SOHOware

AeroGuard IEEE 802.11a/b/g Access Point User's Guide

Version 1.0, March 25, 2004

Table of Contents

Regulatory Information

This Equipment is strictly for indoor use. Furthermore, this equipment is intended to be used in US. All non-US frequencies are permanently disabled. Users do not have option to turn it on.

Federal Communication Commission Interference Statement

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

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

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. 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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

Discontinue Transmitting with Absence of Data or operational failure statement
Comply to FCC 15.407(C), the device shall automatically discontinue transmission in case of either absence of information to transmit or operational failure. These provisions are not intended to preclude the transmission of control or signaling information or the user of repetitive codes used by certain digital technologies to complete frame or burst intervals.

The Baseband processor AR5212 used in this device supports FCC15.407 (C), shall automatically discontinue transmission in case of either absence of information to transmit or

operational failure. The implementation is via queue control unit (to see data is empty or system failed with no data or no-meaningful data) and power management registers built in on this chip to discontinue the Transmitting.
Data transmission is always initiated by software, which is then passed through the MAC, through the digital and analog baseband, and finally to the RF chip. Several special packets (ACKs, CTS, PSPoll, etc...) are initiated by the MAC. These are the only ways by which the digital baseband portion will turn on the RF transmitter, which it then turns off at the end of the packet. Therefore, the transmitter will be on only while one of the aforementioned packets is being transmitted."

Chapter 1
Introducing the 802.11 A/B/G ACCESS POINT

Overview of the Device

The 802.11 A/B/G ACCESS POINT is an access-point based on IEEE 802.11 A/B/G based 2.4-GHz radio technology. It contains an 802.11 A/B/G and a full-duplex 10/100 LAN interfaces. The 802.11 A/B/G ACCESS POINT can function as a simple Access Point (AP), and act as the center point of a wireless network supporting a data rate of up to 54 Mbps. It can also connect these wireless devices to wired network through the LAN interface.

The 802.11 A/B/G ACCESS POINT can also function in a repeater mode, which is used to extend the physical coverage of the wireless network. Finally, the 802.11 A/B/G ACCESS POINT can also function in a Wireless Distribution System (WDS) mode. Multiple 802.11 A/B/G ACCESS POINT's can be configured to operate in the WDS mode to inter-connect wired LAN segments that are attached to these 802.11 A/B/G ACCESS POINT's.

Since the 802.11g shares the same 2.4GHz radio band as the 802.11b technology, it can inter-operate with existing 11Mbps 802.11b devices. Therefore you can protect your existing investment in 802.11b client cards, and migrate to the high-speed 802.11g standard as your needs grow.

To address growing security concerns in a wireless LAN environment, different levels of security can be enabled in the 802.11 A/B/G ACCESS POINT, including:
• To disable SSID broadcast to restrict association to only those client stations that are already pre-configured with the correct SSID
• To enable WEP (Wireless Encryption Protocol) 64, 128, or 156-bit encryption to protect the privacy of your data.
• Support of Access List Control to allow you to grant/deny access to/from specified wireless stations
• Provisioning of centralized authentication through Radius Server(s).
• WPA-PSK (Wi-Fi Proctected Access, Pre-Shared Key) for home users to provide authentication, data integrity, and data privacy.
• WPA (Wi-Fi Proctected Access) works with a RADIUS server to provide stronger authentication as well as data integrity and privacy. authentication as well as data integrity and privacy.

802.11 A/B/G ACCESS POINT Features

- Compliant with draft 802.11a, 802.11b and 802.11g standards with roaming capability.
- Support of the standard access point mode for connection to wireless clients.
- Support of the repeater mode to extend infrastructure coverage.
- Support of the WDS mode for interconnecting LAN segments.
- Static assignment or DHCP client to set the device IP address.
- Multiple security measures: SSID hiding, Access Control List, WEP based encryption (64, 128, 152 bits), enhanced Security with 802.1x using a primary and a backup Radius Server with/without dynamic WEP keys, WPA-PSK, and WPA.
- Extensive monitoring capability such as event logging, traffic/error statistics monitoring. Support of remote logging.
- Easy configuration and monitoring through the use of a Web-browser based GUI, SNMP commands from a remote SNMP management station, and UPnP for users to automatically discover the device.
- Setup Wizard for easy configuration/installation.
- Configuration file download and restore.
- Firmware upgradeable.

