

TEW-455APBO

User Manual

V1.04

Table of Contents

Chapter 1. Before You Start	1
1.1 Preface	1
1.2 Conventions	1
Chapter 2. System Overview	2
2.1 Introduction of TEW-455APBO	2
2.2 System Concept	3
2.3 Product Benefit	4
2.4 Specification.....	4
Chapter 3. Base Installation.....	7
3.1 Hardware Installation	7
3.1.1 Package Contents.....	7
3.1.2 Panel Function Descriptions	7
3.1.3 Hardware Installation Steps	9
3.2 Software Configuration	10
3.2.1 Instruction to Web Management Interface	10
3.2.2 Quick Configuration	12
3.2.2.1 BASE STATION Mode (Point to Point).....	12
3.2.2.2 BRIDGE Mode	16
3.2.2.3 CPE Mode	19
Chapter 4. BASE STATION (Point to Point) Mode Configuration.....	23
4.1 System.....	24
4.1.1 Operating Mode	24
4.1.2 LAN Setup	25
4.1.3 Management.....	27
4.1.4 Time Server	29
4.1.5 SNMP Setup	30
4.2 Wireless	32
4.2.1 General Setup.....	33
4.2.2 Advanced Setup.....	34
4.2.3 Virtual BASE STATION Setup.....	36
4.2.3.1 Virtual BASE STATION General Configuration	37
4.2.3.2 Virtual BS Access Control List (ACL) Setup	43
4.3 Utilities	44
4.3.1 Profile Setting	44
4.3.2 Firmware Upgrade	45
4.3.3 Ping Utility.....	46
4.3.4 Reboot	47
4.4 Status.....	48
4.4.1 Overview.....	49
4.4.2 Client.....	51
4.4.3 Event Log.....	52
Chapter 5. BRIDGE Mode Configuration	53
5.1 System.....	54
5.1.1 Operating Mode	54
5.1.2 LAN Setup	55
5.1.3 Management.....	57
5.1.4 Time Server	59
5.1.5 SNMP Setup	60
5.2 Wireless	62
5.2.1 General Setup.....	63
5.2.2 Advanced Setup.....	64

5.2.3 BRIDGE Setup.....	66
5.3 Utilities	67
5.3.1 Profile Setting	67
5.3.2 Firmware Upgrade	68
5.3.3 Ping Utility.....	69
5.3.4 Reboot	70
5.4 Status.....	71
5.4.1 Overview.....	72
5.4.2 BRIDGE List	74
5.4.3 Event Log.....	75
Chapter 6. CPE Mode Configuration	76
6.1 System.....	77
6.1.1 Operating Mode	77
6.1.2 WAN Setup	78
6.1.3 LAN Setup	82
6.1.4 Management.....	84
6.1.5 Time Server	86
6.1.6 SNMP Setup	87
6.2 Wireless	89
6.2.1 General Setup.....	90
6.2.2 Advanced Setup.....	92
6.2.3 Site Survey	93
6.3 Firewall	94
6.3.1 IP Rule Setup.....	95
6.3.2 MAC Rule Setup	97
6.4 NAT	98
6.4.1 Virtual Server (IP/ Port Forwarding)	99
6.4.2 DMZ.....	101
6.5 Utilities	102
6.5.1 Profile Setting	102
6.5.2 Firmware Upgrade	103
6.5.3 Ping Utility.....	104
6.5.4 Reboot	105
6.6 Status.....	106
6.6.1 Overview.....	107
6.6.2 DHCP Clients.....	110
6.6.3 Event Log.....	111
7. Command Line Interface(CLI).....	112
7.1 Accessing the CLI with Telnet	112
7.2 Using the CLI	113
Appendix A. Windows TCP/IP Settings	116
Appendix B. Valid Characters when using WMI.....	118
Appendix D. All Antenna type for Products.....	122

Chapter 1. Before You Start

1.1 Preface

The 802.11 b/g compliant TEW-455APBO is an outdoor wireless device that can be used for three purposes. It can be deployed as a fixed Point to Point wireless base station between buildings, a bridge between LAN and wireless base station, or it can be used as a fixed wireless point to point between CPE and Internet Service Provider.

The die-cast sealed TEW-455APBO is compact in size and weatherproof. It comes with a mounting kit, for pole or wall mount. It is suitable for both indoor and outdoor usage with its 500mW output power, which is higher than a typical indoor base station (100mW).

This User's Manual provides instructions and reference material for getting started with TEW-455APBO. This guide will also show you how to connect TEW-455APBO to other network devices.

1.2 Conventions

■ Conventions used in the system are :

- Save : Save settings by clicking this button
- Reset : Clear settings by clicking this button
- Reboot : Activate and reboot system settings by clicking this button
- * : Indicate information in the related field is required

■ Conventions used in this manual :

- **Warning** : Indicates a caution or warning message to inform users something might damage the system
- **Note** : Indicates information that the users shall pay attention to.

Chapter 2. System Overview

2.1 Introduction of TEW-455APBO

The 802.11 b/g compliant TEW-455APBO is an outdoor wireless device that can be used for three purposes. It can be deployed as a outdoor fixed point to point between two building or between a building and wireless base station, or The fixed wireless point to point between CPE and Internet Service Provider.

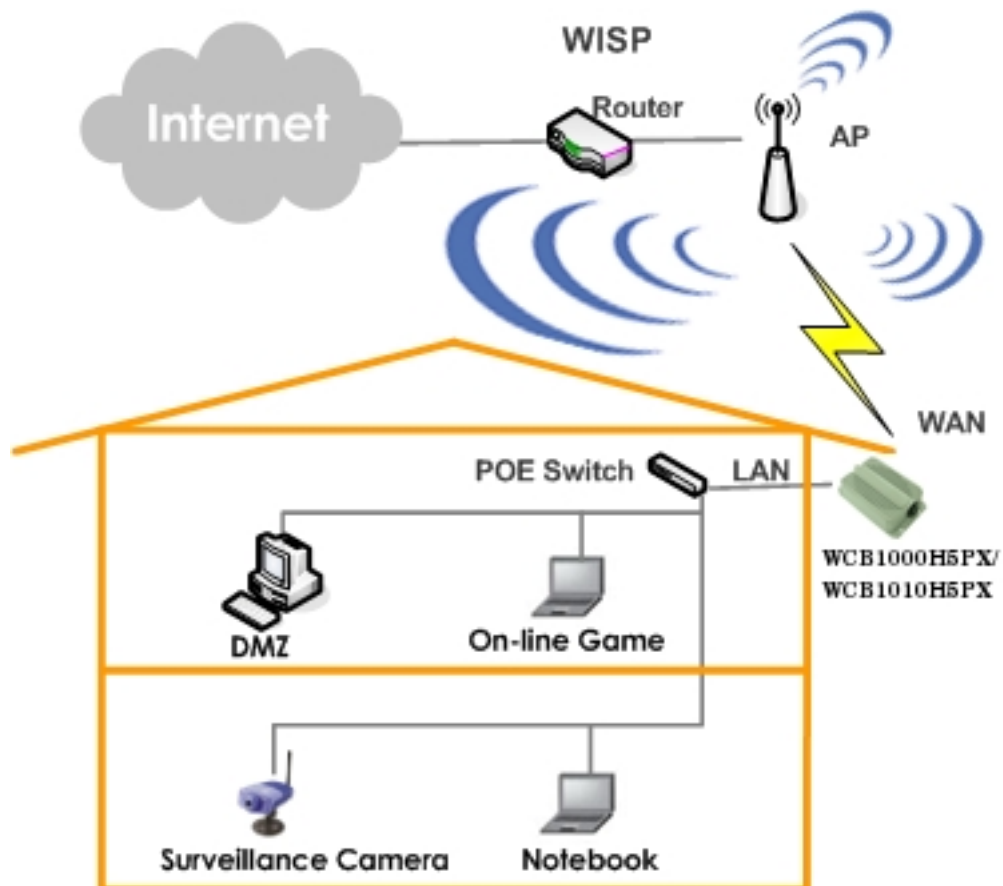
The die-cast sealed TEW-455APBO is compact in size and weatherproof. It comes with a mounting kit, for pole or wall mount. It is suitable for both indoor and outdoor usage with its 500mW output power, which is higher than a typical indoor BS (100mW).

2.2 System Concept

The TEW-455APBO can be used in many applications with examples as follows:

- The Fixed point to point operation (connection between a building and a wireless base station).
- Bridge between LAN and wireless base station.
- The Fixed wireless point to point between CPE and Internet Service Provider.

Note: The device shall be mounted on permanent structures.



2.3 Product Benefit

- 500mW at 2.4GHz Output Power
- Topology : Point to Point;
- Operation Modes : Base station mode(Only point to point), Bridge mode (Bridge), CPE mode(Client Bridge)
- Multiple ESSIDs Capability
- VLAN tag over BRIDGE
- Supporting Qos & 802e WMM
- Business-class WLAN Security & Client Authentications
- Support 3 LEDs Wireless Signal Strength

2.4 Specification

■ Wireless and Wired Interface Standard

→ Wireless :

1. IEEE 802.11g (Up to 54Mbps)
2. IEEE 802.11b (Up to 11Mbps)

→ Ethernet : 1 x IEEE 802.3 and IEEE 802.3u

■ Wireless Radio

→ Frequency band : 2.4GHz

→ Modulations :

1. 802.11b : DSSS (CCK, DQPSK, DBPSK)
2. 802.11g : OFDM (64-QAM, 16-QAM, QPSK, BPSK)

→ Channels :

1. USA (Channel 1~11)
2. Japan (Channel 1~14)
3. Europe (Channel 1~13)

→ Data Rate with auto fallback : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 and 1 Mbps

→ Receiver Sensitivity :

1. 802.11b : 11Mbps@-89dBm
2. 802.11g : 54Mbps@-74dBm

→ RF transmission power : 27dBm /500mW (

→ WCB1000H5PX provides a N-Female reverse connector.

WCB1010H5PX built-in 12.8dBi at 2.4GHz Sector Directional Antenna (Horizontal : 110 degree, Vertical : 60 degree)

■ General Base Station Features

- Number of ESSID : 8
- Three mode : BASE STATION P to P Mode, BRIDGE Mode and CPE Mode
- Slot Time, ACK/CTS Timeout support
- RSSI threshold support
- TX burst support
- Beacon interval : adjustable to best adapt to the deployment environment
- IBSP : to facilitate faster roaming for the stations among different BASE STATION nearby
- 802.11g protection : to let the transmission rate of the associated 802.11g stations not to be affected with surrounding existence of 802.11b stations
- RTS and fragmentation control
- Adjustable transmission power : 9 Levels (*Note)
- Wireless site survey : for scanning the surrounding base stations for connection
- VLAN tag support

■ Gateway Features in the CPE Mode

- Built-in NAT mode : to support IP sharing on the LAN side for multiple users(subscribers) to get access to the Internet
- Built-in DHCP server for issuing local IP addresses
- Built-in DNS client
- IP/ Port forwarding and DMZ
- IP/ MAC rule filtering

■ Security

- Data encryption : WEP (64/128/152-bits), WPA/WPA2 with TKIP or AES-CCMP
- User Authentication : WEP, IEEE 802.1X, WPA-PSK, WPA-Enterprise, MAC ACL
- Setting for TKIP/ CCMP/AES key's refreshing period
- Support IEEE 802.11 mixed mode; open and shared key authentication
- Hidden ESSID : broadcast SSID option can be turned off to prevent SSID broadcast to the public
- Station Isolation setting : when enabled, all stations associated with this BASE STATION can not communicate with each other
- Support data encryption over BRIDGE link

Note: The Power Level only can be adjusted lower than default 9 Level. Each Level is 3dBm lower from default maximum output power. The default output Power for each channel is in the bellowed table.

Channel	Channel 1	Channel 2~10	Channel 11
Fixed Maximum Output Power	18.34 dBm	26.85 dBm	16.77 dBm

■ Administration

- Web-based management interface
- Remote configuration and management
- Remote firmware upgradeable
- Software one-button-click to reset back to factory defaults
- Utilities for system configuration backup and restoration
- SNMP MIBII support (v2c/ v3)
- NTP time synchronization
- Syslog client
- Support Event Log
- Support statistics on total transmission encountered and transmitting error occurred

■ Hardware Specifications

- Die cast case : weather proof, compliant with IP67 standard
- On board surge protection
- LED Indication : Power x 1; Ethernet x 1; Wireless x 1; Signal Strength x 3

■ Physical and Power

- PoE : DC 48V/ 0.4 A
- Form factor : Wall or Pole Mountable
- Dimensions (W x D x H) : 6.5" x 3.8" x 1.9" (165 x 96 x 48 mm)
- Weight: 15.9 lbs (7.2 kg)

■ Environment

- Operation temperature : -30°C ~ 60°C
- Storage temperature : -30°C ~ 85°C
- Operation humidity : 100% maximum (Non-condensing)
- Storage humidity : 100% (Non-condensing)

■ Standard Pack Accessories

- PSE : Power Sourcing Equipment x 1
- AC Cable x 1
- Mounting Kit x 1

Chapter 3. Base Installation

3.1 Hardware Installation

3.1.1 Package Contents

The standard package contents of TEW-455APBO :

- | | |
|-------------------------------------|-----|
| ■ TEW-455APBO | x 1 |
| ■ Quick Installation Guide | x 1 |
| ■ CD-ROM (with User Manual and QIG) | x 1 |
| ■ PSE with AC Cable | x 1 |
| ■ Mounting Kit | x 1 |



Warning : It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

3.1.2 Panel Function Descriptions

TEW-455APBO

Front Panel



Rear Panel



1. Reset Button : System reboot button press until LED flashed and release for system reboot or for reset to factory default press, LED flashes keep pressing until LED becomes static
2. Power : Red LED ON indicates power on, and OFF indicates power off
3. Signal Strength : Yellow LED ON indicates Low Signal (CPE Mode)
4. Signal Strength : Green LED ON indicates Normal Signal (CPE Mode) or (BRIDGE Mode Only)
5. Signal Strength : Green LED ON indicates High Signal (CPE Mode) or (BASE STATION Mode Only)
6. WLAN : Green LED FLASH indicates Wireless ON, and FLASH quickly indicates

TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

Wireless Transmit quickly.

7. Ethernet : Green LED ON indicates connection, OFF indicates no connection
8. PoE Connector : For connecting to PSE
9. N-Type reverse Connector : For connecting to N-Type Female reverse connector



Note :

In CEP Mode, the LED 3 ON indicates the signal Low (Signal ≤ 10 RSSI); the LED 3 and 4 ON indicate the signal Normal ($10 < \text{Signal} \leq 40$ RSSI); the LED 3, 4 and 5 ON indicate the signal High (Signal > 40).

Only LED 4 ON indicates the operating mode is BRIDGE Mode; only LED 5 ON indicates the operating mode is BASE STATION Mode.

3.1.3 Hardware Installation Steps

Please follow the steps mentioned below to install the hardware of TEW-455APBO:



Front Panel



Rear Panel

1. Connect N-type reverse antenna to the N-type reverse connector on the rear panel.
2. Connect PSE to the PoE connector on the front panel.
3. Connect an Ethernet cable to the PSE and the other end to a computer.
4. Power on the PSE in order to supply power to TEW-455APBO

3.2 Software Configuration

3.2.1 Instruction to Web Management Interface

TEW-455APBO supports web-based configuration. Upon the completion of hardware installation, TEW-455APBO can be configured through a PC/NB by using its web browser such as Internet Explorer version 6.0.

- Default IP Address : 192.168.2.254
- Default IP Netmask : 255.255.255.0
- Default User Name and Password : admin / default

Step

■ IP Segment Set-up for Administrator's PC/NB

Set the IP segment of the administrator's computer to be in the same range as TEW-455APBO for accessing the system. Do not duplicate the IP Address used here with IP Address of TEW-455APBO or any other device within the network

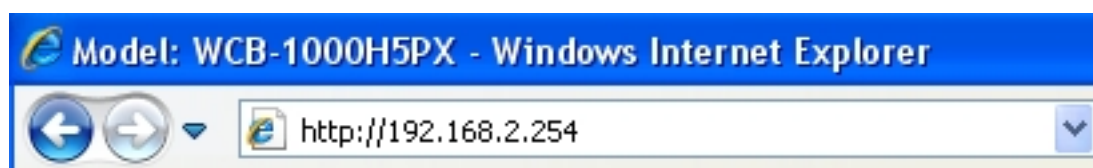
Example of Segment :

The value for underlined area can be changed as desired; the valid range is 1 ~ 254. However, 254 shall be avoided as it is already used by TEW-455APBO; use 10 as an example here.

- IP Address : 192.168.2.10
- IP Netmask : 255.255.255.0

■ Launch Web Browser

Launch as web browser to access the web management interface of system by entering the default IP Address, <http://192.168.2.254>, in the URL field, and then press **Enter**.



■ System Login

The system manager Login Page then appears.

Enter "**admin**" as **User name** and "**default**" as **Password**, and then click OK to login to the system.



Connect to 192.168.2.254

WCB-1000H5PX

User name:

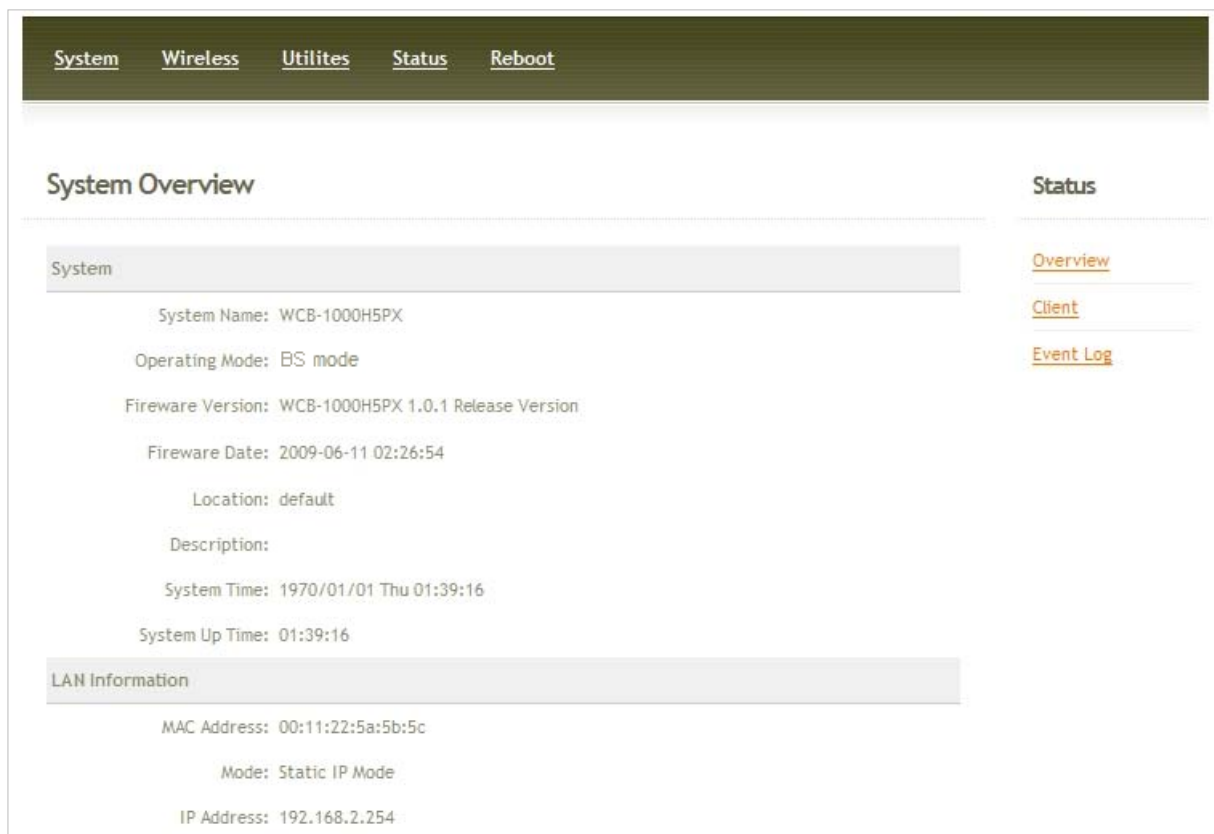
Password:

Remember my password

OK Cancel

■ Login Success

System Overview page will appear after successful login.



