# MOXA AirWorks AWK-1200-AP
# User's Manual

# *www.moxa.com/product*

**First Edition, July 2007**

**Moxa Networking Co., Ltd.**
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231
Web: www.moxa.com

**MOXA Technical Support**
Worldwide:       support@moxa.com
The Americas     support@usa.moxa.com

# MOXA AirWorks AWK-1200-AP
# User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

## Copyright Notice

Copyright © 2007 Moxa Networking Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

## Trademarks

MOXA is a registered trademark of the Moxa Group.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

## Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of MOXA.

MOXA provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. MOXA reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, MOXA assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

# Table of Contents

# 1

# Introduction

The following topics are covered in this chapter:

- ❑ **Overview**
- ❑ **Package Checklist**
- ❑ **Product Features**
- ❑ **System Requirements**
- ❑ **Inline Power Injector (PoE)**

# Overview

The AWK-1200 Access Point/Bridge and AP Client is ideal for applications that are hard to wire, too expensive to wire, or use mobile equipment that connects to a TCP/IP network. The AWK-1200 series is rated to operate at temperatures ranging from -20 to 70°C, and its weatherproof design allows you to set up a WLAN, or extend existing wired networks to outdoor locations. In addition, you do not need to worry about setting up a power supply for outdoor applications, since the AWK-1200's PoE (Power over Ethernet) design makes it easy to deploy.

# Package Checklist

The product package contains the following items.

- AWK-1200-AP
- Power cord
- 48 VDC, 0.38A Inline Power Injector (PoE)
- 30 m RJ45 CAT-5 Ethernet cable
- 1.8 m RJ45 CAT-5 cross-over cable
- 3 m grounding wire
- Document and Software CD
- Wall/mast mounting kit
- Band clamp
- Two 5dBi Omni-type antennas (N-type connector)

# Product Features

- Outdoor enclosure in compliance with versatile industrial IP (Ingress Protection) level covering IP68
- RF transmit power: 802.11b mode @ 11 Mbps data rate
- RF transmit power: 802.11g mode @ 54 Mbps data rate
- Supports 48 VDC 0.38A Power-over-Ethernet (PoE)
- MIB-I support
- MAC address based access control

# System Requirements

Installing the AWK-1200-AP requires the following:

- Windows-based PC/AT compatible computer (PC system requirements: better than PIII 800 or other 100% compatible equipment; OS: Windows 2000/XP), or Ethernet data device that has an RJ45 Ethernet port to run the configuration program or a TCP/IP connection to the Ethernet network.
- 10/100 Base-T Ethernet RJ45 Ethernet cable for connecting to an Ethernet network.
- AC power outlet (100 to 240V, 50 to 60 Hz) to supply power.

# Inline Power Injector (PoE)

The AWK-1200-AP is equipped with an Inline Power Injector module. The Inline Power Injector (PoE) delivers both data and power to the AWK-1200-AP unit through a single Ethernet cable, and provides the following benefits to improve the performance vs. installation cost ratio.

- Great for areas that do not have a ready power supply, such as the roof of a house.
- Allows placing the AWK-1200-AP unit closer to the antenna, to make installation easier, and reduce signal loss over antenna cabling.
- Ethernet signal travels well over CAT 5 cable but 2.4 GHz signal doesn't do as well over antenna cabling.
- Ethernet cabling is much cheaper than antenna cabling.

# 2

# Getting Started

This chapter describes the procedures for installing the AWK-1200-AP.

The following topics are covered:

❑ **First Time Installation and Configuration**
❑ **Locating the Data Input and PoE Ports**
❑ **What to Check before You Install the AWK-1200-AP**
❑ **Basic Configuration**
   ➢ Basic Configuration Steps
   ➢ Logging into the Web Interface
   ➢ Configuring Operating Mode, IP Address, Subnet Mask, Default Route IP, DNS Server IP
   ➢ Configuring the Wireless SSID
   ➢ Configuring Wireless Encryption
   ➢ Changing the Supervisor Account & Password
   ➢ Upgrading the Firmware

# First Time Installation and Configuration

After unpacking the system, make sure the following items are present and in good condition. Refer to pictures below to see what each item looks like.

1. AWK-1200-AP
2. Power cord
3. 48 VDC, 0.38A Inline Power Injector (PoE)
4. 30 m RJ45 CAT-5 Ethernet cable
5. 1.8 m RJ45 CAT-5 cross-over cable
6. 3 m grounding wire
7. Document and Software CD
8. Wall/mast mounting kit
9. Screws
10. Two 5 dBi Omni-type antennas (N-type connector)

| 1. AWK-1200-AP | 2. Power cord | 3. PSE Injector | 4. 30 m cable |
|---|---|---|---|
| | | | |
| **5. 1.8 m cable** | **6. Grounding wire** | **7. CD** | **8. Wall mount** |
| | | | |
| **9. Screws** | **10. Antenna** | | |
| | | | |
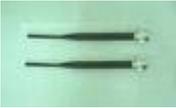
# Locating the Data Input and PoE Ports

After unpacking the system, locate the following ports on the AWK-1200-AP unit. The numbers next to each item refer to the pictures in Figure 2-1.
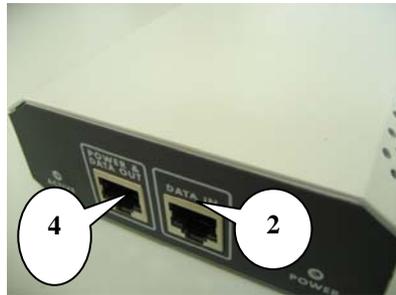
### Interface on the AWK-1200-AP Unit

- **Ethernet Port 1**: for connecting the 30 m RJ45 CAT-5 Ethernet cable.