Network Configuration Examples

A group of wireless stations communicating with each other is called a Basic Service Set (BSS) and is identified by a unique SSID.

When an 802.11 A/B/G ACCESS POINT is used, it can be configured to operate in the following three network configurations

AS AN ACCESS POINT

When configured in the Access Point mode, the 802.11 A/B/G ACCESS POINT allows a group of wireless stations to communicate with each other through it. Such a network is called an Infrastructure BSS. The 802.11 A/B/G ACCESS POINT further provides bridging functions between the wireless network and the wired LAN network. When multiple access points are connected to the same LAN segment, stations can **roam** from one 802.11 A/B/G ACCESS POINT to another without losing their connections, as long as they are using the same SSID. This is shown in the diagram below (TBD)

AS A STAND-ALONE REPEATER

The purpose of a repeater is to expand an existing infrastructure BSS. When configured to operate in the Repeater Mode, the 802.11 A/B/G ACCESS POINTs sit between wireless stations and a "root" AP whose BSS is being expanded, as shown below: (TBD)

AS A POINT TO MULTI-POINTS BRIDGE

When configured to operate in the Wireless Distribution System (WDS) Mode, the 802.11 A/B/G ACCESS POINT provides bridging functions between the LAN behind it and separate LANs behind other AP's operating in the WDS mode. The system will support up to eight such AP's in a WDS configuration. Note that an 802.11 A/B/G ACCESS POINT running in the WDS mode can also support wireless stations simultaneously, as shown in the left most AP in the diagram below: **(TBD)**

Setting Up the device The 802.11 A/B/G ACCESS POINT

can be managed remotely by a PC through either the wired or wireless network. To do this, the 802.11 A/B/G ACCESS POINT must first be assigned an IP address, which can be done using one of the following two methods.

STATIC IP

The default IP address of the LAN interface of an 802.11 A/B/G ACCESS POINT is a *private IP address* of **192.168.1.1**, and a *network mask* of 255.255.255.0. This means IP addresses of other devices on the LAN should be in the range of 192.168.1.2 to 192.168.1.254. This IP address can be modified to either a different address in this same subnet or to an address in a different subnet, depending on the existing netwrok settings (if there is any) or user's preference.

AUTOMATIC IP

The 802.11 A/B/G ACCESS POINT can also be configured to "obtain" an IP address automatically from a DHCP server on the network. This address is called "dynamic" because it is only *dynamically* assigned to the device, which may change depending on the IP assignment policy used by the DHCP server on the network. Since the IP address in this case may change from time to time, this method is not recommended - unless the user uses UPnP or other management tools that do not depend on a fixed IP address.

Chapter 2

Installing the 802.11 A/B/G ACCESS POINT

This section describes the installation procedure for the 802.11 A/B/G ACCESS POINT. It starts with a summary of the content of the package you have purchased, followed by steps of how to power up and connect the 802.11 A/B/G ACCESS POINT. Finally, this section explains how to configure a Windows PC to communicate with the 802.11 A/B/G ACCESS POINT.

What's in the Box?

The 802.11 A/B/G ACCESS POINT package contains the following items:

- One 802.11 A/B/G ACCESS POINT
- One 12V DC power adapter with a mini DIN 3 pin connector
- CD of the 802.11 A/B/G ACCESS POINT User' Guide

Connecting the Cables

The Back Panel of the 802.11 A/B/G ACCESS POINT appears as follows:

Follow these steps to install your 802.11 A/B/G ACCESS POINT:

Step 1. Connect a LAN hub to the LAN port on the 802.11 A/B/G ACCESS POINT using the supplied LAN cable.

Step 2. Connect the power adapter to an electrical outlet and the 802.11 A/B/G ACCESS POINT.

Configuration Steps Required for the 802.11 A/B/G ACCESS POINT

This section describes configuration required for the 802.11 A/B/G ACCESS POINT before it can work properly in your network.

First, it is assumed that in your LAN environment, a separate DHCP server will be available for assigning dynamic (and often private) IP addresses to requesting DHCP clients. This means that the 802.11 A/B/G ACCESS POINT normally will not need to enable the DHCP server function.

