IEEE 802.11A+G ACCESS POINT

User's Guide

Version 1.0, Aug 2003

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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.

Table of Content

Chapter 1

1.Introduction to the 802.11a+g Access Point

The 802.11a+g Access Point, an IEEE 802.11a and 802.11g based Wireless Access Point, contains two IEEE 802.11a and 802.11g based radios and one 802.3 RJ45 interfaces. It functions as a super wireless "Access Point" with increased bandwidth and extended coverage area (to about 400 meters in an open space, as opposed to 150 meters for typical APs using omni antennas). It implements advanced features such as VLAN (Virtual LAN) and advanced security control to meet the increasing needs in today's enterprise environment.

On the wired network side, the 802.11a+g Access Point consists of two RJ45 Fast Ethernet interfaces that can be optionally grouped to operate in a link aggregation mode to provide 54 Mbps bandwidth between wireless and wired networks.

This manual gives a high level overview of the 802.11a+g Access Point, followed by information on how to configure the 802.11a+g Access Point to operate in various applications.

It will also cover how to use your web browser to configure the 802.11a+g Access Point and to perform various management functions, e.g., upgrading the software, or viewing the system log.

This manual consists of the following chapters:

Chapter 1, *Introductio*n, summarizes features and capabilities of the 802.11a+g Access Point.

Chapter 2, *Installing the* 802.11a+g Access Point, summarizes steps you should follow to install the 802.11a+g Access Point and configure a PC in order to manage/configure the 802.11a+g Access Point.

Chapter 3, *Configuring the* 802.11a+g Access Point, describes how to log in to the Web Manager, the browser screen, and steps needed to configure your 802.11a+g Access Point. It gives easy-to-follow instructions for Internet access and provides a guide to basic 802.11a+g Access Point configuration.

Chapter 4, *Advanced Configuratio*n, provides information on advanced Wireless Access Point configuration.

Chapter 5, *Managing your* 802.11a+g Access Point, describes other management features of the 802.11a+g Access Point.

Key Features

- Configurable to be 2 x 802.11a or 2 x 802.11g or 1 x 802.11a + 1 x 802.11g mode
- Wi-Fi certificated interoperability
- Support Primary & Secondary RADIUS server
- Compliant with 802.11a, 802.11g and 802.11b 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
- Built-in DHCP Server to Assign IP Addresses to wireless clients automatically
- Extensive monitoring capability such as event logging, traffic/error statistics monitoring
- Easy configuration and monitoring through the use of a Web-browser based GUI, a Command Line Interface (CLI) through a remote telnet session, or SNMP commands from a remote SNMP management station
- Extending VLAN to the wireless network by supporting SSID-to-VLAN mapping. Each SSID can be assigned a unique security policy
- Extensive monitoring capabilities including event logging, traffic/error statistics monitoring
- Multiple security mechanisms: to disable SSID broadcast, to define an access control list, to enable WEP based encryption (with a key that is up to 128 bits in size), WPA, plus enhanced security using 802.1x together with a primary and a backup RADIUS Server
- Easy configuration and monitoring through the use of a Web-browser based GUI, a Command Line Interface (CLI) through a remote telnet session, or SNMP commands from a remote SNMP management station

MULTIPLE RADIOS

The 802.11a+g Access Point supports 2 standards-based IEEE 802.11a+g radios in the wireless network..

Its key components can be summarized as follows:

Channel selection: During the system start-up time, the 802.11a+g Access Point chooses the best channel combination for all of its 2 radio devices so that interference with other neighboring RF devices can be minimized.

Selection of a radio: When a new client wishes to communicate, it will search for available radios by entering either the "passive" or "active" scanning mode, or a combination of the two. With passive scanning, the client listens for beacon frames from all radios, and with active scanning, the client broadcasts Probe requests and waits for Probe responses from any radios. In case, the client can persistently issue association requests to the same radio – such as when a client has been designed to associate with the AP with the strongest signal level.

MULTIPLE SSIDS AND VLAN

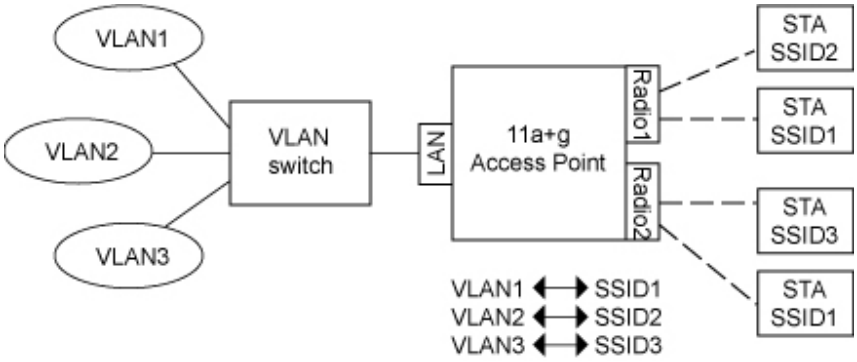
A bridged network can be logically segmented into multiple VLANs. VLANs are logical groupings of network devices regardless of their locations or the LAN segments they attach to. VLAN groups essentially allow private networks to be defined.

The 802.11a+g Access Point supports the 802.1Q based VLAN in the wired network, which is further extended into the wireless network through the support of SSID to VLAN mapping.

When mapping is enabled and when a wireless interface receives a frame destined for the wired network, the 802.11a+g Access Point will search in the SSID-to-802.1p/Q mapping table for a match with the frame's SSID. When found, the corresponding 802.1 tag shown in the matched entry will be added to the frame before it is sent out. The tag configured in the SSID-to-802.1p/Q tag table consists of an 802.1Q VLAN ID and 802.1p priority bits.

When a wired interface receives a frame destined for the wireless LAN, the 802.11a+g Access Point will search in the SSID-to-802.1p/Q mapping table for a match with the frame's VLAN ID. When found, the corresponding SSID shown in the matched entry will be added to the frame, and the 802.1p/Q tag removed before it is sent out.

The following diagram gives an example of a network consisting of 3 VLANs and 4 wireless clients.



SECURITY CONTROL

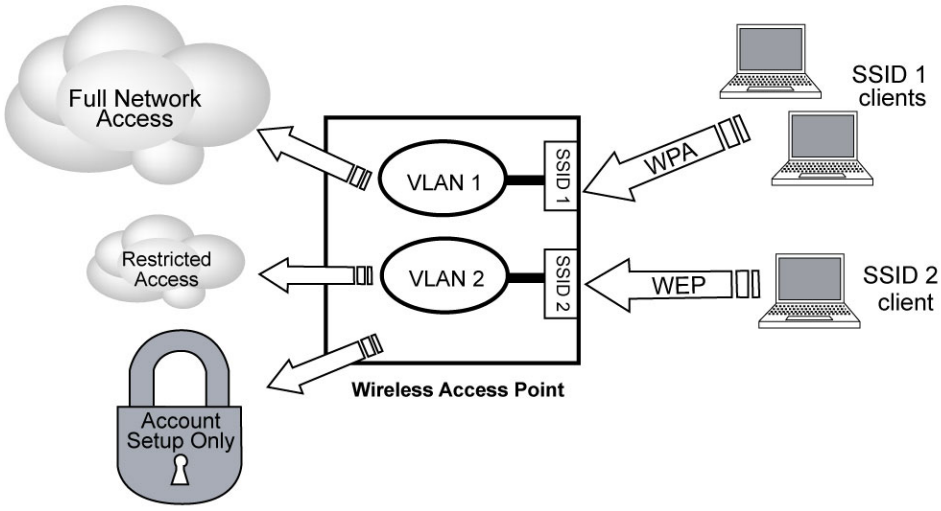
The 802.11a+g Wireless Access Point provides several important features that allow very fine control over wireless security.

The access point provides a full complement of advanced authentication and encryption mechanisms. WiFi Protected Access (WPA) is fully supported, using either pre-shared keys or keys provided through 802.1x using an external server. In addition, both static and 802.1x-supported WEP is available.

Typically, wireless access points have struggled to simultaneously support users using inconsistent security methods. The 802.11a+g Access Point is able to meet this challenge, through its special ***Multiple SSID*** capability. The network administrator can configure the access point with a list of SSIDs (network names) that it will recognize. The 802.11a+g Access Point is able to simultaneously authenticate with any combination of clients that specify any of the SSIDs in that list. (Only a single SSID is actually sent in the beacon from the access point.)

Wireless system administrators face two significant issues that are addressed by the Multiple SSID support in the 802.11a+g Access Point. The first is the sheer number of different security mechanisms currently in use, and their incomplete interoperability. Second is the desire to differentiate clients into specific categories and vary their privileges accordingly.

Each SSID can present a different set of security requirements to its clients (i.e. WPA, WEP, or clear text). Even more significantly, each SSID can be associated with a separate VLAN type interface, allowing tight control over the access that is granted to different clients. For example, clients who use one SSID to associate may be required to use WPA with full 802.1x-based authentication, and are then granted full access to the LAN. Other clients may associate with the access point using a different SSID that only requires static WEP keys, but places those clients on a much more restricted VLAN. Yet another SSID, using clear text (no encryption), could place associated clients on a special VLAN for account set-up. (See diagram.)



The Multiple SSID support in the 802.11a+g Access Point provides wireless system administrators with both an easy solution to the mix-and-match security methods in use today and a powerful tool for creating multiple classes of clients with a single access point.

In addition to these encryption and authentication security methods, the 802.11a+g Access Point wireless access point also provides full ***access control*** based on the client device's MAC address. A list of authorized client MAC addresses is maintained in the access point. When a new client attempts to associate, its MAC address is checked against the list. If the address is in the list, the client is allowed to establish a connection to the access point; otherwise, the client is not allowed to connect.

Because the most powerful forms of WPA and WEP security rely on an external RADIUS server to authenticate users (via 802.1x), the reliability of the RADIUS server becomes critical to the overall operation of the wireless access point. To provide a robust mechanism for authentication, the 802.11a+g Access Point allows a secondary, ***backup RADIUS server*** to be specified. In this case, if the access point loses communications with the primary RADIUS server for any reason, the backup server will be used instead. This ability to use a redundant server greatly increases the overall reliability of the security and authentication mechanism.

