

AP981X/AP981WX

User Manual

V1.0.1

Table of Contents

Chapter 1. Introduction.....	1
1.1 Overview.....	1
1.2 Features.....	1
1.3 Specification.....	3
1.4 Panel Function Descriptions.....	6
Chapter 2. Installation and Configuration.....	7
2.1 Installation the AP981X/AP981WX.....	7
2.2 Software Configuration	10
2.2.1 Instruction to Web Management Interface.....	10
2.2.2 Quick Configuration.....	11
2.2.2.1 AP Mode.....	11
2.2.2.2 WDS Mode.....	15
Chapter 3. AP Mode Configuration.....	18
3.1 System	19
3.1.1 Operating Mode.....	19
3.1.2 LAN Setup.....	20
3.1.3 Management.....	22
3.1.4 Time Server.....	24
3.1.5 SNMP Setup.....	25
3.2 Wireless	27
3.2.1 General Setup.....	28
3.2.2 Advanced Setup.....	29
3.2.3 Virtual AP Setup.....	31
3.2.3.1 Virtual AP General Configuration.....	32
3.2.3.2 Virtual AP Access Control List (ACL) Setup.....	40
3.3 Utilities.....	41
3.3.1 Profile Setting.....	41
3.3.2 Firmware Upgrade.....	42
3.3.3 Ping Utility.....	43
3.3.4 Reboot.....	44
3.4 Status.....	45
3.4.1 Overview.....	46
3.4.2 Client.....	48
3.4.3 Event Log.....	49
Chapter 4. WDS Mode Configuration.....	50
4.1 System	51
4.1.1 Operating Mode.....	51
4.1.2 LAN Setup.....	52
4.1.3 Management.....	54
4.1.4 Time Server.....	56
4.1.5 SNMP Setup.....	57
4.2 Wireless	59

4.2.1 General Setup.....	60
4.2.2 Advanced Setup.....	61
4.2.3 WDS Setup.....	63
4.3 Utilities.....	64
4.3.1 Profile Setting.....	64
4.3.2 Firmware Upgrade.....	65
4.3.3 Ping Utility.....	66
4.3.4 Reboot.....	67
4.4 Status.....	68
4.4.1 Overview.....	69
4.4.2 WDS List.....	71
4.4.3 Event Log.....	72
5. Command Line Interface(CLI).....	73
5.1 Accessing the CLI with Telnet.....	73
5.2 Using the CLI.....	74
Appendix A. Windows TCP/IP Settings.....	77
Appendix B. Valid Characters when using WMI.....	79

Chapter 1. Introduction

1.1 Overview

The AP981X/AP981WX 802.11B/G 500mW wireless access point is designed to fit into a standard single gang box and bring the benefits of both a RJ-45 wired connection as well as WiFi wireless connection. The AP981X/AP981WX can be installed and configured easily into any new wireless network or integrated within an existing wired network resulting in a more flexible and cost-effective wireless deployment. And, a network administrator can centrally manage the AP981X/AP981WX via a Web browser or an SNMP MIB browser. With included PoE, power and data are supplied to the unit using CAT5 Ethernet cable.

The AP981X/AP981WX is ideal for institutions that are already wired for CAT5 and now need both a wired connection as well as a wireless solution in each room. The AP981X/AP981WX has an RJ-45 connector on the front of the unit so a user will not lose their wired connection while obtaining a wireless connection in each room.

AP981X/AP981WX is compliant with the latest wireless industrial security standards that are required in those tightly secured enterprise network environments. Its Wireless Distribution System (WDS) feature allows for flexible extension of wireless coverage.

AP981X/AP981WX's easy-to-use web-based administrative interface make the configuration task and client management simple and straightforward. In addition, CLI and SNMP management interfaces are also supported by AP981X/AP981WX.

The built-in software interfaces of AP981X/AP981WX has allow for communicating with other types of network management servers. When managed by backend controlling gateway, AP981X/AP981WX can further provide enhanced values in a well managed WLAN solution.

1.2 Features

AP981X/AP981WX' rich features and easy-to-use tools for configuration and administration make it a truly flexible multiple-functional Access Point. It adapts efficiently into all size of WLAN deployments, from a simple standalone AP coverage to a large enterprise's WLAN that spans across multiple sites and has to be centrally managed, and highly secured.

■ High Speed IEEE 802.11 g and Backward Compatible with 802.11b

AP981X/AP981WX is equipped with a high-speed IEEE 802.11g wireless network interface based on Atheros™ chipset, delivering reliable performance with maximum wireless transmission rates of up to 54Mbps. It is backward compatible with IEEE 802.11b standard.

■ WDS Wireless Modes for Extending Wireless Coverage

To increase wireless network coverage, it is also able to create structural WDS (Bridge or Repeater) links connecting to other WDS-capable APs. WDS links can serve as AP981X/AP981WX's LAN connections to replace Ethernet ports, or simply bridge the wired side and the wireless side as a single network.

■ **Supporting IEEE 802.1p/1Q Quality Service and IEEE801.11e Wireless Multi-Media**

For bandwidth thirsty multimedia applications like voice, audio and video, AP981X/AP981WX supports for IEEE 801.11e Wireless Multi-Media (WMM) and IEEE 802.1p/IEEE 802.1Q Quality of Service (QoS) tagging features.

■ **Capability of Client Isolation and Serving as Multiple Virtual APs**

Multiple-SSID capability is to use just one AP to simultaneously emulate up to 8 APs with different BSSIDs by utilizing the Atheros™'s virtual AP (VAP) technology and separate their packets by using different VLAN IDs. Hence, using one AP is able to act as if there are actually 4 different APs deployed in the same area. Client isolation is also supported by AP981X/AP981WX that clients under an AP are isolated with each other.

■ **Enterprise Class WLAN Security by Encryptions and Client Authentications**

To protect data transmission over the air, AP981X/AP981WX can be configured to filter out unauthorized wireless clients with built-in MAC-based access control list or via a back-end RADIUS server by sending an authentication request when a client is trying to get connected to it. Additionally, AP981X/AP981WX also has many advanced security options including 64/128/152 bit WEP, WPA/WPA2 with IEEE 802.1x or PSK (Pre-Shared Key). Other security features included are: Wireless LAN segmentation, Rouge AP detection, and Disable SSID Broadcast, and the option of station-isolation.

■ **Multiple Administration Interfaces for Network Management**

AP981X/AP981WX provides three types of administrative interfaces, web-based management interface, CLI, and SNMP to configure and manage the network deployment.

■ **Built-In antenna**

AP981X/AP981WX is embedded with a chip antenna providing E.I.R.P of 30db compared to the usual 20db from normal access points in the market place. As an option for special ODM design we have reserved RF connector onboard to provide antenna diversity features.

1.3 Specification

■ Wireless and Wired Interface Standard

- Wireless :
 1. IEEE 802.11g (Up to 54Mbps)
 2. IEEE 802.11b (Up to 11Mbps)
- Ethernet : 2 x RJ-45 (One support Passive Power Over Ethernet)

■ 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

■ General Access Point Features

- Number of ESSID : 8
- Number of associated clients per AP : 32
- Two mode : AP Mode and WDS Mode
- WDS Mode : to extend wireless coverage by connecting wirelessly to another WDS capable AP.
Support up to 8 WDS links
- Slot Time, ACK/CTS Timeout support
- RSSI threshold support
- TX burst support
- Beacon interval : adjustable to best adapt to the deployment environment
- IAPP : to facilitate faster roaming for the stations among different APs nearby
- Support EZ-Connection with security
- 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
- Wireless site survey : for scanning the surrounding access points for connection
- VLAN tag support

■ 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 AP can not communicate with each other
- Support data encryption and VLAN tag over WDS link

■ 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
- DHCP client
- Syslog client
- Support Event Log
- Support statistics on total transmission encountered and transmitting error occurred

■ Hardware Specifications

- LED Indication : Power x 1; Ethernet x 1; WLAN x 1
- EZ-Connection with security Push Button
- Reset/Restart Push Button