System Wireless Utilites Status Reboot

System Overview

System

System Name: WCB-1000H5PX

Operating Mode: BS mode

Fireware Version: WCB-1000H5PX 1.0.1 Release Version

Fireware Date: 2009-06-11 02:26:54

Location: default

Description:

System Time: 1970/01/01 Thu 01:39:16

System Up Time: 01:39:16

LAN Information

MAC Address: 00:11:22:5a:5b:5c

Mode: Static IP Mode

IP Address: 192.168.2.254

Status

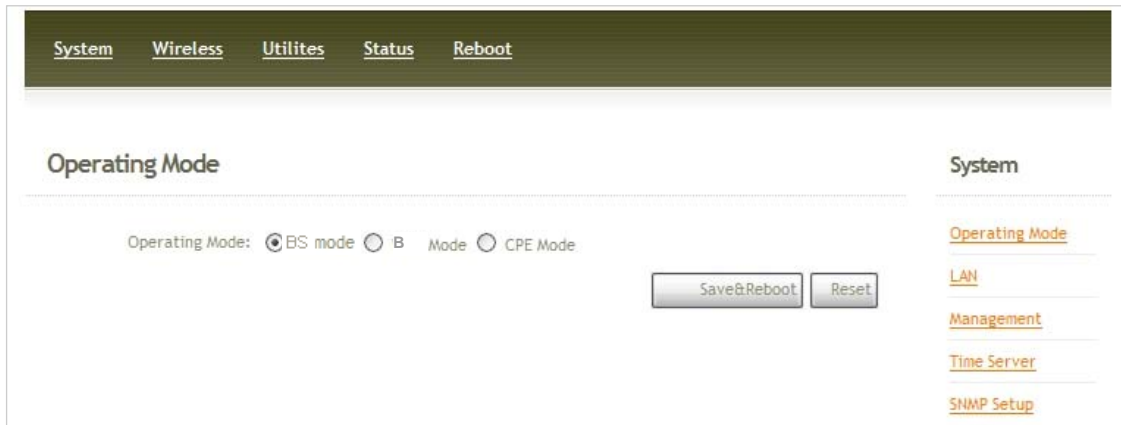
[Overview](#)

[Client](#)

[Event Log](#)

3.2.2 Quick Configuration

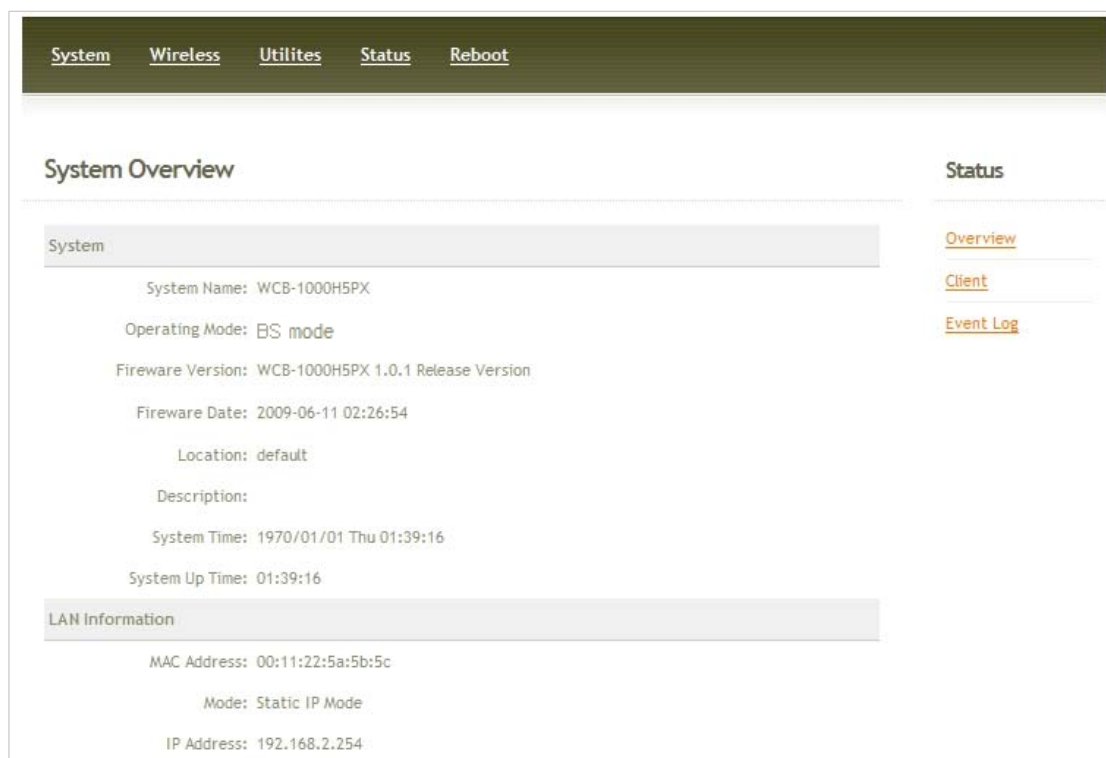
TEW-455APBO is a three mode system which can be configured either as a gateway or an base station as desired. This section provides a step-by-step configuration procedure for basic installation of BASE STATION Mode, BRIDGE Mode and CPE Mode.



3.2.2.1 BASE STATION Mode (Point to Point)

Step 1 : Mode Confirmation

Ensure the Operating Mode is currently at BASE STATION mode; the web management UI can be viewed at the **Status** section under the **System Overview** page.



Step 2 : Change Password

Click **System -> Management** and then **Admin Configuration** page appears.

Enter a new password, and verify it again in the **New Password** and **Check New Password** field respectively. Click **Save** button, and process with steps followed.

Step 3 : LAN IP Settings

Click **System -> LAN**, and then **Network Setup** page appears.

Enable "Static IP" and "DNS", and enter the related information in the field marked with red asterisks. Click **Save** button to save the settings.

Step 4 : Time Zone settings

Click **System -> Time Server**, and then **Time Server Setup** page appears.

Enable “Setup Time Use NTP”, and then enter the related information. Click **Save** button to save the settings.

Step 5 : ESSID Settings

Click **Wireless -> Virtual BASE STATION Setup**, and then **VBS Setup** page appears.

Enable	VBS	ESSID	Encryption	ACL Mode	ACL Setup	EDIT
<input type="checkbox"/>	VBS 0	BS00	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 1	BS01	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 2	BS02	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 3	BS03	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 4	BS04	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 5	BS05	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 6	BS06	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 7	BS07	disabled	disabled	Setup	Edit

Enable “VBS0”, and then click **Save** button to save settings. Click “Edit” and then **VBS0 Configuration** page appears.

VBS 0 Configuration

General

ESSID :

Hidden SSID : Enable Disable

Client Isolation : Enable Disable

WMM : Enable Disable

IAPP Support : Enable Disable

Maximum Clients : (1 - 32, default 32)

VLAN ID : Enable Disable (1~4049)

Security Type : ▼

Wireless

[General Setup](#)

[Advanced Setup](#)

[Virtual AP Setup](#)

Setup broadcast ESSID for easy identification of system when device is trying to associate with service. Click **Save** button to save settings

Step 6 : Security Settings

In **VBS0 Configuration** page, select WEP in “Security Type” pull down menu. The WEP setting field will show up immediately.

WEP

Key Length : ▼

WEP auth method : Open system Shared

Passphrase : (5 ,13, 16 ASCII Format)

WEP Key 1 : (10, 26, 32 HEX Format)

WEP Key 2 : (10, 26, 32 HEX Format)

WEP Key 3 : (10, 26, 32 HEX Format)

WEP Key 4 : (10, 26, 32 HEX Format)

Enter the WEP key information required in the WEP settings field, and the same information will also be used to set up devices which will then be using TEW-455APBO's services.

Click **Reboot** to activate all settings configured so far.

Congratulation !

The BASE STATION mode is now successfully configured.

3.2.2.2 BRIDGE Mode

Step 1 : Mode Confirmation

Ensure the Operating Mode is currently at BRIDGE mode; the web management UI can be viewed at the **Status** section under the **System Overview** page.

The screenshot displays the 'System Overview' page. On the left, under the 'System' section, the following information is listed: System Name: WCB-1000H5PX, Operating Mode: B mode, Firmware Version: WCB-1000H5PX 1.0.0 Release Version, Firmware Date: 2009-06-17 02:19:42, Location: default, Description: (empty), System Time: 1970/01/01 Thu 00:51:47, and System Up Time: 51:47. Below this is the 'LAN Information' section, showing MAC Address: 00:11:22:5a:5b:5c, Mode: Static IP Mode, and IP Address: 192.168.2.254. On the right side, under the 'Status' header, there are three links: Overview, Bridge List, and Event Log.

Step 2 : Change Password

Click **System -> Management** and then **Admin Configuration** page appears.

The screenshot shows the 'Admin Configuration' page. The 'System Information' section contains input fields for System Name (WCB-1000H5PX), Description, and Location (default). The 'Admin Password' section has two input fields: 'New Password:' and 'Check New Password:', with a note '(If you don't want to change, don't type anything)'. The 'Admin Login Methods' section has two checked checkboxes: 'Enable HTTP' with a port of 80 (Default:80) and 'Enable Telnet' with a port of 23 (Default:23). At the bottom right, there are 'Save' and 'Reset' buttons. On the right side of the page, under the 'System' header, there are links for Operating Mode, LAN, Management, Time Server, and SNMP Setup.

Enter a new password, and verify it again in the **New Password** and **Check New Password** field respectively. Click **Save** button, and process with steps followed.

Step 3 : LAN IP Settings

Click **System** -> **LAN**, and then **Network Setup** page appears.

Enable “Static IP” and “DNS”, and enter the related information in the field marked with red asterisks. Click **Save** button to save the settings.

Step 4 : Time Zone settings

Click **System** -> **Time Server**, and then **Time Server Setup** page appears.

Enable “Setup Time Use NTP”, and then enter the related information. Click **Save** button to save the settings.

Step 5 : Enable BRIDGE Peer's MAC Address

Click **Wireless** -> **BRIDGE Setup**, and then **BRIDGE Setup** page appears.

Wireless Setup Sub Menu

BRIDGE Setup

WMM : Enable Disable

Security Type :

Enable	BRIDGE Peer's MAC Address	VLAN ID (0 is not set.)	Description
<input type="checkbox"/>	01. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	02. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	03. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	04. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	05. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	06. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	07. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	08. <input type="text" value=": : : : :"/>	<input type="text"/>	<input type="text"/>

[General Setup](#)
[Advanced Setup](#)
[Bridge Setup](#)

Enable “BRIDGE Peer's MAC Address”, and then enter the related information. Click **Save** button to save the settings.

Step 6 : Wireless General Settings

Click **Wireless** -> **General Setup**, and then **General Setup** page appears.

Wireless Setup Wireless

General Setup

MAC address : 00:11:22:5a:5b:5d

Band Mode :

Transmit Rate Control :

Country :

Channel :

Tx Power :

[General Setup](#)
[Advanced Setup](#)
[Virtual BS Setup](#)

Select the “Channel” and “Transmit Rate Control” information required in the General Setup field. The information must be the same the other BRIDGE device.

Click **Reboot** to activate all settings configured so far.

Congratulation !

The BRIDGE mode is now successfully configured.

3.2.2.3 CPE Mode

Step 1 : Mode Confirmation

Ensure the Operating Mode is currently at CPE mode; the web management UI can be viewed at the **Status** section under the **System Overview** page.

System Overview	Status
<p>System</p> <p>System Name: WCB-1000H5PX</p> <p>Operating Mode: CPE mode</p> <p>Fireware Version: WCB-1000H5PX 1.0.1 Release Version</p> <p>Fireware Date: 2009-06-11 08:14:40</p> <p>Location: default</p> <p>Description:</p> <p>System Time: 1970/01/01 Thu 00:27:10</p> <p>System Up Time: 27:10</p>	<p>Overview</p> <p>DHCPD Clients</p> <p>Event Log</p>
<p>WAN Information</p> <p>Mode: Static IP</p> <p>MAC Address: 00:11:22:5a:5b:5d</p> <p>IP Address: 192.168.1.254</p> <p>IP Netmask: 255.255.255.0</p>	

Step 2 : Change Password

Click **System -> Management** and then **Admin Configuration** page appears.

Admin Configuration	System
<p>System Information</p> <p>System Name: <input type="text" value="WCB-1000H5PX"/></p> <p>Description: <input type="text"/></p> <p>Location: <input type="text" value="default"/></p>	<p>Operating Mode</p> <p>WAN</p> <p>LAN</p> <p>Management</p> <p>Time Server</p> <p>SNMP Setup</p>
<p>Admin Password</p> <p>New Password: <input type="text"/> (If you don't want to change , don't type anything)</p> <p>Check New Password: <input type="text"/></p>	
<p>Admin Login Methods</p> <p><input checked="" type="checkbox"/> Enable HTTP Port : <input type="text" value="80"/> (Default:80)</p> <p><input checked="" type="checkbox"/> Enable Telnet Port : <input type="text" value="23"/> (Default:23)</p>	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Enter a new password, and verify it again in the **New Password** and **Check New Password** field respectively. Click **Save** button, and process with steps followed.

Step 3 : Site Survey

Click **Wireless -> Site Survey**, and then **CPE Site Survey** page appears. The system will automatically scan and display the scan results on all BASE STATION existing near by the system.

CPE Site Survey						Wireless
Scan Result						General Setup
						Advanced Setup
						Site Survey
ESSID	MAC Address	Channel	Signal Level	Security	Setup	
AP00	00:11:A3:07:01:07	1	-71 dBm	WEP	<input type="button" value="SETUP"/>	
AP51_2	0A:0D:0B:13:6B:18	4	-72 dBm	WEP	<input type="button" value="SETUP"/>	
AP51_3	0E:0D:0B:13:6B:18	4	-71 dBm	WPA-PSK2(TKIP)	<input type="button" value="SETUP"/>	
AP51_1	06:0D:0B:13:6B:18	4	-71 dBm	WEP	<input type="button" value="SETUP"/>	
AP01	06:11:A3:07:01:07	1	-72 dBm	WEP	<input type="button" value="SETUP"/>	
AP02	0A:11:A3:07:01:07	1	-72 dBm	None	<input type="button" value="SETUP"/>	
AP51_0	00:0D:0B:13:6B:18	4	-70 dBm	WPA-PSK(TKIP)	<input type="button" value="SETUP"/>	
HomeIP	00:0E:2E:4A:24:40	6	-93 dBm	WPA-PSK(TKIP)	<input type="button" value="SETUP"/>	



Note : The scan result displayed here is an example only.

Step 4 : Select BASE STATION to be Associated

Search for the BASE STATION to be associated with from the Scan Result list provided in **Step 3**; use **BS00** as an example here where the BASE STATION is encrypted via WEP security type.

Step 5 : Security Settings

Click **SETUP** button of the **BS00**, and related information will display in **Wireless Configuration** page.

Enter the information required in the Wireless Configuration page. Information to be entered shall be exactly the same as configured in the **BS00 Base Station**.

Click **Save** to save the settings.

Wireless Configuration	Wireless
General Setup	
Advanced Setup	
Site Survey	
General Setup	
ESSID : <input type="text" value="BS00"/>	
Band Mode: <input type="text" value="802.11b+802.11g"/>	
Transmit Rate Control: <input type="text" value="Auto"/>	
Country: <input type="text" value="US"/>	
Channel: <input type="text" value="1"/>	
Tx Power: <input type="text" value="Level 9"/>	
Security Type: <input type="text" value="WEP"/>	
WEP	
Key Length: <input type="text" value="64 bits"/>	
WEP auth method: <input type="checkbox"/> Open system <input type="checkbox"/> Shared	
<input checked="" type="radio"/> WEP Key 1: <input type="text"/>	
<input type="radio"/> WEP Key 2: <input type="text"/>	
<input type="radio"/> WEP Key 3: <input type="text"/>	
<input type="radio"/> WEP Key 4: <input type="text"/>	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Step 6 : WAN Settings

Click **System** -> **WAN**, and then **WAN Setup** page appears.

WAN Setup	System
Operating Mode	
WAN	
LAN	
Management	
Time Server	
SNMP Setup	
Internet Connection Type	
Mode: <input checked="" type="radio"/> Static IP <input type="radio"/> Dynamic IP <input type="radio"/> PPPoE	
<input checked="" type="radio"/> Keep Default MAC Address	
<input type="radio"/> Clone MAC Address: 00:1a:92:9f:a4:9b	
<input type="radio"/> Manual MAC Address: <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	
Static IP	
Choose this option to set static IP informatin provided to you by your ISP.	
IP Address: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="254"/>	
IP Netmask: <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>	
IP Gateway: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>	
DNS	
DNS: <input checked="" type="radio"/> No Default DNS Server <input type="radio"/> Specify DNS Server IP	
Primary: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Secondary: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Enable “Static IP”, and then enter the related information. Click **Save** button to save the settings. (**Default WAN IP is 192.168.1.254**)

Step 7 : LAN Settings

Click **System** -> **LAN**, and then **LAN Setup** page appears.

Enter the “IP Address” and “IP Netmask” of the LAN Setup.

Step 8 : Time Zone settings

Click **System** -> **Time Server**, and then **Time Server Setup** page appears.

Enable “Setup Time Use NTP”, and then enter the related information. Click **Save** button to save the settings.

Click **Reboot** button to activate all settings configured so far.

Congratulation !

The CPE mode is now successfully configured.

Chapter 4. BASE STATION (Point to Point) Mode Configuration

When BASE STATION mode is activated, the system can be configured as an Base station. This section provides information in configuring the BASE STATION mode with graphical illustrations. TEW-455APBO provides functions as stated below where they can be configured via a user-friendly web based interface.

Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Settings	Profiles Settings	System Overview
	LAN	Advanced Settings	Firmware Upgrade	Associate Client Status
	Management	Virtual BASE STATION	Ping Utility	Event Log
	Time Server		Reboot	
	SNMP			

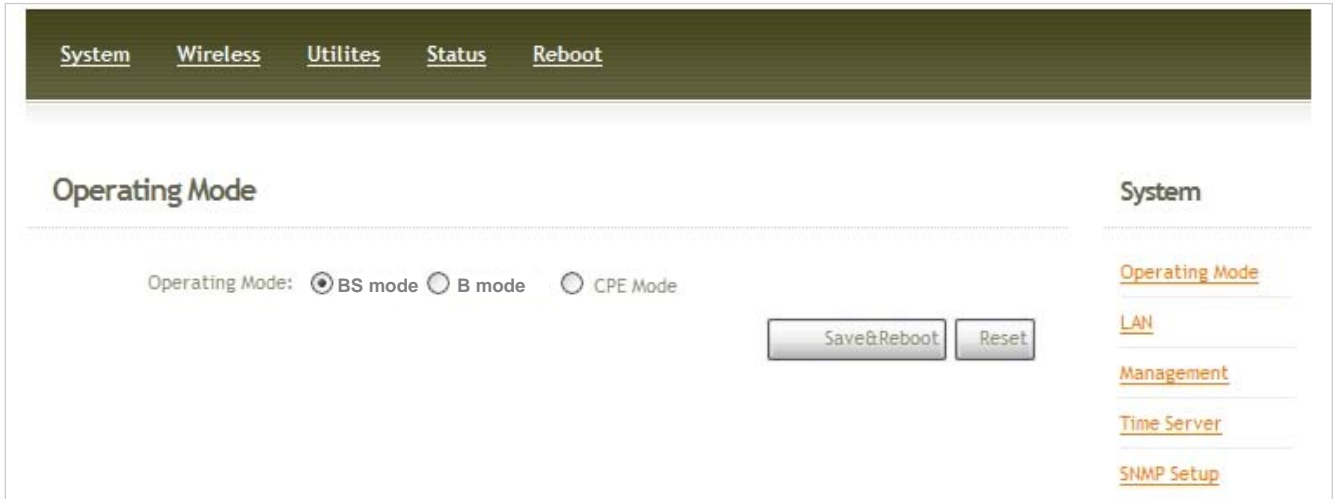
Table 4-1: BASE STATION Mode Functions

The screenshot shows the 'System Overview' page of the TEW-455APBO web interface. At the top, there is a navigation bar with tabs for 'System', 'Wireless', 'Utilites', 'Status', and 'Reboot'. The main content area is divided into two columns. The left column, titled 'System Overview', contains a 'System' section with the following details: System Name: WCB-1000H5PX, Operating Mode: BS mode, Fireware Version: WCB-1000H5PX 1.0.1 Release Version, Fireware Date: 2009-06-11 02:26:54, Location: default, Description: (empty), System Time: 1970/01/01 Thu 01:39:16, and System Up Time: 01:39:16. Below this is a 'LAN Information' section with: MAC Address: 00:11:22:5a:5b:5c, Mode: Static IP Mode, and IP Address: 192.168.2.254. The right column, titled 'Status', contains three links: 'Overview', 'Client', and 'Event Log'.