Specification

Product Name	IEEE 802.11a+g Wireless LAN Access Point
Core Logic, CPU	Intel xScale IXP425
Core Logic, WLAN	2 x Atheros WLAN
RTOS	Monta Vista PE 3.0
Standard	• IEEE 802.11a • IEEE 802.11b • IEEE 802.11g • IEEE 802.1d Spanning tree • IEEE 802.1x Authentication • IEEE 802.1q Tagged VALN • IEEE 802.3u
Frequency Range	• US/Canada: 11 (1~11) • Major EU countries: 13 (1~13) • Japan 11 (1~14)
WLAN Network Architecture Type	• Infrastructure • WDS
Wireless Transfer Data Rate for IEEE 802.11a & g Draft Standard	IEEE 802.11a & 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/1.2A Input • PCB Dimension: 100 mm x 100 mm • Desktop Instillation • Wall Mountable
Hardware & Antenna	• 1 x RJ45 • 1 x Reset Button • 2x External antennas, 2x embedded antenna • 4 x LED (1 x Power, 1 x LAN, 2 x WLAN)
DHCP Server	• Build-in DHCP server • Support static DHCP assignment • Support Class A, B & C Private IP address & subnet
Security	• WEP 64 bit, 128 bit Encryption • MAC Access Control for the wireless interface • EAP & 802.1x support • Primary & secondary RADIUS server
Management	• Web-Based Management Tool • UPnP • SNMP V1 & V2 • MIB: Ethernet, MIB II, 802.11 • Command line interface with Telnet • Upload & download text-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 • CE • TELEC • DGT
Certificate	• Wi-Fi Class 2.4 GHz 802.11g (Planning)

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

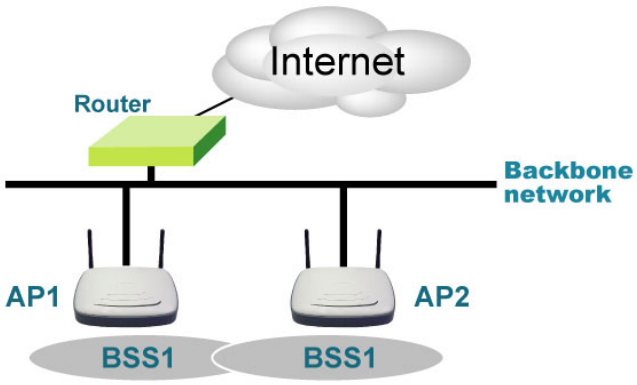
When an 802.11a+g Access Point is used, it can be configured to operate in the following three network configurations

AS AN ACCESS POINT

When configured in the Access Point mode, the 802.11a+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 802.11a+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 802.11a+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.



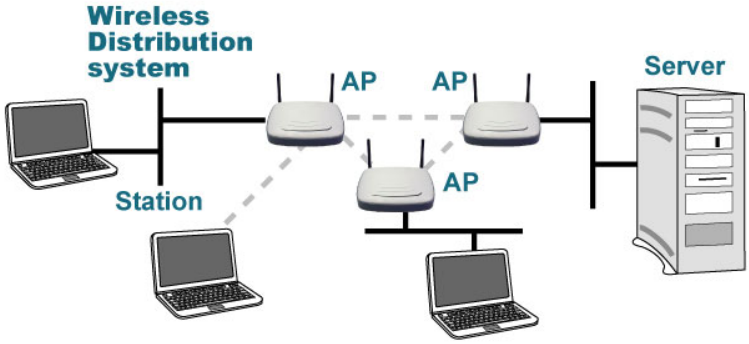
AS A STAND-ALONE REPEATER

The purpose of a repeater is to expand an existing infrastructure BSS. When configured to operate in the Repeater Mode, the 802.11a+g Access Points sit between wireless stations and a "root" AP whose BSS is being expanded, as shown below:

AS A POINT TO MULTI-POINTS BRIDGE

When configured to operate in the Wireless Distribution System (WDS) Mode, the 802.11a+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 802.11a+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:



Setting Up the device

The 802.11a+g Access Point can be managed by a local PC on either the wired or wireless LAN network. To do this, the 802.11a+g Access Point must have an IP address, which can be statically configured, or is dynamically obtained from a DHCP server on the LAN. For reasons to be given in Chapter 3, static IP address assignment is preferred.

STATIC IP

The default IP address of the LAN interface of an 802.11a+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 settings of the DHCP server in the network.

AUTOMATIC IP

The 802.11a+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 in 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

2. Installing the 802.11a+g Access Point

This section describes the content of the package you have purchased, then how to connect and power up your 802.11a+g Access Point, and finally how to configure a PC or wireless client to access/control your 802.11a+g Access Point.

What's in the Box?

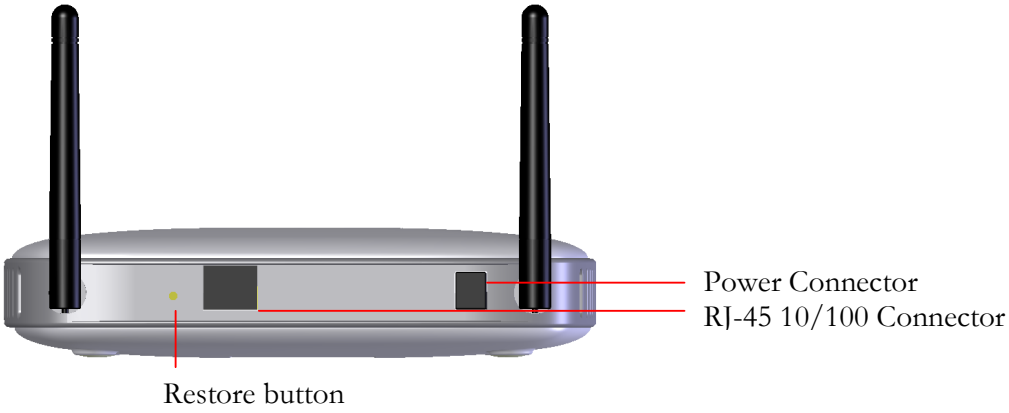
The 802.11a+g Access Point package comes with the following items:

- One 802.11a+g Wireless Access Point

- One 12V 2.5A DC power adapter with a barrel connector
- One Category-5 LAN cable with RJ-45 connector
- One copy of the 802.11a+g Access Point User' Guide

A physical look at the back panel

The following illustration shows the rear panel of the Wireless Access Point.



(1) 1 RJ-45 10/100 connector for connecting to an external Ethernet Switch/Hub with auto-sensing.

(2) 1 DC power connector for connecting through a DC power adapter (included as part of the product) to the wall power outlet.

(3) A Restore button can be used to restore the configuration back to its manufacture settings

A physical look at the front panel

(1) The LEDs on the front of the 802.11a+g Access Point reflect the operational status of the unit.

802.11a+g Access Point LED Description

Label	Power (LED:Red)	LAN (LED:Green)	WLAN 1 (LED:Green)	WLAN 2 (LED:Green)
Steady Red/Green	Power	Link is active	Link is active	Link is active
OFF	No Power	No LAN connection	N/A	N/A
FLASH	N/A	XMT/RCV Data	XMT/RCV Data	XMT/RCV Data

Connecting the Cables

This device is typically installed on the ceiling. Before you actually mount the device, you need to configure the device's IP address. After IP address setting is done, you can manage the device via a Web browser, telnet, or from an SNMP management station remotely. Follow the steps below to configure the 802.11a+g Access Point.

Step 1 Connect a PC/Workstation to the LAN port of the Wireless Access Point.

Step 2 Connect the DC adapter to the Wireless Access Point and an electrical outlet.

To Prepare a PC/wireless client to Configure the 802.11a+g Access Point

This section describes configuration required for the 802.11a+g Access Point before it can work properly in your network.

First, it is assumed that in your LAN environment, a separate DHCP server is available to assign dynamic (and often private) IP addresses to requesting DHCP clients. This means that the 802.11a+g Access Point normally will not need to enable the DHCP server function.

Additionally, since you need to perform various configuration changes to the 802.11a+g Access Point, such as the SSID, Channel number, the WEP key… etc., it is desirable to associate a fixed IP address with the 802.11a+g Access Point, which is why the 802.11a+g Access Point is shipped with a factory default private IP address of 192.168.1.1 (and a network mask of 255.255.255.0).

During the system installation time, you need to set up an isolated environment with the 802.11a+g Access Point and a PC or a wireless client, and then perform the following steps:

Manually change the IP address of the PC/wireless client to become 192.168.1.2 (refer to the steps described in Setting up a Windows PC or wireless client for static IP or as a DHCP client)

If you use wireless client for the configuration, the 802.11a+g Access Point comes with a default SSID "wlan", you can set up your client's wireless connection with the Access Point by scanning for the SSID "wlan".

Connect the PC/wireless client to the 802.11a+g Access Point and change its configuration to a static IP address reserved by your LAN administrator based on the DHCP server setting. For example, if the DHCP server assigns IP addresses of range 192.168.23.1-192.168.23.254 to DHCP client devices, it can reserve 192.168.23.10 for the 802.11a+g Access Point. Please note that at this point the PC/wireless client will lose communication contact with the 802.11a+g Access Point, as they no longer belong to the same IP network address space.

Change the setting of the PC/wireless client back to "obtain IP addresses dynamically".

From then on, any wireless client configured to "obtain IP addresses dynamically" will work with the AP, with each other, or with devices on the wired LAN network.

Configuring a PC running MS-Windows 95/98/Me:

1. Click the Start Button, and select Settings.
2. Click the Control Panel. The Win95/98/Me Control Panel will appear.
3. Open the Network setup window by double-clicking the Network icon.
4. Check your list of Network items. If TCP/IP is already installed, proceed to step 5. Otherwise: (You may need your Windows CD to complete the installation of TCP/IP.)
   - Click the ADD button.
   - In the Network Component Type dialog box, select Protocol.
   - In the Select Network Protocol dialog box, select Microsoft.
   - In the Network Protocols area of the same dialog box, select TCP/IP and click OK.
5. With TCP/IP installed, select TCP/IP from the list of Network Components.
6. In the TCP/IP window, check each of the tabs and verify the following settings:
   Bindings: Select Client for Microsoft Networks and Files and printer sharing for Microsoft Networks
   Gateway: All fields are blank.
   DNS Configuration: Select Disable DNS.
   WINS Configuration: Select Use DHCP for WINS Resolution.
   IP address: Select the Obtain IP address automatically radio button.
7. Reboot the PC.

Configuring a PC running MS-Windows XP/2000:

1. Click the Start button, and choose Control Panel (in Classic View).
2. In the Control Panel, double-click Network Connections.
3. Double-click Local Area Connection.
4. In the LAN Area Connection Status window, select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

Setting up a Windows PC or wireless client for static IP or as DHCP clients

The following will give detailed steps on 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.

For the case of using a LAN attached PC, the PC must have an Ethernet interface installed properly, be connected to the 802.11a+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.

For the case of using a wireless client, the client must also have a wireless interface installed properly, be physically within the radio range of the 802.11a+g Access Point, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

Confirming your PC's IP Configuration:

There are two tools useful for finding out a computer's IP address and default gateway:

WINIPCFG (for Windows 95/98/Me) Select the Start button, and choose Run. Type winipcfg, and a window will appear listing the IP configuration. You can also type winipcfg in the MS-DOS prompt.