### Interface on the Inline Power Injector

- **Data Input Port 2**: for connecting the cross-over Ethernet Cable to a PC or straight-through Ethernet cable to a Hub, Switch, or Router.
- **DC Input Port 3**: power adaptor; 48V, 0.38A DC input.
- **Power & Data Output Port 4**: for connecting the 30 m RJ45 CAT-5 Ethernet cable.

## Device Figures



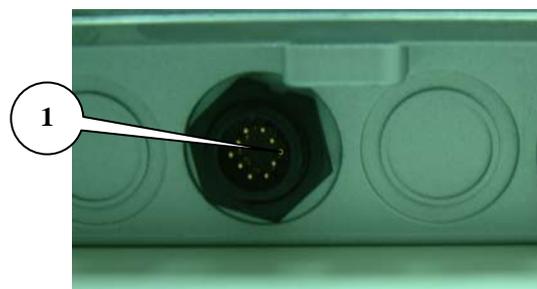**POE picture1**                                          **POE picture2**



**Figure 2-1**

*Power and Data Interface location on the PoE denoted by numbers 1-4.*

## Mounting the AWK-1200-AP on a Wall or Mast

- The AWK-1200-AP can be mounted on the wall, and you can use the Wall Mount kit to mount the AWK-1200-AP as shown in **Figure 2-2**.
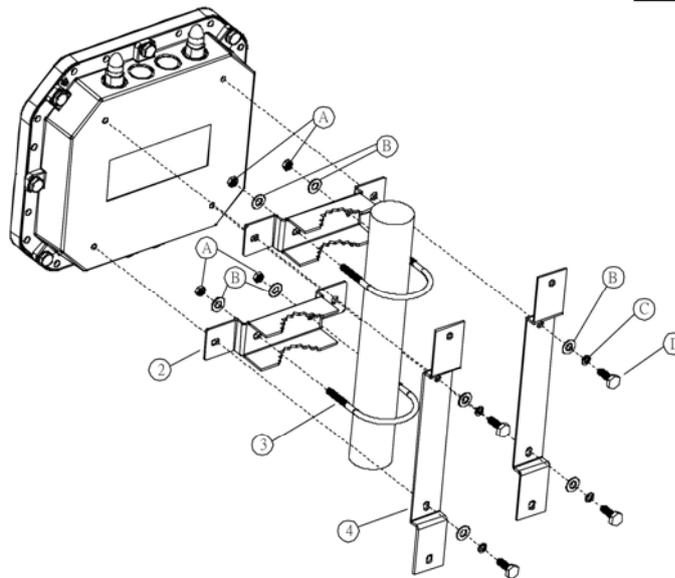


**Figure 2-2**

2-3

# What to Check before You Install the AWK-1200-AP

Before installing the AWK-1200-AP for outdoor applications or hard-to-reach locations, we recommend configuring and testing all devices first.

For configuring the AWK-1200-AP, please follow the steps below to power up the AWK-1200-AP (refer to Figure 2-4).

**Step 1:**
Connect the DC plug of the AC/DC power adapter into the **DC Input Port** of the Inline Power Injector and the wall-mount plug into a power outlet or power strip (refer to page 2-2). The Power LED on the Inline Power Injector will light up.

**Step 2:**
Run the cross-over Ethernet cable from the **Data Input Port** (refer to page 2-2) to the Ethernet port on a PC.

**Step 3:**
Connect the 30 m CAT 5 Ethernet cable to the AWK-1200-AP. Hand tighten the connector.

**Step 4:**
Connect the other end of the 30 m CAT 5 cable to the PoE labeled POWER & DATA OUT. This is the power side of the PoE that will power up the AWK-1200-AP.

When the AWK-1200-AP receives power over the Ethernet cable, the AWK-1200-AP will start the boot up sequence, and the Active LED on the Inline Power Injector will light up.

You can use a web browser, such as Microsoft Internet Explorer or Netscape Navigator, to configure the AWK-1200-AC from a remote host or PC.
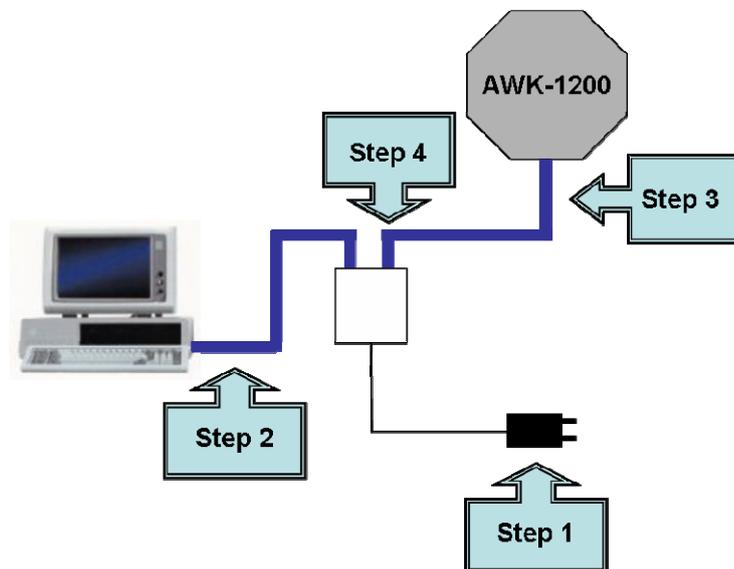
**Figure 2-4**

# Basic Configuration

## Basic Configuration Steps

This section describes a basic 2-step configuration procedure to set up the AWK-1200-AP.