Figure 4-1: BASE STATION Mode Main Page

4.1 System

This section provides information in configuring the following functions: **Operating Mode**, **LAN Setup**, **Management**, **Time Server**, **SNMP Setup**



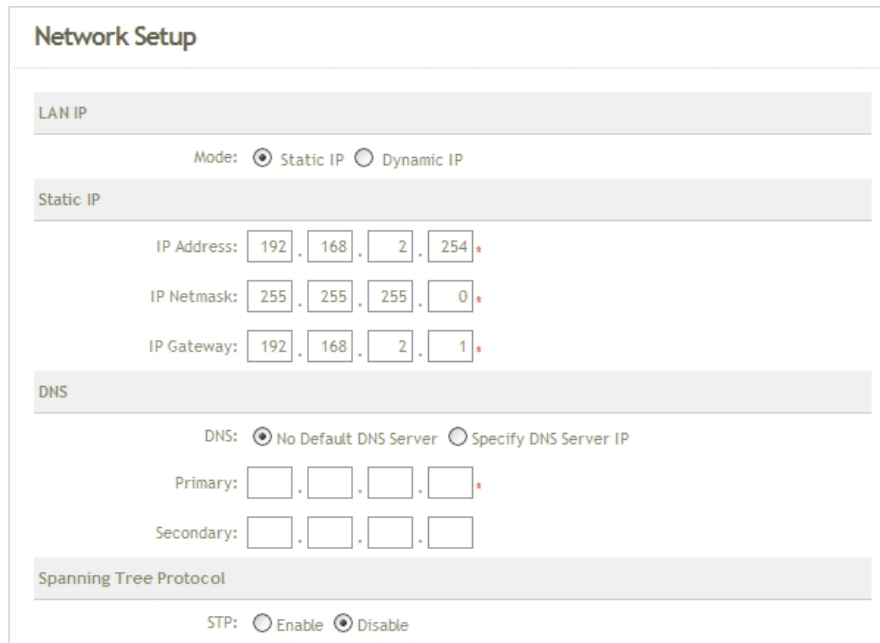
4.1.1 Operating Mode

TEW-455APBO supports three operation modes; BASE STATION mode , BRIDGE mode and CPE mode. The administrator can set the desired mode via this page, and then configure the system according to their deployment needs.

- ✓ **BS Mode** : Check **BS Mode** button to enable BASE STATION mode, and then click “**Save&Reboot**” to activate the setting.
- ✓ **B Mode** : Check **B Mode** button to enable Bridge mode, and then click “**Save&Reboot**” to activate the setting.
- ✓ **CPE Mode** : Check **CPE Mode** button to enable CPE mode, and then click “**Save&Reboot**” to activate the setting.

4.1.2 LAN Setup

Here is the instruction for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.



Network Setup

LAN IP

Mode: Static IP Dynamic IP

Static IP

IP Address: 192 . 168 . 2 . 254 *

IP Netmask: 255 . 255 . 255 . 0 *

IP Gateway: 192 . 168 . 2 . 1 *

DNS

DNS: No Default DNS Server Specify DNS Server IP

Primary: . . . *

Secondary: . . .

Spanning Tree Protocol

STP: Enable Disable

- **Mode** : Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
- ➔ **Static IP** : The administrator can manually setup the LAN IP address when static IP is available/ preferred.



Static IP

IP Address: 192 . 168 . 2 . 254 *

IP Netmask: 255 . 255 . 255 . 0 *

IP Gateway: 192 . 168 . 2 . 1 *

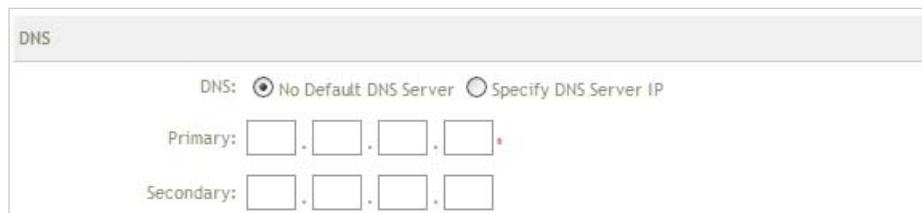
- ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
- ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1
- ➔ **Dynamic IP** : This configuration type is applicable when the WCB1000H5PX/ WCB1010H5PX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.



Dynamic IP

Hostname:

- ✓ **Hostname** : The Hostname of the LAN port
- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.



DNS

DNS: No Default DNS Server Specify DNS Server IP

Primary: . . . *

Secondary: . . .

- **Primary** : The IP address of the primary DNS server.
- **Secondary** : The IP address of the secondary DNS server.

■ Spanning Tree Protocol

The spanning tree network protocol provides a loop free topology for any bridged LAN. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



Spanning Tree Protocol

STP: Enable Disable

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.1.3 Management

The administrator can later obtain the geographical location of the system via the information configured here. The administrator also can change system password and configure system login methods. Please click **System -> Management** and follow the below settings.

■ System Information

- **System Name** : Enter a desired name or use the default provided.
- **Description** : Denote further information of the system.
- **Location** : Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.

- **Admin Password** : The admin manager can change its respected password. Enter the new password, and then verify the new password in the Check New Password filed. Click **Save** button to activate the new password.

- **New Password** : Please input the new password of administrator.
- **Check New Password** : Please input again the new password of administrator.

TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

- **Admin Login Methods** : The admin manager can enable or disable system login methods, it also can change services port. Click **Save** button to activate the admin login methods.

Admin Login Methods	
<input checked="" type="checkbox"/> Enable HTTP	Port : <input type="text" value="80"/> (Default:80)
<input checked="" type="checkbox"/> Enable Telnet	Port : <input type="text" value="23"/> (Default:23)

- **Enable HTTP** : Select Enable HTTP to activate HTTP Service
- **HTTP Port** : Please input 1 ~ 65535 value to set HTTP Port; default value is 80
- **Enable Telnet** : Select Enable HTTP to activate HTTP Service
- **Telnet Port** : Please input 1 ~ 65535 value to set HTTP Port; default value is 23

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.1.4 Time Server

System time can be configured via this page where manual setting and NTP server configuration are both supported. Please click on **System -> Time Server** and follow the below setting.

- **Local Time** : Display the current time of the system.
- **Setup Time Use NTP** : Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
 - **Default NTP Server** : Select the NTP Server from the drop-down list.
 - **Time Zone** : Please set a time zone from where the accurate time can be supplied, **(GMT+08:00) Taipei** for example.
 - **Daylight saving time** : Enable Daylight saving time from where the accurate time needed.
- **User Setup** : Enable User Setup and Click **Set Time** button; the system time can be configured manually.

- **Set Time** : Click Set Time button, the Time field should be changed automatically.
- **Set the time** : Select the appropriate **Year, Month, Day, Hour, Minute** and **Second** from the drop-down list.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.1.5 SNMP Setup

SNMP is an application-layer protocol that provides a message of format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely. Please click on **System -> SNMP Setup** and follow the below setting.

- **v2c** : Check v2c button to activate SNMP v2c agent or unchecked to deactivate this function.

- **ro community** : Enter the community strings that allows read-only access to the system's SNMP information.
- **rw community** : Enter the community strings that allows read/write access to the system's SNMP information.

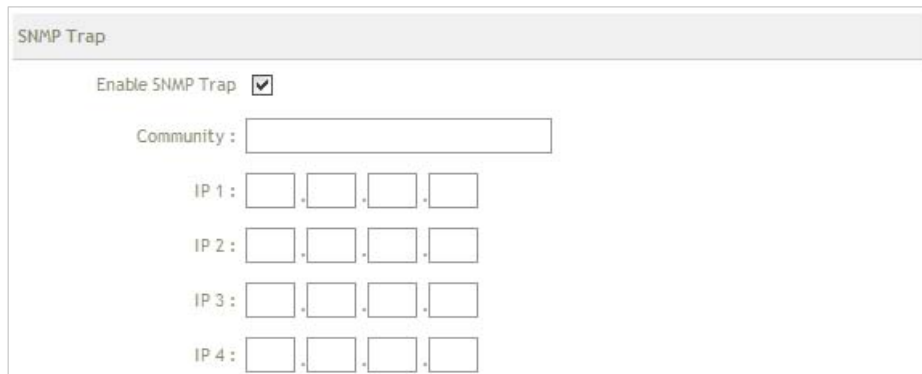
- **v3** : Check v3 button to activate SNMP v3 agent or unchecked to deactivate this function. SNMPv3 supports the highest available levels of security for SNMP communication.

- **SNMP ro user** : Enter the community strings that allows read-only access to the system's SNMP information.
- **SNMP ro password** : Enter the password that allows read-only access to the system's SNMP information.
- **SNMP rw user** : Enter the community strings that allows read/write access to the system's SNMP information.

information.

→ **SNMP rw password** : Enter the password that allows read/write access to the system's SNMP information.

- **SNMP Trap** : Events on cold start, interface up & down, and association & disassociation can be reported via this function to an assigned server.



The image shows a web-based configuration interface for SNMP Traps. At the top, there is a header 'SNMP Trap'. Below it, there is a checkbox labeled 'Enable SNMP Trap' which is checked. Underneath, there is a text input field labeled 'Community :'. Below the community field, there are four rows of IP address input fields, each labeled 'IP 1 :', 'IP 2 :', 'IP 3 :', and 'IP 4 :'. Each IP field is a four-digit box with a dot separator between digits.

→ **Community** : Enter the community strings required by the remote host computer that will receive trap messages or notices send by the system.

→ **IP** : Enter the IP address of the remote host computer that will receive the trap messages.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.2 Wireless

The system manager can configure related wireless settings, **General Settings**, **Advanced Settings**, **Virtual BASE STATION Setting**, **Security Settings**, and **Access Control Settings**.

The screenshot shows a web-based configuration interface for a wireless access point. At the top, there is a dark navigation bar with the following menu items: [System](#), [Wireless](#), [Utilites](#), [Status](#), and [Reboot](#). Below this, the main content area is titled "Wireless Setup". On the right side of this area, there is a sub-menu titled "Wireless" with three options: [General Setup](#) (highlighted), [Advanced Setup](#), and [Virtual BS mode](#). The "General Setup" section is active and displays the following configuration options:

- MAC address : 00:11:22:5a:5b:5d
- Band Mode: 802.11b+802.11g (dropdown menu)
- Transmit Rate Control: Auto (dropdown menu)
- Country: US (dropdown menu)
- Channel: 1 (dropdown menu)
- Tx Power: Level 9 (dropdown menu)

At the bottom right of the configuration area, there are two buttons: "Save" and "Reset".

4.2.1 General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

The screenshot shows the 'Wireless Setup' interface. The 'General Setup' section is active, displaying the following configuration:

- MAC address : 00:11:22:5a:5b:5d
- Band Mode : 802.11b+802.11g
- Transmit Rate Control : Auto
- Country : US
- Channel : 1
- Tx Power : Level 9

On the right side of the interface, there are three navigation links: [General Setup](#), [Advanced Setup](#), and [Virtual BS mode](#).

- **MAC address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are 801.11b, 802.11g and 802.11b+802.11g.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from 1 to 54Mbps for 802.11g and 802.11b/g modes, or 1 to 11Mbps for 802.11b mode.
- **Country** : Select the desired country code from the drop-down list; the options are US, ETSI and Japan.
- **Channel** : The channel range will be changed by selecting different country code. The channel range from 1 to 11 for US country code, or 1 to 13 for ETSI country code, or 1 to 14 for Japan.
- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select the LEVEL 1 to LEVEL 9 you needed for your environment. If you are not sure of which setting to choose, then keep the default setting, LEVEL 9.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for BASE STATION's RF general settings and will be applied to all VBSs.

4.2.2 Advanced Setup

The administrator can change the Slot Time, ACK/CTS Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

The screenshot shows the 'Wireless Setup' interface with the 'Advanced Setup' tab selected. The settings are as follows:

Parameter	Value	Range / Default
Slot Time	20	(1 - 1489, default 20, slottime = 9 + distance / 300)
ACK Timeout	48	(1 - 372, default 48, acktimeout = slottime *2 +3)
CTS Timeout	48	(1 - 744, default 48)
RSSI Threshold	24	((-128) - 127, default 24)
Beacon Interval	100	(10 - 5000, default 100)
DTIM Interval	1	(1 - 15, default 1)
Fragment Threshold	2346	(256 - 2346, default 2346)
RTS Threshold	2346	(1 - 2346, default 2346)
Short Preamble	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
802.11g Protection Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

- **Slot Time** : Enter the desired slot time for the BASE STATION.
- **ACK Timeout** : The time interval for waiting the “ ACKnowledgment frame”. If the ACK is not received within that timeout period then the packet will be re-transmitted. Higher ACK Timeout will decrease the packet lost, but the throughput will be growing worse.
- **CTS Timeout** : Enter the desired CTS timeout for the BASE STATION.



Note : Slot Time and ACK/CTS Timeout settings for long distance links. It is important to change the value to find the optimal setting. A value too low will give very low throughput, A high value may slowdown the link.

- **RSSI Threshold** : RSSI Threshold can be used to control the level of noise received by the device.
- **Beacon Interval** : Enter a value between 10 and 5000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the base station and the wireless network.

TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

- **DTIM Interval** : Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will let the wireless client save energy more, but the throughput will be growing worse.
- **Fragment Threshold** : The value specifies the maximum size of packet allowed before data is fragmented into multiple packets. Please use this value to tune the wireless connection if lots of retransmission happens. Enter a value ranging from 256 to 2346.
- **RTS Threshold** : Tuning the Request to Send, RTS threshold will help the system control its access to medium and alleviate the hidden node problem. Enter a value ranging from 1 to 2346.
- **Short Preamble** : The short preamble provides 56-bit Synchronization field to improve WLAN transmission efficiency. Check **Enable** button for using Short Preamble, and **Disable** for using the Long Preamble, 128-bit Synchronization field, option.
- **Tx Burst** : Click **Enable** button to activated Tx Burst, and **Disable** to deactivated Tx Burst.
- **802.11g Protection Mode** : Click **Enable** button to activated 802.11g Protection Mode, and Disable to deactivated 802.11g Protection Mode.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for BASE STATION's RF advanced settings and will be applied to all VBSs.

4.2.3 Virtual BASE STATION Setup

The administrator can create Virtual BASE STATION via this page. Please click on **Wireless -> Virtual BS STATION Setup** and follow the below setting.

The screenshot shows the 'VAP Setup' page with a 'Wireless List' table and a 'Wireless' sidebar. The table lists 8 Virtual Base Stations (VBS 0-7) with columns for Enable, VBS, ESSID, Encryption, ACL Mode, ACL Setup, and EDIT. The 'Enable' column contains unchecked checkboxes. The 'Encryption' and 'ACL Mode' columns are set to 'disabled'. The 'ACL Setup' column contains 'Setup' links, and the 'EDIT' column contains 'Edit' links. At the bottom right of the table are 'Save' and 'Reset' buttons. The sidebar on the right has 'Wireless' as a header and three links: 'General Setup', 'Advanced Setup', and 'Virtual BS mode'.

Enable	VBS	ESSID	Encryption	ACL Mode	ACL Setup	EDIT
<input type="checkbox"/>	VBS 0	BS00	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 1	BS01	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 2	BS02	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 3	BS03	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 4	BS04	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 5	BS05	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 6	BS06	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VBS 7	BS07	disabled	disabled	Setup	Edit

- **Enable** : Click **Enable** button and **Save** button for creating Virtual BASE STATION
- **VBS** : Display number of system's Virtual BASE STATION.
- **ESSID** : Display Virtual BASE STATION's ESSID; default is BS00~BS07.
- **Encryption** : Display Virtual BASE STATION's Security Type; default is disabled.
- **ACL Mode** : Display Virtual BASE STATION's ACL Mode; default is disabled.
- **ACL Setup** : Click Setup button for configuring Virtual BASE STATION's Access Control List.
- **EDIT** : Click Edit button for configuring Virtual BASE STATION's settings and security type.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.2.3.1 Virtual BASE STATION General Configuration

For each Virtual BASE STATION, administrators can configure general settings and wireless security type. Click **Wireless -> Virtual BASE STATION -> EDIT**, and then Virtual BASE STATION Configuration page appears.

VBS 0 Configuration

General

ESSID :

Hidden SSID : Enable Disable

Client Isolation : Enable Disable

WMM : Enable Disable

IAPP Support : Enable Disable

Maximum Clients : (1 - 32, default 32)

VLAN ID : Enable Disable (1-4094)

Security Type : ▼

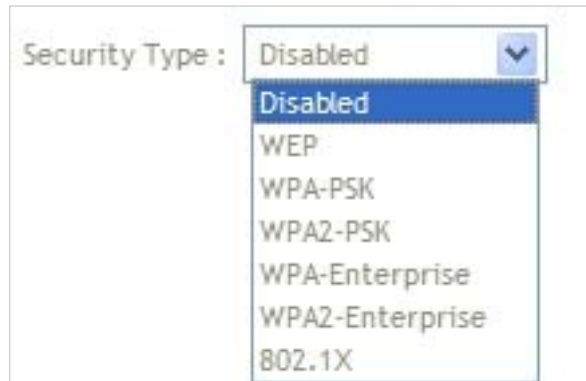
- **ESSID** : Extended Service Set ID indicates the SSID which the clients used to connect to the VBS. ESSID will determine the service type of a client which is assigned to the specified VBS.
- **Hidden SSID** : Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from begin seen on networked.
- **Client Isolation** : Select **Enable**, all clients will be isolated each other, that means all clients can not reach to other clients.
- **WMM** : Select Enable, the packets with QoS WMM will has higher priority.
- **IBSP Support** : Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current base station (BS) and new BS during hand off period.



Note : IBSP supported only for WPA-PSK/WPA2-PSK, WPA-Enterprise/WPA2-Enterprise and 802.1X security type.

- **Maximum Clients** : Enter maximum number of clients to a desired number. For example, while the number of client is set to 5, only 5 clients are allowed to connect with this VBSF.
- **VLAN ID** : Virtual LAN, the system supports tagged VLAN. To enable VLAN function; valid values are from 1 to 4094.


- **Security Type** : Select the desired security type from the drop-down list; the options are WEP, WPA-PSK, WPA2-PSK, WPA-Enterprise, WPA2-Enterprise and 802.1X.



- **Disable** : Data are unencrypted during transmission when this option is selected.
- **WEP** : WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key. Select **WEP** as the security type from the drop down list as desired.

- ✓ **Key Length** : Select the desired options which are **64 bits**, **128 bits** or **152 bits** from drop-down list.
- ✓ **WEP auth Method** : Enable the desired option among **Open system** or **Shared**.
- ✓ **Passphrase** : Enter ASCII format in this field. Click Generate button, and then selected key value will be filled.
- ✓ **WEP Key #** : Select key index is used to designate the WEP key during data transmission. Enter HEX format WEP key value; the system supports up to 4 sets of WEP keys.

- **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.



WPA General

Cipher Suite : AES TKIP

Group Key Update Period : (>=10 seconds)

Master Key Update Period : (>=10 seconds)

Key Type : ASCII HEX

Pre-shared Key :

- ✓ **Cipher Suite** : Check on the respected button to enable either AES or TKIP cipher suites; default is TKIP.
- ✓ **Group Key Update Period** : This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Master Key Update Period** : This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.
- ✓ **Key Type** : Check on the respected button to enable either ASCII or HEX format for the Pre-shared Key.
- ✓ **Pre-shared Key** : Enter the information for pre-shared key; the format of the information shall according to the key type selected.



Note : Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this selected.

WPA General

Cipher Suite : AES TKIP

Group Key Update Period : (>=10 seconds)

Master Key Update Period : (>=10 seconds)

Authentication RADIUS Server

Authentication Server : . . .

Port :

Shared Secret :

EAP Reauth Period :

Accounting RADIUS Server Enable Disable

✓ **WPA General Settings :**

- **Cipher Suite :** Check on the respected button to enable either AES or TKIP cipher suites.
- **Group Key Update Period :** This time interval for re-keying GTK (broadcast/ multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- **Master Key Update Period :** This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.

✓ **Authentication RADIUS Server Settings :**

- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port :** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- **Shared secret :** The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.
- **EAP Reauth Period :** EAP re-authentication period in seconds; default is 3600; 0 = disable re-authentication.
- **Accounting Server :** Check on the respected button to enable either Enable or Disable accounting RADIUS server.

✓ **Accounting Server Settings :**

- **Accounting Server** : Enter the IP address of the Accounting RADIUS server.
- **Port** : The port number used by Accounting RADIUS server. Use the default 1813 or enter port number specified.
- **Shared Secret** : The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.

→ **802.1X** : When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

✓ **Dynamic WEP Settings :**

- **WEP Key length** : Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- **WEP Key Update Period** : The time interval WEP will then be updated; the unit is in seconds; default is 300 seconds; 0 = do not re-key.
- **Group Key Update Period** : This time interval for re-keying GTK (broadcast/ multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

✓ **Authentication RADIUS Server Settings :**

- **Authentication Server** : Enter the IP address of the Authentication RADIUS server.
- **Port** : The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- **Shared secret** : The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.
- **EAP Reauth Period** : EAP reauthentication period in seconds; default is 3600; 0 = disable reauthentication.
- **Accounting Server** : Check on the respected button to enable either Enable or Disable accounting RADIUS server.

✓ **Accounting Server :**

The screenshot shows a configuration window titled "Accounting Server". It contains three input fields: "Accounting Server" with a dotted IP address template (four boxes separated by dots), "Port" with the value "1813" entered, and "Shared Secret" with an empty text box.

- **Accounting Server** : Enter the IP address of the Accounting RADIUS server.
- **Port** : The port number used by Accounting RADIUS server. Use the default 1813 or enter port number specified
- **Shared Secret** : The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.2.3.2 Virtual BS Access Control List (ACL) Setup

In this function, the administrator can be allow or reject clients to access Virtual BS. Please click on **Wireless -> Virtual BS Setup -> ACL Setup** and follow the below setting.