The procedure required to set a static IP address is not too much different from the procedure required to set the device 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.

3. Basic Configuration of the 802.11a+g Access Point

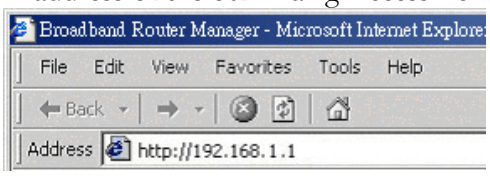
Chapter 3

Although the Command Line Interface (CLI) may also be used to configure the 802.11a+g Access Point, the browser-based configuration mechanism is generally preferred for its ease of use.

The 802.11a+g Access Point is designed so that all basic configuration may be invoked through a standard Web browser such as Internet Explorer.

From a PC or a Wireless client that has been configured as described in Chapter 2, enter the IP address of the 802.11a+g Access Point as the URL in your browser.

To access the 802.11a+g Access Point's management interface for the first time, enter the default IP address of the 802.11a+g Access Point in your Web browser http://192.168.1.1/.



Note: The IP address of your PC must be in the same IP subnet as the 802.11a+g Access Point.

The **Home Page** of the 802.11a+g Access Point screen will appear, with its main menu displayed on the screen, showing the following top-level choices: System Settings, Device Status, Advanced Settings, System Tools, and Help. Selecting any will allow you to navigate to other configuration menus.

Logging On

When you attempt to access a configuration screen from the browser menu, an administrator login screen will appear, prompting you to enter your password to log on. Once you are logged in, you will not be asked to log in again unless your "session" expires such as due to inactivity timeout.

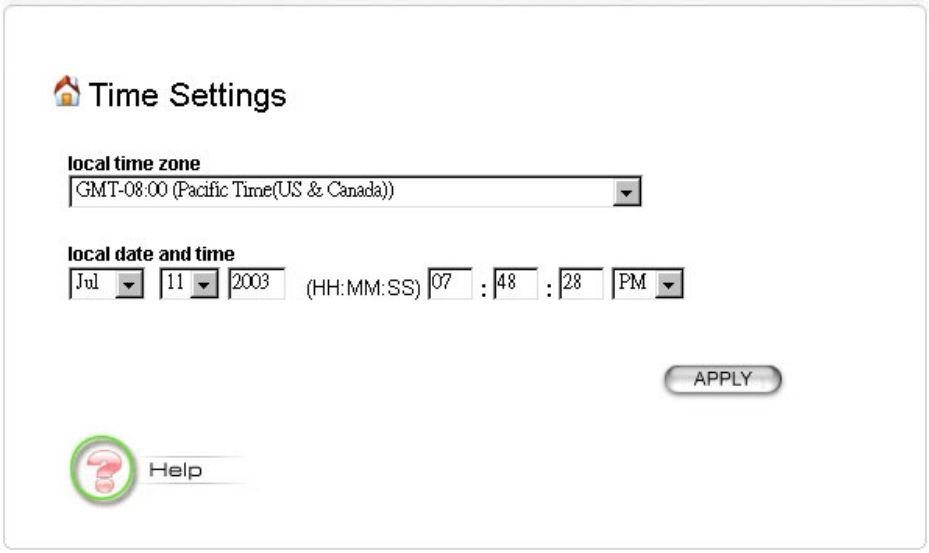
If you are logging in for the first time after you received your 802.11a+g Access Point, you should use the factory default password, "password" to log in. (You should change it as soon as after you log in.)

Characters you type (as your password) will be echoed back as a string of asterisks ("*") for security reasons. After you enter the password, clicking the **LOG ON** button will begin the password verification process and, if successful, your configuration session can begin.

System Settings

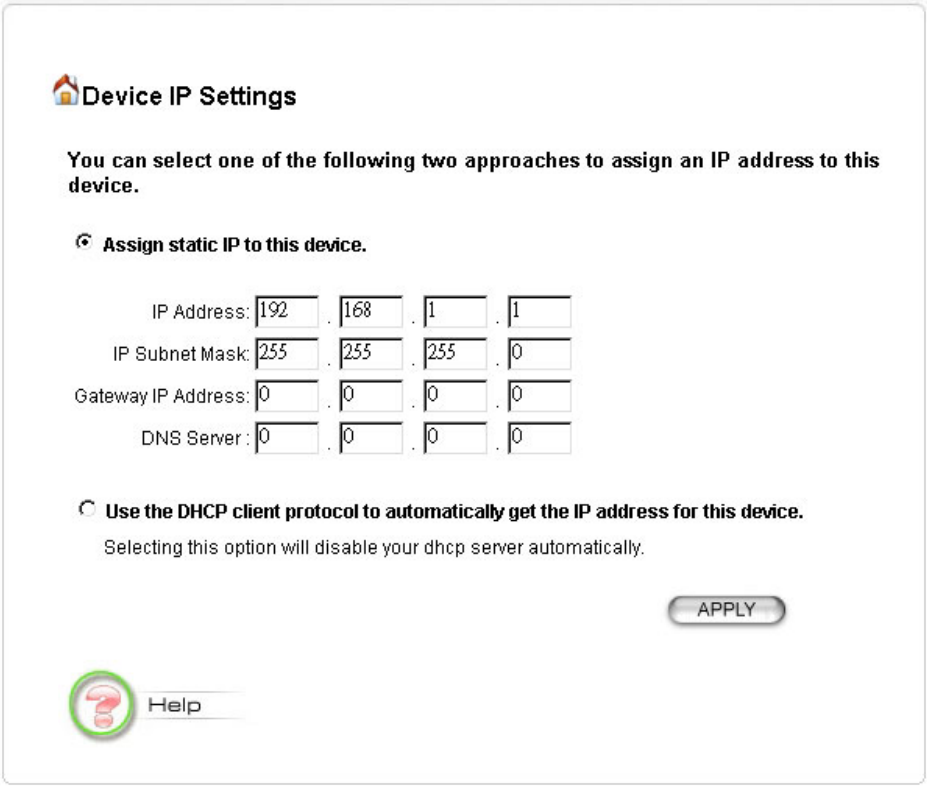
SETTING UP YOUR LOCAL TIME ZONE AND DATE/TIME

After logging in, the **Time Settings** page appears. The Wireless access point time will first be set to the local time of the PC (on which the browser is running). If this time is not correct, modify the appropriate fields as necessary, and then click "APPLY".



DEVICE IP SETTINGS

The **Device IP setting** screen allows you to configure the IP address and subnet mask of your 802.11a+g Access Point: you can configure a static IP address and a subnet mask, or configure it to obtain an IP address and a subnet mask automatically from a DHCP server on the local network.



If you choose to assign a static 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.

This IP address can be modified if necessary, to either a different address in this same subnet or to an address in a different subnet.

> When you modify it, if the DHCP server function of your 802.11a+g Access Point is enabled, the pool of IP addresses it will use for assignment purposes will also be automatcailly adjusted accordingly. For example, if the default IP address is used, the IP address pool for assignment consists of addresses from 192.168.1.2 to 192.168.1.254. However, please do not change the default IP address unless you know exactly what you want to achieve.

Then you should press **APPLY** to effect the change.

If you choose to use an external DHCP Server to automatically assign an IP address to your 802.11a+g Access Point, check the button that says, "**Use the DHCP protocol to automatically get the IP address for this device**", and then press **APPLY** to effect the change.

When an IP address is *dynamically* assigned to the Wireless Access Point, its value can change depending on the IP address assignment policy used by the DHCP server in the network. Since you need to use an IP address to control and manage your 802.11a+g Access Point, without the knowledge of its IP address, in order to access it, you will need to use UPnP (Universal Plug and Play) or other management tools that do not depend on a fixed IP address.

It is strongly recommended that you select the manual static IP address.

Note: If you change the Wireless Access Point's IP address to a different IP network address space, as soon as you click on FINISH you will no longer be able to communicate with your 802.11a+g Access Point. You need to change your IP address and then re-boot your computer in order to resume the communication.

Management access to the 802.11a+g Access Point are restricted to those connections from LAN or wireless clients using SSID that do not have VLAN enabled

CONFIGURE THE SSID SETTINGS

The 802.11a+g Access Point supports multiple SSIDs. Each radio may be configured to support a subset of these SSIDs. However, since the broadcast beacon frame contains only one SSID, only one of these SSIDs will be configured as the primary SSID to be included in the beacon frame. Consequently, client stations wishing to associate with non-primary SSID must explicitly specify the desired SSID. By default, the system will come with a built-in SSID named "**wlan**" which is used as primary SSID for all 2 radios.

Each SSID can be configured to insert an 802.1Q tag into the Ethernet header of all outgoing frames to the wired side. The tag consists of a VLAN ID and 802.1p priority. The system should allow at most one SSID without inserting the tag. If there are more than one SSID set to not including the tag, these SSIDs will function as one bridged network. This means clients will be able to communicate with each other even though they are associated with different SSIDs.

Although the multiple SSID feature allow different security policy to be applied to different SSID, IEEE 802.11 standard was not originally designed for multiple SSID type of configurations mainly due to the following reason.

The Beacon frame carries the special information element when WPA is enabled, and it has the Privacy flag set in the capability field when either 802.1x or WPA is enabled. Since all SSIDs are sharing the same Beacon frame, if these settings are not consistent for all SSIDs, stations may be confused and their behavior may differ depending on their implementation. Detailed information is described in the "Application notes for Security Control for Multiple SSIDs".