**Step 1:**
Modify the factory-default parameters on the web page **"/BASIC/LAN/"**, click **Save Settings** to save the changes, and then click **Continue**.

**Step 2:**
Modify the factory-default parameters on the web page **"/BASIC/Wireless/"**, click **Save Settings** to save the changes, and then click **Reboot the Device** to take activate the configuration changes.

## Logging into the Web Interface

Users can access and configure the AWK-1200-AP through a web browser interface.
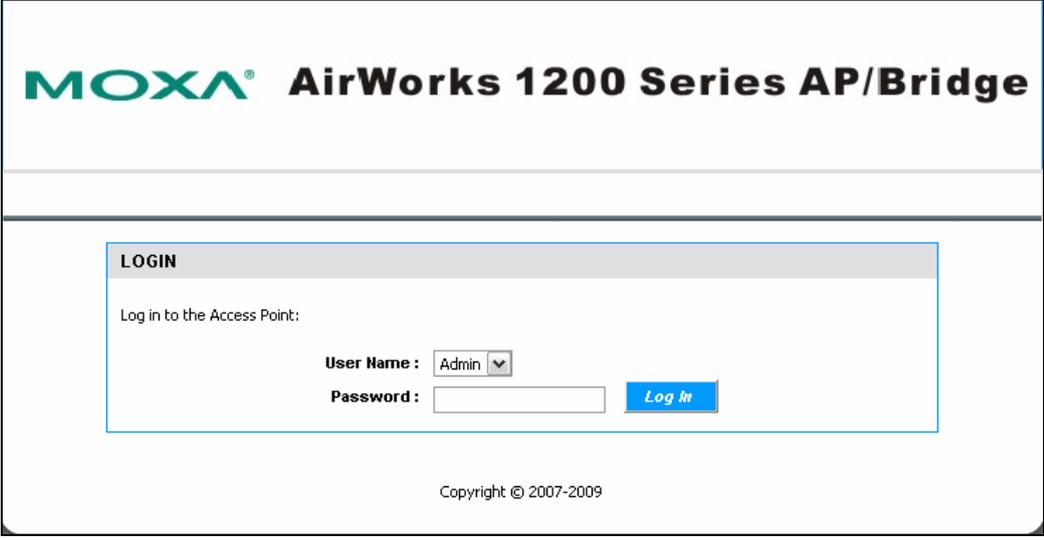
### Web Configuration

Before configuring the AWK-1200-AP, you need to know the IP Address assigned to the unit. The factory default IP Address is **192.168.127.253**. To establish a connection, type **http://192.168.127.253** in the browser's address field.

### Web Access Procedures

Once you identify the IP Address assigned to the AWK-1200-AP, use the web browser to configure the AWK-1200-AP through the browser Interface. The following procedure explains how to configure each item.

**Step 1:** Open your browser and enter the IP address.

**Step 2:** Press <**ENTER**>. The AWK-1200-AP **Login** screen should appear as shown in **Figure 2-5**.



**Figure 2-5**

**Step 3:** Enter **"root"** in the **Password** fields, and then click **Log In** to enter the web configuration user interface screen as shown below.
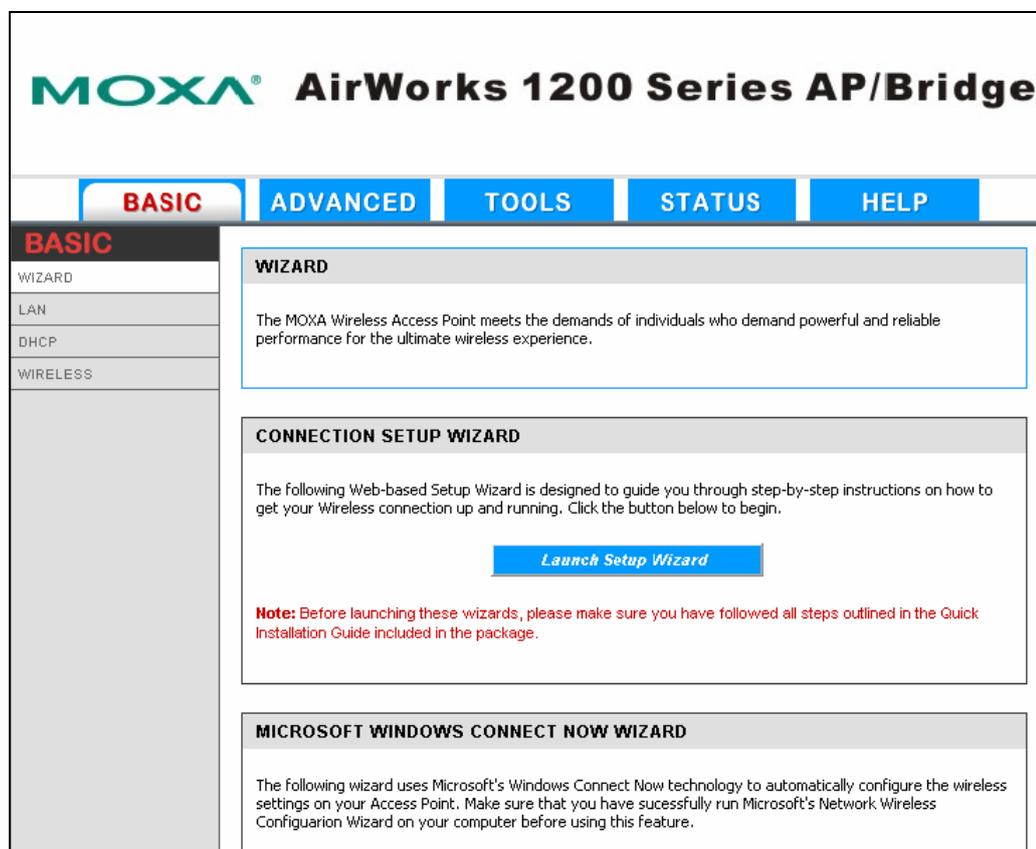