Additionally, since you need to perform various configuration changes to the 802.11 A/B/G ACCESS POINT, including the SSID, Channel number, the WEP key, …, etc., it is necessary to associate a fixed IP address with the 802.11 A/B/G ACCESS POINT, which is why the 802.11 A/B/G ACCESS POINT will be shipped with a factory default private IP address of **192.168.1.1** (and a network mask of 255.255.255.0).

Therefore, during the system installation time, you need to build an isolated environment with the 802.11 A/B/G ACCESS POINT and a PC, and then perform the following steps:

- Manually change the IP address of the PC to become 192.168.1.3

- Connect the PC to the 802.11 A/B/G ACCESS POINT and change its configuration to a static IP address based on your network environment. For example, if there is a DHCP server that assigns IP addresses from the range 192.168.23.10 - 192.168.23.254 to DHCP client devices, it can reserve 192.168.23.10 for the 802.11 A/B/G ACCESS POINT and then the address pool with the DHCP server becomes 192.168.23.11 – 192.168.23.254. If there is no DHCP server on your network environment, you just have to make sure that there is no machine in the environment has the same IP address as another machine. Please note that after you change the IP address of the ACCESS POINT, the PC client may not be able to reach the ACCESS POINT. This is because they may no longer belong to the same IP network address space.

- Change the setting of the PC back to "obtain IP addresses dynamically".
- Now you can put the 802.11 A/B/G ACCESS POINT and the PC to your network where the DHCP server is connected. From then on, any wireless client configured to "obtain IP addresses dynamically" will work with the AP, with each other, and with devices on the wired LAN network.

Setting up a Windows PC or wireless client as DHCP clients

The following will give detailed steps of how to configure a PC or a wireless client to "obtain IP addresses automatically". For other types of configuration, please refer to the corresponding user manual.

In the case of using a LAN attached PC, the PC must have an Ethernet interface installed properly, be connected to the 802.11 A/B/G ACCESS POINT either directly or through an external LAN switch, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

In the case of using a wireless client, the client must also have an 802.11a/b/g wireless interface installed properly, be physically within the radio range of the 802.11 A/B/G ACCESS POINT, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

Then perform the following steps for either of the cases above. To configure types of workstations other than Windows 95/98/NT/2000, please consult the manufacturer's documentation.
Step 1. From the Win95/98/2000 Start Button, select Settings, then Control Panel. The Win95/98/2000 Control Panel displays.
Step 2. Double-click on the *Network* icon.

Step 3. Check your list of Network Components in the Network window Configuration tab. If TCP/IP has already been installed, go to Step 8. Otherwise, select Add to install it now.

Step 4. In the new Network Component Type window, select Protocol. In the new Select Network Protocol window, select Microsoft in the Manufacturers area.

Step 5. In the Network Protocols area of the same window, select TCP/IP, then click OK. You may need your Win95/98 CD to complete the installation. After TCP/IP installation is complete, go back to the Network window shown in Step 4.

Step 6. Select TCP/IP in the list of Network Components.

Step 7. Click *Properties*, and check the settings in each of the TCP/IP Properties window: **Bindings Tab**: both **Client for Microsoft Networks** and **File and printer sharing for Microsoft Networks** should be selected. **Gateway Tab**: All fields should be blank. **DNS Configuration Tab**: **Disable DNS** should be selected. **IP Address Tab**: **Obtain IP address automatically** should be selected.

Step 8. With the 802.11 A/B/G ACCESS POINT powered on, reboot the PC/wireless client. After the PC/wireless client is re-booted, you should be ready to configure the 802.11 A/B/G ACCESS POINT. See Chapter 3.

The procedure required to set a static IP address is not too much different from the procedure required to set to "obtain IP addresses dynamically" - except that at the end of step 7, instead of selecting "obtain IP addresses dynamically, you should specify the IP address explicitly.

A Look at the Front Panel The LEDs on the front of the 802.11 A/B/G ACCESS POINT reflect the operational status of the unit. The status of the LAN, the wireless, and power can be monitored from this display. (LED table TBD)

Connecting More Devices Through A Hub To The 802.11 A/B/G ACCESS POINT

The 802.11 A/B/G ACCESS POINT provides an RJ45 LAN interface that you can use to connect to a PC or an external hub.

