effort		7	1023	2	2048	Optional
WMM Station - Background		15	1023	7	32	Optional
WMM Station - Video		3	7	1	1504	Optional
WMM Station - Voice		7	15	1	3008	Optional

6.3.3 Wi-Fi 3

Parameter	Description	Default Value				
Country		TAIWAN				
Radio Status		Enable				
Wireless Role		Access Point				
Radio Mode		802.11b+g				
Radio Channel		Channel 1, 2412MHz				
Peer Node Distance		100 meters				
SSID		SSID/3				
Transmission Power		15dBm				
Frag. Threshold		2346				
RTS Threshold		2346				
Beacon Interval		100				
DTIM Interval		1				
Wireless Security		None				
VLAN Tagging ID		3				
Layer2 Isolation		Enable				
Maximum Associated Stations		32				
WMM Tx - Best Effort		7	1023	2	0.0	
WMM Tx - Background		15	1023	7	0.0	
WMM Tx - Video		3	7	1	1.5	
WMM Tx - Voice		7	15	1	3.0	
WMM Station - Best Effort		7	1023	2	2048	Optional
WMM Station - Background		15	1023	7	32	Optional
WMM Station - Video		3	7	1	1504	Optional
WMM Station - Voice		7	15	1	3008	Optional

6.3.4 Wi-Fi 4

Parameter	Description	Default Value				
Country		TAIWAN				
Radio Status		Enable				
Wireless Role		Access Point				
Radio Mode		802.11b+g				
Radio Channel		Channel 1, 2412MHz				
Peer Node Distance		100 meters				
SSID		SSID/4				
Transmission Power		15dBm				
Frag. Threshold		2346				
RTS Threshold		2346				
Beacon Interval		100				
DTIM Interval		1				
Wireless Security		None				
VLAN Tagging ID		4				
Layer2 Isolation		Enable				
Maximum Associated Stations		32				
WMM Tx - Best Effort		7	1023	2	0.0	
WMM Tx - Background		15	1023	7	0.0	
WMM Tx - Video		3	7	1	1.5	
WMM Tx - Voice		7	15	1	3.0	
WMM Station - Best Effort		7	1023	2	2048	Optional
WMM Station - Background		15	1023	7	32	Optional
WMM Station - Video		3	7	1	1504	Optional
WMM Station - Voice		7	15	1	3008	Optional

6.4 ACL

6.4.1 ACL for Wi-Fi

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On/Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.4.2 ACL for Wi-Fi 2

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On/Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.4.3 ACL for Wi-Fi 3

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On/Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.4.4 ACL for Wi-Fi 4

Parameter	Description	Default Value	
Wireless MAC ACL Status		Disable	
Add New MAC Address		00:00:00:00:00:00	
Wireless On/Off Scheduling Status		Disabled	
Scheduling on Sunday		0	24
Scheduling on Monday		0	24
Scheduling on Tuesday		0	24
Scheduling on Wednesday		0	24
Scheduling on Thursday		0	24
Scheduling on Friday		0	24
Scheduling on Saturday		0	24

6.5 SNMP

Parameter	Description	Default Value
Agent Status		Enable
System Location		You know where it is.
System Contact		That is you.
System Name		Wireless CPE
System Description		This is a wireless CPE
Read Only Community		public
Read Write Community		public

6.6 EXIT

Chapter 7. *Regulatory Compliance Information*

Federal Communication Commission Interference Statement

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

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna



Caution To meet regulatory restrictions and the safety of the installation, this product **MUST** be **professionally installed**. End user can't install this device by himself

Antenna type	Antenna Gain
Patch	9dBi