Figure 2-6

## Web Configuration Structure

The web configuration user interface shown above in **Figure 2-6** is grouped into a tree structure, and contains the following settings or information.

- **BASIC**
  - ➢ WIZARD
  - ➢ LAN
  - ➢ DHCP
  - ➢ WIRELESS
- **ADVANCED**
  - ➢ MAC ADDRESS FILTER
  - ➢ ADVANCED WIRELESS
- **TOOLS**
  - ➢ ADMIN
  - ➢ TIME
  - ➢ SYSTEM
  - ➢ FIRMWARE

- **STATUS**
  - ➤ DEVICE INFO
  - ➤ WIRELESS
  - ➤ LOGS
  - ➤ STATISTICS
- **HELP**
  - ➤ MENU
  - ➤ BASIC
  - ➤ ADVANCED
  - ➤ TOOLS
  - ➤ STATUS
  - ➤ GLOSSARY

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

# Configuring Operating Mode, IP Address, Subnet Mask, Default Route IP, DNS Server IP

## LAN Settings

The LAN (Local Area Network) settings for the Access Point are **IP Address Mode**, **IP Address**, **Subnet Mask**, and **Default Gateway**. The Access Point's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. This option is available in the **"/BASIC/LAN/"** page as shown in **Figure 2-7**.



**Figure 2-7**

*Get LAN IP From*

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

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

*IP Address*

The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.0.1.

*Subnet Mask*

The subnet mask of the local area network.

*Gateway*

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

*Local Domain Name*

This entry is optional. Enter a domain name for the local network. The AP's DHCP server will give this domain name to the computers on the wireless LAN. So, for example, if you enter mynetwork.net here, and you have a wireless laptop with a name of chris, that laptop will be known as chris.mynetwork.net. Note, however, that if the AP's settings specify **DHCP (Dynamic)** Address, and the router's DHCP server assigns a domain name to the AP, that domain name will override any name you enter here.

# Configuring the Wireless SSID

## Wireless Network Name (also called the SSID)

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, we highly recommend that you change the pre-configured network name. This option is available in the "**/BASIC/WIRELESS/**" page as shown in **Figure 2-8**.

**Figure 2-8**

## Configuring Wireless Encryption

The AWK-1200-AP supports 64-bit and 128-bit WEP encryption.

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

For **128-bit** WEP encryption, an encryption key consists of 26 hexadecimal characters (0-9 and A-F) or 13 ASCII characters.

Modify the WEP encryption parameters on the web page **"/BASIC/WIRELESS/WIRELESS SECURITY MODE"**. If you choose "WEP" enter 1 to 15 characters in the **WEP Key** field, and then click **Save Setting**, **Reboot the Device**.

## Changing the Supervisor Account & Password

Enter the **TOOLS → ADMIN** page, shown below in **Figure 2-9**.



**Figure 2-9**

### ADMIN PASSWORD

Change the ADMIN PASSWORD's user name and password in the **ADMIN PASSWORD Account** field, click **Save Setting**, and then **Reboot the Device** to take activate the configuration changes.

## Upgrading the Firmware

### Updating the Firmware

Enter the **TOOLS → FIRMWARE** page as shown in **Figure 2-10** to upgrade the AWK-1200-AP's firmware. You must select which file (**Program image**) you want to upgrade, and then click the **Upload** button to start the upgrade process.

---

**NOTE**     It takes about 1 minute to complete the restart process.

---



**Figure 2-10**

---

⚠️ **ATTENTION**

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

---

⚠ **ATTENTION**

To meet regulatory restrictions and the safety of the installation, we strongly recommend this product is **professionally installed**.

# 3

# Web Console Configuration

In this chapter, we will explain each web management page of the Web-based Network Manager.

The following topics are covered in this chapter:

- ❑ **Basic**
  - ➢ Wireless
  - ➢ Advanced
- ❑ **Tools**
  - ➢ Admin
  - ➢ Time
  - ➢ System
  - ➢ Firmware
- ❑ **Status**
  - ➢ Device Info
  - ➢ Wireless
  - ➢ Logs
  - ➢ Statistics

# Basic

## Wireless

The section is where you configure the wireless settings for your Access Point. Please note that changes made in this section may also need to be duplicated on your Wireless Client.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server.

```
BASIC WIRELESS SETTINGS

     Wireless Network Name :   EDS7728            (Also called the SSID)
         Visibility Status :   ⊙ Visible  ○ Invisible
       Auto Channel Select :   ☐
                   Channel :   2.437 GHz - CH 6  ▾
         Transmission Rate :   Best (automatic) ▾  (Mbit/s)
              802.11 Mode :   Mixed 802.11g and 802.11b ▾
            Super G™ Mode :   Super G without Turbo ▾
```

*Enable Wireless Radio*
This option turns off and on the wireless connection feature of the Access Point. When you set this option, the following parameters are displayed.