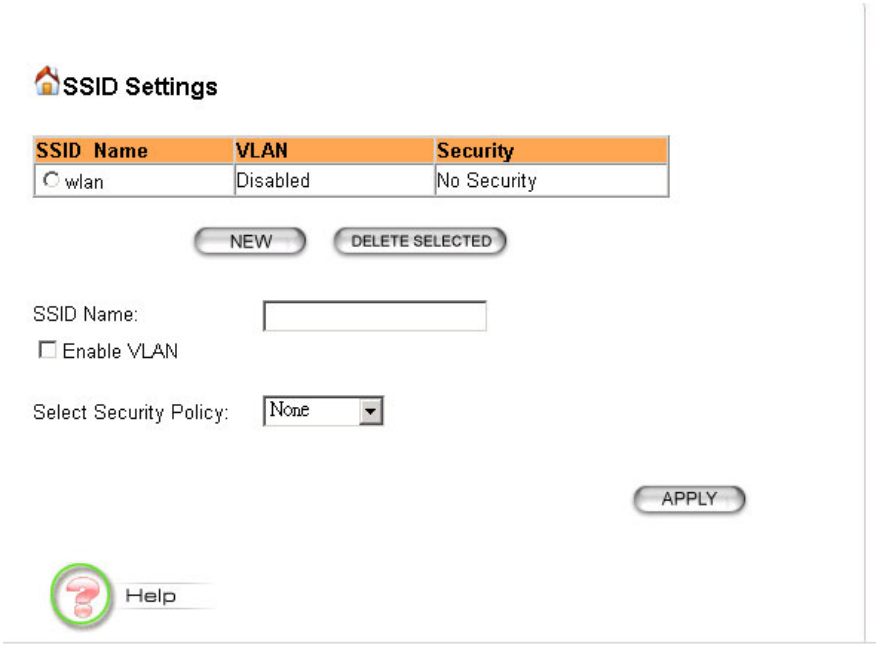
The following policies are supported:

- None: This policy offers no encryption or authentication;
- WEP: Support WEP 64/128 bits;
- 802.1x: 802.1x uses RADIUS infrastructure for wireless clients authentication. When wireless client stations request to access the wireless network, the Wireless Access Point will act as a RADIUS client, and send access requests to RADIUS server. The RADIUS server performs authentication of users and control network access through centralized access policies. If you select this policy, you must configure RADIUS settings;
- WPA with Pre-Shared Key: This is typically used in a SOHO environment where there are no central authentication servers available. When this policy is selected, you will need to manually configure the key in the wireless access point as well as those clients using this very SSID;
- WPA: WPA uses TKIP for data encryption and utilizes a central authentication RADIUS server and implements 802.1x with EAP to provide a framework for strong user authentication. If you select this policy, you must configure RADIUS settings.

We strongly recommend you follow these guidelines when you design your security:

- The system should allow at most one SSID using "none" as security policy. The system assumes that different SSIDs use different WEP keys. The only clients that can receive and process packets are those with the correct WEP keys.
- If WPA or WPA-PSK is not required, setting default security policy to plain text will allow most combination to be used. However, if plain text is not required, use of 802.1x or static WEP as default would work just fine.
- If WPA or WPA-PSK is used in any of the SSIDs, default security policy needs to be WPA or WPA-PSK to allow stations to associate with the access point.

The following describes the SSID related settings.



This screen allows you to configure SSID. On the top of the screen, it will display a list of configured SSID. From this list, you can edit or remove an SSID. If you want to modify the entry, select the radio button for the entry. If you want to delete the entry, select the entry then click DELETE SELECTED. If you want to add an SSID, just clicking the NEW button.

Please note, you can not delete an SSID that is used as a primary SSID for any of the radios.

SSID 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 to communicate. Several wireless devices on a network can have the same SSID. The SSID can be up to 30 characters long.

Enable VLAN: If you want to enable the VLAN feature, select the check box.

VLAN ID: This specifies the VLAN ID value to be included in the 802.1Q tag. This setting must match the VLAN ID setting on the access point. The valid range is from 1 to 4094 inclusive with 1 being the default.

802.1p priority: Select a traffic category from the pull down list, and this will be mapped to the 802.1p based on the following:

Traffic Category	802.1p value
Best Effort	0
Background	1
Excellent Effort	3
Controlled Load	4
Interactive Video	5

Interactive Voice	6
Network Control	7

Select Security Policy:

Select desired security policy from the pull-down list. You can use encryption to protect your data when you are transmitting data in the wireless network.

None: You can select **None** to disable encryption

WEP: Select WEP for static WEP encryption. Then select one of four WEP keys to transmit/receive data in the wireless network.

You can enter a "Passphrase" (a key of up to 30 alphanumerical characters), choose 40-bit, and press the "Generate" button to generate four 40-bit keys in the entries below, or choose 128-bit, and press the **Generate** button to generate one 128-bit key in the first entry.

Alternatively you can manually configure each of them.

When you manually configure a key (an alphanumeric string), the length for a 40-bit WEP must be equal to 5, and that for a 128-bit WEP key must be equal to 13. Once you enable the WEP function, please make sure that exactly the same WEP key is configured in both the Wireless Access Point and client stations.

You can define a key using ASCII or hex characters. A WEP128 ASCII key looks like "An ASCII key!" (13 characters), while a WEP40 hex key looks like "44-12-24-A8-B2" (5 characters).

Please note that some Wireless Client Cards allow Hexadecimal characters only.

802.1x: Select 802.1x will use RADIUS infrastructure for wireless clients authentication.

WPA: Select this will enable the TKIP for data encryption and 802.1x for authentication.

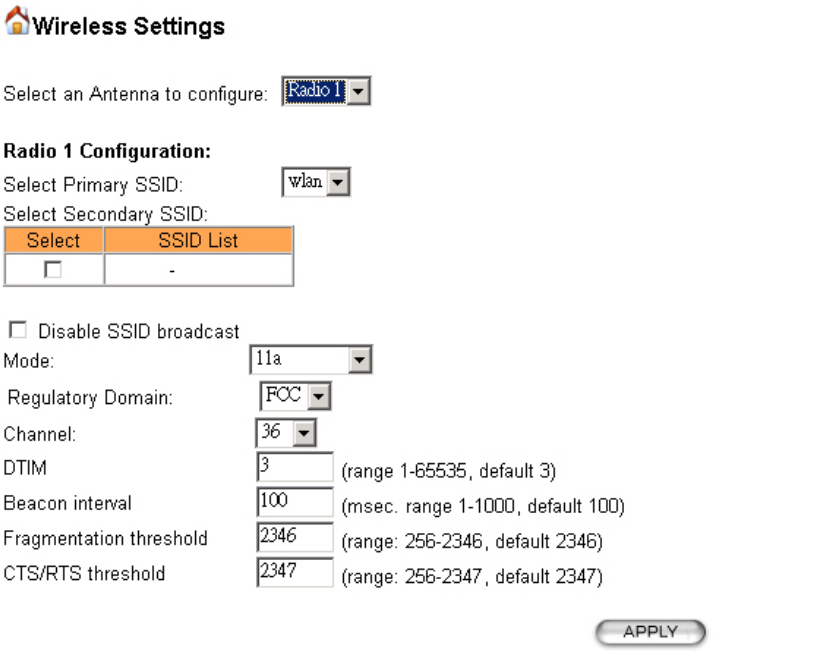
WPA-PSK: Select WPA-PSK to use the statically configured passphrase (pre-shared key) for authentication. The same passphrase should be configured in both the Wireless Access Point and client stations. The length of pre-shared key is between 8 and 63, consisting of alpha-numeric characters.

CONFIGURE YOUR WIRELESS LAN CONNECTION

The IEEE 802.11 specifications require that only one SSID be broadcast in beacon frames, so you must define a primary SSID to be broadcast in IEEE 802.11 beacon frames. All other SSIDs are

secondary SSIDs and are not broadcast in beacon frames. If a client sends a probe request with a secondary SSID, the access point responds with a probe response with a secondary SSID.

In the following configuration screen, you can configure wireless related parameters of your 802.11a+g Access Point:



Select an Antenna to configure: Select the desired radio for configuration from the pull-down list.

Primary SSID: Select one of the SSIDs from available list to be used as the primary SSID.

Secondary SSID List: You can select one or more than one SSIDs to be the secondary SSID.

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 APs in the wireless network. Select **Disable** if you do not want the device to broadcast the SSID.

Mode: You can select the device to run the **802.11g only** protocol, or the **mixed mode** – allowing both 802.11g and 802.11b to co-exist., or 802.11a, or 802.11a turbo mode.

Regulatory Domain: You can select the regulatory domain where the device will be running. Possible choices include FCC, ETSI, France, Spain, and Japan.

Channel: Select the channel from the available list to match your network settings. All devices in the wireless network must use the same channel and share the total bandwidth available.

Note: Suggest to use different channel for the 2 radios to avoid interference problem.
Too adjacent channels may result in interference, too. Suggest to use the default channel. That is Channel 1 for radio1, Channel 6 for radio2.

Note: The available channel numbers are different from country to country.

USA and Canada: CH01~11, Europe: CH01~CH13, Japan: CH01~CH14, France: CH10~CH13, Spain: CH01~CH13

Beacon Interval: The 802.11a+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. Its default value is 100; 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 256-2432 bytes, with a default value of 2432. A value of zero activates the RTS/CTS handshake before every transmission. 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, the frame will be fragmented before transmission. The threshold should have a value of 256-2346 bytes, with a default value of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

DTIM Interval: The 802.11a+g Access Point buffers packets for stations that operate in the power-saving mode. A Delivery Traffic Indication Message (DTIM) contains information on which power-conserving stations have packets waiting to be received. The DTIM interval specifies how often beacon frames should contain DTIMs. It should have a value between 1 and 255, with a default value of **3**.

Chapter 4

4. Advanced Settings

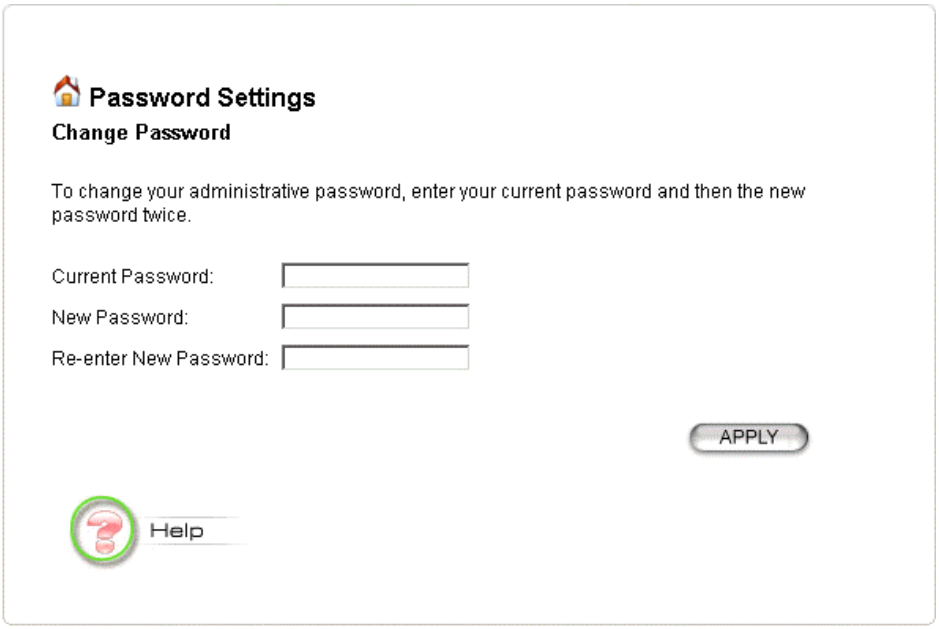
This section contains advanced setting procedures for the 802.11a+g Access Point. It describes modifications that normally you may not need for basic system operation. One exception is changing your password: it is highly recommended that you change the default factory setting as soon as you start to use your 802.11a+g Access Point.