■ **Physical and Power**

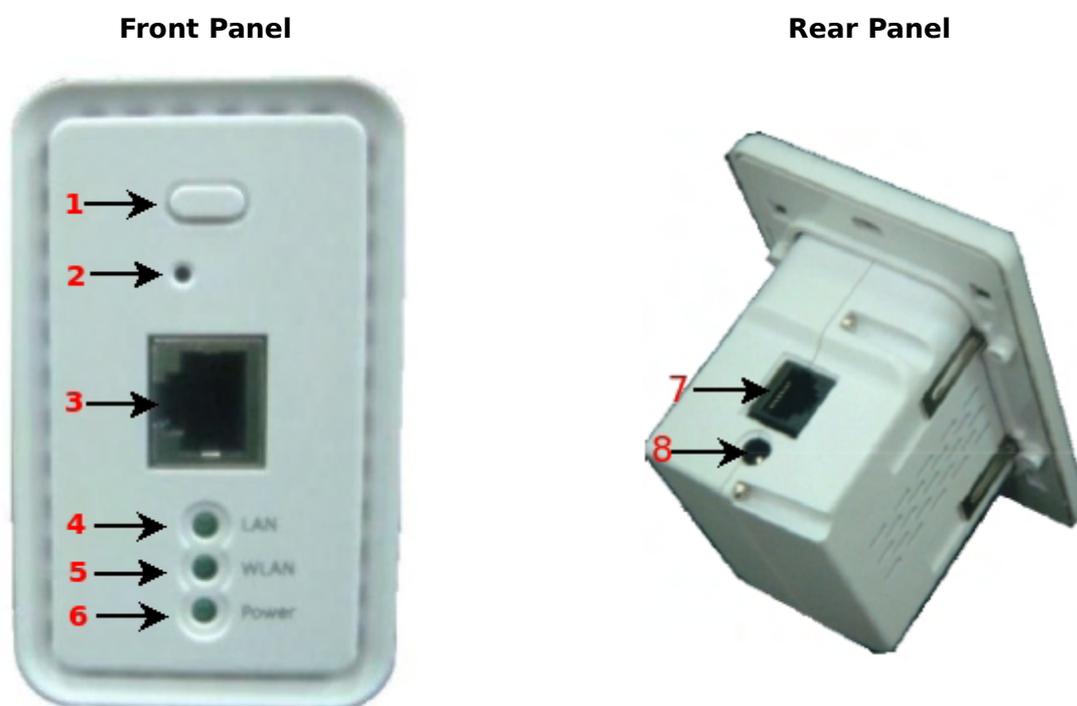
- Power supply : 110-220V AC Power; 12 VDC, 1.5A Input
- PoE : DC 48V/ 0.3 A
- Form factor : In-Wall Type
- Dimensions(HxDxL) : 129.98x79.98x67 mm(Main Unit with Plate); 79.98x34x67 mm(Manu Unit)
- Weight: 60g

■ **Environment**

- Operation temperature : -20°C ~ 50°C
- Storage temperature : -20°C ~ 70°C
- Operation humidity : 10% to 80% Non-condensing
- Storage humidity : 5% to 90% Non-condensing

1.4 Panel Function Descriptions

There are several LED indicators and button on the front of the AP981X/AP981WX. Please refer to the definitions below :



1. EZ-Connection : EZ-Connection with security push button
2. Reset Button :
 - ➔ Press and hold the Reset button for 2 seconds to restart the system. The LED except Power indicator will be off before restarting.
 - ➔ Press and hold the Reset button for more than 10 seconds to reset the system to default configurations.
3. Ethernet : This port is a Private LAN port that authentication is not required for clients to access network via this port.
4. LAN : Green LED ON indicates connection, OFF indicates no connection, and FLASH indicates LAN port Transmit
5. WLAN : Green LED FLASH indicates Wireless ON, and FLASH quickly indicates Wireless Transmit quickly.
6. Power : Green LED ON indicates power on, and OFF indicates power off
7. Ethernet (POE): This port is for connection to external network or POE switch.
8. DC Injector (12V) : Attach the power socket here.

Chapter 2. Installation and Configuration

2.1 Installation the AP981X/AP981WX

➤ AP981X

Make sure the optional mounting kit is included as pictured below

- ✓ 4 x Screws
- ✓ 4 x Mounting Brackets
- ✓ 1 x Faceplate
- ✓ 1 x Frame



Step

Step A : Locate the area you wish to install the Wall AP and affix the frame to the wall



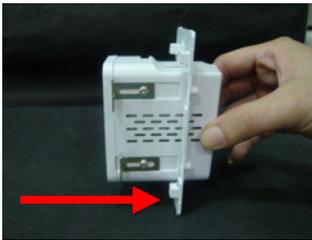
Step B : Measure the depth of the Wall and adjust the mounting bracket accordingly



Step C : Fasten the mounting bracket tightly with the screws on the Wall AP(two on each side)



Step D : Slide the Wall AP into the frame until it is flushed into the Wall



Flushed into the wall

Step E : Fasten tightly the Wall AP into the frame with the included optional screws



Step F : Line-up and push the faceplate onto frame until it snaps securely into place

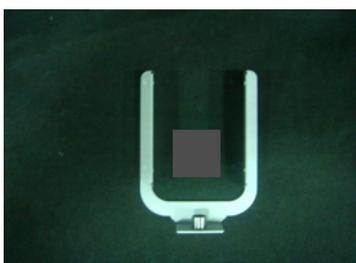


➤ **AP981WX**

Make sure the optional mounting kit is included as pictured below

- ✓ 1 x Frame
- ✓ 1 X Mounting base

Frame



Mounting Base



Step

Step A : Slide the Frame to align with the screw holes on the Wall AP



Step B : Fasten the Frame tightly with the screws on the Wall AP (two on each side)



Step C : Fasten tightly the mounting base onto the frame



Step D : Locate the area you wish to install the Wall AP and affix the mounting base to desire location



2.2 Software Configuration

2.2.1 Instruction to Web Management Interface

AP981X/AP981WX supports web-based configuration. Upon the completion of hardware installation, AP981X/AP981WX 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 AP981X/AP981WX for accessing the system. Do not duplicate the IP Address used here with IP Address of AP981X/AP981WX 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 AP981X/AP981WX; 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.

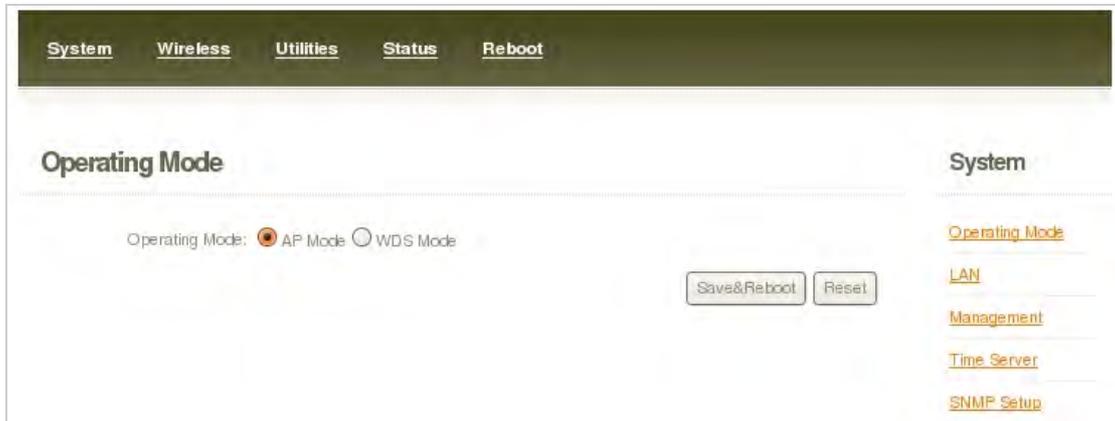


■ Login Success

System Overview page will appear after successful login.

2.2.2 Quick Configuration

AP981X/AP981WX is a three mode system which can be configured either as a gateway or an access point as desired. This section provides a step-by-step configuration procedure for basic installation on AP Mode and WDS Mode



2.2.2.1 AP Mode

Step 1 : Mode Confirmation

Ensure the Operating Mode is currently at AP 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 informations 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 AP Setup**, and then **VAP Setup** page appears.

Enable	VAP	ESSID	Encryption	ACL Mode	ACL Setup	EDIT
<input type="checkbox"/>	VAP 0	AP00	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 1	AP01	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 2	AP02	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 3	AP03	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 4	AP04	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 5	AP05	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 6	AP06	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 7	AP07	disabled	disabled	Setup	Edit

Enable “VAP0”, and then click **Save** button to save settings. Click “Edit” and then **VAP0 Configuration** page appears.

VAP 0 Configuration

General

ESSID :

Hidden SSID : Enable Disable

Client Isolation : Enable Disable

WMM : Enable Disable

IAPP Support : Enable Disable

WPS Support : Enable Disable

Maximum Clients : (1 - 5, default 5)

VLAN ID : Enable Disable (1~4094)

Security Type : ▼

Wireless

[General Setup](#)

[Advanced Setup](#)

[Virtual AP Setup](#)

Setup the broadcasting ESSID for easily identifying the system when device is trying to associate the service. Click **Save** button to save settings

Step 6 : Security Settings

In **VAP0 Configuration** page, select WEP in “Security Type” pull down menu. The WEP setting field will shown 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 informations required in the WEP settings field, and the same information will also be used to set up devices which will then be using AP981X/AP981WX's services.

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

Congratulation !

The AP mode is now successfully configured.