Step 1. Plug this end into any port of an Ethernet hub/switch Connect to the LAN port

Chapter 3

Basic Configuration of the 802.11 A/B/G ACCESS POINT

This section describes the basic configuration procedure for the 802.11 A/B/G ACCESS POINT. It describes how to set up the 802.11 A/B/G ACCESS POINT for wireless connections, and the configuration of the local LAN environment.

The 802.11 A/B/G ACCESS POINT is designed so that all basic configuration may be effected through the a standard Web browser such as Microsoft Internet Explorer.

From a PC that has been configured as described in Chapter 2, enter the IP address of the 802.11 A/B/G ACCESS POINT as the URL in your browser, e.g. **`http://192.168.1.1`**.

Note: The IP address of your PC must be in the same IP subnet as the 802.11 A/B/G ACCESS POINT.

The Home Page of the 802.11 A/B/G ACCESS POINT screen will appear, with its main menu displayed on the right hand side of the window. The main menu includes the following choices: Setup Wizard, Device Status, Advanced Settings, System Tools, and Help; these can be used to navigate to other menus.

Logging On If you attempt to access a configuration item from the browser menu, an administrator login screen will appear, prompting you for the password in order to log on. If you are logging on for the first time, you should use the factory default setting "**password**". The password is always displayed as a string of asterisks ("*"). Click the **LOG ON** button to start the configuration session.

Setup Wizard

The Setup Wizard will guide you through a series of configuration screens to set up the basic functionality of the device. After you finish these screens, press the "finish" button on the last screen to make all your modifications effective.

TIME SETTINGS After logging in, the **time settings** page appears. The device time is automatically set to the local time of the management PC at the first time a connection is made. To modify the device's time, modify the appropriate fields, then click **NEXT**.

DEVICE IP SETTINGS

The **Device IP setting** screen allows you to configure the IP address and subnet of the device. Although you can rely on a DHCP server to assign an IP address to the 802.11 A/B/G ACCESS POINT automatically, it is recommended that you configure a static IP address manually in most applications.

If you choose to assign the IP address manually, check the button that says "**Assign static IP to this device**" and then fill in the following fields

IP Address and **IP Subnet Mask:** These values default to 192.168.1.1 and 255.255.255.0, respectively. It is important to note that there are similar addresses falling in the standard *private IP address* range and it is an essential security feature of the device. Because of this private IP address, the device can no longer be accessed (seen) from the Internet.

Gateway IP Address: Enter the IP address of your default gateway

DNS Server: The Domain Name System (DNS) is a server on the Internet that translates logical names such as "www.yahoo.com" to IP addresses like 66.218.71.80. In order to do this, a query is made by the requesting device to a DNS server to provide the necessary information. If your system administrator requires you to manually enter the DNS Server addresses, you should enter them here.

Click **Next** to go to the next screen.

If you choose to use a DHCP Server to acquire an IP address for the 802.11 A/B/G ACCESS Point automatically, check the button that says, "**Use the DHCP protocol to automatically get the IP address for this device**". Then click **Next** to go to the next screen. Again, as a reminder, it is recommended that your 802.11 A/B/G ACCESS POINT should be assigned a static IP address in order to make it easy for you to manage the device later on.

WIRELESS SETTINGS

Network Name (SSID): The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the wireless network (i.e. in the same BSS). Several access points on a network can have the same SSID. The SSID length is up to 32 characters. The default SSID is "**wlan**".

Disable SSID Broadcasting: An access point periodically broadcasts its SSID along with other information, which allows client stations to learn its existence while searching for access points in a wireless network. Check **Disable** if you do not want the device to broadcast the SSID.

WLAN mode: The wireless module is IEEE 802.11a IEEE 802.11g and 802.11b compliant, and choosing "**11g/b**" allows both 802.11b and 802.11g client stations to get associated. However, choosing "**11g**" allows only 802.11g client stations to get associated and get better overall performance. 802.11a is not compliant with either 802.11b or 802.11g; choosing **"11a"** only allows 802.11a client stations to get associated. Since there is only one RF amplifier in the equipment, user can only select one particular mode restricted by GUI (i.e., IEEE 802.11g, IEEE 802.11b or IEEE 802.11a, are mutually exclusive choice).

Channel: Select a channel from the available list to use. All devices in a BSS must use the same channel. You can select **Auto** to let the system pick up the best channel for you.