Password Settings

Your 802.11a+g Access Point comes with a default factory password of "password". After you start using the Wireless Access Point, you should change the default password.

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

If you forgot the password, the only way to recover it is to return the device to its default state as shipped from the factory. To restore the password to the default password, please refer to the section, "What if I forgot the Password?" in the user manual.

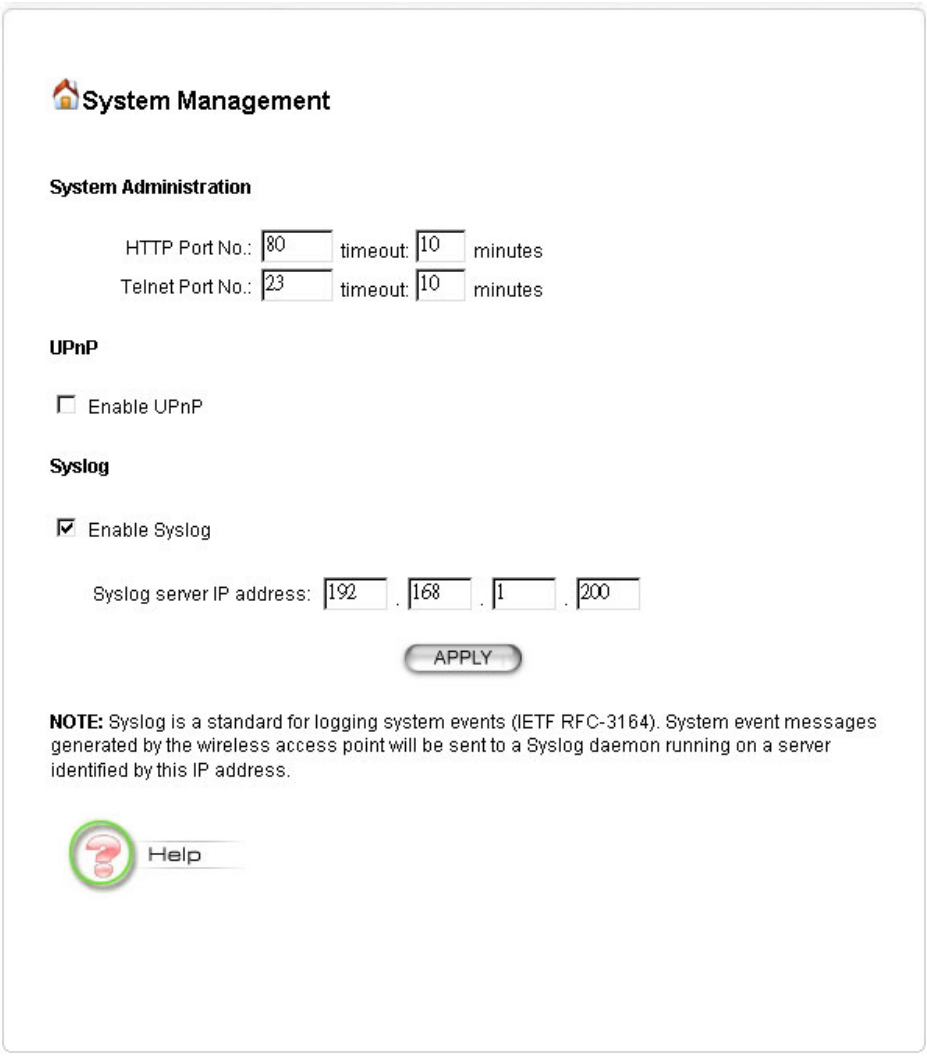


System Management

Clicking the **System Management** button allows system related parameters to be configured for the 802.11a+g Access Point.

System Administration: The Wireless Access Point allows you to designate special port numbers other than the standard 80 and 23, respectively, for **http** or **telnet** for remote management. It also allows you to specify the duration of idle time (inactivity) before a web browser or telnet session times out. The default time-out value is 10 minutes.

UPnP: The Wireless Access Point's Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover the Wireless access point and automatically show an icon on its screen. You can double-click the icon to access the Wireless access point directly (without having to specify its IP address).

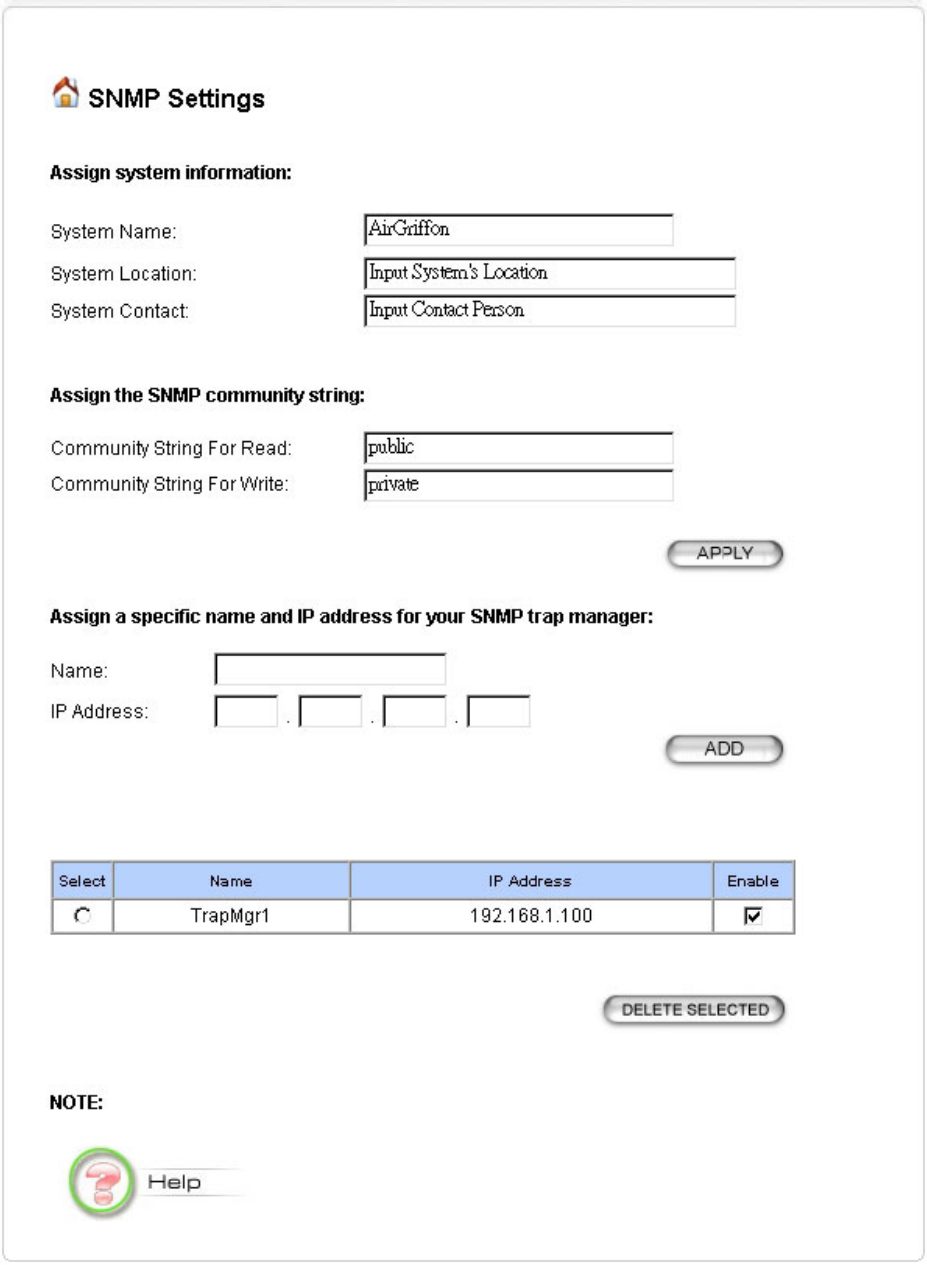


Syslog: Syslog is an IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164). When the 802.11a+g Access Point encounters an error or warning condition (e.g., a log-in attempt with an invalid password), it will create a log in the system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

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

SNMP Settings

This screen allows you to configure SNMP parameters including the system name, the location and contact information. Additionally, you can configure the 802.11a+g Access Point to send SNMP Traps to remote SNMP management stations. Traps are unsolicited alert messages that 802.11a+g Access Point sends to remote management stations.



System Name: A name that you assign to your 802.11a+g Access Point. It is an alphanumeric string of up to 30 characters.

System Location: Description of where your 802.11a+g Access Point is physically located. It is an alphanumeric string of up to 64 characters.

System Contact: Contact information for the system administrator responsible for managing your 802.11a+g Access Point. It is an alphanumeric string of up to 64 characters.

Community String For Read: If you intend the Wireless access point to be managed from a remote SNMP management station, you need to configure a read-only "community string" for read-only operation. The community string is an alphanumeric string of up to 32 characters.

Community String For Write: For read-write operation, you need to configure a write "community string".

A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the Wireless access point) and sent to in the network.

You can define trap managers in the system.

You can add a trap manager by entering a **name**, an **IP address**, followed by pressing the **ADD** button.

You can delete a trap manager by selecting the corresponding entry and press the **DELETE SELECTED** button.

You enable a trap manager by checking the **Enable** box in the corresponding entry or disable the trap manager by un-checking the Enable box.

DHCP Server Settings

The DHCP server option allows the 802.11a+g Access Point to assign IP addresses to DHCP client devices on your wired or wireless LAN to obtain IP addresses automatically.

If you want the Wireless access point to act as a DHCP server and assign private IP addresses to requesting DHCP clients on the LAN, you need to check the **Enable DHCP Server** box.

You can select one of the following two ways to assign IP addresses:

Assigns IP addresses to wired or wireless clients from the following range:

When IP addresses are assigned to a requesting DHCP client, after the "**lease time**", the client is expected to renew the lease. Its default value is 10080 minutes (7 days).

The **from** and **to** range of IP addresses to be assigned to requesting DHCP clients can be configured manually, with the default being 2 to 254.

After you enter the information, you should press **APPLY**.