2.2.2.2 WDS Mode

Step 1 : Mode Confirmation

Ensure the Operating Mode is currently at WDS 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: AP981X</p> <p>Operating Mode: WDS mode</p> <p>Firmware Version: Cen-AP-G2H5 Beta V0.0.5</p> <p>Firmware Date: 2009-07-16 03:24:29</p> <p>Location: default</p> <p>Description: InWall AP WiFi,G ,500mW</p> <p>System Time: 1970/01/01 Thu 00:00:44</p> <p>System Up Time: 44</p> <p>LAN Information</p> <p>MAC Address: 00:11:a3:07:01:03</p>	<p>Overview</p> <p>WDS List</p> <p>Event Log</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="AP981X"/></p> <p>Description: <input type="text" value="InWall AP WiFi,G ,500mW"/></p> <p>Location: <input type="text" value="default"/></p> <p>Admin Password</p> <p>New Password: <input type="password"/> (If you don't want to change , don't type anything)</p> <p>Check New Password: <input type="password"/></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> <p><input type="button" value="Save"/> <input type="button" value="Reset"/></p>	<p>Operating Mode</p> <p>LAN</p> <p>Management</p> <p>Time Server</p> <p>SNMP Setup</p>

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 informations 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 WDS Peer's MAC Address

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

Wireless Setup

Sub Menu

WDS Setup

WMM : Enable Disable

Security Type :

Enable	WDS 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="checkbox"/>	02. <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	03. <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	04. <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	05. <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	06. <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	07. <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	08. <input type="text"/>	<input type="text"/>	<input type="text"/>

General Setup
Advanced Setup
WDS Setup

Enable "WDS 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 :

Save Reset

General Setup
Advanced Setup
Virtual AP Setup

Select the "Channel" and "Transmit Rate Control" informations required in the General Setup field. The informations must the same the other WDS device.

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

Congratulation !

The WDS mode is now successfully configured.

Chapter 3. AP Mode Configuration

When AP mode is activated, the system can be configured as an Access Point. This section provides information in configuring the AP mode with graphical illustrations. AP981X/AP981WX 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 AP	Ping Utility	Event Log
	Time Server		Reboot	
	SNMP			

Table 3-1: AP Mode Functions

The screenshot displays the web interface for the AP Mode Main Page. At the top, there is a navigation bar with tabs for [System](#), [Wireless](#), [Utilities](#), [Status](#), and [Reboot](#). The main content area is divided into two sections: **System Overview** and **LAN Information**. The **System Overview** section lists the following details:

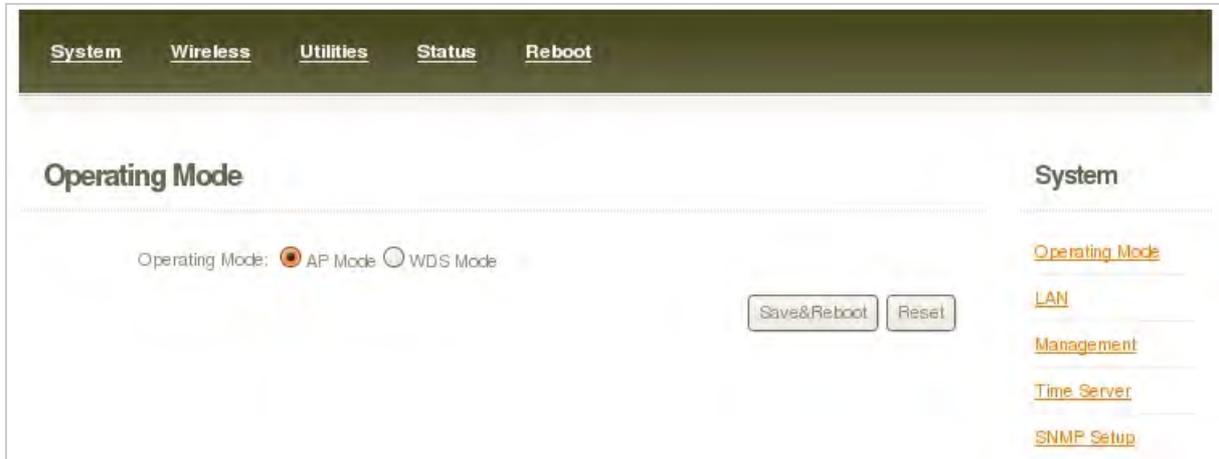
- System Name: AP981X
- Operating Mode: AP mode
- Firmware Version: Cen-AP-G2H5 Beta V0.0.5
- Firmware Date: 2009-07-16 03:24:29
- Location: default
- Description: InWall AP WiFiG ,500mW
- System Time: 1970/01/01 Thu 00:00:43
- System Up Time: 43

The **LAN Information** section shows the MAC Address: 00:11:a3:07:01:03. On the right side of the page, there is a **Status** section with links for [Overview](#), [Client](#), and [Event Log](#).

Figure 3-1: AP Mode Main Page

3.1 System

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



3.1.1 Operating Mode

AP981X/AP981WX supports three operation modes; AP mode , WDS mode and CPE mode. The administrator can set the desired mode via this page, and then configure the system according to their deployment needs.

- ✓ **AP Mode** : Check **AP Mode** button to enable AP mode, and then click "**Save&Reboot**" to activate the setting.
- ✓ **WDS Mode** : Check **WDS Mode** button to enable AP mode, and then click "**Save&Reboot**" to activate the setting.

3.1.2 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 AP981X/AP981WX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

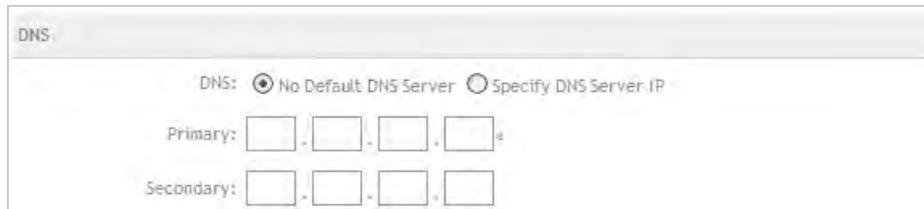


Dynamic IP

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

3.1.3 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.

The screenshot shows the 'Admin Configuration' page with a 'System' sidebar. The 'System Information' section contains three input fields: 'System Name' (AP981X), 'Description' (InWall AP WiFi,G ,500mW), and 'Location' (default). The 'Admin Password' section has 'New Password' and 'Check New Password' fields. The 'Admin Login Methods' section has checkboxes for 'Enable HTTP' (Port: 80) and 'Enable Telnet' (Port: 23). 'Save' and 'Reset' buttons are at the bottom right.

■ 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 close-up shows the 'Admin Password' section with 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)'.

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

- **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

3.1.4 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

3.1.5 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.
- **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 title bar labeled "SNMP Trap". Below the title bar, 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 consists of four small boxes separated by dots, representing 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

3.2 Wireless

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

The screenshot displays the 'Wireless Setup' configuration page. At the top, a navigation bar includes links for 'System', 'Wireless', 'Utilites', 'Status', and 'Reboot'. The main content area is titled 'Wireless Setup' and features a 'General Setup' section. The MAC address is shown as 00:11:22:5a:5b:5d. The Band Mode is set to 802.11b+802.11g, Transmit Rate Control is Auto, Country is US, Channel is 1, and Tx Power is Level 9. On the right side, there is a 'Wireless' sidebar with links for 'General Setup', 'Advanced Setup', and 'Virtual AP Setup'. At the bottom right, there are 'Save' and 'Reset' buttons.

System	Wireless	Utilites	Status	Reboot
Wireless Setup				
General Setup				
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				
<input type="button" value="Save"/> <input type="button" value="Reset"/>				

3.2.1 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' tab is active. 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. On the right side, there are links for General Setup, Advanced Setup, and Virtual AP Setup.

- **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 is for AP's RF general settings and will be applied to all VAPs.

3.2.2 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

Wireless

[General Setup](#)

[Advanced Setup](#)

[Virtual AP Setup](#)

- **Slot Time** : Enter the desired slot time for the AP.
- **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 AP.



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 access point 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.
- **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 unactivated Tx Burst.
- **802.11g Protection Mode** : Click **Enable** button to activated 802.11g Protection Mode, and Disable to unactivated 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 is for AP's RF advanced settings and will be applied to all VAPs.