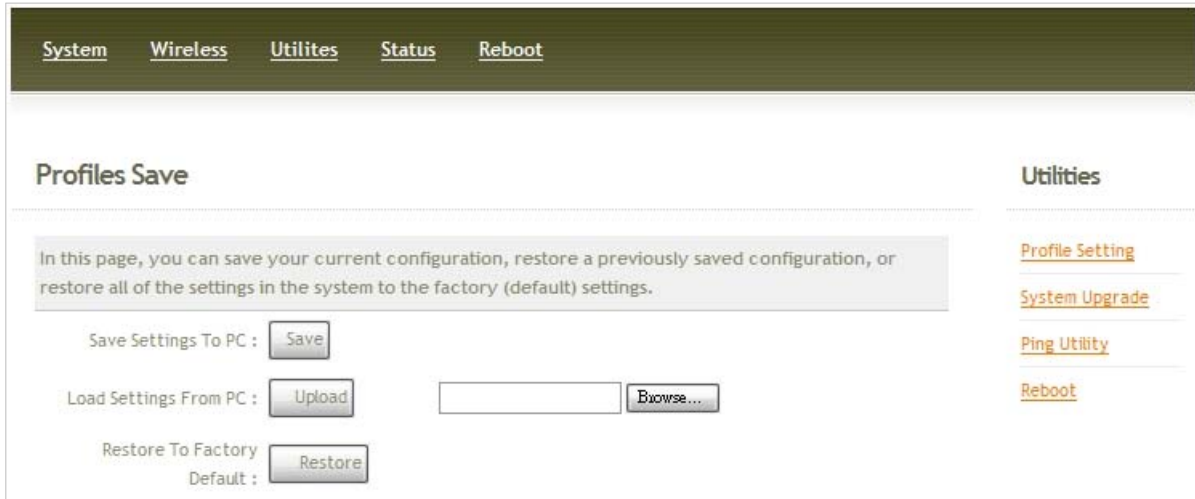
The screenshot shows the 'VAP 0 ACL List Configuration' web interface. It is divided into two main sections: 'ACL Rule' and 'ACL LIST'. In the 'ACL Rule' section, there is a label 'Access Control Type:' followed by a dropdown menu currently set to 'Disable' and a 'Save' button. The 'ACL LIST' section contains a label 'MAC Address:' followed by an empty text input field and an 'Add' button. Below the input field, the text 'No ACL list data' is displayed.

- **Access Control Type** : Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.
- **MAC Address** : Enter MAC address in this field. There are **20** users maximum allowed in this MAC address list.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.3 Utilities

The administrator can maintain the system via this page: **Profile Setting**, **System Upgrade**, **Ping Utility**, and **Reboot**.



4.3.1 Profile Setting

Current settings on the system can be backed up, or previous backed up settings can be restored as well as resetting the system back to factory default can be performed via this page. Please click on **Utilities -> Profile Setting** and follow the below setting.



- **Save Settings to PC** : Click **Save** button to save the current system settings to a local disk, i.e. the HDD of a local computer or Compact Disc.
- **Load Settings from PC** : Click **Browse** button to search for a previously saved backup file, and then click **Upload** button to upload the settings; the system will then be configured to the same settings as specified by the backup file.
- **Restore To Factory Default** : Click **Restore** button to load the factory default settings of WCB1000H5PX/ WCB1010H5PX, and then **Success Message** page appears. Click **Reboot** button to set default configuration.

4.3.2 Firmware Upgrade

To upgrade the system firmware, click **Browse** to search for the new firmware file, and then click **Upgrade** button to execute the upgrade process.

Firmware Upgrade

From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local haddisk.

Firmware Version: WCB-1000H5PX 1.0.1 Release Version

Firmware Date: 2009-06-11 02:26:54

Update Firmware:

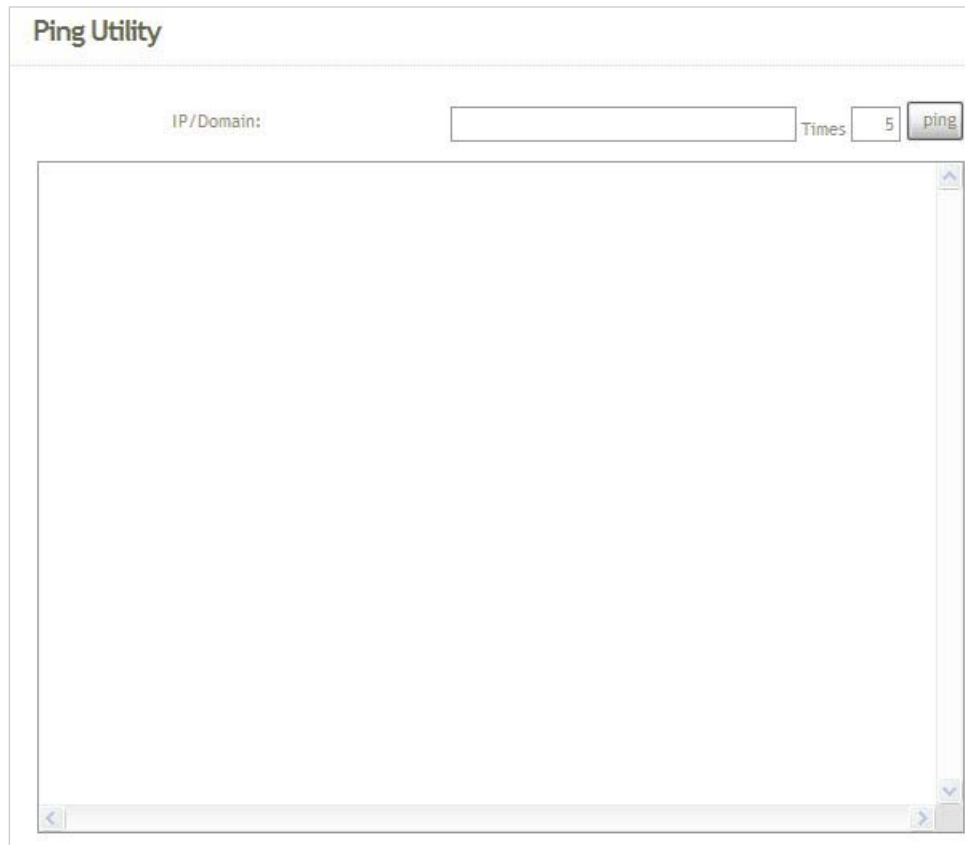
**Note :**

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

4.3.3 Ping Utility

The administrator can diagnose the network connectivity via this function. Please click on

Utilities -> Ping Utility and follow the below setting.



The screenshot shows a web-based utility window titled "Ping Utility". At the top, there is a label "IP/Domain:" followed by a text input field. To the right of this field is a "Times" label, a small input field containing the number "5", and a button labeled "ping". Below these controls is a large, empty rectangular area with a vertical scrollbar on the right side, intended for displaying the ping results.

- **IP/Domain** : Enter the desired domain name or IP address of the target device for diagnosis purpose, i.e. www.google.com, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
- **Time** : Enter the time for ping utility; default is 5, maximum is 50.

4.3.4 Reboot

This function allows the administrator to safely restart the TEW-455APBO. Click **Reboot** to restart the system immediately, and the whole process will take about three minutes to complete.



The Restart page as displayed below appears during the rebooting period. If turning off the power is necessary, please allow the restart process to be completed before turning off the system.



The **System Overview** page appears upon the completion of reboot.

4.4 Status

Information of the current system settings can be reviewed via this page; statuses of **Overview**, **Clients**, and **Event Log** are displayed in this interface.

The screenshot displays the 'Status' page of the TEW-455APBO web interface. The navigation bar at the top includes tabs for 'System', 'Wireless', 'Utilites', 'Status', and 'Reboot'. The main content area is titled 'System Overview' and is divided into two columns. The left column contains system information, and the right column contains status links.

System Overview	Status
System	Overview
System Name: WCB-1000H5PX	Client
Operating Mode: .BS Mode	Event Log
Fireware Version: WCB-1000H5PX 1.0.1 Release Version	
Fireware Date: 2009-06-11 02:26:54	
Location: default	
Description:	
System Time: 1970/01/01 Thu 01:39:16	
System Up Time: 01:39:16	
LAN Information	
MAC Address: 00:11:22:5a:5b:5c	
Mode: Static IP Mode	
IP Address: 192.168.2.254	

4.4.1 Overview

Detailed information on **System**, **LAN Information**, and **Wireless Information** can be reviewed via this page.

- **System** : Display the information of the system.

System
System Name: WCB-1000H5PX
Operating Mode: BS Mode
Firmware Version: WCB-1000H5PX 1.0.1 Release Version
Firmware Date: 2009-06-11 02:26:54
Location: default
Description:
System Time: 1970/01/01 Thu 01:39:16
System Up Time: 01:39:16

- **System Name** : The name of the system.
 - **Operating Mode** : The mode currently in service.
 - **Firmware Version** : The current firmware version installed.
 - **Firmware Date** : The build time of the firmware installed.
 - **Location** : The reminding note on the geographical location of the system. For more information, please refer to **Section 4.1.3-Management** .
 - **Description** : Please refer to **Section 4.1.3-Management** .
 - **System Time** : The current time of the system.
 - **System Up Time** : The time period that the system has been in service since last boot-up.
- **LAN Information** : Display the information of the LAN interface.

LAN Information
MAC Address: 00:11:22:5a:5b:5c
Mode: Static IP Mode
IP Address: 192.168.2.254
IP Netmask: 255.255.255.0
IP Gateway: 192.168.2.1
Primary DNS:
Secondary DNS:
Receive bytes: 2846
Receive packets: 39
Transmit bytes: 2028
Transmit packets: 14

- **MAC Address** : The MAC address of the LAN port.
 - **Mode** : The current mode of the LAN port.
 - **IP Address** : The IP address of the LAN port.
 - **IP Netmask** : The IP netmask of the LAN port.
 - **IP Gateway** : The gateway IP address of the LAN port.
 - **Primary DNS** : The current primary DNS server of the system.
 - **Secondary DNS** : The current secondary DNS server of the system.
 - **Receive bytes** :The current receive bytes of the LAN port.
 - **Receive packets** : The current receive packets of the LAN port.
 - **Transmit bytes** : The current transmit bytes of the LAN port.
 - **Transmit packets** : The current transmit packets of the LAN port.
- **Wireless Information** : Display the Virtual BS configuration information of the system.

Wireless Information				
VBS	ESSID	Status	Security Type	Clients
VBS 0	BS00	off	disabled	0
VBS 1	BS01	off	disabled	0
VBS 2	BS02	off	disabled	0
VBS 3	BS03	off	disabled	0
VBS 4	BS04	off	disabled	0
VBS 5	BS05	off	disabled	0
VBS 6	BS06	off	disabled	0
VBS 7	BS07	off	disabled	0

- **VBS** : Display number of system's Virtual BS.
- **ESSID** : Extended Service Set ID of the Virtual BS.
- **Status** : Display Virtual BS status currently.
- **Security Type** : Security type activated by the Virtual BS.
- **Clients** : Number of clients currently associated to the Virtual BS.

4.4.2 Client

The administrator can obtain detailed Information such as VBS, ESSID, MAC Address, RSSI, and Idle Time of all associated clients via this page.



The screenshot shows a web interface titled "System Overview". Below the title is a section labeled "Associated Client Status" which contains a table. The table has six columns: AP, ESSID, MAC ADDRESS, RSSI, Last TX time, and Disconnect. The table is currently empty, displaying the text "no clients!!" in the center.

AP	ESSID	MAC ADDRESS	RSSI	Last TX time	Disconnect
no clients!!					

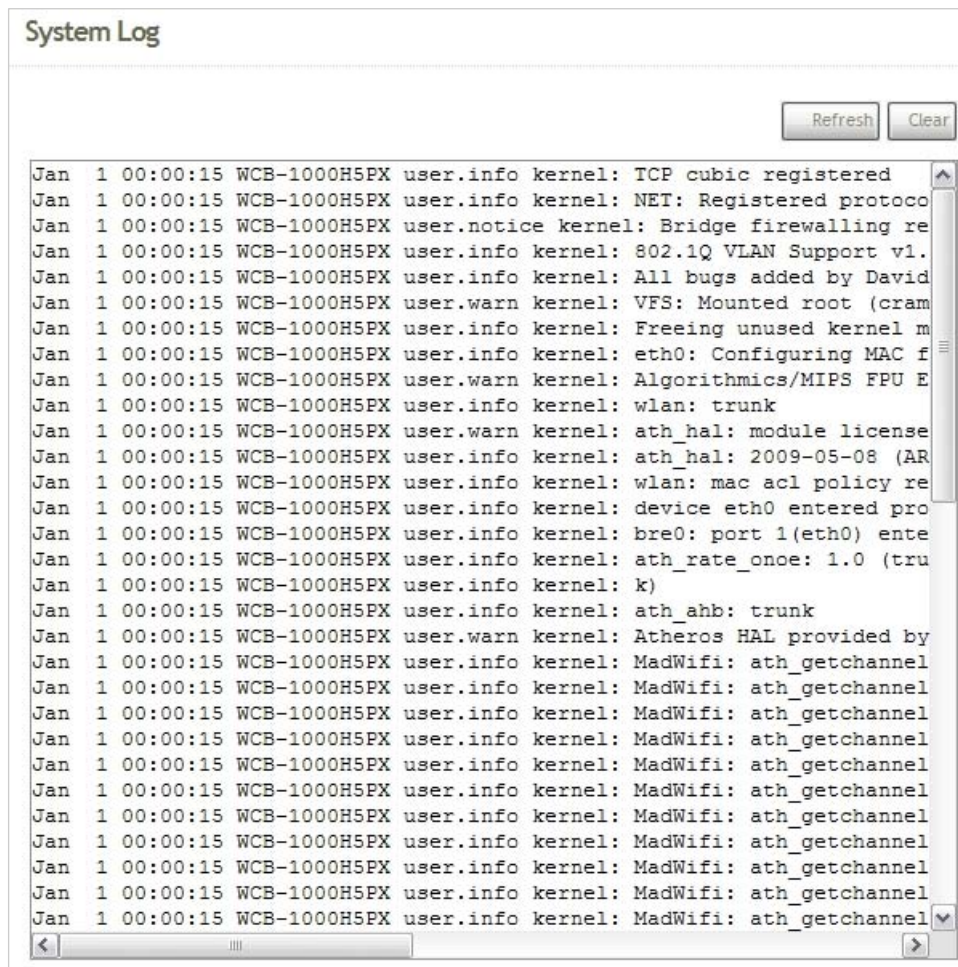
- **BS** : Virtual BS which the device is associated with.
- **ESSID** : ESSID which the device is associated with.
- **RSSI** : Indicate the RSSI of the respective client's association.
- **Idle Time** : Time period that the associated client is inactive (units in seconds).
- **Disconnect** : **Administrator** can kick out a specific client, click Kick button to disconnect specific client



Note : In Disconnect function of Associated Client Status, the client may be re-connect immediately. IF you want deny client associate system, please refer to **Section 4.3.2-Virtual BS ACL Configuration**.

4.4.3 Event Log

The reported system events can be reviewed here.



- **Date/ Time:** The date and time when the event occurred.
- **Hostname:** The name of the host which records the event. It helps the administrator identify the source of the reported events.
- **Process name (with square brackets):** Indicate the process with which the specific event is associated.
- **Description:** Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

Chapter 5. BRIDGE Mode Configuration

When BRIDGE mode is activated, the system can be configured as a repeater or client bridge. This section provides information in configuring the BRIDGE mode with graphical illustrations. TEW-455APBO provides functions as stated below where they can be configured via a user-friendly web based interface.

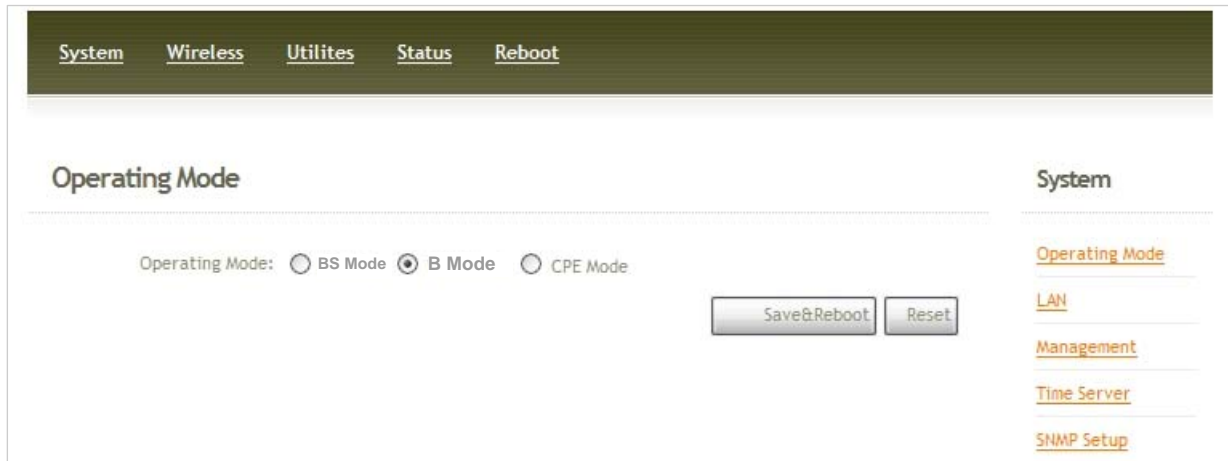
Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Settings	Profiles Settings	System Overview
	LAN	Advanced Settings	Firmware Upgrade	BRIDGE List
	Management	BRIDGE Setup	Ping Utility	Event Log
	Time Server		Reboot	
	SNMP			

Table 5-1: BRIDGE Mode Functions

Figure 5-1: BRIDGE Mode Main Page

5.1 System

This section provides information in configuring the following functions: **Operating Mode**, **LAN Setup**, **Management**, **Time Server**, **SNMP Setup**



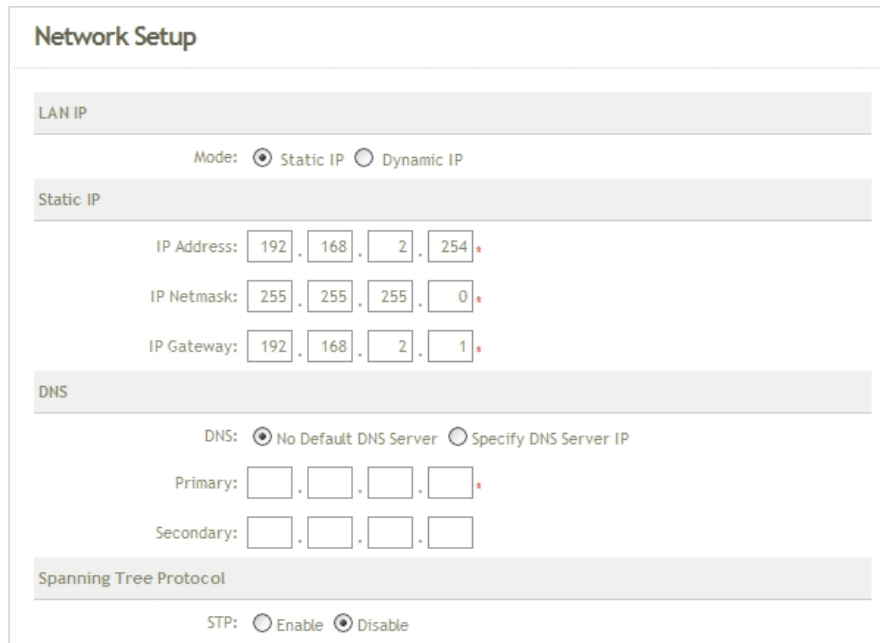
5.1.1 Operating Mode

TEW-455APBO supports three operation modes; BS mode, BRIDGE mode and CPE mode. The administrator can set the desired mode via this page, and then configure the system according to their deployment needs.

- ✓ **BS Mode** : Check **BS Mode** button to enable BS mode, and then click "**Save&Reboot**" to activate the setting.
- ✓ **BRIDGE Mode** : Check **B Mode** button to enable Bridge mode, and then click "**Save&Reboot**" to activate the setting.
- ✓ **CPE Mode** : Check **CPE Mode** button to enable CPE mode, and then click "**Save&Reboot**" to activate the setting.

5.1.2 LAN Setup

Here is instruction for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.



Network Setup

LAN IP

Mode: Static IP Dynamic IP

Static IP

IP Address: 192 . 168 . 2 . 254 *

IP Netmask: 255 . 255 . 255 . 0 *

IP Gateway: 192 . 168 . 2 . 1 *

DNS

DNS: No Default DNS Server Specify DNS Server IP

Primary: . . . *

Secondary: . . .

Spanning Tree Protocol

STP: Enable Disable

- **Mode** : Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
- ➔ **Static IP** : The administrator can manually setup the LAN IP address when static IP is available/ preferred.



Static IP

IP Address: 192 . 168 . 2 . 254 *

IP Netmask: 255 . 255 . 255 . 0 *

IP Gateway: 192 . 168 . 2 . 1 *

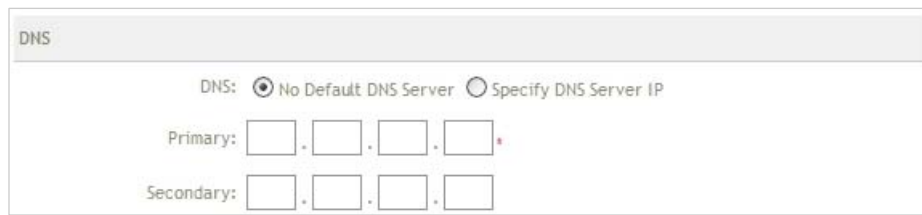
- ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
- ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1
- ➔ **Dynamic IP** : This configuration type is applicable when the WCB1000H5PX/ WCB1010H5PX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.