*Wireless Network Name*
When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, as described below). This name is also referred to as the SSID. For security purposes, we highly recommend changing the pre-configured network name.

*Visibility Status*
The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

*Auto Channel Select*
If you select this option, the Access Point automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the Access Point uses the channel that you specify with the following **Channel** options.

*Channel*
A wireless network uses specific channels in the 2.4 GHz wireless spectrum to handle communication between clients. Some channels in your area may get interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

*Transmission Rate*
By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

### *802.11 Mode*

If all of your devices can connect in 802.11g Mode, you can change the mode to 802.11g only. If you have some devices that are 802.11b, leave the setting at Mixed.

### *Super G™ Mode*

**Super G without Turbo:** Performance enhancing features such as Packet Bursting, FastFrames, and Compression.

### *WEP*

WEP is a method of encrypting data for wireless communication, and is intended to provide the same level of privacy as a wired network. However, WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so that you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

**Example:**

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)



### *WPA-Personal and WPA-Enterprise*

Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The **WPA Mode** further refines the variant that the Access Point should employ.

**WPA Mode:** WPA is the older standard; select this option if the clients that will be used with the Access Point only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the Access Point tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the Access Point associates only with clients that also support WPA2 security.

**Cipher Type:** The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the Access Point negotiates the cipher type with the client, and uses AES when available.

**Group Key Update Interval:** The amount of time before the group key used for broadcast and multicast data is changed.

*WPA-Personal*

This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

**Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

**Example:**

**Wireless Networking technology enables ubiquitous communication**



*WPA-Enterprise*

This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

**Authentication Timeout:** Amount of time before a client will be required to re-authenticate.

**RADIUS Server IP Address:** The IP address of the authentication server.

**RADIUS Server Port:** The port number used to connect to the authentication server.

**RADIUS Server Shared Secret:** A pass-phrase that must match with the authentication server.

**MAC Address Authentication:** If this is selected, the user must connect from the same computer whenever logging into the wireless network.

**Advanced:**

**Optional Backup RADIUS Server**

**3-4**

This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding. The fields **Second RADIUS Server IP Address, RADIUS Server Port, Second RADIUS server Shared Secret, Second MAC Address Authentication** provide the corresponding parameters for the second RADIUS Server.

**WPA**

WPA requires stations to use high grade encryption and authentication. NOTE: WDS will not function with WPA security.

WPA Mode : WPA
Cipher Type : TKIP
Group Key Update Interval : 3600 (seconds)

**EAP (802.1X)**

When WPA enterprise is enabled, the Access Point uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : 60 (minutes)
RADIUS server IP Address : 0.0.0.0
RADIUS server Port : 1812
RADIUS server Shared Secret : radius_shared
MAC Address Authentication : ☑
Advanced >>

# Advanced

### MAC Address Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adaptor(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adaptor.

**MAC ADDRESS FILTER**

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

Save Settings    Don't Save Settings

**ENABLE**

Enable MAC Address Filter : ☐

### Enable MAC Address Filter

When this is enabled, computers are granted or denied network access depending on the mode of the filter.

**NOTE**    Configuring this feature incorrectly could prevent machines from accessing the network. In this case, you can regain access by activating the factory defaults button on the Access Point itself.

**3-5**

*Filter Settings*

**Mode**

When "only allow listed machines" is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When "only deny listed machines" is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.

**Filter Wireless Clients**

When this option is selected, the MAC address filters will be applied to wireless network clients.

**Filter Wired Clients**

When this option is selected, the MAC address filters will be applied to wired network clients.

*Add/Edit MAC Address*

In this section, you can add entries to the MAC Address List below, or edit existing entries.

**Enable**

MAC address entries can be activated or deactivated with this checkbox.

**MAC Address**

Enter the MAC address of the desired computer or connect to the Access Point from the desired computer, and then click the **Copy Your PC's MAC Address** button.

**Save**

Saves the new or edited MAC Address entry in the following list. When you finish updating the MAC Address List, you must still click the **Save Settings** button at the top of the page to activate the changes.

*MAC Address List*

The section lists the current MAC Address filters. A MAC Address entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit MAC Address" section is activated for editing.

*Advance Wireless*



**3-6**

*Fragmentation Threshold*

This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance.

*RTS Threshold*

This setting should remain at its default value of 2346. If you encounter inconsistent data flow, only minor modifications to the value are recommended.

*Beacon Period*

Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value of between 20 and 1000. The default value is set to 100 milliseconds.

*DTIM Interval*

A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

*802.11d Enable*

Enables 802.11d operation. 802.11d is a wireless specification for operation in additional regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains, or countries). The current 802.11 standard defines operation in only a few regulatory domains (countries). This supplement adds the requirements and definitions necessary to allow 802.11 WLAN equipment to operate in markets not served by the current standard. Enable this option if you are operating in one of these "additional regulatory domains."

*Transmit Power*

Normally, the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

*WDS Enable*

When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel number.

*WDS AP MAC Address*

Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.

**3-7**

# Tools

## Admin

The Admin option is used to set a password for access to the Web-based management. By default, no password configured. We highly recommend that you create a password to keep your new Access Point secure.



### *Admin Password*

Enter a password for the user "admin". This user will have full access to the web-based management interface.

### *User Password*

Enter a password for the user "user". This user will have read-only access to the web-based management interface.

### *Access Point Name*

The name of the Access Point can be changed here.