3.2.3 Virtual AP Setup

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

Enable	VAP	ESSID	Encryption	ACL Mode	ACL Setup	EDIT
<input type="checkbox"/>	VAP 0	AP00	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 1	AP01	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 2	AP02	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 3	AP03	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 4	AP04	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 5	AP05	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 6	AP06	disabled	disabled	Setup	Edit
<input type="checkbox"/>	VAP 7	AP07	disabled	disabled	Setup	Edit

- **Enable** : Click **Enable** button and **Save** button for creating Virtual AP
- **VAP** : Display number of system's Virtual AP.
- **ESSID** : Display Virtual AP's ESSID; default is AP00~AP07.
- **Encryption** : Display Virtual AP's Security Type; default is disabled.
- **ACL Mode** : Display Virtual AP's ACL Mode; default is disabled.
- **ACL Setup** : Click Setup button for configuring Virtual AP's Access Control List.
- **EDIT** : Click Edit button for configuring Virtual AP'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

3.2.3.1 Virtual AP General Configuration

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

VAP0 Configuration

General

ESSID :

Hidden SSID : Enable Disable

Client Isolation : Enable Disable

WMM : Enable Disable

IAPP Support : Enable Disable

WPS Support : Enable Disable

Maximum Clients : (1 - 32, default 32)

VLAN ID : Enable Disable (1~4094)

Security Type :

Wireless

[General Setup](#)

[Advanced Setup](#)

[Virtual AP Setup](#)

- **ESSID** : Extended Service Set ID indicates the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which is assigned to the specified VAP.
- **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.
- **IAPP 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 access point (AP) and new AP during hand off period.



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

- **WPS Support** : Wi-Fi Protected Setup(WPS) uses WPA-PSK/WPA2-PSK for encryption. It does not provide additional security.



Note : IAPP and WPS only can enabled on one VAP.

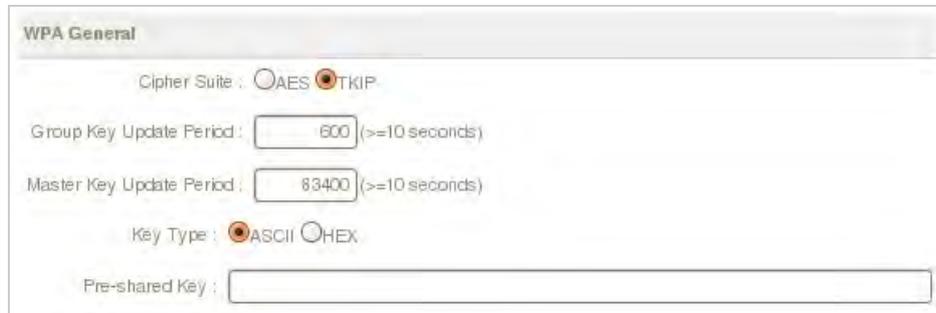
- **Maximum Clients** : Enter maximum number of clients to a desired number. For example, while the number of client is set to 32, only 32 clients are allowed to connect with this VAP.
- **VLAN ID** : Virtual LAN, the system supports tagged VLAN. To enable VLAN function; valid values are from 1 to 4094.
- **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 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**.
- ✓ **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 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.
- ✓ **Group Key Update Period** : This time interval for rekeying 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 rekeying 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)

EAP Reauth Period :

Authentication RADIUS Server

Authentication Server : . . .

Port :

Shared Secret :

Accounting RADIUS Server Enable Disable

Secondary Authentication RADIUS Server

Authentication Server : . . .

Port :

Shared Secret :

✓ **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 rekeying 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 rekeying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.
- **EAP Reauth Period :** EAP reauthentication period in seconds; default is 3600; 0 = disable reauthentication.

✓ **Authentication RADIUS Server Settings :**

Authentication RADIUS Server

Authentication Server : . . .

Port :

Shared Secret :

Accounting RADIUS Server Enable Disable

- **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.
- **Accounting Server :** Check on the respected button to enable either Enable or Disable accounting RADIUS server.

✓ **Accounting Server Settings :**

The screenshot shows a configuration window titled "Accounting Server". It has three input fields: "Accounting Server" (IP address), "Port" (set to 1813), and "Shared Secret" (text field).

- **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.

✓ **Secondary Authentication RADIUS Server Settings :**

The screenshot shows a configuration window titled "Secondary Authentication RADIUS Server". It has three input fields: "Authentication Server" (IP address), "Port" (set to 1812), and "Shared Secret" (text field).

- **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.
- **Accounting Server :** Check on the respected button to enable either Enable or Disable accounting RADIUS server.

✓ **Accounting Server Settings :**

The screenshot shows a configuration window titled "Accounting Server". It has three input fields: "Accounting Server" (IP address), "Port" (set to 1813), and "Shared Secret" (text field).

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

The screenshot shows the configuration interface for Dynamic WEP and RADIUS servers. It is divided into three main sections:

- Dynamic WEP Settings:**
 - WEP Key Length: 64bits 128bits
 - WEP Key Update Period:
 - EAP Reauth Period:
- Authentication RADIUS Server:**
 - Authentication Server: . . .
 - Port:
 - Shared Secret:
 - Accounting RADIUS Server: Enable Disable
- Secondary Authentication RADIUS Server:**
 - Authentication Server: . . .
 - Port:
 - Shared Secret:

✓ **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 the WEP will then be updated; the unit is in seconds; default is 300 seconds; 0 = do not rekey.
- **EAP Reauth Period** : EAP reauthentication period in seconds; default is 3600; 0 = disable reauthentication.

✓ **Authentication RADIUS Server Settings :**

The screenshot shows the configuration interface for the Authentication RADIUS Server. It includes the following fields:

- Authentication Server: . . .
- Port:
- Shared Secret:
- Accounting RADIUS Server: Enable Disable

- **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.
- **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.

✓ **Secondary 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.
- **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.

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

3.2.3.2 Virtual AP Access Control List (ACL) Setup

In this function, the administrator can be allow or reject clients to access Virtual AP. Please click on **Wireless -> Virtual AP 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. In the 'ACL LIST' section, there is 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

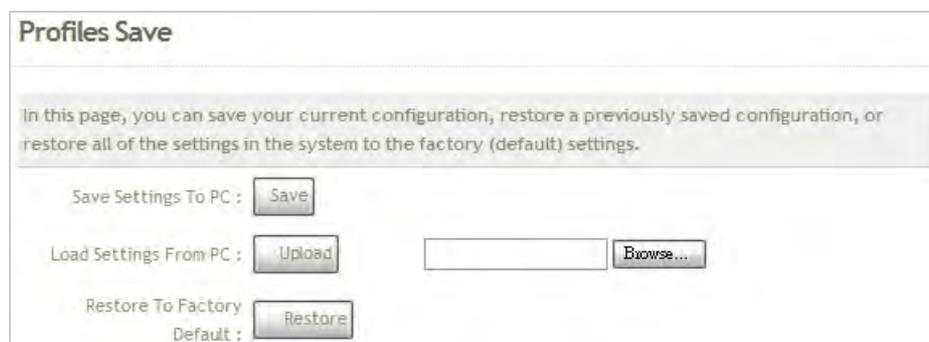
3.3 Utilities

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



3.3.1 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 AP981X/AP981WX, and then **Success Message** page appears. Click **Reboot** button to set default configuration.

3.3.2 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.

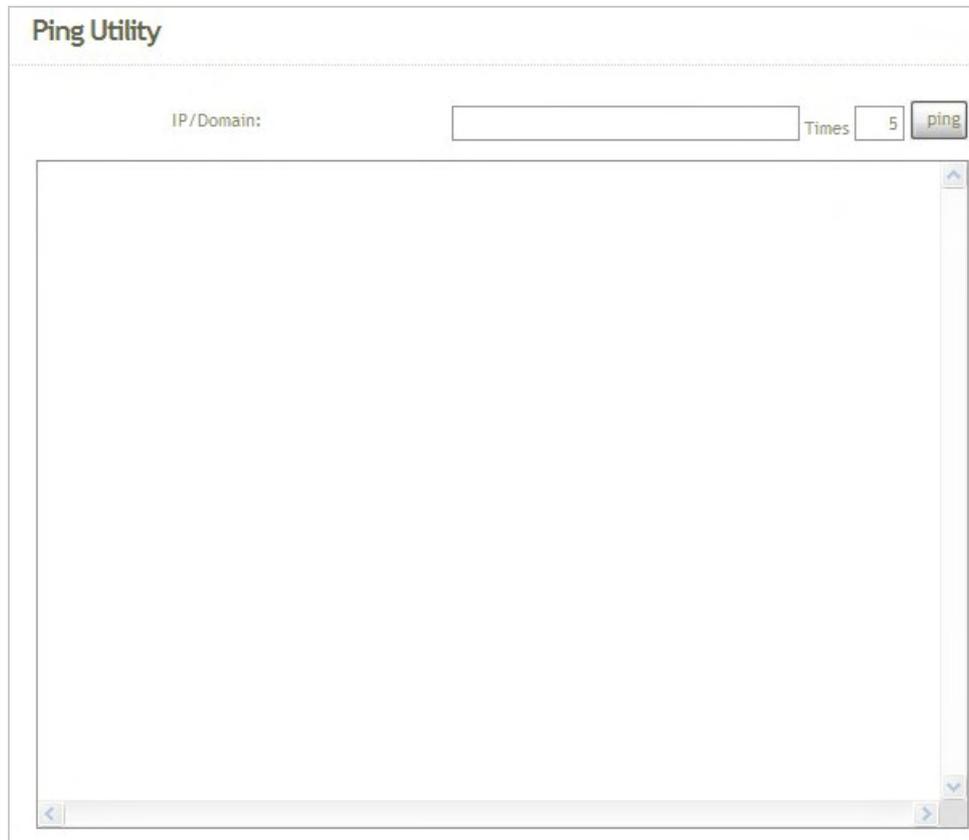
Firmware Upgrade	Utilities
<p>From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local hardisk.</p> <p>Firmware Version: Cen-AP-G2H5 Beta V0.0.5</p> <p>Firmware Date: 2009-07-16 03:24:29</p> <p>Update Firmware: <input type="text"/> 浏览...</p> <p>Upgrade Clear</p>	<p>Profile Setting</p> <p>System Upgrade</p> <p>Ping Utility</p> <p>Reboot</p>

**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.

3.3.3 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 interface titled "Ping Utility". It features a form with the following elements:

- A label "IP/Domain:" followed by a text input field.
- A label "Times" followed by a numeric input field containing the value "5".
- A "ping" button.
- A large, empty rectangular area below the form, which serves as the "Result" field for displaying the ping output.