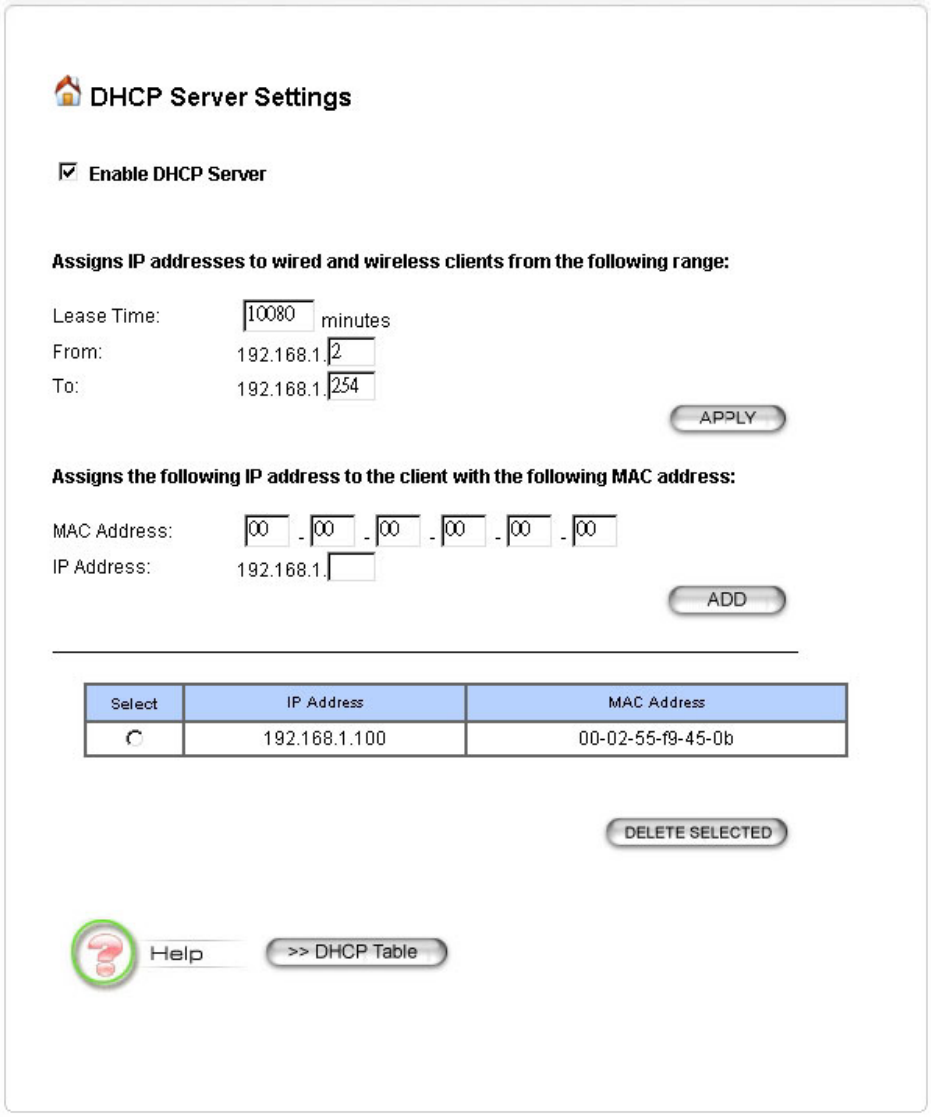
Assigns the following IP address to the client with the following MAC address:

You can also specify the **IP address** to be assigned to a device with a pre-configured **MAC address**.

You can add such a mapping by entering a MAC address, and the IP address to be assigned, followed by pressing the **ADD** button. Up to 20 mappings can be added.

You can delete a mapping by **select**ing the corresponding entry and press the **DELETE SELECTED** button.

DHCP Table: Press this button will cause the screen to jump to DHCP client table page.



MAC Filtering Settings

The 802.11a+g Access Point allows you to define a list of MAC addresses. One of three mutually exclusive rules can be selected to forward/filter data packets based on these MAC addresses.

- **Disable MAC address control list**: When this radio button is selected, no MAC address filtering will be performed.
- **Enable GRANT address control list**: When this radio button is selected, only packets received from the wireless LAN interface with the configured MAC addresses will be allowed/forwarded.

- **Enable DENY address control list**: When this radio button is selected, only packets received from the wireless LAN interface with the configured MAC addresses will be denied/filtered.

Once a choice is made, the choice applies to all filtering rules.

To add a filtering rule, configure the following:

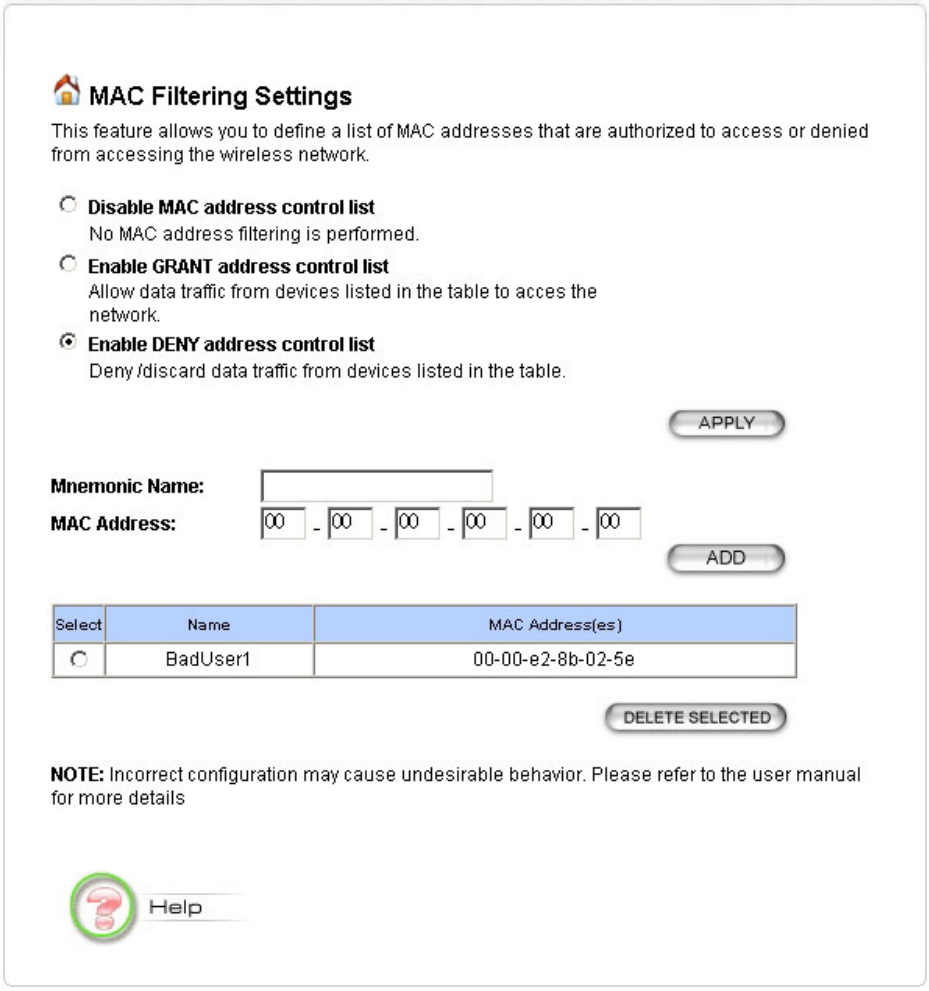
Mnemonic Name: the name to identify the filter

MAC Address: the MAC address for grant or deny.

After you finish the above, you can press the **ADD** button to add the entry to the table.

You can delete an entry by **select**ing the corresponding entry and press the **DELETE SELECTED** button.

Note: Improper setting of MAC address and usage of wireless to configure may make you lose your management session after pressing "Apply".



RADIUS Settings

RADIUS servers provide centralized authentication services to wireless clients. Up to two RADIUS servers can be defined, one acting as a primary, and the other acting as a backup. Two user authentication methods can be enabled with an external RADIUS server: one based on **MAC** address filter, the other based on 802.1x .

MAC address filtering based authentication requires a MAC address filter table to be created in either the 802.11a+g Access Point and/or the RADIUS server. During the Authentication phase, 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 which 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 stations to be authenticated, in this case your 802.11a+g Access Point.

Depending on the security policy you selected, the 802.1x EAP will be automatically enabled if any of selected policies includes WPA, or 802.1x. The system will support the following popular EAP types: EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP with MS-CHAP v2.

Here is a description of how the RADIUS server retry algorithm is implemented in the 802.11a+g Access Point software:

After a RADIUS request is sent, the 802.11a+g Access Point will wait 1 second for a reply. If no reply is received, the request frame is resent. The wait period for a reply is doubled every time, and the request is sent repeatedly, up to the value configured in **RADIUS Server Retry Times**.

The same attempt and retry logic is used for the secondary server.

A configurable interval value, **RADIUS Server Reattempt Period**, controls how many minutes the access point will use the backup server before again attempting to use the primary server. Once the interval expires, the primary will again be used, independent of the success/failure history of the primary or backup server.

The following describes RADIUS related settings:

Enable MAC Address Access Control: Check this box if you want to enable the MAC authentication feature on an external RADIUS server.

Enable Primary Server: To configure the primary server, check the "Enable Primary Server" box, and configure the following parameters: Please note, you must enable the primary server first before you can enable the secondary server.

Server IP: The IP address of the RADIUS server

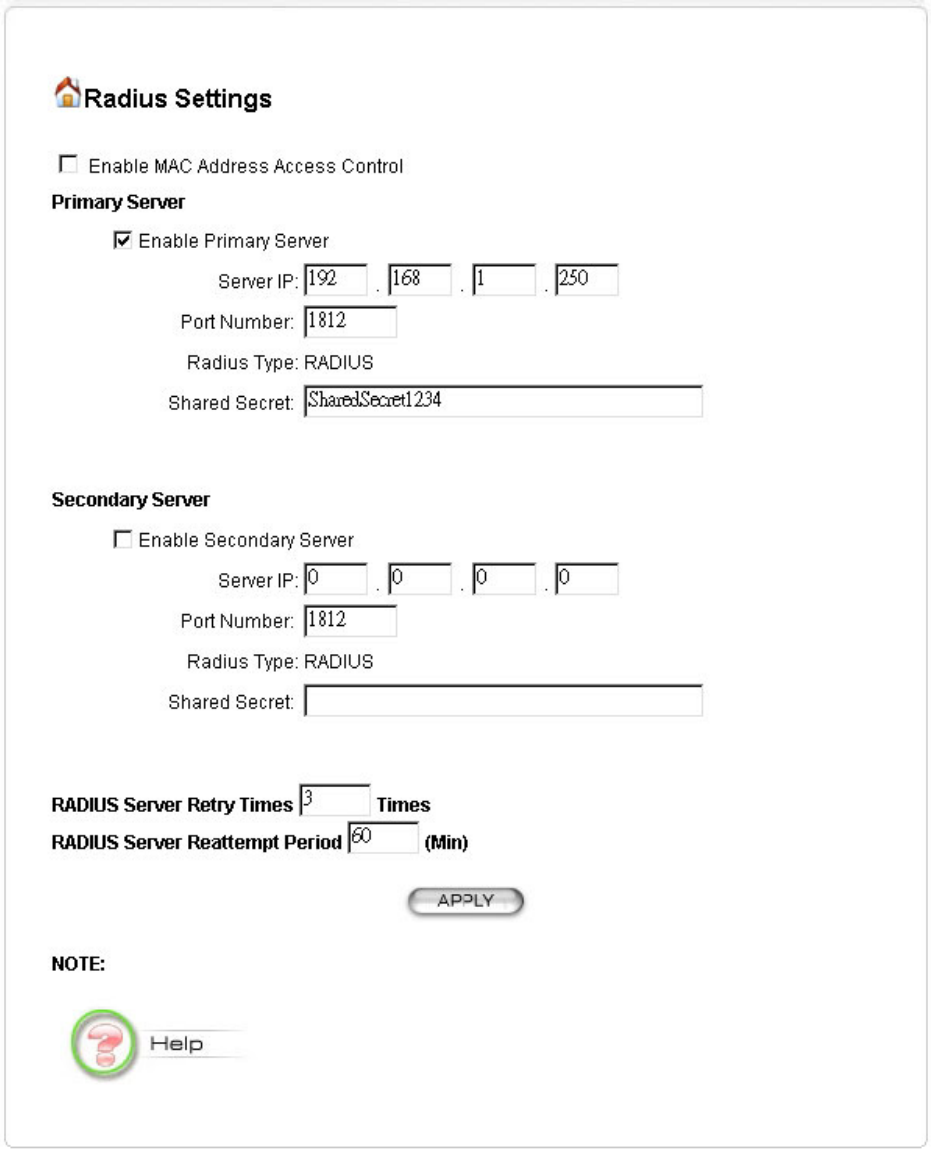
Port Number: The port number your RADIUS server uses for authentication. The default setting is 1812.