Security Policy: You can select different security policy to provide association authentication and/or data encryption.

WEP allows you to use data encryption to secure your data from being eavesdropped by malicious people. It allows 3 types of key: 64 (**WEP64**), 128 (**WEP128**), and 152 (**WEP152**) bits. You can configure up to 4 keys using either **ASCII** or **Hex**adecimal format.

Key Settings: The length of a **WEP64** key must be equal to 5 bytes, a **WEP128** key is 13 bytes, and a **WEP152** key is 16 bytes. For WEP64 and WEP128, you can just enter a pass-phrase and click the **GENERATE** button to generate the four keys. So you can use a mnemonic string as the pass-phrase instead of memorizing the four keys.

Key Index: You have to specify which of the four keys will be active.

Once you enable the WEP function, please make sure that both the 802.11 A/B/G ACCESS POINT and the wireless client stations use the same key.

Note: Some wireless client cards only allow Hexadecimal digits for WEP keys. Please note that when configuring WEP keys, a WEP128 ASCII key looks like "**This is a key**"(13 characters), while a WEP128 Hex key looks like "5**4-68-69-73-20-69-73-20-61-20-6b-65-79**"(13 bytes).

802.1x allows users to leverage a RADIUS server to do association authentications. You can also enable dynamic WEP keys (64, 128, 152-bit) to have data encryption. Here you do not have to enter the WEP key manually because it will be generated automatically and dynamically.

NOTE: After you have finished the configuration wizard, you have to configure the Radius Settings in Advanced Settings in order to make the 802.1x function work.

WPA-PSK Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the 802.11 A/B/G ACCESS POINT and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Re-key Interval: A group key is used for multicast/broadcast data, and the rekey interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. 60 seconds is a reasonable time, and it is used by default.

WPA Wi-Fi Protected Access (WPA) requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required. The **Encryption Type** and **Group Re-key Interval** settings are same as WPA-PSK.

Finish Setup Wizard and Save Your Settings

After stepping through the Wizard's pages, you can press the **FINISH** button for your modification to take effect. This also makes your new settings saved into the permanent memory on your system.

Congratulations! You are now ready to use the 802.11 A/B/G ACCESS POINT.

Note: If you change the device's IP address, as soon as you click on FINISH you will no longer be able to communicate with your 802.11 A/B/G ACCESS POINT. You need to change your IP address and then re-boot your computer in order to resume the communication.

Advanced Settings

The advanced settings tab on the top row of the window allows you to perform modifications that normally you may not need to do for general operations except changing your password from the default factory setting (this is highly recommended for security purposes).

Password Settings The default factory password is "**password**". To change the password, press the **Password Settings** button to enter the **Password Settings** screen, then enter the current password followed by the new password twice. The entered characters will appear as asterisks.

System Management Clicking the **System Management** button to configure system related parameters to for the 802.11 A/B/G ACCESS POINT.

Management Utility Port Definition: The standard port settings for the HTTP Web server and the Telnet utility may be replaced by entering new port numbers in these fields.
Management Session Time-out: This setting specifies the duration of idle time (inactivity) before a web browser or telnet management session times out. The default time-out value is 10 minutes.

UPnP: The Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover this 802.11 A/B/G ACCESS Point and automatically show an icon on the screen. Then a user can double-click the icon to access this device directly (without having to find out its IP address).

Syslog: Syslog is an IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164). When the 802.11 A/B/G ACCESS POINT encounters an error or warning condition (e.g., a log-in attempt with an invalid password), it will create a log in the system log table. To be able to remotely view such system log events, you need to check the **Enable Syslog** box and configure the IP address of a Syslog daemon. When doing so, the 802.11 A/B/G ACCESS POINT will send logged events over network to the daemon for future reviewing.

Syslog server IP address: The IP address of the PC where the Syslog daemon is running.

MAC Filtering Settings

The 802.11 A/B/G ACCESS POINT allows you to define a list of MAC addresses that are allowed or denied to access the wireless network

Disable MAC address control list: When selected, no MAC address filtering will be performed.

Enable GRANT address control list: When selected, data traffic from only the specified devices in the table will be allowed in the network.

Enable DENY address control list: When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

To add a MAC address into the table, enter a mnemonic name and the MAC address, then click **ADD**.