- **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.

3.3.4 Reboot

This function allows the administrator to safely restart the AP981X/AP981WX. 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.

3.4 Status

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

The screenshot displays the web interface for the AP981X/AP981WX. At the top, a dark green navigation bar contains the following tabs: [System](#), [Wireless](#), [Utilities](#), [Status](#), and [Reboot](#). The main content area is split into two columns. The left column, titled "System Overview", features a "System" section with the following information:

- System Name: AP981X
- Operating Mode: AP mode
- Firmware Version: Cen-AP-G2H5 Beta V0.0.5
- Firmware Date: 2009-07-16 03:24:29
- Location: default
- Description: InWall AP WiFiG ,500mW
- System Time: 1970/01/01 Thu 00:00:43
- System Up Time: 43

Below the System section is a "LAN Information" section with the following detail:

- MAC Address: 00:11:a3:07:01:03

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

3.4.1 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: AP981X
Operating Mode: AP mode
Firmware Version: Cen-AP-G2H5 Beta V0.0.5
Firmware Date: 2009-07-16 03:24:29
Location: default
Description: InWall AP WiFi,G ,500mW
System Time: 1970/01/01 Thu 00:00:43
System Up Time: 43

- **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 AP configuration information of the system.

Wireless Information				
VAP	ESSID	Status	Security Type	Clients
VAP 0	AP00	off	disabled	0
VAP 1	AP01	off	disabled	0
VAP 2	AP02	off	disabled	0
VAP 3	AP03	off	disabled	0
VAP 4	AP04	off	disabled	0
VAP 5	AP05	off	disabled	0
VAP 6	AP06	off	disabled	0
VAP 7	AP07	off	disabled	0

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

3.4.2 Client

The administrator can obtain detailed Information such as VAP, 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 "no clients!!" in the center.

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

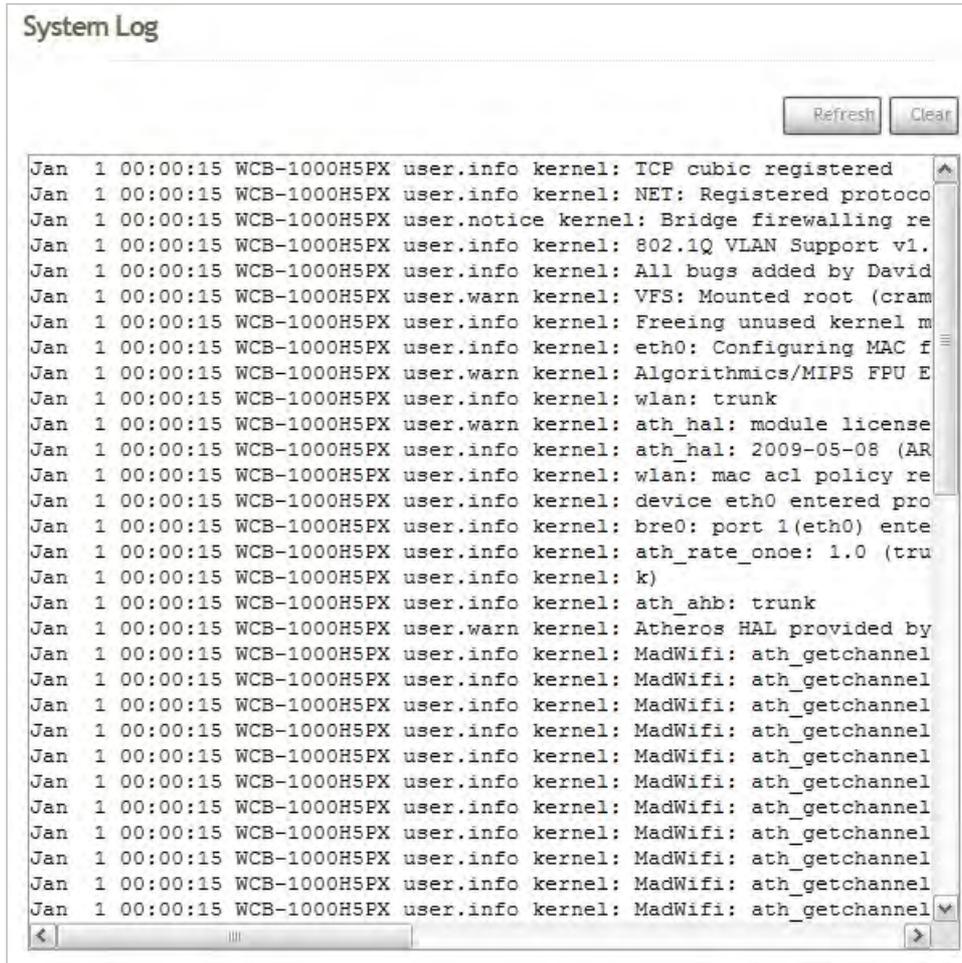
- **AP** : Virtual AP which the device is associated with.
- **ESSID** : ESSID which the device is associated with.
- **RSSI** : Indicate the RSSI of the respective client's association.
- **Last Idle Time** : Time period that the associated client is inactive (units in seconds).
- **Disconnect : Administrator** 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 AP ACL Configuration**.

3.4.3 Event Log

The reported system events can be reviewed here.



The screenshot shows a 'System Log' window with a scrollable text area and 'Refresh' and 'Clear' buttons. The log entries are as follows:

```

Jan 1 00:00:15 WCB-1000H5PX user.info kernel: TCP cubic registered
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: NET: Registered protocol family 10
Jan 1 00:00:15 WCB-1000H5PX user.notice kernel: Bridge firewalling rules
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: 802.1Q VLAN Support v1.3
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: All bugs added by David
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: VFS: Mounted root (crashfs) on
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: Freeing unused kernel memory
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: eth0: Configuring MAC filter
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: Algorithmics/MIPS FPU Emulation
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: wlan: trunk
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: ath_hal: module license
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: ath_hal: 2009-05-08 (AR7130)
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: wlan: mac acl policy registered
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: device eth0 entered promiscuous
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: br0: port 1(eth0) entered
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: ath_rate_onoff: 1.0 (true)
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: k
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: ath_ahb: trunk
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: Atheros HAL provided by
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: MadWifi: ath_getchannel

```

- **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 4. WDS Mode Configuration

When WDS mode is activated, the system can be configured as an repeater or client bridge. This section provides information in configuring the WDS mode with graphical illustrations.

AP981X/AP981WX 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	WDS List
	Management	WDS Setup	Ping Utility	Event Log
	Time Server		Reboot	
	SNMP			