Dynamic IP

Hostname:

- ✓ **Hostname** : The Hostname of the LAN port
- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.



DNS

DNS: No Default DNS Server Specify DNS Server IP

Primary: . . . *

Secondary: . . .

- **Primary** : The IP address of the primary DNS server.
- **Secondary** : The IP address of the secondary DNS server.

■ **Spanning Tree Protocol**

The spanning tree network protocol provides a loop free topology for any bridged LAN. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



Spanning Tree Protocol

STP: Enable Disable

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.1.3 Management

The administrator can later obtain the geographical location of the system via the information configured here. The administrator also can change system password and configure system login methods. Please click **System -> Management** and follow the below settings.

■ System Information

- **System Name** : Enter a desired name or use the default provided.
- **Description** : Denote further information of the system.
- **Location** : Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.

- **Admin Password** : The admin manager can change its respected password. Enter the new password, and then verify the new password in the Check New Password filed. Click **Save** button to activate the new password.

- **New Password** : Please input the new password of administrator.
- **Check New Password** : Please input again the new password of administrator.

TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

- **Admin Login Methods** : The admin manager can enable or disable system login methods, it also can change services port. Click **Save** button to activate the admin login methods.

Admin Login Methods	
<input checked="" type="checkbox"/> Enable HTTP	Port : <input type="text" value="80"/> (Default:80)
<input checked="" type="checkbox"/> Enable Telnet	Port : <input type="text" value="23"/> (Default:23)

- **Enable HTTP** : Select Enable HTTP to activate HTTP Service
- **HTTP Port** : Please input 1 ~ 65535 value to set HTTP Port; default value is 80
- **Enable Telnet** : Select Enable HTTP to activate HTTP Service
- **Telnet Port** : Please input 1 ~ 65535 value to set HTTP Port; default value is 23

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.1.4 Time Server

System time can be configured via this page where manual setting and NTP server configuration are both supported. Please click on **System -> Time Server** and follow the below setting.

- **Local Time** : Display the current time of the system.
- **Setup Time Use NTP** : Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
 - **Default NTP Server** : Select the NTP Server from the drop-down list.
 - **Time Zone** : Please set a time zone from where the accurate time can be supplied, **(GMT+08:00) Taipei** for example.
 - **Daylight saving time** : Enable Daylight saving time from where the accurate time needed.
- **User Setup** : Enable User Setup and Click **Set Time** button; the system time can be configured manually.

- **Set Time** : Click Set Time button, the Time field should be changed automatically.
- **Set the time** : Select the appropriate **Year, Month, Day, Hour, Minute** and **Second** from the drop-down list.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.1.5 SNMP Setup

SNMP is an application-layer protocol that provides a message of format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely. Please click on **System -> SNMP Setup** and follow the below setting.

- **v2c** : Check v2c button to activate SNMP v2c agent or unchecked to deactivate this function.

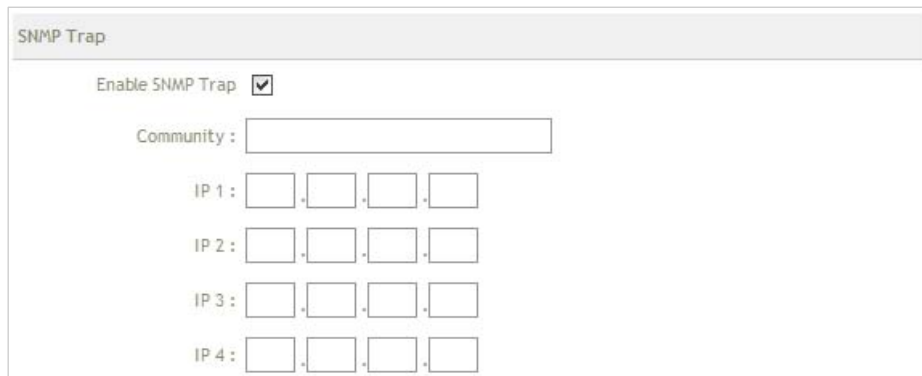
- **ro community** : Enter the community strings that allows read-only access to the system's SNMP information.
- **rw community** : Enter the community strings that allows read/write access to the system's SNMP information.

- **v3** : Check v3 button to activate SNMP v3 agent or unchecked to deactivate this function. SNMPv3 supports the highest available levels of security for SNMP communication.

- **SNMP ro user** : Enter the community strings that allows read-only access to the system's SNMP information.
- **SNMP ro password** : Enter the password that allows read-only access to the system's SNMP information.
- **SNMP rw user** : Enter the community strings that allows read/write access to the system's SNMP information.

information.

- **SNMP rw password** : Enter the password that allows read/write access to the system's SNMP information.
- **SNMP Trap** : Events on cold start, interface up & down, and association & disassociation can be reported via this function to an assigned server.



The image shows a web-based configuration interface for SNMP Traps. At the top, there is a header 'SNMP Trap'. Below it, there is a checkbox labeled 'Enable SNMP Trap' which is checked. Underneath, there is a text input field labeled 'Community :'. Below that, there are four rows of IP address input fields, each labeled 'IP 1 :', 'IP 2 :', 'IP 3 :', and 'IP 4 :'. Each IP field is represented by four small boxes separated by dots, indicating the octets of an IP address.

- **Community** : Enter the community strings required by the remote host computer that will receive trap messages or notices send by the system.
- **IP** : Enter the IP address of the remote host computer that will receive the trap messages.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.2 Wireless

The system manager can configure related wireless settings, **General Setup**, **Advanced Setup**, **BRIDGE Setup**.

The screenshot shows a web interface for configuring wireless settings. At the top, there is a navigation bar with tabs for [System](#), [Wireless](#), [Utilites](#), [Status](#), and [Reboot](#). The main content area is titled "Wireless Setup" and is divided into two columns. The left column contains the "General Setup" section, which includes the following fields:

- MAC address : 00:11:22:5a:5b:5d
- Band Mode: 802.11b+802.11g (dropdown menu)
- Transmit Rate Control : Auto (dropdown menu)
- Country : US (dropdown menu)
- Channel : 1 (dropdown menu)
- Tx Power : Level 9 (dropdown menu)

The right column is titled "Sub Menu" and contains three links: [General Setup](#), [Advanced Setup](#), and [Bridge Setup](#). At the bottom right of the configuration area, there are two buttons: "Save" and "Reset".

5.2.1 General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

The screenshot shows the 'Wireless Setup' configuration page. The 'General Setup' section is highlighted. The MAC address is 00:11:22:5a:5b:5d. The Band Mode is set to 802.11b+802.11g. The Transmit Rate Control is set to Auto. The Country is set to US. The Channel is set to 1. The Tx Power is set to Level 9. There are 'Save' and 'Reset' buttons at the bottom right.

- **MAC address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are 801.11b, 802.11g and 802.11b+802.11g.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from 1 to 54Mbps for 802.11g and 802.11b/g modes, or 1 to 11Mbps for 802.11b mode.



Note : Trying to Adjust **Transmit Rate Control** for long distance links, BRIDGE link may be get better throughput.

- **Country** : Select the desired country code from the drop-down list; the options are US, ETSI and Japan.
- **Channel** : The channel range will be changed by selecting different country code. The channel range from 1 to 11 for US country code, or 1 to 13 for ETSI country code, or 1 to 14 for Japan.
- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select the LEVEL 1 to LEVEL 9 you needed for your environment. If you are not sure of which setting to choose, then keep the default setting, LEVEL 9.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page is for BRIDGE's RF general settings and will be applied to all BRIDGE Links.

5.2.2 Advanced Setup

The administrator can change the Slot Time, ACK/CTS Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

Wireless Setup

Advanced Setup

Slot Time : (1 - 1489, default 20, slottime = 9 + |distance / 300|)

ACK Timeout : (1 - 372, default 48, acktimeout = slottime *2 +3)

CTS Timeout : (1 - 744, default 48)

RSSI Threshold : ((-128) - 127, default 24)

Beacon Interval : (10 - 5000, default 100)

DTIM Interval : (1 - 15, default 1)

Fragment Threshold : (256 - 2346, default 2346)

RTS Threshold : (1 - 2346, default 2346)

Short Preamble : Enable Disable

Tx Burst : Enable Disable

802.11g Protection Mode : Enable Disable

Sub Menu

[General Setup](#)

[Advanced Setup](#)

[Bridge Setup](#)

- **Slot Time** : Enter the desired slot time for the BRIDGE.
- **ACK Timeout** : The time interval for waiting the “ACKnowledgment frame”. If the ACK is not received within that timeout period then the packet will be re-transmitted. Higher ACK Timeout will decrease the packet lost, but the throughput will be growing worse.
- **CTS Timeout** : Enter the desired CTS timeout for the BRIDGE.



Note : Slot Time and ACK/CTS Timeout settings for long distance links. It is important to change the value to find the optimal setting. A value too low will give very low throughput, A high value may slowdown the link.

- **RSSI Threshold** : RSSI Threshold can be used to control the level of noise received by the device.
- **Beacon Interval** : Enter a value between 10 and 5000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the base station and the wireless network.
- **DTIM Interval** : Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will let the wireless client save energy more, but the throughput will be growing worse.

TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

- **Fragment Threshold** : The value specifies the maximum size of packet allowed before data is fragmented into multiple packets. Please use this value to tune the wireless connection if lots of retransmission happens. Enter a value ranging from 256 to 2346.
- **RTS Threshold** : Tuning the Request to Send, RTS threshold will help the system control its access to medium and alleviate the hidden node problem. Enter a value ranging from 1 to 2346.
- **Short Preamble** : The short preamble provides 56-bit Synchronization field to improve WLAN transmission efficiency. Check **Enable** button for using Short Preamble, and **Disable** for using the Long Preamble, 128-bit Synchronization field, option.
- **Tx Burst** : Click **Enable** button for using Tx Burst, and **Disable** for non using Tx Burst.
- **802.11g Protection Mode** : Click **Enable** button for using 802.11g Protection Mode, and Disable for non using 802.11g Protection Mode.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for BRIDGE's RF general settings and will be applied to all BRIDGE Links.

5.2.3 BRIDGE Setup

The administrator can create BRIDGE Links via this page. Please click on **Wireless -> BRIDGE Setup** and follow the below setting.

Wireless Setup

Bridge Setup

WMM : Enable Disable

Security Type :

Enable	Bridge Peer's MAC Address	VLAN ID (0 is not set.)	Description
<input type="checkbox"/>	01. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	02. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	03. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	04. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	05. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	06. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	07. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	08. <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>

Sub Menu

- [General Setup](#)
- [Advanced Setup](#)
- [Bridge Setup](#)

- **WMM** : Select Enable, the packets with QoS WMM will has higher priority.
- **Security Type** : Configure an appropriate security type for the BRIDGE link, either **Disabled** or **WEP**; the type needs to be the same as that configured on BRIDGE peer.

Security Type :

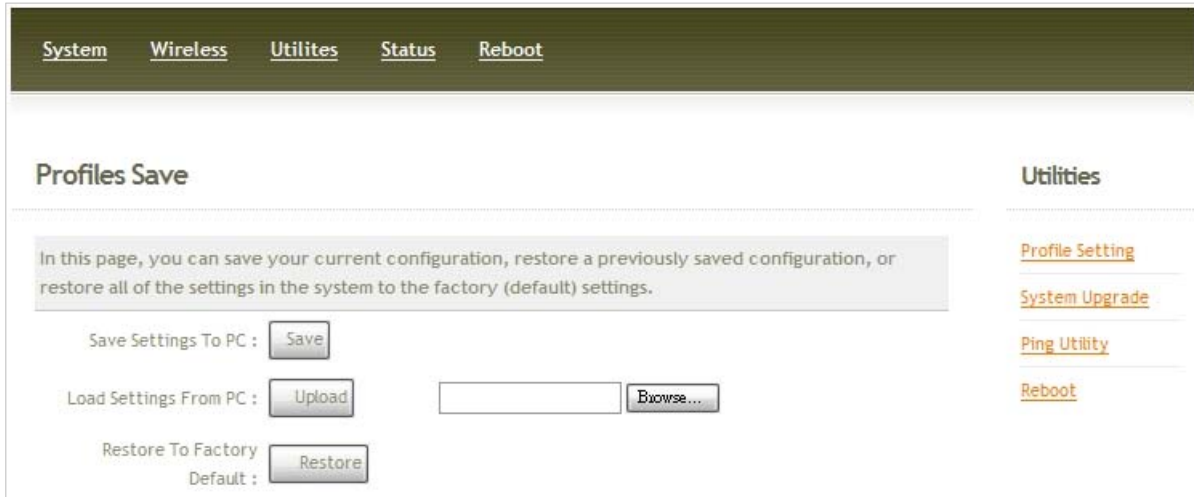
Key Length : Key : (10, 26 and 32 HEX characters)

- ✓ **Key Length** : Select the desire option are **64 bits**, **128 bits** or **152 bits** from drop-down list.
- ✓ **Key** : Provide the WEP key value. The key value should be HEX digits format.
- **Enable** : Click **Enable** button to create BRIDGE link.
- **BRIDGE Peer's MAC Address** : Enter the MAC address of BRIDGE peer.
- **VLAN ID** : Virtual LAN, the system supports tagged VLAN. To enable VLAN function; valid values are from 1 to 4094; 0 is disabled.
- **Description** : Description of BRIDGE link.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.3 Utilities

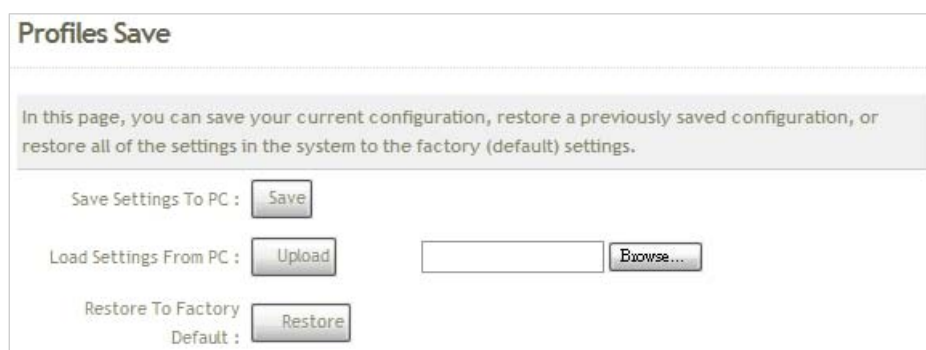
The administrator can maintain the system via this page: **Profile Setting**, **System Upgrade**, **Ping Utility**, and **Reboot**.



5.3.

1 Profile Setting

Current settings on the system can be backed up, or previous backed up settings can be restored as well as resetting the system back to factory default can be performed via this page. Please click on **Utilities -> Profile Setting** and follow the below setting.



- **Save Settings to PC** : Click **Save** button to save the current system settings to a local disk, i.e. the HDD of a local computer or Compact Disc.
- **Load Settings from PC** : Click **Browse** button to search for a previously saved backup file, and then click **Upload** button to upload the settings; the system will then be configured to the same settings as specified by the backup file.
- **Restore To Factory Default** : Click **Restore** button to load the factory default settings of WCB1000H5PX/ WCB1010H5PX, and then **Success Message** page appears. Click **Reboot** button to set default configuration.

5.3.2 Firmware Upgrade

To upgrade the system firmware, click **Browse** to search for the new firmware file, and then click **Upgrade** button to execute the upgrade process.

Firmware Upgrade

From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local haddisk.

Firmware Version: WCB-1000H5PX 1.0.1 Release Version

Firmware Date: 2009-06-11 02:26:54

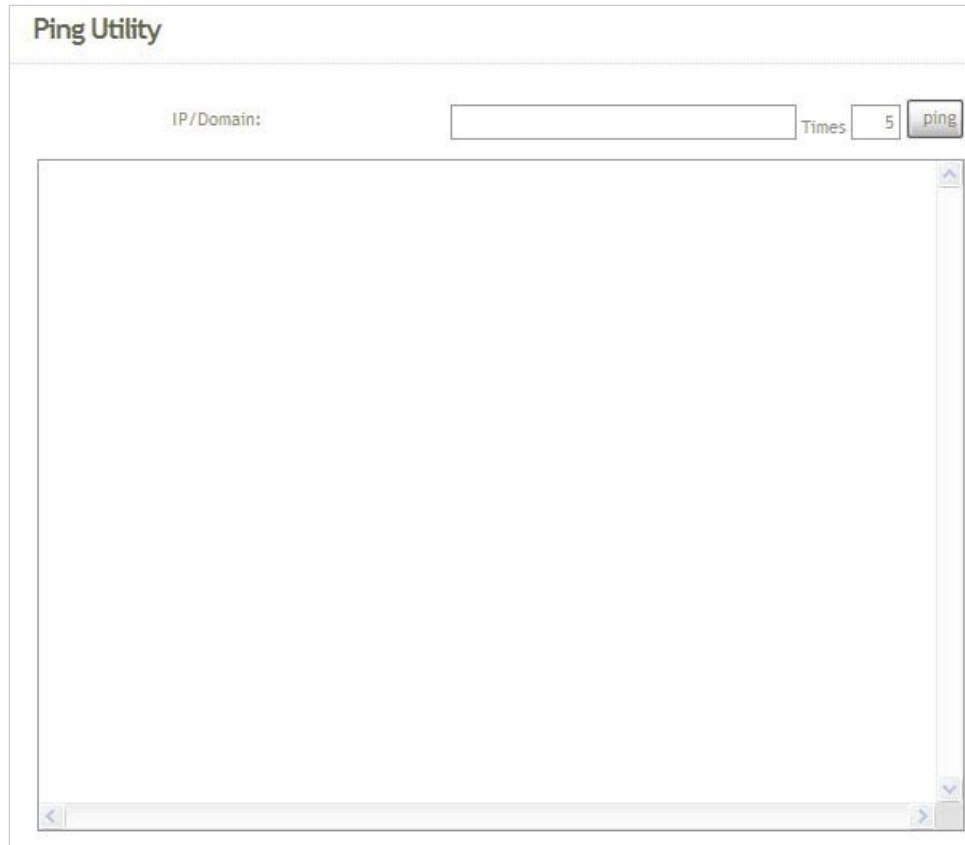
Update Firmware:

**Note :**

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

5.3.3 Ping Utility

The administrator can diagnose the network connectivity via this function.



The screenshot shows a web browser window titled "Ping Utility". At the top, there is a label "IP/Domain:" followed by an empty text input field. To the right of the input field is a "Times" label, a small input field containing the number "5", and a "ping" button. Below these elements is a large, empty rectangular area with a vertical scrollbar on the right and a horizontal scrollbar at the bottom, intended for displaying the results of the ping test.

- **IP/Domain** : Enter the desired domain name or IP address of the target device for diagnosis purpose, i.e. www.google.com, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
- **Time** : Enter the time for ping utility; default is 5, maximum is 50.

5.3.4 Reboot

This function allows the administrator to safely restart the TEW-455APBO. Click **Reboot** to restart the system immediately, and the whole process will take about three minutes to complete.



The Restart page as displayed below appears during the rebooting period. If turning off the power is necessary, please allow the restart process to be completed before turning off the system.



The **System Overview** page appears upon the completion of reboot.

5.4 Status

Information of current system settings can be over viewed via this page; statuses of **Overview**, **BRIDGE List**, and **Event Log** are displayed in this interface.

The screenshot displays the web interface for the TEW-455APBO. At the top, a dark green navigation bar contains the following menu items: [System](#), [Wireless](#), [Utilites](#), [Status](#), and [Reboot](#). The main content area is split into two columns. The left column is titled "System Overview" and contains two sections: "System" and "LAN Information". The "System" section lists the following details: System Name: WCB-1000H5PX, Operating Mode: B mode, Firmware Version: WCB-1000H5PX 1.0.0 Release Version, Firmware Date: 2009-06-17 02:19:42, Location: default, Description: (empty), System Time: 1970/01/01 Thu 00:51:47, and System Up Time: 51:47. The "LAN Information" section lists: MAC Address: 00:11:22:5a:5b:5c, Mode: Static IP Mode, and IP Address: 192.168.2.254. The right column is titled "Status" and contains three links: [Overview](#), [WDS List](#), and [Event Log](#).

5.4.1 Overview

Detailed information on **System** and **LAN Information** can be reviewed via this page.

- **System** : Display the information of the system.

System
System Name: WCB-1000H5PX
Operating Mode: B mode
Firmware Version: WCB-1000H5PX 1.0.0 Release Version
Firmware Date: 2009-06-17 02:19:42
Location: default
Description:
System Time: 1970/01/01 Thu 00:51:47
System Up Time: 51:47

- **System Name** : The name of the system.
 - **Operating Mode** : The mode currently in service.
 - **Firmware Version** : The current firmware version installed.
 - **Firmware Date** : The build time of the firmware installed.
 - **Location** : The reminding note on the geographical location of the system. For more information, please refer to **Section 4.1.3-Management** .
 - **Description** : Please refer to **Section 4.1.3-Management** .
 - **System Time** : The current time of the system.
 - **System Up Time** : The time period that the system has been in service since last boot-up.
- **LAN Information** : Display the information of the LAN interface.