Shared Secret: This is used by your RADIUS server in the Shared Secret field in RADIUS protocol messages. The shared secret configured in the 802.11a+g Access Point must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.

Enable Secondary Server: To configure the secondary server, check the "Enable Secondary Server" box, and configure the same parameters as for the primary server.

RADIUS Server Retry Times: The number of times the 802.11a+g Access Point should attempt to contact the server before giving up.

RADIUS Server Reattempt Period: This is the amount of time the Wireless Access Point will wait before it tries to reconnect to the primary RADIUS server if the secondary RADIUS server is in operation at the time.

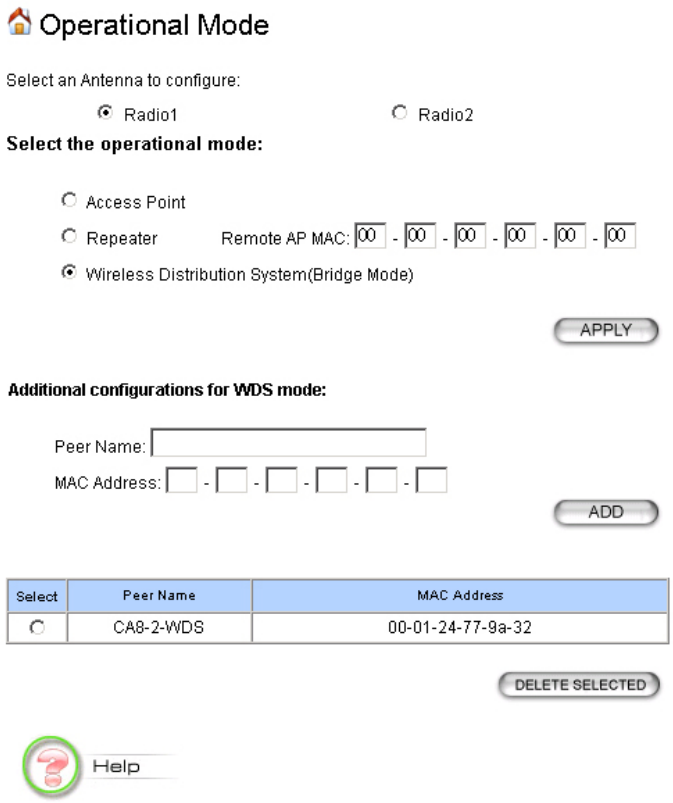


Operational Mode

The 802.11a+g Access Point can be configured to operate in one of the following three modes as mentioned previously in Chapter 1:

- As an Access Point
- As a repeater, or
- As a Wireless Distribution System

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



Chapter 5

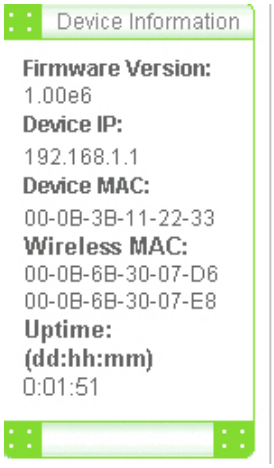
5. Managing your 802.11a+g Access Point

This Chapter covers other management aspects of your 802.11a+g Access Point:

- How to view the device status
- How to view the system log
- How to upgrade your 802.11a+g Access Point firmware
- How to save or restore configuration changes
- How to reboot your 802.11a+g Access Point
- What if you forgot the password

How to View the device Status

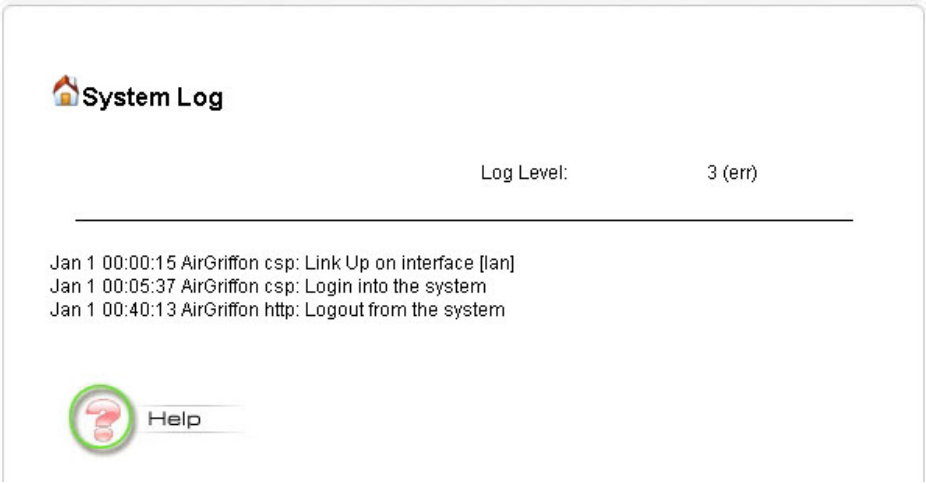
You can monitor the system status and get general device information from the **Device Information** screen:



How to View the System Log

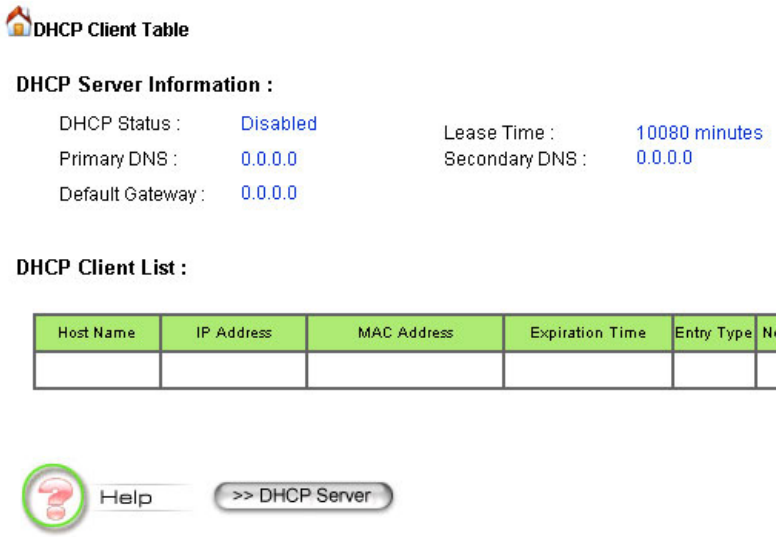
The 802.11a+g Access Point maintains a system log that you can use to track events that have occurred in the system. Such event messages can sometimes be helpful in determining the cause of a problem that you may have encountered.

You can select **System Log** on the left 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 (e.g., a low number such as 2 means critical).



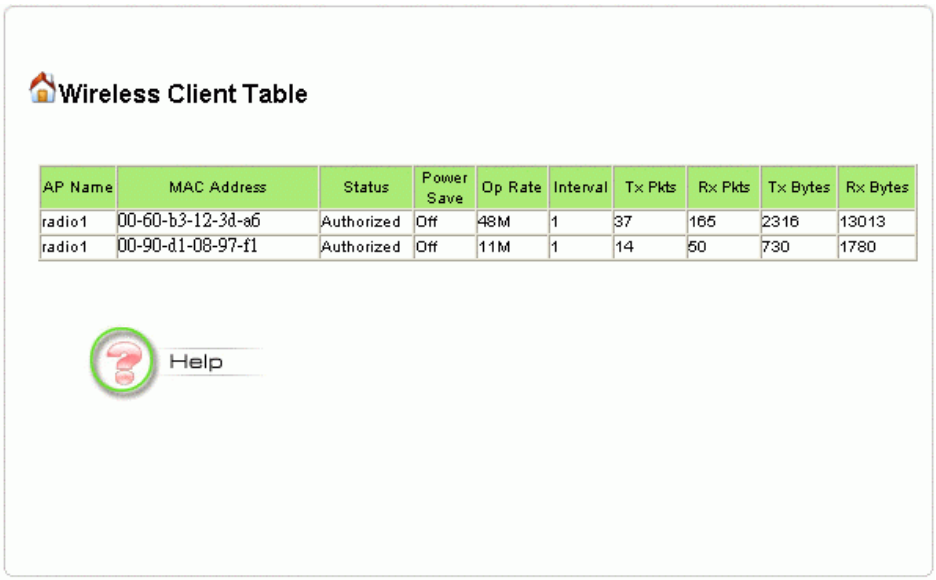
DHCP Client Table

The DHCP client table lists current DHCP clients connected with its host name, IP address, MAC address, expiration time, and entry type.



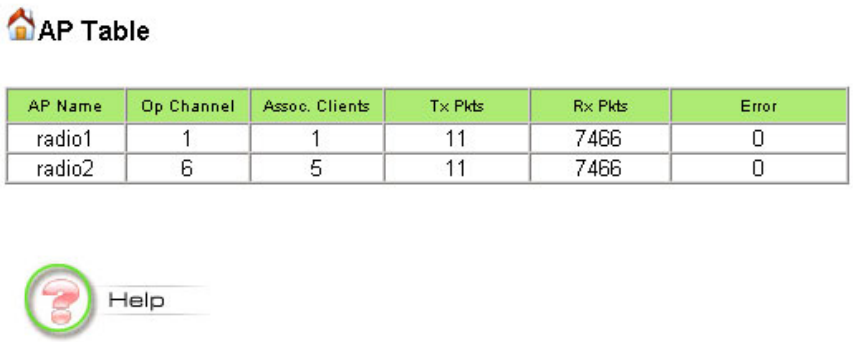
Wireless Client Table

The wireless client table lists the current wireless clients with its MAC address, state, transmitted packets, and received packets.