Table 4-1: WDS Mode Functions

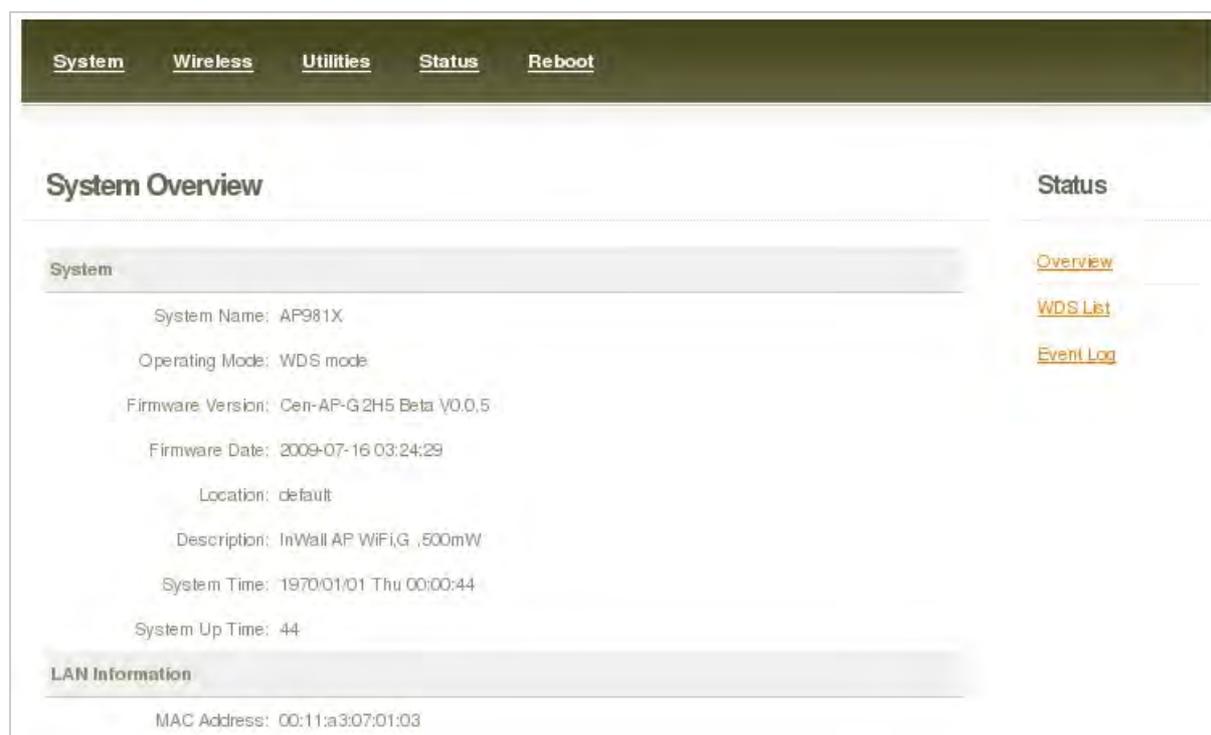
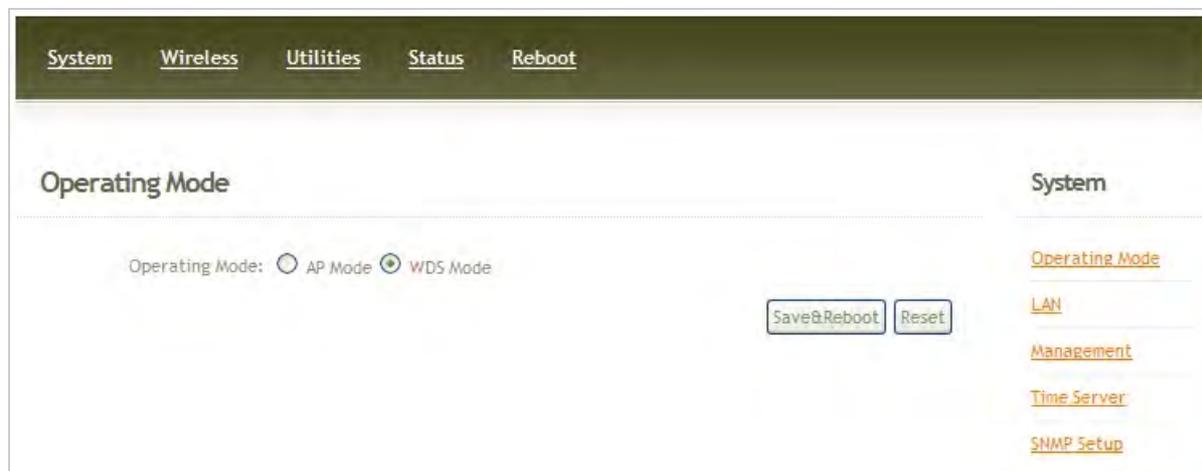


Figure 4-1: WDS Mode Main Page

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

AP981X/AP981WX supports three operation modes; AP mode , WDS mode and CPE mode. The administrator can set the desired mode via this page, and then configure the system according to their deployment needs.

- ✓ **AP Mode** : Check **AP Mode** button to enable AP mode, and then click "**Save&Reboot**" to activate the setting.
- ✓ **WDS Mode** : Check **WDS Mode** button to enable AP mode, and then click "**Save&Reboot**" to activate the setting.

4.1.2 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 *

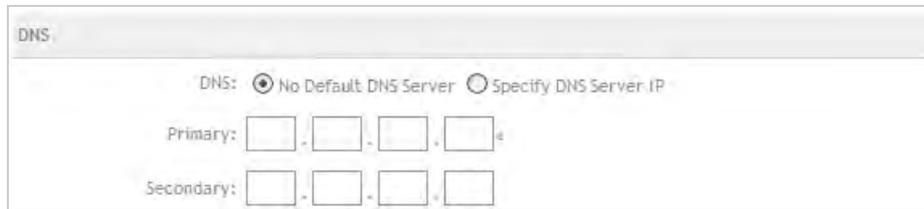
- ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
- ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1
- ➔ **Dynamic IP** : This configuration type is applicable when the AP981X/AP981WX 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.



- **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.



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.

The screenshot shows the 'Admin Configuration' page with a 'System' sidebar. The 'System Information' section contains three input fields: 'System Name' (AP981X), 'Description' (InWall AP WiFi,G ,500mW), and 'Location' (default). The 'Admin Password' section has 'New Password' and 'Check New Password' fields 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' (Port: 80) and 'Enable Telnet' (Port: 23). 'Save' and 'Reset' buttons are at the bottom right.

■ 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 close-up shows the 'Admin Password' section with two input fields: 'New Password:' and 'Check New Password:'. A note next to the first field reads: '(If you don't want to change , don't type anything)'.

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

- **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.

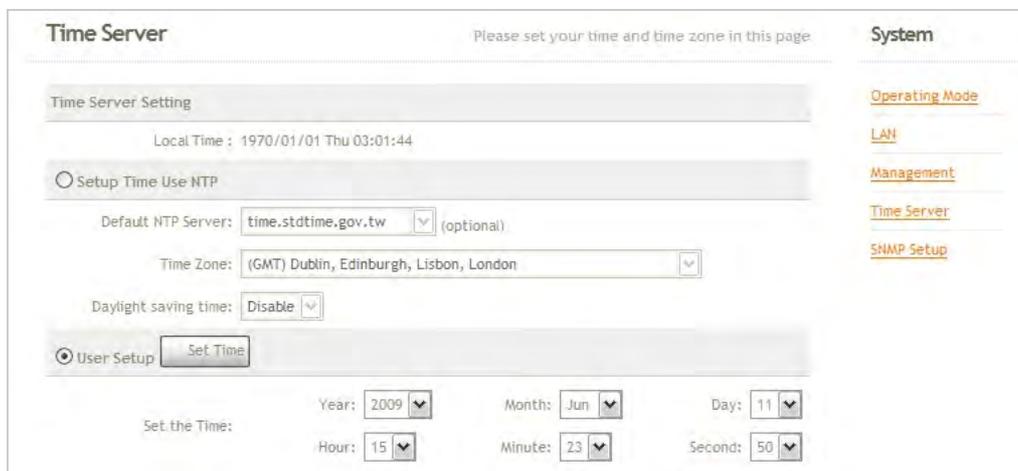
Admin Login Methods	
<input checked="" type="checkbox"/> Enable HTTP	Port : <input type="text" value="80"/> (Default:80)
<input checked="" type="checkbox"/> Enable Telnet	Port : <input type="text" value="23"/> (Default:23)

- **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.
- **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.



- **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 Setup**, **Advanced Setup**, **WDS Setup**.

The screenshot shows a web-based configuration interface for wireless settings. At the top, there is a navigation bar with tabs for [System](#), [Wireless](#), [Utilites](#), [Status](#), and [Reboot](#). The main heading is **Wireless Setup**. On the right side, there is a **Sub Menu** with links for [General Setup](#), [Advanced Setup](#), and [WDS Setup](#). The **General Setup** section is highlighted and contains 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)

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.

- **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, WDS 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 WDS's RF general settings and will be applied to all WDS Links.

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.

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](#)

[WDS Setup](#)

- **Slot Time** : Enter the desired slot time for the WDS.
- **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 WDS.



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 access point 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.
- **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 is for WDS's RF general settings and will be applied to all WDS Links.

4.2.3 WDS Setup

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

Wireless Setup

WDS Setup

WMM : Enable Disable

Security Type :

Enable	WDS 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="checkbox"/>	02. <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="checkbox"/>	04. <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="checkbox"/>	06. <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="checkbox"/>	08. <input type="text"/> : <input type="text"/>	<input type="text"/>	<input type="text"/>

Sub Menu

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

- **WMM** : Select Enable, the packets with QoS WMM will has higher priority.
- **Security Type** : Configure an appropriate security type for the WDS link, either **Disabled** or **WEP**; the type needs to be the same as that configured on WDS 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 WDS link.
- **WDS Peer's MAC Address** : Enter the MAC address of WDS 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 WDS link.