LAN Information
MAC Address: 00:11:22:5a:5b:5c
Mode: Static IP Mode
IP Address: 192.168.2.254
IP Netmask: 255.255.255.0
IP Gateway: 192.168.2.1
Primary DNS:
Secondary DNS:
Receive bytes: 2846
Receive packets: 39
Transmit bytes: 2028
Transmit packets: 14

- **MAC Address** : The MAC address of the LAN port.
- **Mode** : The current mode of the LAN port.
- **IP Address** : The IP address of the LAN port.
- **IP Netmask** : The IP netmask of the LAN port.
- **IP Gateway** : The gateway IP address of the LAN port.
- **Primary DNS** : The current primary DNS server of the system.
- **Secondary DNS** : The current secondary DNS server of the system.
- **Receive bytes** :The current receive bytes of the LAN port.
- **Receive packets** : The current receive packets of the LAN port.
- **Transmit bytes** : The current transmit bytes of the LAN port.
- **Transmit packets** : The current transmit packets of the LAN port.

5.4.2 BRIDGE List

The administrator can obtain detailed Information such as BRIDGE, Status, MAC Address, RSSI, and Last Tx Time of all BRIDGE link via this page.

Bridge Link Status				
Bridge Link Status				
WDS	Status	MAC Address	RSSI	Last TX Time
WDS1	off	(null)	0	0
WDS2	off	(null)	0	0
WDS3	off	(null)	0	0
WDS4	off	(null)	0	0
WDS5	off	(null)	0	0
WDS6	off	(null)	0	0
WDS7	off	(null)	0	0
WDS8	off	(null)	0	0

- **BRIDGE** : BRIDGE which the device is linked with.
- **Status** : Display BRIDGE status.
- **MAC address** : Display MAC address of BRIDGE peer.
- **RSSI** : Indicate the RSSI of the respective BRIDGE linked.
- **Last TX time** : Indicate the last receive packet of the respective BRIDGE linked.

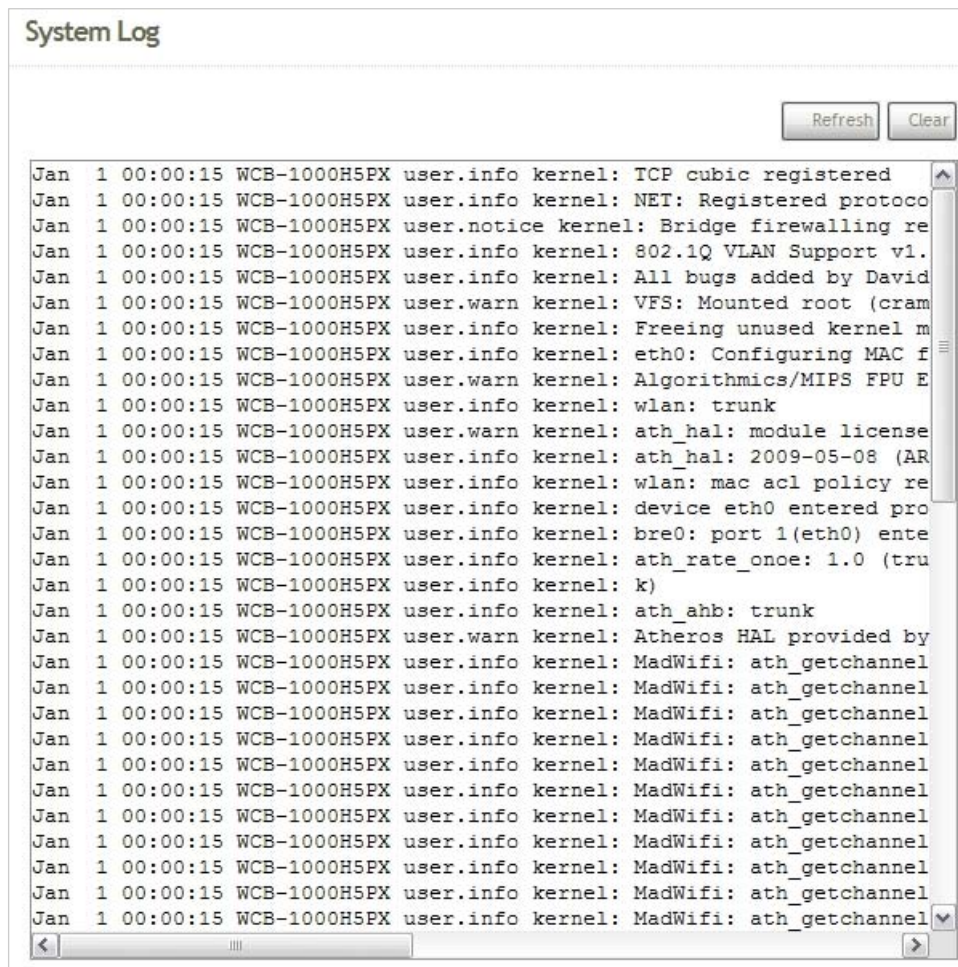


Note :

If RSSI display 0, you need check BRIDGE configuration. Verify **MAC Address, Channel** and **Security type** is the same; also adjust system's antenna angle. When BRIDGE link used on long distance, you need to adjust **Transmit Rate Control, Slot Time** and **ACK/CTS Timeout**.

5.4.3 Event Log

The reported system events can be reviewed here.



- **Date/ Time:** The date and time when the event occurred.
- **Hostname:** The name of the host which records the event. It helps the administrator identify the source of the reported events.
- **Process name (with square brackets):** Indicate the process with which the specific event is associated.
- **Description:** Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

Chapter 6. CPE Mode Configuration

When CPE mode is activated, the system can be configured as a CPE. This section provides information in configuring the CPE mode with graphical illustrations. TEW-455APBO provides functions as stated below where they can be configured via a user-friendly web based interface.

OPTION	System	Wireless	Firewall	NAT	Utilities	Status
Functions	Operating Mode	General Settings	IP Rule Setup	Virtual Server	Profiles Settings	System Overview
	WAN	Advanced Settings	MAC Rule Setup	DMZ	Firmware Upgrade	DHCP Clients
	LAN	Site Survey			Ping Utility	Event Log
	Management				Reboot	
	Time Server					
	SNMP					

Table 6-1: CPE Mode Functions

The screenshot displays the CPE Mode Main Page. At the top, there is a navigation menu with the following items: [System](#), [Wireless](#), [Firewall](#), [NAT](#), [Utilities](#), [Status](#), and [Reboot](#). The main content is split into two columns. The left column, titled "System Overview", contains the following information:

- System** (Section Header)
- System Name: WCB-1000H5PX
- Operating Mode: CPE mode
- Firmware Version: WCB-1000H5PX 1.0.0 Release Version
- Firmware Date: 2009-06-17 02:19:42
- Location: default
- Description:
- System Time: 1970/01/01 Thu 00:00:43
- System Up Time: 43
- WAN Information** (Section Header)
- Mode: Static IP
- MAC Address: 00:11:22:5a:5b:5d
- IP Address: 192.168.1.254

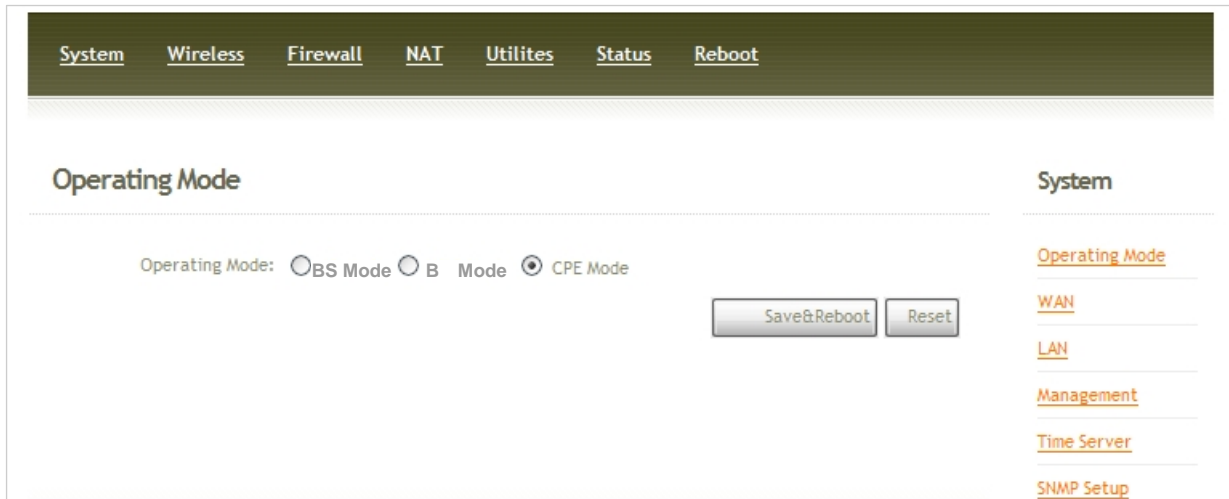
The right column, titled "Status", contains the following links:

- [Overview](#)
- [DHCPD Clients](#)
- [Event Log](#)

Figure 6-1: CPE Mode Main Page

6.1 System

This section provides information in configuring the following functions: **Operating Mode**, **WAN Setup**, **LAN Setup**, **Management**, **Time Server**, **SNMP Setup**



6.1.1 Operating Mode

TEW-455APBO supports three operation modes; BS mode , BRIDGE mode and CPE mode. The administrator can set the desired mode via this page, and then configure the system according to their deployment needs.

- ✓ **BS Mode** : Check **BS Mode** button to enable BS mode, and then click "**Save&Reboot**" to activate the setting.
- ✓ **BRIDGE Mode** : Check **B Mode** button to enable Bridge mode, and then click "**Save&Reboot**" to activate the setting.
- ✓ **CPE Mode** : Check **CPE Mode** button to enable CPE mode, and then click "**Save&Reboot**" to activate the setting.

6.1.2 WAN Setup

Here is instruction for how to setup the WAN. Please click on **System -> WAN** and follow the below setting.

The screenshot displays the WAN Setup configuration page. At the top, there are navigation tabs: System, Wireless, Firewall, NAT, Utilities, Status, and Reboot. The main heading is "WAN Setup". Below it, the "Internet Connection Type" section has three radio buttons: "Static IP" (selected), "Dynamic IP", and "PPPoE". Under "Static IP", there are three options for MAC Address: "Keep Default MAC Address" (selected), "Clone MAC Address: 00:1a:92:9f:a4:9b", and "Manual MAC Address" with input fields. The "Static IP" section includes a note: "Choose this option to set static IP informatin provided to you by your ISP." Below this, there are input fields for "IP Address" (192, 168, 1, 254), "IP Netmask" (255, 255, 255, 0), and "IP Gateway" (192, 168, 1, 1). The "DNS" section has two radio buttons: "No Default DNS Server" (selected) and "Specify DNS Server IP". Below are input fields for "Primary" and "Secondary" DNS servers. At the bottom right, there are "Save" and "Reset" buttons.

- **Mode** : Check "Static IP", "Dynamic IP" and "PPPoE" button as desired to set up the system IP of WAN port.
- ➔ **Static IP** : The administrator can manually setup the WAN IP address when static IP is available/ preferred.

This is a close-up of the "Static IP" configuration section. It features a grey header "Static IP" and a light grey box containing the instruction: "Choose this option to set static IP informatin provided to you by your ISP." Below this, there are three rows of input fields: "IP Address" with values 192, 168, 1, 254; "IP Netmask" with values 255, 255, 255, 0; and "IP Gateway" with values 192, 168, 1, 1.

- ✓ **IP Address** : The IP address of the WAN port; default IP address is 192.168.1.254
- ✓ **IP Netmask** : The Subnet mask of the WAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway** : The default gateway of the WAN port; default Gateway is 192.168.1.1

- **Dynamic IP** : This configuration type is applicable when the WCB1000H5PX/ WCB1010H5PX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically. If the IP Address do not assigned from DHCP server, the system need manual connect to DHCP server. Please refer to Section **6.6.2-Overview (WAN Information)**

Dynamic IP

Hostname:

- ✓ **Hostname** : The Hostname of the WAN port

- **PPPoE** : This configuration type is applicable when the WCB1000H5PX/ WCB1010H5PX is connected to a network with the presence of a PPPoE server.

PPPoE

Choose this opeiotn if your ISP uses PPPoE.(From most DSL users)

User name:

Password:

MTU: (576~1492)

Idle Time: (0~60 minutes)

Auto Reconnect:

- ✓ **User Name** : Enter User Name for PPPoE connection
- ✓ **Password** : Enter Password for PPPoE connection
- ✓ **MTU** : MTU stands for Maximum Transmission Unit. For PPPoE connections, you may need to set the MTU setting in order to work correctly with your ISP. Default is 1492 bytes.
- ✓ **Idle Time** : The time of inactivity before disconnecting your PPPoE session. Enter an Idle Time (in minutes) to define a maximum period of time for which the Internet connect is maintained during inactivity. If the connection is inactive for longer than the defined Idle Time, then the connection will be dropped.
- ✓ **Auto Reconnect** : Click Auto Reconnect button, the system will be auto reconnect with PPPoE server through WAN port. If unclick this button, the system need manual connect to PPPoE server. Please refer to Section **6.6.2-Overview (WAN Information)**

- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.

- **Primary** : The IP address of the primary DNS server.
- **Secondary** : The IP address of the secondary DNS server.

- **Bandwidth** : The administrator can control download and upload of bandwidth.

- **Upload** : Enter 256 to 8192 digital number, the unit is Kbits
- **Download** : Enter 256 to 8192 digital number, the unit is Kbits

- **MAC Address Clone** : The MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. Some ISPs require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the system using the MAC Address Clone feature.

- **Keep Default MAC Address** : Keep the default MAC address of WAN port on the system.
- **Clone MAC Address** : If you want to clone the MAC address of the PC you are currently using go configure the system, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.



Note : The Clone MAC Address field will display MAC address of the PC you are connected with the system currently.

→ **Manual Address** : Enter the MAC address registered with your ISP.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.1.3 LAN Setup

Here is instruction for how to setup the local IP Address and Netmask. Please click on

System -> LAN and follow the below setting.

LAN Setup

LAN IP

IP Address: 192 . 168 . 2 . 254 *

IP Netmask: 255 . 255 . 255 . 0 *

DHCP Setup

DHCP: Enable Disable

Start IP: 192 . 168 . 2 . 10 *

End IP: 192 . 168 . 2 . 30 *

DNS1 IP: . . . *

DNS2 IP: . . .

WINS IP: . . .

Domain:

Spanning Tree Protocol

STP: Enable Disable

- **LAN IP** : The administrator can manually setup the LAN IP address.
 - ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
 - ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0

- **DHCP Setup** : Devices connected to the system can obtain an IP address automatically when this service is enabled.

DHCP Setup

DHCP: Enable Disable

Start IP: 192 . 168 . 2 . 10 *

End IP: 192 . 168 . 2 . 30 *

DNS1 IP: . . . *

DNS2 IP: . . .

WINS IP: . . .

Domain:

- **DHCP** : Check **Enable** button to activate this function or **Disable** to deactivate this service.
- **Start IP / End IP**: Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients.
- **DNS1 IP** : Enter IP address of the first DNS server; this field is required.
- **DNS2 IP** : Enter IP address of the second DNS server; this is optional.
- **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain** : Enter the domain name for this network.

■ **Spanning Tree Protocol**

The spanning tree network protocol provides a loop free topology for any bridged LAN. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



Spanning Tree Protocol

STP: Enable Disable

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.1.4 Management

The administrator can later obtain the geographical location of the system via the information configured here. The administrator also can change system password and configure system login methods. Please click **System -> Management** and follow the below settings.

The screenshot shows the 'Admin Configuration' page with a sidebar on the right labeled 'System'. The sidebar contains links for 'Operating Mode', 'WAN', 'LAN', 'Management', 'Time Server', and 'SNMP Setup'. The main content area is divided into three sections:

- System Information:** Contains three input fields: 'System Name' (with value 'WCB-1000H5PX'), 'Description', and 'Location' (with value 'default').
- Admin Password:** Contains two input fields: 'New Password:' and 'Check New Password:'. A note next to the 'New Password' field says '(If you don't want to change , don't type anything)'. There is also a 'Save' button.
- Admin Login Methods:** Contains two checked checkboxes: 'Enable HTTP' and 'Enable Telnet'. Next to each is a 'Port' field with a value and a default value in parentheses: '80 (Default:80)' for HTTP and '23 (Default:23)' for Telnet.

■ System Information

- **System Name :** Enter a desired name or use the default provided.
- **Description :** Denote further information of the system.
- **Location :** Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.

- **Admin Password :** The admin manager can change its respected password. Enter the new password, and then verify the new password in the Check New Password filed. Click **Save** button to activate the new password.

This is a close-up of the 'Admin Password' section from the screenshot above. It shows two input fields: 'New Password:' and 'Check New Password:'. A note next to the 'New Password' field says '(If you don't want to change , don't type anything)'. There is also a 'Save' button.

- **New Password :** Please input the new password of administrator.
- **Check New Password :** Please input again the new password of administrator.

TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

- **Admin Login Methods** : The admin manager can enable or disable system login methods, it also can change services port. Click **Save** button to activate the admin login methods.

Admin Login Methods	
<input checked="" type="checkbox"/> Enable HTTP	Port : <input type="text" value="80"/> (Default:80)
<input checked="" type="checkbox"/> Enable Telnet	Port : <input type="text" value="23"/> (Default:23)

- **Enable HTTP** : Select Enable HTTP to activate HTTP Service
- **HTTP Port** : Please input 1 ~ 65535 value to set HTTP Port; default value is 80
- **Enable Telnet** : Select Enable HTTP to activate HTTP Service
- **Telnet Port** : Please input 1 ~ 65535 value to set HTTP Port; default value is 23

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.1.5 Time Server

System time can be configured via this page where manual setting and NTP server configuration are both supported.

- **Local Time** : Display the current time of the system.
- **Setup Time Use NTP** : Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
 - **Default NTP Server** : Select the NTP Server from the drop-down list.
 - **Time Zone** : Please set a time zone from where the accurate time can be supplied, **(GMT+08:00) Taipei** for example.
 - **Daylight saving time** : Enable Daylight saving time from where the accurate time needed.
- **User Setup** : Enable User Setup and Click **Set Time** button; the system time can be configured manually.

- **Set Time** : Click Set Time button, the Time field should be changed automatically.
- **Set the time** : Select the appropriate **Year, Month, Day, Hour, Minute** and **Second** from the drop-down list.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.1.6 SNMP Setup

SNMP is an application-layer protocol that provides a message of format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

button to activate SNMP v2c agent or unchecked to deactivate this function.

→ **ro community** : Enter the community strings that allows read-only access to the system's SNMP information.

→ **rw community** : Enter the community strings that allows read/write access to the system's SNMP information.

- **v3** : Check v3 button to activate SNMP v3 agent or unchecked to deactivate this function. SNMPv3 supports the highest available levels of security for SNMP communication.

→ **SNMP ro user** : Enter the community strings that allows read-only access to the system's SNMP

information.

- **SNMP ro password** : Enter the password that allows read-only access to the system's SNMP information.
 - **SNMP rw user** : Enter the community strings that allows read/write access to the system's SNMP information.
 - **SNMP rw password** : Enter the password that allows read/write access to the system's SNMP information.
- **SNMP Trap** : Events on cold start, interface up & down, and association & disassociation can be reported via this function to an assigned server.



The image shows a web-based configuration interface for SNMP Traps. At the top, there is a header 'SNMP Trap'. Below it, there is a checkbox labeled 'Enable SNMP Trap' which is checked. Underneath, there is a text input field labeled 'Community :'. Below the community field, there are four rows of IP address input fields, labeled 'IP 1 :', 'IP 2 :', 'IP 3 :', and 'IP 4 :'. Each IP field is a four-digit box with a dot separator between digits.

- **Community** : Enter the community strings required by the remote host computer that will receive trap messages or notices send by the system.
- **IP** : Enter the IP address of the remote host computer that will receive the trap messages.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.2 Wireless

This section will guide users through wireless setting for TEW-455APBO to associate with its up link BS.

The screenshot displays the 'Wireless Configuration' page of the TEW-455APBO web interface. At the top, a navigation bar includes links for System, Wireless, Firewall, NAT, Utilites, Status, and Reboot. The main heading is 'Wireless Configuration'. Below this, a 'General Setup' section contains the following configuration options:

- ESSID: default
- Band Mode: 802.11b+802.11g
- Transmit Rate Control: Auto
- Country: US
- Channel: Auto
- Tx Power: Level 9
- Security Type: Disabled

At the bottom right of the configuration area are 'Save' and 'Reset' buttons. On the right side of the page, a 'Wireless' sidebar contains links for 'General Setup', 'Advanced Setup', and 'Site Survey'.