### *Admin Idle Timeout*

The amount of time before the administration session (either remote or local) is closed when there is no activity.

### *Save Configuration*

This option allows you to save the Access Point's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

*Restore Configuration from File*
Use this option to load previously saved Access Point configuration settings.

*Save Configuration To Wireless Network Setup Wizard*
If your PC's operating system is Windows XP Service Pack 2 (SP2) or later and you are using Windows Internet Explorer (IE) as your browser, you can use this option to save key parts of the Access Point's current wireless security settings to your PC with Windows Connect Now (WCN) technology. The settings will then be available to propagate to other wireless devices.

## Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the Access Point's internal system clock.



### Set the Date and Time Manually

If you do not have the NTP Server option in effect, you can either manually set the time for your Access Point here, or you can click the **Copy Your Computer's Time Settings** button to copy the time from the computer you are using. (Make sure that computer's time is set correctly.)

| NOTE | If the Access Point loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain the correct time for schedules and logs, you must either enter the correct time after you restart the Access Point, or you must enable the NTP Server option. |
|---|---|

## System

This section allows you to reboot the device, and restore the Access Point to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

**SYSTEM**

**System Settings**

The System Settings section allows you to reboot the device, or restore the Access Point to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

**SYSTEM COMMANDS**

> **Reboot the Device**

> **Restore all Settings to the Factory Defaults**

*Reboot the Device*

This restarts the Access Point. Useful for restarting when you are not near the device.

*Restore all Settings to the Factory Defaults*

This option restores all configuration settings back to the settings that were in effect at the time the Access Point was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your Access Point configuration settings, you can do so from the **Tools →
Admin** page.

# Firmware

The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance.

**FIRMWARE**

**Firmware Upgrade**

The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance.

> **Save Settings**     **Don't Save Settings**

**FIRMWARE INFORMATION**

Current Firmware Version : Moxa_FW_ver 1.0.1
Current Firmware Date : 2007/07/03

**FIRMWARE UPGRADE**

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools -> Admin screen.

To upgrade the firmware, your PC must have a wired connection to the Access Point. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload : [                    ] [瀏覽...]

**Upload**

**3-10**

To upgrade the firmware, follow these steps:

1. Click the **Browse** button to locate the upgrade file on your computer.

2. Once you have found the file to be used, click the **Upload** button below to start the firmware upgrade process. This could take a minute or more.

3. Wait for the Access Point to reboot. This can take another minute or more.

4. Confirm the updated firmware revision on the status page.

*Firmware Information*
The version numbers of the firmware currently installed in your Access Point and the most recent upgrade that is available are displayed here.

*Firmware Upgrade*

| NOTE | Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the Access Point by wire. |
|------|---|

| NOTE | Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the **Tools → Admin** screen. |
|------|---|

*Upload*
Once you have a firmware update on your computer, use this option to browse to the file, and then upload the information to the Access Point.

# Status

## Device Info

All of your Internet and network connection details are displayed on the Device Info page. The firmware version is also displayed here.

| NOTE | Some browsers have limitations that make it impossible to update the WAN status display when the status changes. Some browsers require that you refresh the display to obtain updated status. Some browsers report an error condition when trying to obtain WAN status. |
|------|---|

**DEVICE INFO**

**Device Information**

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

**GENERAL**

Time : 2004年1月31日 上午 11:46:36
Firmware Version : Moxa_FW_ver  1.0.1 , 2007/07/03

**LAN**

MAC Address : 00:40:C7:FD:00:84
IP Address : 192.168.127.253
Subnet Mask : 255.255.255.0
DHCP Server : Enabled
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0

*LAN Computers*

This area of the screen continually updates to show all DHCP enabled computers and devices connected to the LAN side of your Access Point. The detection "range" is limited to the address range as configured in DHCP Server. Computers that have an address outside of this range will not appear. If the DHCP Client (i.e. a computer configured to "Automatically obtain an address") supplies a Host Name then that will also be shown. Any computer or device that has a static IP address that lies within the detection "range" may show, however its host name will not.

## Wireless

The wireless section allows you to view the wireless clients that are connected to your wireless Access Point.

*MAC Address*

The Ethernet ID (MAC address) of the wireless client.

*IP Address*

The LAN-side IP address of the client.

*Mode*

The transmission standard being used by the client. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively.

*Rate*

The actual transmission rate of the client in megabits per second.

*Signal*

This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the Access Point and the wireless device.

**3-12**

**WIRELESS**

**Associated Wireless Client List**

Use this option to view the wireless clients that are connected to your wireless Access Point.

**NUMBER OF WIRELESS CLIENTS : 0**

| MAC Address | IP Address | Mode | Rate | Signal(%) |
|---|---|---|---|---|

# Logs

The Access Point automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the Access Point logs. You can define what types of events you want to view and the level of events to view. This Access Point also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

**LOGS**

**System Logs**

Use this option to view the Access Point logs. You can define what types of events you want to view and the event levels to view. This Access Point also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

**LOG OPTIONS**

**What to View :** ☑ System

**View Levels :** ☑ Critical ☑ Warning ☑ Informational

[ Apply Log Settings Now ]

**LOG DETAILS**

[ Refresh ]   [ Clear ]   [ Save Log ]

[INFO] Sat Jan 31 11:48:54 2004 Log viewed by IP address 192.168.127.222
[INFO] Sat Jan 31 10:47:37 2004 Allowed configuration authentication by IP address 192.168.127.222
[INFO] Sat Jan 31 10:46:12 2004 Initialization complete, starting DHCP server
[INFO] Sat Jan 31 10:46:10 2004 DHCP Server Parameter 19 was added to the parameter database
[INFO] Sat Jan 31 10:46:10 2004 DHCP Server Parameter 3 was added to the parameter database
[INFO] Sat Jan 31 10:46:10 2004 DHCP Server Parameter 1 was added to the parameter database
[INFO] Sat Jan 31 10:46:06 2004 Device initialized
[INFO] Sat Jan 31 10:46:06 2004 Wireless Link is up
[INFO] Sat Jan 31 10:46:06 2004 Stored configuration to non-volatile memory
[INFO] Thu Jan 01 00:00:00 1970 Loaded configuration from non-volatile memory

***What to View***

Select the kinds of events that you want to view.