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

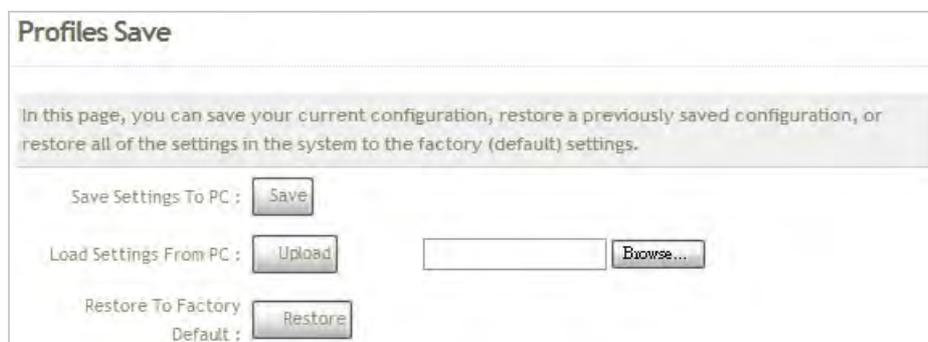
4.3 Utilities

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 AP981X/AP981WX, 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.

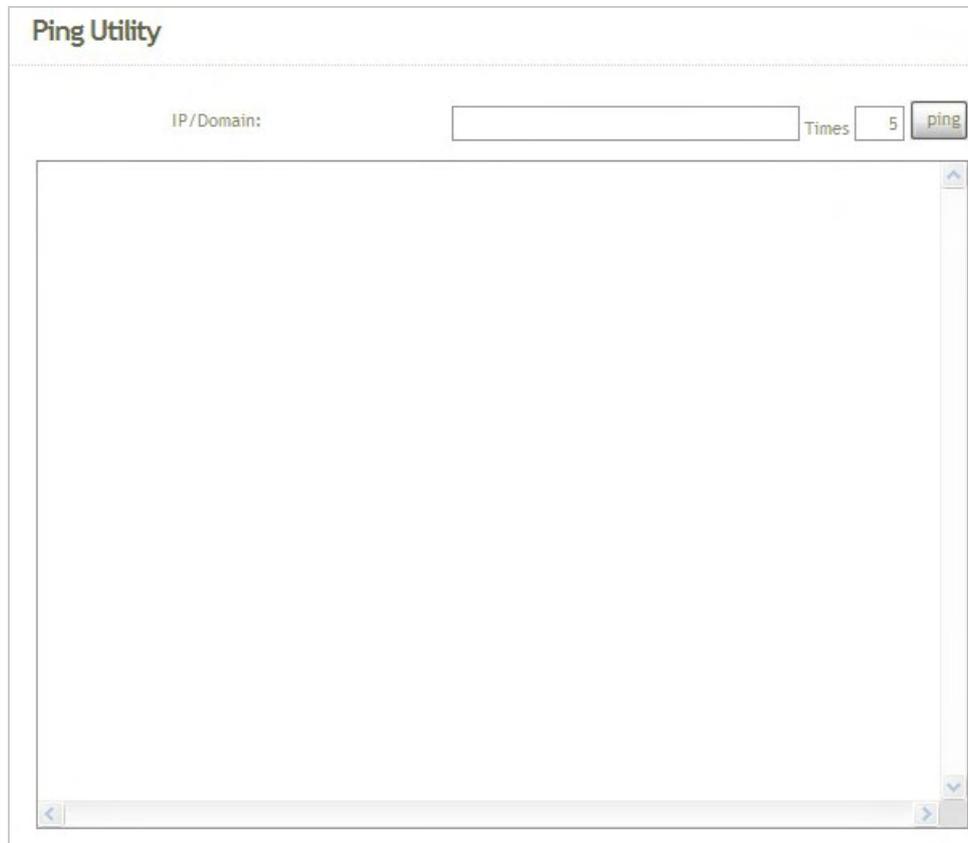
Firmware Upgrade	Utilities
<p>From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local hardisk.</p> <p>Firmware Version: Cen-AP-G2H5 Beta V0.0.5</p> <p>Firmware Date: 2009-07-16 03:24:29</p> <p>Update Firmware: <input type="text"/> <input type="button" value="浏览..."/></p> <p><input type="button" value="Upgrade"/> <input type="button" value="Clear"/></p>	<p>Profile Setting</p> <p>System Upgrade</p> <p>Ping Utility</p> <p>Reboot</p>

**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.



The screenshot shows a web interface titled "Ping Utility". It features a form with the following elements:

- A label "IP/Domain:" followed by a text input field.
- A label "Times" followed by a numeric input field containing the value "5".
- A "ping" button.
- A large, empty rectangular area below the form, which serves as the "Result" field for displaying the ping output.

- **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 AP981X/AP981WX. 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 current system settings can be over viewed via this page; statuses of **Overview**, **WDS List**, and **Event Log** are displayed in this interface.

The screenshot displays the web interface for the AP981X/AP981WX. At the top, a dark green navigation bar contains the following tabs: [System](#), [Wireless](#), [Utilities](#), [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: AP981X
 - Operating Mode: WDS mode
 - Firmware Version: Cen-AP-G2H5 Beta V0.0.5
 - Firmware Date: 2009-07-16 03:24:29
 - Location: default
 - Description: InWall AP WiFi,G ,500mW
 - System Time: 1970/01/01 Thu 00:00:44
 - System Up Time: 44
- LAN Information**
 - MAC Address: 00:11:a3:07:01:03

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

4.4.1 Overview

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

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

System
System Name: AP981X
Operating Mode: WDS mode
Firmware Version: Cen-AP-G2H5 Beta V0.0.5
Firmware Date: 2009-07-16 03:24:29
Location: default
Description: InWall AP WiFi,G ,500mW
System Time: 1970/01/01 Thu 00:00:44
System Up Time: 44

- **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.

4.4.2 WDS List

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

WDS Link Status				
WDS 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

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

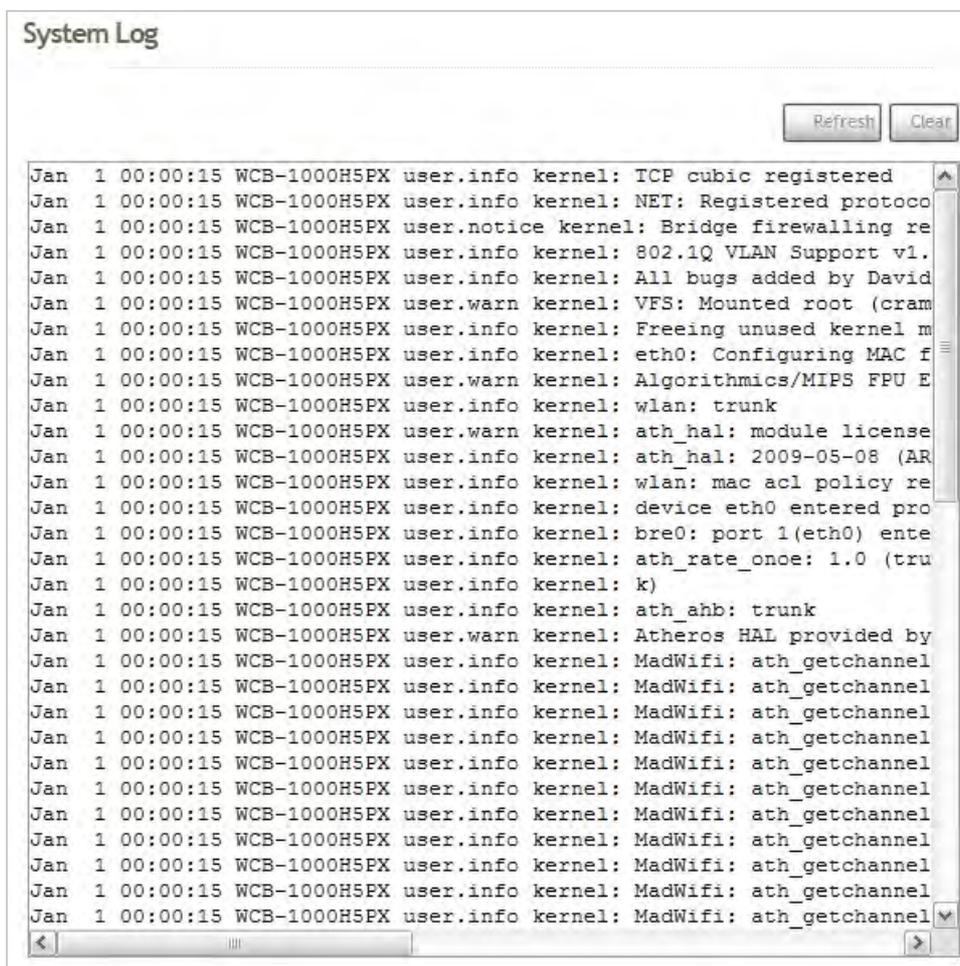


Note :

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

4.4.3 Event Log

The reported system events can be reviewed here.