The table lists all configured MAC Filter entries. To delete entries, check the corresponding **select** boxes and then press **DELETE SELECTED**

Wireless Settings

Beacon Interval: The 802.11 A/B/G ACCESS POINT broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted

- in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.
-

RTS Threshold:
RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

Fragmentation Threshold: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

DTIM Interval: The 802.11 A/B/G ACCESS POINT buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255, with a default value of **3**.

Operational Mode The 802.11 A/B/G ACCESS POINT can be configured to operate in one of the following three modes as mentioned previously in Chapter 1: (1) Access Point (2) Repeater (3) Wireless Distribution System (WDS)

When configured as a WDS, you need to further configure the name and MAC address of its peer WDS devices.

Radius Settings Radius servers provide centralized authentication services to wireless clients. Two Radius servers can be defined: one acts as a primary, and the other acts as a backup.

Two user authentication methods can be enabled: one based on MAC address filter, the other based on 802.1x EAP authentication.

MAC address filtering based authentication requires a MAC address filter table to be created in either the 802.11 A/B/G ACCESS POINT (as described in the section *MAC Filtering Settings*) and/or the Radius server. During the authentication phase of a wireless station, the MAC address filter table is searched for a match against the wireless client's MAC address to determine whether the station is to be allowed or denied to access the network.

The Radius server can also be used for 802.1x EAP authentication. IEEE 802.1x is an IEEE standard that is based on a framework that involves stations to be authenticated (called Supplicant), an authentication server (a Radius Server) that provides authentication services, and an authenticator that provides necessary translation and mediating functions between the authentication server and the stations to be authenticated. The 802.11 A/B/G ACCESS POINT acts as an authenticator, and it relays authentication messages between the RADIUS server and client devices being authenticated.

IEEE 802.1x EAP authentication is enabled by selecting the **Security Policy** as **802.1x** or **WPA**, and this selection is in the **Wireless Settings** under **Setup Wizard**.
Enable MAC Address Access Control: Check this option to enable MAC address access control through a RADIUS server.

Enable Primary/Secondary Server: Check this if you want to enable RADIUS authentication using the primary/secondary Radius Server. If both are selected, the primary server will be tried first.

Server IP: The IP address of the RADIUS server

Port Number: The port number that your RADIUS server uses for authentication. The default setting is 1812.

Shared secret: This is used by your RADIUS server in the Shared Secret field in Radius protocol messages. The shared secret configured in the 802.11 A/B/G ACCESS POINT must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.

Retry Times: The number of times the 802.11 A/B/G ACCESS POINT should attempt to contact the primary server before giving up.

Reattempt Period: After failed to contact the primary RADIUS server, the 802.11 A/B/G ACCESS POINT will re-attempt to contact the primary server every this number of minutes.

Chapter 4
Managing the 802.11 A/B/G ACCESS POINT

This Chapter covers other management aspects of your 802.11 A/B/G ACCESS POINT:
How to view the device status

- How to view the system log
- How to upgrade the firmware of your 802.11 A/B/G ACCESS POINT
- How to save or restore configuration changes
- How to reset the configuration to the factory default.
- How to reboot your 802.11 A/B/G ACCESS POINT
- What if you forgot the password

How to View the device Status

You can monitor the system status and get general device information from the **Device Information** screen:
This is at the left-bottom corner of the **Device Status** window.

How to View the System Log

The 802.11 A/B/G ACCESS POINT maintains a system log that you can use to track events that have occurred in the system. Such event messages can sometimes be helpful in determining the cause of a problem that you may have encountered.

You can select **System Log** on the left side of the **Device Status** window to view log events recorded in the system. The System Log entries are shown in the main screen along with the log level, the severity level of messages that are being displayed (lower is severer), and the uptime, which is the amount of time since the 802.11 A/B/G ACCESS POINT was boot-up.

Wireless Client Table The wireless client table lists the current wireless clients and its MAC address, state, and traffic statistics. You can check this table by clicking **Wireless Client Table** at the left side of the **Device Status window**.

Bridge Table The bridge table shows all MAC entries learned from the wired LAN interface, wireless clients, and WDS peers (if running in the WDS mode). You can check this table by clicking **Bridge Table** at the left side of the **Device Status window**.