AP Table

The AP table shows the current status of the radios in the system.



Upgrading Firmware

You can upgrade your 802.11a+g Access Point's firmware (the software that controls your 802.11a+g Access Point's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems you have encountered when using the current version. System upgrade can be performed through the System Upgrade option as follows:

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

Step 2: To update the 802.11a+g Access Point firmware, first download the firmware from the distributor's web site to your local disk. Then from the above screen enter the path and filename of the

firmware (or click **Browse** to select the path and filename of the firmware). Next, Click the **Upgrade** button.

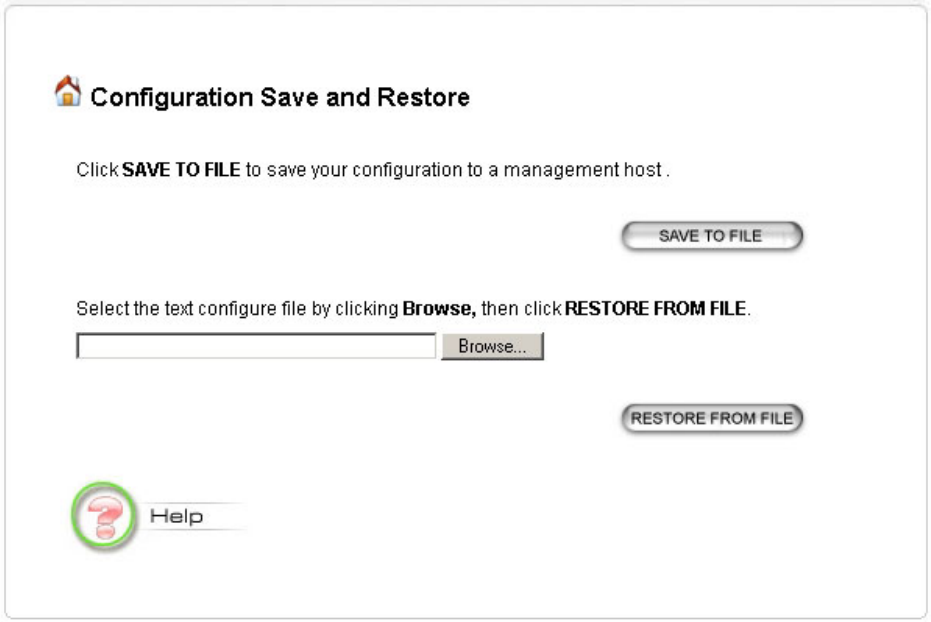
The new firmware will begin loading to your 802.11a+g Access Point. After a message appears telling you that the operation is complete, you need to reset the system to have the new firmware take effect.

Note: It is recommended that you do not upgrade your 802.11a+g Access Point **if you are happy with its operation.**

How to Save or Restore Configuration Changes

You can save system configuration settings to a file, and later download it back to the 802.11a+g Access Point system by following the steps below.

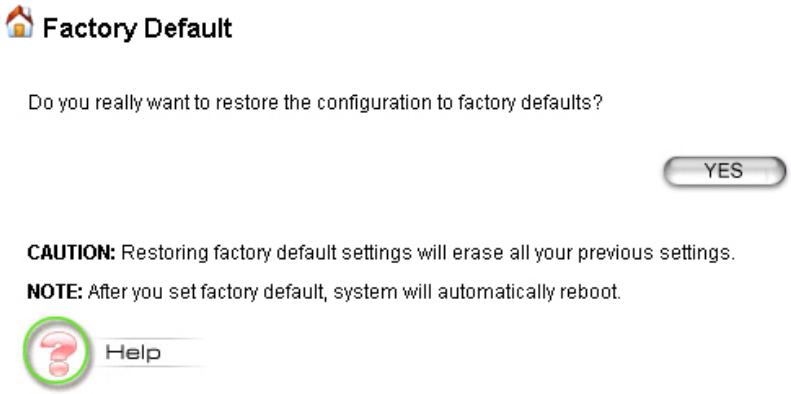
Step 1 Select **Configuration Save and Restore** from the **System Tools** menu and the following screen displays:



How to set your 802.11a+g Access Point to Factory Default

You can reset your 802.11a+g Access Point to the factory default from the Brower. To reset it:

Step 1 Select **Factory Default** from the System Tools menu, the following screen shows:

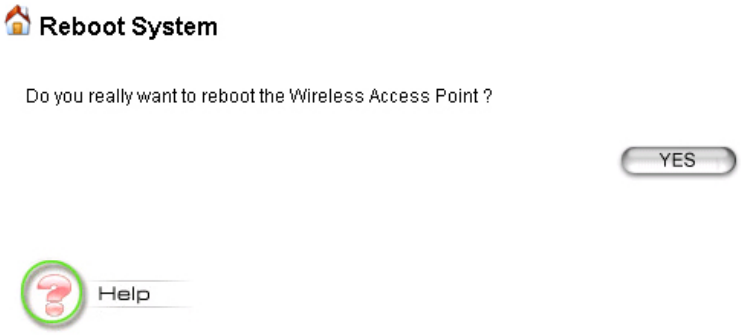


Step 2 Click **YES** to restore the configuration to factory default.

How to Reboot your 802.11a+g Access Point

You can reset your 802.11a+g Access Point from the Brower. To reset it:

Step 1 Select **Reboot System** from the System Tools menu, the following screen shows:



Step 2 Click **YES** to reset the 802.11a+g Access Point.

Note: Resetting the 802.11a+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 device for two seconds. Please note that this will require you to re-enter all of your configuration data.

Chapter

6

6. Command Line Interface

This document defines the Command Line Interface (CLI) for the 802.11a+g Access Point. The CLI is accessible through a Telnet session.

General guidelines

When the 802.11a+g Access Point is powered up, the user can use a standard telnet application from a PC connected to the network to perform configuration and management functions. This is done by typing the telnet command, "telnet <the 802.11a+g Access Point's ip>" (the default is 192.168.1.1) and pressing a return key, the user will see a system sign-on message followed by a password prompt as follows.

Wireless Access Point Manager Console Version: rev_no
Please enter your password: ********

A default password "*password*" has been pre-configured with the system. The user should use it to log into the system until the password is explicitly changed using the ***change password*** command. Note that the entered password is case-sensitive. This password may also be changed using the browser-based GUI configuration utility.

A default password "*password*" has been pre-configured with the system. The user should use it to log into the system until the password is explicitly changed using the ***change password*** command. Note that the entered password is case-sensitive. This password may also be changed using the browser-based GUI configuration utility.

The password entered will be echoed as asterisks (*). After the Carriage Return is entered, if the password string is validated, the command prompt ***Command>*** will be displayed, and the user can then issue other commands. Otherwise, the password prompt will be redisplayed.

Most commands are single-line commands, and commands are not context sensitive: each command is independent of other commands before or after it.

The command syntax is straightforward.

The following briefly summarizes the guideline for the interface.

- At any time, the user can type a "**?**" (preceded by a space) to request context-sensitive help on what the user can enter next.
- At any time, the user can type control-p (^p, by pressing both the Ctrl key and the p key at the same time) to repeat the previous command, or control n to return to the following (next)

command. At startup, typing ^p or ^n will not cause anything to happen - since previous commands do not yet exist. In normal operation, typing ^p will cause the previous command to show, and the cursor will sit at the end of the command. At this point, the user can either type a carriage return to accept the command, or type backspaces to edit the command from the end. Up to 15 previously entered commands can be invoked through ^p's and ^n's.

- If a keyword is expected when the user types " ?", all valid keywords will be displayed. The command typed in so far will then be displayed again along with the cursor sitting at the end, waiting for the user to continue.
- If the user types in part of the keyword but does not type in the entire word, the user can then enter a tab or space for the system to automatically complete the keyword if the characters typed in so far can uniquely identify the keyword. If the characters typed in so far do not uniquely identify a keyword, a list of possible keywords will be displayed.

If the user is not sure what to type next, he or she can type "?" to display the possible keywords that match the current CLI command input.

If an interactive mode is entered, the system will prompt for each required parameter, such as:

…

select regulatory domain (fcc, fcc/etsi/france/spain/japan):

enter channel number (10, 1-14):

…

The first prompt means there are five choices (FCC, ETSI, France, Spain, or Japan), with FCC being the current setting. The second prompt means a number between 1 and 14 is expected, with 10 being the current setting.

During the first time a particular parameter is configured, typing a carriage return will cause the default value to be selected. Otherwise, typing a carriage return means no change to the current value.

Express Mode vs. Advanced Mode of operation

The Command Line Interface operates in one of two modes: ***Express Mode*** or ***Advanced Mode***. In Express Mode, not all parameters are displayed. Default values are set for those parameters not displayed in multi-line commands. In Advanced Mode, users have the option to modify all possible values appropriate to each operation.

The user can toggle between Express Mode and Advanced Mode by typing ^E (Control-E) at any time. Normally, the system prompt will be changed by appending ">>" to the configured prompt when in Advanced Mode.

Conventions

The following notations will be used:

- lan means the LAN port;
- wlan means the Wireless port;
- <> specifies the arguments of the command, <1-4> means a number between 1 to 4;
- [ ] indicates a required or optional parameter, or choice of parameters;
- MacAddr, or XX-XX-XX-XX-XX-XX means any MAC address in hexadecimal format, where each nn can be 00, 01, ... 99, 0A, 0B, 0C, 0D, 0E, 0F, 10, 11,… FF;
- ipAddr, netmask, or xxx.xxx.xxx.xxx means any ip address or network mask, where xxx is a decimal integer between 0 and 255;
- the term *string* means a string of characters up to the specified length, which may be enclosed in double quotes (") (required if the string contains embedded blanks;
- Names representing filters and MAC addresses should be up to 30 characters in length; password and SNMP community read/write strings are up to 15 characters in length. When the password and SNMP community write string are entered, they are echoed back as a string of "*"s for protection, while other parameters, such as WEP keys, are echoed back the way they are typed (in clear text).

Command List

From a functional point of view, CLI commands will be grouped into the following categories:

(1) System
(2) Port
(3) Filtering
(4) DHCP Server
(5) SNMP
(6) Diagnostics
(7) Security
(8) Wireless

The command format will be described in the following sections, some with description and examples as follows:

Command Syntax

Description: the description of the command is given here.

Example:

```
Command>>> command (with parameters)
```

Output …