The screenshot shows a 'System Log' window with a scrollable list of events. At the top right, there are 'Refresh' and 'Clear' buttons. The log entries are as follows:

```

Jan 1 00:00:15 WCB-1000H5PX user.info kernel: TCP cubic registered
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: NET: Registered protocol family 10
Jan 1 00:00:15 WCB-1000H5PX user.notice kernel: Bridge firewalling rules
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: 802.1Q VLAN Support v1.3
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: All bugs added by David
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: VFS: Mounted root (crashfs) on
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: Freeing unused kernel memory
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: eth0: Configuring MAC filter
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: Algorithmics/MIPS FPU Emulation
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: wlan: trunk
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: ath_hal: module license
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: ath_hal: 2009-05-08 (AR7131)
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: wlan: mac acl policy registered
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: device eth0 entered promiscuous
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: br0: port 1(eth0) entered
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: ath_rate_onoff: 1.0 (true)
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: k
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: ath_ahb: trunk
Jan 1 00:00:15 WCB-1000H5PX user.warn kernel: Atheros HAL provided by
Jan 1 00:00:15 WCB-1000H5PX user.info kernel: MadWifi: ath_getchannel

```

- **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.

5. Command Line Interface(CLI)

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

5.1 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.



3. Enter username and password on the Telnet session. And the command line session appears. The default username is "**admin**", and password is "**default**"

5.2 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 informations
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 5-1: 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.
 - ✓ **AP Mode :** Enable all of Virtual AP, 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      34    0      0     0     0     0
hwe0   137        155      32    0      0     0     0     0
wifi0  528        64       32    0      0     0     0     0
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       38    0      0     0     0     0
ath6   0          0       38    0      0     0     0     0
ath7   0          0       38    0      0     0     0     0

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

```



```
Ping :>
-----
Destination : _____
Specify Packet Size <-s> : _____
Flood Ping <-f> : [ ]

'-': Up, '=': Down, '/': Del, Space, Enter
```

- ✓ **Destination** : Enter the specify destination.
- ✓ **Specify Packet Size** : Enter specify packet size.
- ✓ **Flood Ping** : Click **Space** to enable or disable flood ping.

Click **Enter** to activated function. The processing of ping will be activated.

```
Pinging [192.168.2.1] -s 1472 -flood <'I' to Stop>
```

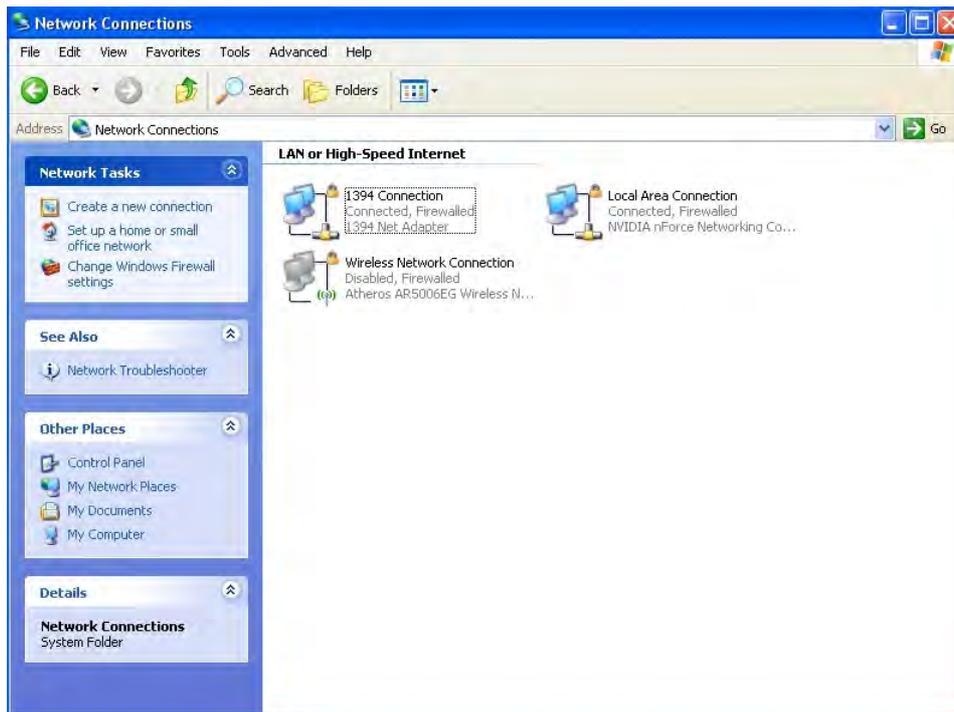
Click **I** to stop precessing, and the statistic of ping will be display.

```
>> 6693 packets transmitted, 6688 packets received, 0% packet loss
>> round-trip min/avg/max = 3.1/7.8/67.0 ms
[ Approximate Throughput = 3076923 b/s = 3076 kb/s ]
```

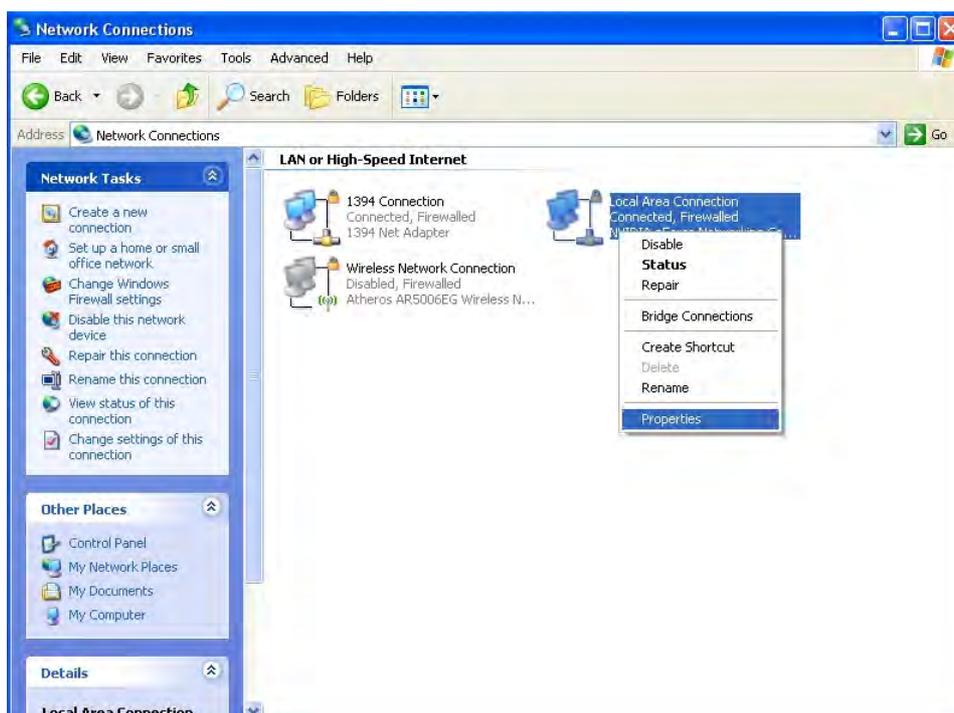
Appendix A. Windows TCP/IP Settings

■ Windows XP

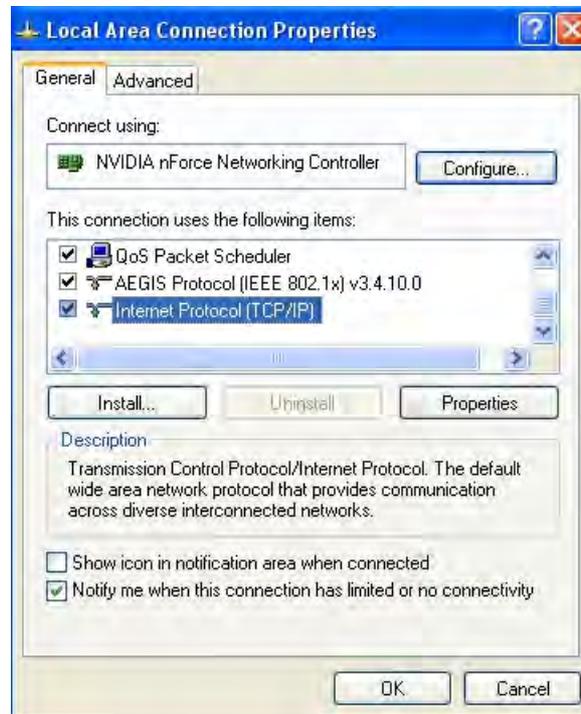
1. Click **Start -> Settings -> Control Panel**, and then “**Control Panel**” window appears. Click on “**Network Connections**”, and then “**Network Connections**” window appears.



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



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



- 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 B 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 @ - _ .
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/RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . =
	RO/RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . =
	RO/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 B Valid Characters for using WMI (continued)

Block	Field	Valid Characters
Advanced Setup	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
Virtual AP 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	
WDS 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

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)

Federal Communications Commission (FCC) Statement

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

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.