> System

***View Levels***

Select the level of events that you want to view.

> Critical
> Warning
> Informational

***Apply Log Settings Now***

**3-13**

Click this button after changing Log Options to make them effective and permanent.

### Refresh

Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.

### Clear

Clicking this button erases all log entries.

### Save Log

Select this option to save the Access Point log to a file on your computer.

## Statistics

The Statistics page displays all of the LAN, WAN, and Wireless packet transmit and receive statistics.

**STATISTICS**

**Network Traffic Stats**

Traffic Statistics display Receive and Transmit packets passing through your Access Point.

| Refresh Statistics | Clear Statistics |
|---|---|

**LAN STATISTICS**

| | |
|---|---|
| Sent : 3313 | Received : 4609 |
| TX Packets Dropped : 0 | RX Packets Dropped : 0 |
| Collisions : 0 | Errors : 0 |

**WIRELESS STATISTICS**

| | |
|---|---|
| Sent : 2242 | Received : 0 |
| TX Packets Dropped : 0 | Errors : 0 |

### Sent

The number of packets sent from the Access Point.

### Received

The number of packets received by the Access Point.

### TX Packets Dropped

The number of packets that were dropped while being sent due to errors, collisions, or Access Point resource limitations.

### RX Packets Dropped

The number of packets that were dropped while being received due to errors, collisions, or Access Point resource limitations.

### Collisions

The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).

*Errors*

The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.

# A
# Specifications

| WLAN | |
|---|---|
| Standards | IEEE802.11g/b for wireless LAN, IEEE802.3u 10/100BaseTX for Ethernet LAN, IEEE802.3af for Power over Ethernet |
| Frequency Range | 2.4-2.4835 GHz, Direct Sequence Spread Spectrum (DSSS) |
| Data Rate & Modulation | OFDM@54 Mbps, CCK@11/5.5 Mbps, DQPSK@2 Mbps and DBSK@1 Mbps |
| Operating Channels | USA: 1-11 (US) Europe: 1-13 (EU) |
| Security | WEP, WPA, WPA2, IEEE802.1X, MAC address filtering, Hide SSID, Layer 2 Isolation For AP Client: 64-bit and 128-bit WEP encryption, WPA |
| Data Rates | 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps |
| Transmit Power | Typ. 17dBm@1, 2, 5.5 and 11 Mbps, 17dBm@6 Mbps, 14dBm@54 Mbps |
| RX Sensitivity | Typ. -72dBm@54 Mbps |

| Software Features | |
|---|---|
| Protocols | HTTP, DHCP, TCP/IP, RADIUS, DNS, NetBIOS, AppleTalk, and IPX/SPX |
| Configuration | Web-based management |
| Client OS Support | Windows 95/98/2000/ME/NT/XP, Unix and Macintosh |

| Interface | |
|---|---|
| Antenna | 5dBi External/SMA connector (AP/Bridge), 9dBi Internal (AP Client) |
| RJ45 port | 10/100BaseT(X) auto negotiation speed |

| Power | |
|---|---|
| Input Voltage | Active Ethernet (IEEE802.3af), 48 VDC |
| Input Current | 0.35A |

| **Mechanical** | |
| --- | --- |
| Casing | IP68 (AP/Bridge), IP67 (AP Client) |
| Dimensions (W × L × D) | AWK-1200-AP: 284.4 × 254.3 × 77.5 mm |
| | 11.20 × 10.01 × 3.05 in |
| | AWK-1200-AC: 165.8 × 195.8 × 60.3 mm |
| | 6.53 × 7.71 × 2.37 in |
| Installation | Wall or Mast Mounting (optional kit) |

| **Environmental** | |
| --- | --- |
| Operating Temperature | -20 to 70°C (-4 to 158°F) |
| Storage Temperature | -40 to 80°C (-40 to 176°F) |
| Ambient Relative Humidity | 5 to 95% (non-condensing) |

| **Regulatory Approvals** | |
| --- | --- |
| Emissions | FCC, CE |
| **WARRANTY** | 5 years |

**A-2**

# B

# Default Settings

## BASIC

## WIZARD

### CONNECTION SETUP WIZARD

| Parameter | Description | Default Value |
|---|---|---|
| Password | Web Login password | Admin |
| Verify Password | | root |
| Time | Time Zone | GTM-08:00, Tijuana |

### MICROSOFT WINDOWS CONNECT WIZARD

### WIRELESS SECURITY SETUP WIZARD

| Parameter | Description | Default Value |
|---|---|---|
| Wireless Network Name (SSID) | A name that can be easily recognized by wireless clients. | MOXA |
| SECURE YOUR WIRELESS NETWORK | In order to protect your network from hackers and unauthorized users. | NONE |
| Time | Time Zone | GTM-08:00, Tijuana |