6.2.1 General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

- **ESSID** : Assign Service Set ID for the wireless system.
- **Band Mode** : Select an appropriate wireless band; bands available are 801.11b, 802.11g and 802.11b+802.11g.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from 1 to 54Mbps for 802.11g and 802.11b/g modes, or 1 to 11Mbps for 802.11b mode.
- **Country** : Select the desired country code from the drop-down list; the options are US, ETSI and Japan.
- **Channel** : The channel range will be changed by selecting different country code. The channel range from 1 to 11 for US country code, or 1 to 13 for ETSI country code, or 1 to 14 for Japan.
- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select the LEVEL 1 to LEVEL 9 you needed for your environment. If you are not sure of which setting to choose, then keep the default setting, LEVEL 9.
- **Security Type** : Select the desired security type from the drop-down list; the options are WEP, WPA-PSK and WPA2-PSK.
 - **Disable** : Data are unencrypted during transmission when this option is selected.
 - **WEP** : WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bits , 128-bits or 152-bits shared key algorithm. Select **WEP** as the security type from drop-down list as desired. The WEP key configured here must be exactly the same as the key on the base station that this system is associated with.

- ✓ **Key Length** : Select the desire option are **64 bits**, **128 bits** or **152 bits** from drop-down list.
- ✓ **WEP auth Method** : Enable the desire option among **Open system** or **Shared**.
- ✓ **WEP Key #** : Select key index is used to designate the WEP key during data transmission. Enter HEX format WEP key value; the system support up to 4 sets of WEP keys.

→ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2)Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

- ✓ **Cipher Suite** : Check on the respected button to enable either AES or TKIP cipher suites; default is TKIP.
- ✓ **Key Type** : Check on the respected button to enable either ASCII or HEX format for the Pre-shared Key.
- ✓ **Pre-shared Key** : Enter the information for pre-shared key; the format of the information shall according to the key type selected.



Note : Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes.

6.2.2 Advanced Setup

The administrator can change the Slot Time, ACK/CTS Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

The screenshot displays the 'Wireless Setup' interface. The 'Advanced Setup' section is active, showing the following configurations:

- Slot Time: 20 (range 1 - 1489, default 20, slottime = 9 + |distance / 300|)
- ACK Time: 48 (range 1 - 372, default 48, acktimeout = slottime * 2 + 3)
- CTS Timeout: 48 (range 1 - 744, default 48)
- Fragment Threshold: 2346 (range 256 - 2346, default 2346)
- RTS Threshold: 2346 (range 1 - 2346, default 2346)
- Short Preamble: Enable Disable
- Tx Burst: Enable Disable
- WMM: Enable Disable

The right sidebar shows the 'Wireless' menu with links for [General Setup](#), [Advanced Setup](#), and [Site Survey](#).

- **Slot Time** : Enter the desired slot time for the BRIDGE.
- **ACK Timeout** : The time interval for waiting the “ ACKnowledgment frame”. If the ACK is not received within that timeout period then the packet will be re-transmitted. Higher ACK Timeout will decrease the packet lost, but the throughput will be growing worse.
- **CTS Timeout** : Enter the desired CTS timeout for the BRIDGE.
- **Fragment Threshold** : The value specifies the maximum size of packet allowed before data is fragmented into multiple packets. Please use this value to tune the wireless connection if lots of retransmission happens. Enter a value ranging from 256 to 2346.
- **RTS Threshold** : Tuning the Request to Send, RTS threshold will help the system control its access to medium and alleviate the hidden node problem. Enter a value ranging from 1 to 2346.
- **Short Preamble** : The short preamble provides 56-bit Synchronization field to improve WLAN transmission efficiency. Check **Enable** button for using Short Preamble, and **Disable** for using the Long Preamble, 128-bit Synchronization field, option.
- **Tx Burst** : Click **Enable** button for using Tx Burst, and **Disable** for non using Tx Burst.
- **WMM** : Select Enable, the packets with QoS WMM will has higher priority.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes.

6.2.3 Site Survey

Base station located around the system can be found via the scan function. The administrator can then select a desired BS to be associated with via this page. Please click on

Wireless -> Site Survey.

CPE Site Survey

Scan Result					
ESSID	MAC Address	Channel	Signal Level	Security	Setup
AP00	00:11:A3:07:01:07	1	-71 dBm	WEP	<input type="button" value="SETUP"/>
AP51_2	0A:0D:0B:13:6B:18	4	-72 dBm	WEP	<input type="button" value="SETUP"/>
AP51_3	0E:0D:0B:13:6B:18	4	-71 dBm	WPA-PSK2(TKIP)	<input type="button" value="SETUP"/>
AP51_1	06:0D:0B:13:6B:18	4	-71 dBm	WEP	<input type="button" value="SETUP"/>
AP01	06:11:A3:07:01:07	1	-72 dBm	WEP	<input type="button" value="SETUP"/>
AP02	0A:11:A3:07:01:07	1	-72 dBm	None	<input type="button" value="SETUP"/>
AP51_0	00:0D:0B:13:6B:18	4	-70 dBm	WPA-PSK(TKIP)	<input type="button" value="SETUP"/>
HomeIP	00:0E:2E:4A:24:40	6	-93 dBm	WPA-PSK(TKIP)	<input type="button" value="SETUP"/>

Wireless

- [General Setup](#)
- [Advanced Setup](#)
- [Site Survey](#)

-
- **SSID** : Service Set ID of the BS or repeater found around the system.
- **MAC Address** : MAC address of the respected BS.
- **Channel** : The channel number currently used by the respective BS.
- **Signal** : The signal strength of the respected BS.
- **Security** : Security type enabled by the respected BS.
- **Setup** : Click Setup to configure settings for associating with the respected BS.

6.3 Firewall

Current firewall functions supported are IP filter and MAC filter. The system's firewall enhances the security of your network, you can also enable a variety of filters to further protect your network.

The screenshot displays the Firewall configuration interface. At the top, a navigation bar includes links for System, Wireless, Firewall, NAT, Utilities, Status, and Reboot. The main content area is divided into two sections: IP Rule Configuration and Firewall.

IP Rule Configuration

IP Rules

Source Address/Mask :

Source Port : (min:1, max:65535 or Range xxxxx:xxxxx)

Destination Address/Mask :

Destination Port : (min:1, max:65535 or Range xxxxx:xxxxx)

In/Out : In Out

Protocol : TCP UDP ICMP

Listen : Yes No

Action : Deny Pass

Side : LAN WAN Both

No IP RULE list data

Firewall

[IP Rule Setup](#)

[MAC Rule Setup](#)

6.3.1 IP Rule Setup

The administrator can setting IP Filter via this page, Please click on **Firewall -> IP Rule Setup** and follow the below setting.

- **Source Address/Mask** : Enter the desired source IP address and netmask; the mask must be a plain number, i.e. 192.168.2.10/32
- **Source Port** : The source port(s) required for this rule. A single port may be given, or a range may be given as **start:end** , which will match all ports from *start* to *end*, inclusive.
- **Destination Address/Mask** : Enter the desired destination IP address and netmask; the mask must be a plain number, i.e. 192.168.1.10/32
- **Destination Port** : The destination port(s) required for this rule. A single port may be given, or a range may be given as **start:end** , which will match all ports from *start* to *end*, inclusive.
- **In/Out** : This option used for specialized packet alteration. The system support In (INPUT : for packets coming into the interface itself) or Out (FORWARD : for altering packets being routed through the interface)
- **Protocol** : This option allows you to select protocol type. The system support TCP, UDP or ICMP.
- **Listen** : Enable **Yes** to match TCP packets only with the SYN flag.
- **Active** : Enter **Deny** to DROP specialized packet; **Pass** to ACCET the specialized packet
- **Side** : Select specified interface via which a packet was received.

- **Save** : Click **Save** button to activate the new creation.

- **Reset** : Click **Reset** button to clear configuration field.

There are 20 rules maximum allowed in this list.

#	Source		Destination		In/Out	Protocol	Listen	Action	Side	Del	Edit
	Address/Mask	Port	Address/Mask	Port							
1	192.168.1.10/32	22	192.168.1.254/32	22	in	tcp	n	deny	wan	Del	Edit

-
- **Del** : Click **Del** to remove desired rule.
- **Edit** : Click **Edit** to edit desired rule.

Click **Reboot** button to activate your changes.

6.3.2 MAC Rule Setup

The administrator can setting MAC Filter via this page, Please click on **Firewall -> MAC Rule Setup** and follow the below setting.

The screenshot shows the 'Firewall Configuration' interface. Under the 'MAC Rules' section, there is a label 'Action:' followed by a dropdown menu currently showing 'Disabled' and a 'save' button. Below this is the 'Add Mac' section with a 'MAC address' input field and an 'Add' button. At the bottom of the configuration area, it says 'No MAC RULE list data'.

- **Action** : Select the desired access control rule from the drop-down list; the options are Disable, Deny All and Allow All.
- **MAC Address** : Enter MAC address in this field. There are 20 rules maximum allowed in this MAC address list.
- **Add** : Click **Add** button to activate the new creation.

Rules	MAC	DEL	Rules	MAC	DEL
1.	00:0b:6b:00:aa:ba	<input type="button" value="DEL"/>	2.	00:0b:6b:00:aa:bb	<input type="button" value="DEL"/>

-
- **DEL** : Click **DEL** button to remove the rule.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes.

6.4 NAT

Current NAT functions supported are IP/ Port forwarding and DMZ, Demilitarized Zone. The administrator can open a certain area in the network to the Internet for limited and controlled access for special purpose such as gaming server or conferencing center.

[System](#)
[Wireless](#)
[Firewall](#)
[NAT](#)
[Utilites](#)
[Status](#)
[Reboot](#)

Virtual Server Configuration

Virtual Server is used to allow Internet users to access LAN services

Virtual Server : Enable Disable

Description :

Private IP : . . .

Protocal Type : TCP UDP

Private Port : (min:1, max:65535 or Range xxxxxx:xxxxx)

Public Port : ((min:1, max:65535 or Range xxxxxx:xxxxx)

NAT

[Virtual Server](#)

[DMZ](#)

Virtual Server Rule List

Status	Description	Protocol	Private IP	Pubbic Port	Local Port	Del	Edit
No Rule!							

6.4.1 Virtual Server (IP/ Port Forwarding)

A certain area in the network can be exposed to the Internet in a limited and controlled way for on-line game or video conferencing via this page. Please ensure the internal port to be used is not occupied by other applications. Please click on **NAT -> Virtual Server** and follow the below setting.

Virtual Server Configuration

Virtual Server is used to allow Internet users to access LAN services

Virtual Server : Enable Disable

Description :

Private IP : . . .

Protocol Type : TCP UDP

Private Port : (min:1, max:65535 or Range xxxxx:xxxxx)

Public Port : ((min:1, max:65535 or Range xxxxx:xxxxx)

Virtual Server Rule List

Status	Description	Protocol	Private IP	Public Port	Local Port	Del	Edit
No Rule!							

- **Virtual Server** : Check **Enable** button to activate this rule, and **Disable** to deactivate.
- **Description** : Enter appropriate text to denote name of the Virtual server.
- **Private IP** : The corresponding IP address of the LAN port used for the respected service. Enter the LAN IP address of the assigned host.
- **Protocol Type** : The communication protocol of session. Select an appropriate protocol type, either TCP or UDP protocol.
- **Private Port** : The private port(s) required for this rule. A single port may be given, or a range may be given as **start:end** , which will match all ports from *start* to *end*, inclusive.
- **Public Port** : The public port(s) required for this rule. A single port may be given, or a range may be given as **start:end** , which will match all ports from *start* to *end*, inclusive.



Note :

The Private Port and Public Port can be different, but the port range need the same.
example : Public Port is 10 to 20, the Private Port can be 30 to 40 or other 10 ports range.

- **Save** : Click **Save** button to activate the new creation.
- **Reset** : Click **Reset** button to clear configuration field.

There are 20 rules maximum allowed in this Virtual Server Rule List

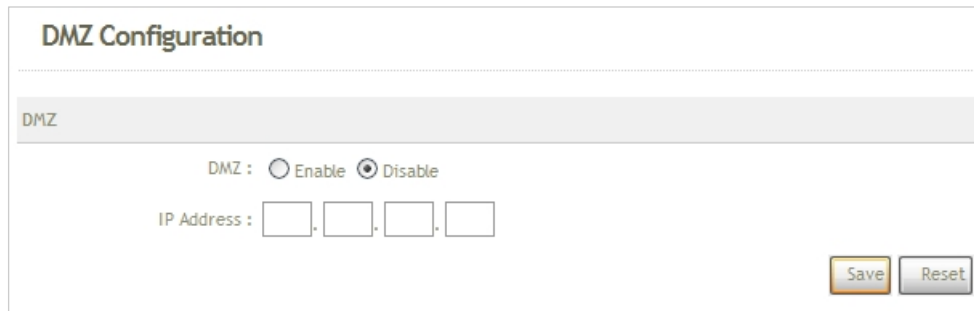
Virtual Server Rule List								
	Status	Description	Protocol	Private IP	Public Port	Local Port	Del	Edit
1	on	Forwarding Test	tcp	192.168.1.10	21	21	Del	Edit

- **Del** : Click **Del** to remove desired rule.
- **Edit** : Click **Edit** to edit desired rule.

Click **Reboot** button to activate your changes.

6.4.2 DMZ

The Demilitarized Zone, DMZ, allows a computer or server to be exposed to the Internet for special purpose, i.e. a web server, where external users can access the location without authentication. Please click on **NAT -> DMZ** and follow the below setting.



The image shows a web-based configuration interface for DMZ. At the top, it is titled "DMZ Configuration". Below the title is a sub-section labeled "DMZ". There are two radio buttons: "Enable" (which is unselected) and "Disable" (which is selected). Below the radio buttons is a label "IP Address:" followed by four input boxes for entering the IP address, separated by dots. At the bottom right of the configuration area, there are two buttons: "Save" and "Reset".

- **DMZ** : Check **Enable** button to activate this function, and **Disable** to deactivate.
- **IP Address** : Enter the IP address of the computer or server to be used as DMZ host; only one DMZ host can be activate at any time period.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes.

6.5 Utilities

The administrator can maintain the system via this page: **Profile Setting**, **System Upgrade**, **Ping Utility**, and **Reboot**.

6.5.1 Profile Setting

Current settings on the system can be backed up, or previous backed up settings can be restored as well as resetting the system back to factory default can be performed via this page. Please click on **Utilities -> Profile Setting** and follow the below setting.

- **Save Settings to PC** : Click **Save** button to save the current system settings to a local disk, i.e. the HDD of a local computer or Compact Disc.
- **Load Settings from PC** : Click **Browse** button to search for a previously saved backup file, and then click **Upload** button to upload the settings; the system will then be configured to the same settings as specified by the backup file.
- **Restore To Factory Default** : Click **Restore** button to load the factory default settings of TEW-455APBO, and then **Success Message** page appears. Click **Reboot** button to set default configuration.

6.5.2 Firmware Upgrade

To upgrade the system firmware, click **Browse** to search for the new firmware file, and then click **Upgrade** button to execute the upgrade process.

Firmware Upgrade

From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local haddisk.

Firmware Version: WCB-1000H5PX 1.0.1 Release Version

Firmware Date: 2009-06-11 02:26:54

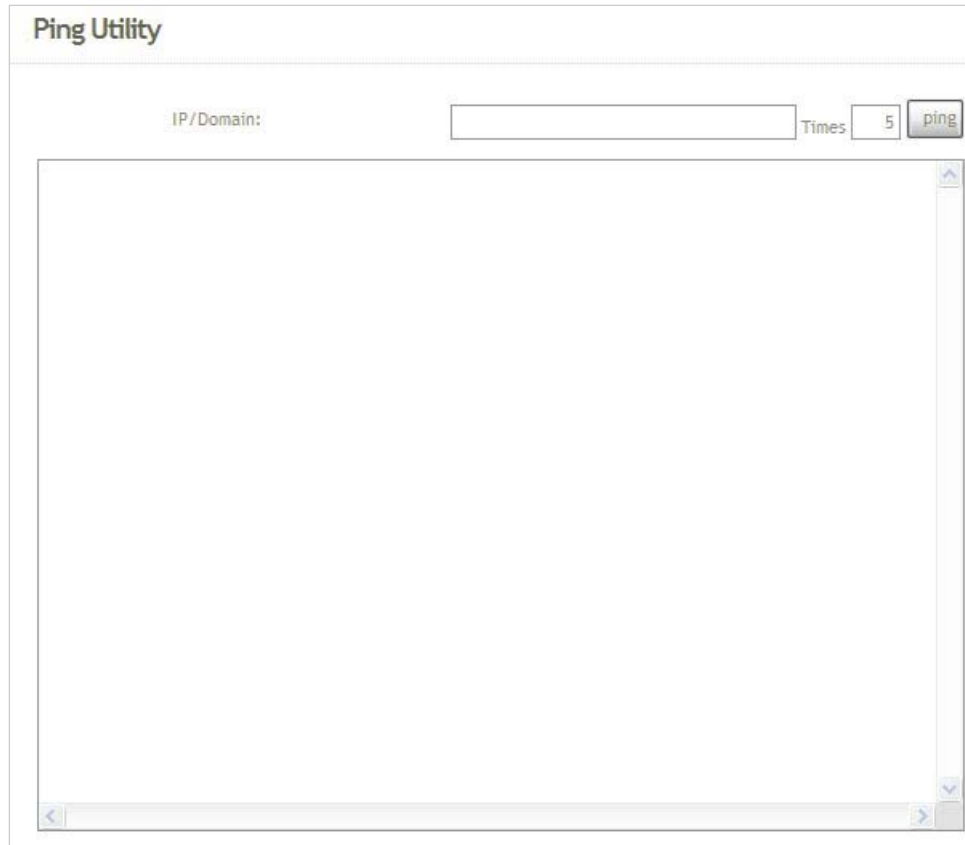
Update Firmware:

**Note :**

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

6.5.3 Ping Utility

The administrator can diagnose the network connectivity via this function.



The screenshot shows a web browser window titled "Ping Utility". At the top, there is a label "IP/Domain:" followed by an empty text input field. To the right of the input field is a "Times" label, a small input field containing the number "5", and a "ping" button. Below these elements is a large, empty rectangular area with a vertical scrollbar on the right and a horizontal scrollbar at the bottom, intended for displaying the results of the ping test.

- **IP/Domain** : Enter the desired domain name or IP address of the target device for diagnosis purpose, i.e. www.google.com, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
- **Time** : Enter the time for ping utility; default is 5, maximum is 50.

6.5.4 Reboot

This function allows the administrator to safely restart the TEW-455APBO. Click **Reboot** to restart the system immediately, and the whole process will take about three minutes to complete.



The Restart page as displayed below appears during the rebooting period. If turning off the power is necessary, please allow the restart process to be completed before turning off the system.



The **System Overview** page appears upon the completion of reboot.

6.6 Status

Information of current system settings can be over viewed via this page; statuses of **Overview**, **DHCP Clients**, and **Event Log** are displayed in this interface.

The screenshot displays the web interface for the TEW-455APBO. At the top, there is a navigation bar with the following tabs: [System](#), [Wireless](#), [Firewall](#), [NAT](#), [Utilites](#), [Status](#), and [Reboot](#). The main content area is divided into two columns. The left column is titled "System Overview" and contains the following information:

- System**
 - System Name: WCB-1000H5PX
 - Operating Mode: CPE mode
 - Firmware Version: WCB-1000H5PX 1.0.0 Release Version
 - Firmware Date: 2009-06-17 02:19:42
 - Location: default
 - Description:
 - System Time: 1970/01/01 Thu 00:00:43
 - System Up Time: 43
- WAN Information**
 - Mode: Static IP
 - MAC Address: 00:11:22:5a:5b:5d
 - IP Address: 192.168.1.254

The right column is titled "Status" and contains three links: [Overview](#), [DHCPD Clients](#), and [Event Log](#).

6.6.1 Overview

Detailed information on **System**, **WAN Information**, **CPE Wireless Information** and **LAN Information** can be reviewed via this page.

- **System** : Display the information of the system.

System
System Name: WCB-1000H5PX
Operating Mode: CPE mode
Firmware Version: WCB-1000H5PX 1.0.0 Release Version
Firmware Date: 2009-06-17 08:01:20
Location: default
Description:
System Time: 1970/01/01 Thu 00:22:46
System Up Time: 22:46

- **System Name** : The name of the system.
 - **Operating Mode** : The mode currently in service.
 - **Firmware Version** : The current firmware version installed.
 - **Firmware Date** : The build time of the firmware installed.
 - **Location** : The reminding note on the geographical location of the system. For more information, please refer to **Section 4.1.3-Management** .
 - **Description** : Please refer to **Section 4.1.3-Management** .
 - **System Time** : The current time of the system.
 - **System Up Time** : The time period that the system has been in service since last boot-up.
- **WAN Information** : Display the information of the WAN interface.