Upgrading Firmware

You can upgrade the firmware of your 802.11 A/B/G ACCESS POINT (the software that controls your 802.11 A/B/G ACCESS POINT's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have

encountered with the current version. System upgrade can be performed through the System Upgrade window as follows:

Step 1 Select **System Tools,** then **Firmware Upgrade** from the menu and the following screen displays: (TBD)

Step 2 To update the 802.11 A/B/G ACCESS POINT firmware, first download the firmware from the distributor's web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will begin being loaded to your 802.11 A/B/G ACCESS POINT. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

Note: It is recommended that you do not upgrade your 802.11 A/B/G ACCESS POINT unless the new firmware contains a new feature that you want or if it contains a fix to a problem that you've encountered.

How to Save or Restore Configuration Changes

You can save system configuration settings to a file, and later download it back to the 802.11 A/B/G ACCESS POINT by following the steps below.

Step 1 Select **Configuration Save and Restore** from the **System Tools** menu and you will see the following screen:

Step 2 Enter the path of the configuration file to save-to/restore-from (or click the **Browse** button to locate the configuration file). Then click the **SAVE TO FILE** button to save the current configuration into the specified file, or click the **RESTORE FROM FILE** button to restore the system configuration from the specified file.

How to reset the configuration to the factory default

You can reset the configuration of your 802.11 A/B/G ACCESS POINT to the factory default settings. To do it:

Step 1 Select **Factory Default** from the **System Tools** menu, you will see the following screen:

Step 2 Click **YES** to go ahead and restore the configuration to the factory default.

How to Reboot your 802.11 A/B/G ACCESS POINT

You can reset your 802.11 A/B/G ACCESS POINT from the Browser. To reset it:

Step 1 Select **Reboot System** from the **System Tools** menu, you will see the following screen: (TBD)

Step 2 Click **YES** to reboot the 802.11 A/B/G ACCESS POINT.

Note: Resetting the 802.11 A/B/G ACCESS POINT disconnects any active clients, and therefore will disrupt any current data traffic.

What if you Forgot the Password?

If you forgot the password, the only way to recover is to clear the device configuration and return the unit to its original state as shipped from the factory. You can do this by pressing the hardware "restore" button on the back of the device and hold for **two seconds**. Please note that this will also clear your current configuration and restore the configuration from the factory default.

Product Specification

Product Name AeroGuard IEEE 802.11a/b/g Access Point

Control Number AAP1000

Core Logic, Intel XScale CPU 425, 266 Mhz

WLAN Atheros 5212 **OS** Linux® 2.4.14

Standard • IEEE 802.11a/b/g • IEEE 802.1d Spanning Tree • IEEE 802.1x • IEEE 802.3u Ethernet protocol

WLAN Network Architecture Type • Infrastructure • Bridge Mode (WDS) • Repeater Mode

Wireless Transfer Data Rate for IEEE 802.11a Draft Standard IEEE 802.11a Standard: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps with auto fallback

Wireless Transfer Data Rate for IEEE 802.11g Draft Standard IEEE 802.11g Draft Standard: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps with auto fallback

Wireless Transfer Data Rate for IEEE 802.11b 11, 5.5, 2 & 1 Mbps with auto fallback

Physical Specification • External Power Adapter with DC12V/3.6A Input • PCB Dimension: 180 mm x 100 mm • Desktop Instillation • Wall/Ceiling Mountable

Hardware & Antenna • 1 x RJ45 Guest, 4 x x RJ45 Trusted • 1 x Restore Button • 2x External Antenna • 3 x LED (1 x Power, 1 x LAN, 1 x WLAN)

Security • WEP 64-bit, 128-bit, 152-bit Encryption • MAC Access Control for the wireless interface • EAP & 802.1x support • Support Primary & secondary RADUIUS server • WPA and WPA-PSK

Management • Web-Based Management Tool • UPnP • Upload & download test-based configuration file via HTTP browser • Firmware upgrade via HTTP browser • SysLog

IP Address Assignment • DHCP Client • Static IP Address

Environmental Specification • Operation Temperature: 0^0 ~40^0 C. • Storage Temperature: -20^0 ~ 65^0 C • Operating Humidity: 10% ~80% (without Condensation)

EMC Certification • FCC • Wi-Fi Class 2.4 GHz, 5.8GHz 802.11 A/B/G (Planning)