## LAN

| Parameter | Description | Default Value |
|---|---|---|
| Get LAN IP from | A name that can be easily recognized by wireless clients | Static IP (Manual) |
| IP Address | In order to protect your network from hackers and unauthorized users. | 192.168.127.253 |
| Subnet Mask | | 255.255.255.0 |
| Gateway | | 0.0.0.0 |
| Local Domain Name | | NULL |

# DHCP

## ENABLE

| Parameter | Description | Default Value |
| --- | --- | --- |
| Enable DHCP Server | | Select |

## DHCP SETTING

| Parameter | Description | Default Value |
| --- | --- | --- |
| DHCP IP Address Range | | 192.168.127.100 ~ 192.168.127.199 |
| Primary DNS | | 0.0.0.0 |
| Secondary DNS | | 0.0.0.0 |
| DHCP Lease Time | | 1440 |
| Always broadcast | | Select |

## ADD DHCP RESERVATION

| Parameter | Description | Default Value |
| --- | --- | --- |
| Enable | Enable DHCP RESERVATION | Select |
| IP Address | | 0.0.0.0 |
| MAC Address | | 00: 00: 00: 00: 00: 00: |
| Copy Your PC's MAC Address | If you click this icon your PC's MAC will appear in the table | |
| Computer Name | | NULL |

# WIRELESS

## ENABLE

| Parameter | Description | Default Value |
| --- | --- | --- |
| Enable DHCP Server | | Select |

## BASIC WIRELESS SETTING

| Parameter | Description | Default Value |
| --- | --- | --- |
| Wireless Network Name (SSID) | | MOXA |
| **Visibility Status** | | Visible |
| **Auto Channel Select** | | Select |
| **REGION ID** | | 4 |
| **Channel** | | |

| **Transmission Rate** | | BEST (Automatic) |
|---|---|---|
| **802.11 Mode** | | MIX 802.11g AND 802.11b |
| **Super G™ Mode** | | Super G without Turbo |

## WIRELESS SECURITY MODE

| **Parameter** | **Description** | **Default Value** |
|---|---|---|
| Security Mode | | None |

# ADVANCED

## MAC Address Filter

| **Parameter** | **Description** | **Default Value** |
|---|---|---|
| Enable MAC Address Filter | | No Select |

## Advanced Wireless

| **Parameter** | **Description** | **Default Value** |
|---|---|---|
| Fragmentation Threshold | | 2346 |
| RTS | | 2346 |
| Beacon Period | | 100 |
| DTIM Interval | | 1 |
| 802.11d | | No Select |
| Transmit Power | | High |
| WDS Enable | | No Select |

# TOOLS

## ADMIN

### ADMIN PASSWORD

| **Parameter** | **Description** | **Default Value** |
|---|---|---|
| Password | Web Login password | Admin |
| Verify Password | | root |

### USER PASSWORD

| **Parameter** | **Description** | **Default Value** |
|---|---|---|
| Password | Web Login password | admin |
| Verify Password | | |

**B-3**

## SAVE AND RESTORE CONFIGURATION

## SAVE CONFIGURATION TO WIRELESS NETWORK SETUP WIZARD

# TIME

### TIME CONFIGURATION

| Parameter | Description | Default Value |
|---|---|---|
| **Time Zone** | | **GTM-08:00, Tijuana** |

### SET THE DATE AND TIME MANUALLY

| Parameter | Description | Default Value |
|---|---|---|
| Year | | 2004 |
| Month | | Jan |
| Day | | 31 |
| Hour | | 1 |
| Minute | | 7 |
| Second | | 45 |
| A.M. / P.M. | | PM |

# SYSTEM

| Parameter | Description | Default Value |
|---|---|---|
| Reboot the Device | | |
| Restore all Setting to the Factory Defaults | | |
| Factory Defaults | | |

# FIRMWARE

| Parameter | Description | Default Value |
|---|---|---|
| Upload File | Program Image | Upgrade bin |

**B-4**

# C

# Regulatory Compliance Information

## 15.21

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

## Prohibition of co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

## 15.105 Federal Communications Commission (FCC) Requirements, Part 15

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.

## Caution Statement of the FCC Radio Frequency Exposure

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247(b)(4) addressing RF Exposure from radio frequency devices. The radiation output power of this Wireless LAN device is far below the FCC radio frequency exposure limits.

Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation—as a mobile or portable device but use in a body-worn way is strictly prohibit. When using this device, a certain separation distance between antenna and nearby persons has to be kept to ensure RF exposure compliance.

## Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

## MPE Statement (Safety Information)

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

## Safety Information

**CAUTION:** To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

**C-2**

Free Manuals Download Website

[http://myh66.com](http://myh66.com)

[http://usermanuals.us](http://usermanuals.us)

[http://www.somanuals.com](http://www.somanuals.com)

[http://www.4manuals.cc](http://www.4manuals.cc)

[http://www.manual-lib.com](http://www.manual-lib.com)

[http://www.404manual.com](http://www.404manual.com)

[http://www.luxmanual.com](http://www.luxmanual.com)

[http://aubethermostatmanual.com](http://aubethermostatmanual.com)

Golf course search by state

[http://golfingnear.com](http://golfingnear.com)

Email search by domain

[http://emailbydomain.com](http://emailbydomain.com)

Auto manuals search

[http://auto.somanuals.com](http://auto.somanuals.com)

TV manuals search

[http://tv.somanuals.com](http://tv.somanuals.com)