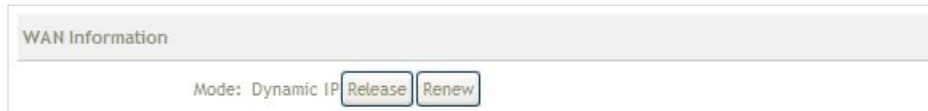
WAN Information
Mode: Static IP
MAC Address: 00:11:22:5a:5b:5d
IP Address: 192.168.1.254
IP Netmask: 255.255.255.0
IP Gateway: 192.168.1.1
Primary DNS:
Secondary DNS:
Receive bytes: 0
Receive packets: 0
Transmit bytes: 0
Transmit packets: 0

→ **Mode** : The current mode of the WAN port.



Note : The WAN port specified Dynamic IP, and the **Release** and **Renew** button will be show up. The WAN port specified PPPoE, and the **Connect** and **Disconnect** button will be show up.

- ✓ **Dynamic IP** : Click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.



- ✓ **PPPoE** : Click **Connect** button to assigned IP address from PPPoE server. **Disconnect** button to release IP address of WAN port.



- **MAC Address** : The MAC address of the WAN port.
- **IP Address** : The IP address of the WAN port.
- **IP Netmask** : The IP netmask of the WAN port.
- **IP Gateway** : The gateway IP address of the WAN port.
- **Primary DNS** : The current primary DNS server of the system.
- **Secondary DNS** : The current secondary DNS server of the system.
- **Receive bytes** : The current receive bytes of the WAN port.
- **Receive packets** : The current receive packets of the WAN port.
- **Transmit bytes** : The current transmit bytes of the WAN port.
- **Transmit packets** : The current transmit packets of the WAN port.

- **CPE Wireless Information** : Display the information of the Wireless interface.



TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

- **ESSID** : Display Extended Service Set ID of the wireless currently.
- **Security** : Display security type of the wireless currently.
- **Status** : Display connection status of the wireless currently.

If the system associate with BS, the BSSID, RSSI and Last Tx Time will be show up.

```

BSSID: 00:0d:0b:13:6b:18
RSSI: 42
Last RX Time: 0.070000

```

- **BSSID** : Indicate the Basic Service Set ID of the associated BS
- **RSSI** : Indicate the RSSI of the associated BS.
- **Last Tx Time** : **Indicate** the last receive packet of the associated BS

- **LAN Information** : Display the information of the LAN interface.

```

LAN Information
MAC Address: 00:11:22:5a:5b:5c
IP Address: 192.168.2.254
IP Netmask: 255.255.255.0
Receive bytes: 654
Receive packets: 6
Transmit bytes: 306
Transmit packets: 5

```

- **MAC Address** : The MAC address of the LAN port.
- **IP Address** : The IP address of the LAN port.
- **IP Netmask** : The IP netmask of the LAN port.
- **Receive bytes** :The current receive bytes of the LAN port.
- **Receive packets** : The current receive packets of the LAN port.
- **Transmit bytes** : The current transmit bytes of the LAN port.
- **Transmit packets** : The current transmit packets of the LAN port.

6.6.2 DHCP Clients

The administrator can obtain DHCP client's IP/MAC address via this page.

DHCP Status	
DHCP Client List	
IP	MAC
none	none

- **IP** : The IP address assigned by DHCP server to the specific LAN device.
- **MAC address** : The MAC address of the LAN device.

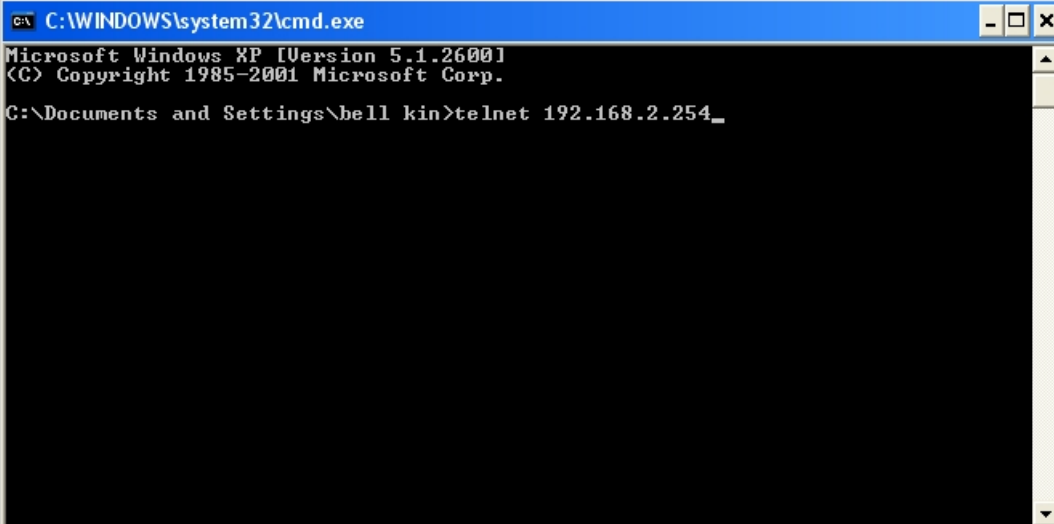
7. Command Line Interface(CLI)

The administrator can be used **help**, **showinfo**, **pwinfo**, **set**, **reboot**, **default** and **password** functions from Telnet session.

7.1 Accessing the CLI with Telnet

Follow these steps to access the CLI with Telnet of Windows XP.

1. Click **Start -> Run**, and type "**cmd**" in the "**Run**" window. The command window appears.
2. Enter "**telnet 192.168.2.254**" to connect with system.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\bell kin>telnet 192.168.2.254_
```

3. Enter username and password on the Telnet session. And the command line session

appears. The default username is "**admin**", and password is "**default**"

7.2 Using the CLI

After accessing the CLI, the administrator can use command on the system.

Command	Description
help	Display all commands description
show info	Display System and LAN information
pwinfo	Wireless Information Display Utility
set	Configure LAN IP address, netmask, gateway, and system mode.
reboot	Restart the system
default	Restore system default setting
password	Change admin password

Table 7-1: System command list

- **Using pwinfo command** : Type pwinfo command, the Wireless Information Display Utility appears.

```

Telnet 192.168.2.254
Wireless Information Display Utility

+-----+
| Choose Device |
+-----+
| [*] No Device |
| ',-':Up, '=':Down |
+-----+

'Q'uit, 'W'ireless, 'S'ignal, s'T'op-Signal, 'P'ing

```

- **Choose Device** : Select the desired physical interface name of wireless.
 - ✓ **BS Mode** : Enable all of Virtual BS, the Choose Device window will be display **ath0** to **ath7**. Enter the desired device, the window will be display result.

```

Telnet 192.168.2.254
Wireless Information Display Utility

Using : [ath0]

Signal: _

Show_cnt : /proc/net/wireless, /proc/net/dev
Iface  RxPacket  TxPacket  nwid  crypt  frag  retry  misc  MsBcn
eth0   139        155
bre0   137        155
wifi0  528        64
ath0   0           0      34     0      0      0      0      0
ath1   0           0      34     0      0      0      0      0
ath2   0           0      32     0      0      0      0      0
ath3   0           0      32     0      0      0      0      0
ath4   0           0      32     0      0      0      0      0
ath5   0           0      30     0      0      0      0      0
ath6   0           0      30     0      0      0      0      0
ath7   0           0      30     0      0      0      0      0

'Q'uit, 'W'ireless, 'S'ignal, s'T'op-Signal, 'P'ing

```

TEW-455APBO 14dBi High Power Wireless Outdoor PoE Access Point

- ✓ **BRIDGE Mode** : Enable all of BRIDGE link, the Choose Device window will be display **wds0** to **wds7**. Enter the desired device, the window will be display result.

```

Wireless Information Display Utility
Using : [wds0]
Signal: _
Show_cnt : /proc/net/wireless, /proc/net/dev
Iface RxPacket TxPacket nwid crypt frag retry misc MsBcn
eth0 129 146
bre0 126 146
wifi0 455 9
ath0 0 1 38 0 0 0 0 0
ath0.wds0 0 1 0 0 0 0 0 0
ath0.wds1 0 1 0 0 0 0 0 0
ath0.wds2 0 1 0 0 0 0 0 0
ath0.wds3 0 1 0 0 0 0 0 0
ath0.wds4 0 1 0 0 0 0 0 0
ath0.wds5 0 1 0 0 0 0 0 0
ath0.wds6 0 1 0 0 0 0 0 0
ath0.wds7 0 1 0 0 0 0 0 0
'Q'uit, 'W'ireless, 'S'ignal, s'T'op-Signal, 'P'ing

```

- ✓ **CPE Mode** : The Choose Device window only display **ath0**. Click **Enter**, the window will be display result.

```

Wireless Information Display Utility
Using : [ath0]
Signal: _
Show_cnt : /proc/net/wireless, /proc/net/dev
Iface RxPacket TxPacket nwid crypt frag retry misc MsBcn
eth0 236 266
wifi0 3679 130
ath0 0 12
bre0 232 266
'Q'uit, 'W'ireless, 'S'ignal, s'T'op-Signal, 'P'ing

```

- **'Q'uit** : Type **Q** to close this utility.
- **'W'ireless** : Type **W** to open **Choose Device** window.
- **'S'ignal** : Type **S** to open **Peer MAC Address** window. Type the desired MAC address of associated peer to display.

```

Peer MAC Address
00:0D:0B:13:6B:18
<Enter>

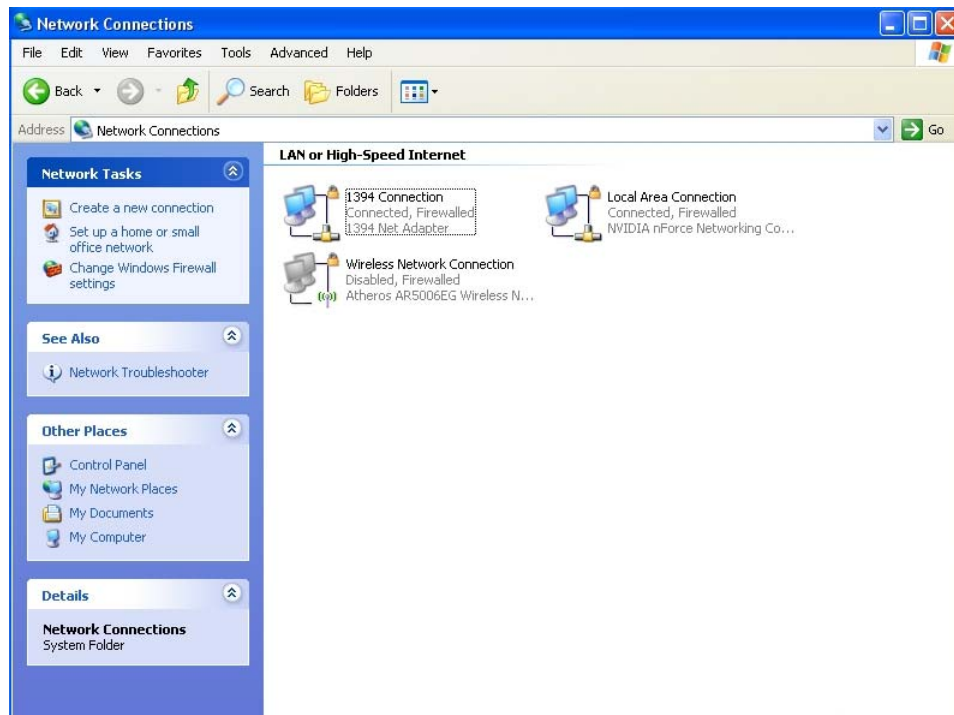
```

Click **Enter** to show signal strength of associated peer. The unit is RSSI.

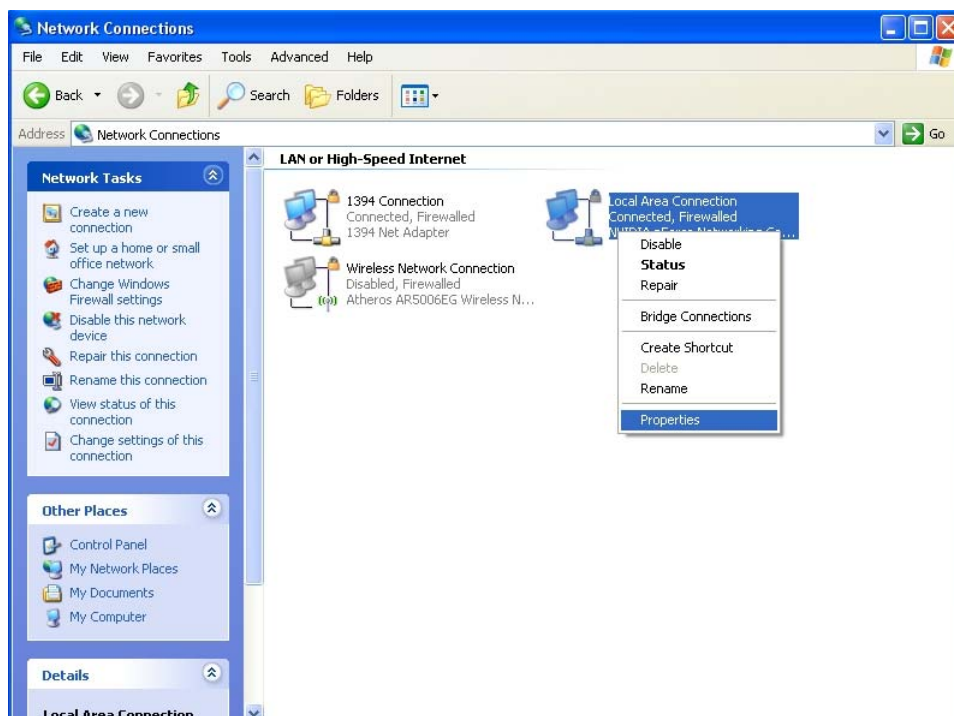
Appendix A. Windows TCP/IP Settings

■ Windows XP

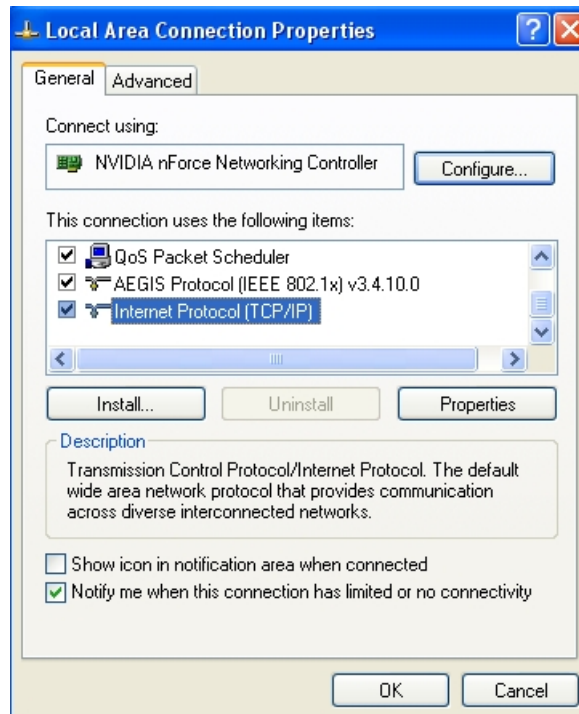
1. Click **Start -> Settings -> Control Panel**, and then “**Control Panel**” window appears. Click on “**Network Connections**”, and then “**Network Connections**” window appears.



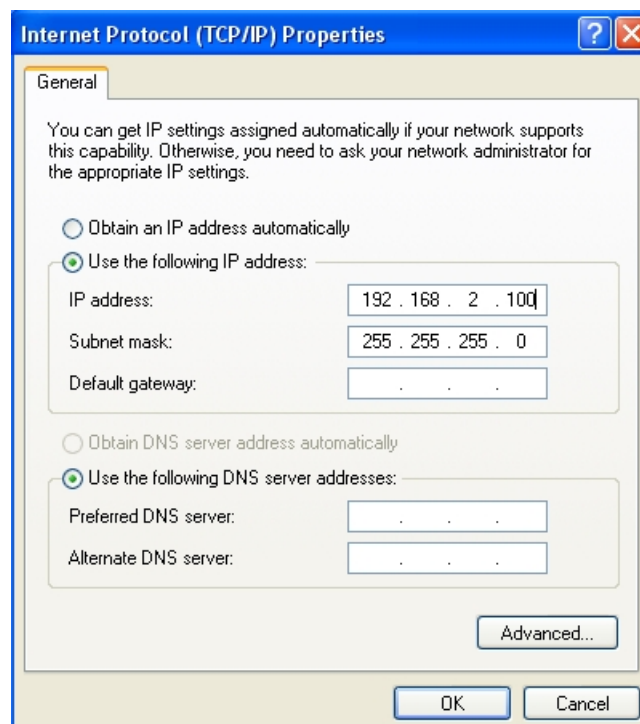
2. Click right on “**Local Area Connection**”, and select **Properties**.



3. In “**Local Area Connection Properties**” window, select “**Internet Protocol (TCP/IP)**” and click on **Properties** button.



4. Select “Use the following IP address”, and type in
IP address : 192.168.2.100
Subnet mask : 255.255.255.0



Appendix B. Valid Characters when using WMI

Table C Valid Characters for using WMI

Block	Field	Valid Characters
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Primary	IP Format; 1-254
	Secondary	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
WAN	Manual MAC Address	12 HEX chars
	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
	User name	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . =
	Password	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . =
	MTU	576 ~ 1492
	Idle Time	0 ~ 60 minutes
	Primary	IP Format; 1-254
	Secondary	IP Format; 1-254
DHCP Server	Start IP	IP Format; 1-254
	End IP	IP Format; 1-254
	DNS1 IP	IP Format; 1-254
	DNS2 IP	IP Format; 1-254
	WINS IP	IP Format; 1-254
	Domain	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . =

Table C Valid Characters for using WMI (continued)

Block	Field	Valid Characters
Management	System Name	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	Description	Length : 32 0-9, A-Z, a-z Space ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	Location	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	Check New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	HTTP Port	1 ~ 65535
	Telnet Port	1 ~ 65535
SNMP	RO community	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	RW community	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	RO user	Length : 31 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	RO password	Length : 8 ~ 32 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	RW user	Length : 31 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	Community	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	IP	IP Format; 1-254

Table C Valid Characters for using WMI (continued)

Block	Field	Valid Characters
General Setup (CPE Mode)	ESSID	Length : 31 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	WEP Key	10, 26, 32 HEX chars
	Shared Key	1 ~ 63 ASCII chars; 64 HEX chars
Advanced Setup (BS&BRIDGE Mode)	Slot Time	1 ~ 1489
	ACK Time	1 ~ 372
	CTS Time	1 ~ 744
	RSSI Threshold	-128 ~ 127
	Beacon Interval	10 ~ 5000
	Date Beacon Rate	1 ~ 15
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2346
Advanced Setup (CPE Mode)	Slot Time	1 ~ 1489
	ACK Time	1 ~ 372
	CTS Time	1 ~ 744
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2346
Virtual BS Setup	ESSID	Length : 31 0-9, A-Z, a-z ~!@#\$%^*()_+-{} :<>?[]/;'` , . =
	Maximum Clients	1 ~ 32
	VLAN ID	1 ~ 4094 ; 0 is disable
	Pass phrase	5, 13, 16 ASCII chars
	WEP Key	10, 26, 32 HEX chars
	Group Key Update	10 ~ 99999999 seconds
	Master Key Update	10 ~ 99999999 seconds
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Authentication Server	IP Format; 1-254
	Authentication Port	1 ~ 65535
	Shared Secret	1 ~ 64 characters
	EAP Reauth Period	300 ~ 99999999; default is 3600, 0 is disable
	Accounting Server	IP Format; 1-254
	Accounting Port	1 ~ 65535
WEP Key Update	0 ~ 99999999 ; default is 300, 0 is disable	

Table C Valid Characters for using WMI (continued)

Block	Field	Valid Characters
BRIDGE Setup	ESSID	Length : 31 0-9, A-Z, a-z ~!@#\$%^*()_+ - {} : < > ? [] / ; ` , . =
	Peer's MAC Address	12 HEX chars
	VLAN ID	1 ~ 4094 ; 0 is disable
	Description	Length : 32 0-9, A-Z, a-z Space ~!@#\$%^*()_+ - {} : < > ? [] / ; ` , . =
	WEP Key	10, 26, 32 HEX chars
IP Rule Setup	Source Address	IP Format; 1-254
	Source Mask	0 ~ 32
	Source Port	1 ~ 65535
	Destination Address	IP Format; 1-254
	Destination Mask	0 ~ 32
	Destination Port	1 ~ 65535
MAC Rule Setup	MAC address	MAC Format; 12 HEX chars
Virtual Server	Description	Length : 32 0-9, A-Z, a-z space ~!@#\$%^*()_+ - {} : < > ? [] / ; ` , . =
	Private IP	IP Formate; 1-254
	Private Port	1 ~ 65535
	Public Port	1 ~ 65535
DMZ	IP Address	IP Format; 1-254

Appendix D. All Antenna type for Products

A. Internal Patch 1 Antenna (Antenna Gain : 12.84dBi)





Federal Communications Commission (FCC) Statement

15.21

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

15.105(b)

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 or more 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 of the device.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The minimum separation distance between antenna and people is 30 cm.