AAP 3000

WLAN TurboSecure™ AP/Bridge/Repeater

User's Manual

Version 1.0

WARNING - Disclaimer

Do not use this device in applications for which any failure of the wireless link or any data error may cause death, injury or damage of any kind.

Aboundi Inc., its Sales, Manufacturing and Design Organizations, Reps., Distributors, VARs and distribution channels are absolutely not liable for any death, injury, property damage, loss of data, and loss of business of any other unmentioned loss. The aforementioned entities are not liable even in the event that any of these entities were apprized of the specifics or generalities of an application or intended installation at any time.

Radio Linkages of any type can be fragile and tenuous. Over 1/5th of the entire population of the world now owns cellular telephones, and as any user of a cell phone knows, the cell phone radio communications link may be easily disrupted or completely lost simply by turning your head or by other small environmental movements or changes. This clearly demonstrates to everyone the fragility of any radio link and why radio should not be used for critical implementations, or where death, personal injury, physical damage, property damage or environmental damage may result.

Aboundi Inc products are not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to the operation of nuclear facilities, aircraft navigation, vital communication systems, air traffic control, life support machines, weapons systems, or any industry in which environmental disruptions or technology failure could lead directly to death, personal injury, physical damage, property damage or environmental damage.

Statement of Conditions
The content described in this manual may be improved or changed at any time and it is subject to be changed without notice.
Manufacturer assumes no responsibility for errors contained herein or for direct, indirect, special, incidental or consequential damages with the furnishing, performance, or use of this manual or equipment supplied with it, even if manufacturer of its suppliers have been advised of the possibility of such damages.

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

Limited Warranty

This product is warranted by manufacturer to be free from defects in material and workmanship for one (1) year from the date of purchase unless otherwise stated.

During this period if this product is found to be defective in material or workmanship, manufacturer or one of its authorized service facilities will at its option either repair or replace this product without charge, subject to the following conditions, limitations and exclusions:

This warranty extends to the original consumer purchaser only and is not assignable or transferable.

This warranty shall not apply to any product which has been subjected to misuse, abuse, abnormal use, negligence, alteration or accident, or has had its serial number altered or removed.

This warranty does not apply to any defects or damage directly or indirectly caused by or resulting from the use of unauthorized replacement parts and/or service performed by unauthorized personnel.

This warranty does not apply to the software driver that accompanies this product.

This warranty is made expressly in lieu of all other warranties, expressed or implied, including but not limited to any implied warranty of merchantability of fitness for a particular purpose, and all other obligations on the part of Manufacturer provided, however, that if the disclaimer of implied warranties is ineffective under applicable law, the duration of any implied warranties arising by operation of law shall be limited to one (1) year from the date of purchase or such longer period as may be required by applicable law.

Manufacturer hereby disclaims any and all liabilities for consequential and incidental damages arising out of or in connection with any breach of this warranty or any other claim with respect to this product, including but not limited to claims of negligence, strict liability in tort or breach of contract.

Table of Contents

1. Introduction

Thank you for purchasing this 802.11g AAP3000 WLAN TurboSecure^{TM} AP/Bridge/Repeater (hereafter we call this product as AAP3000). The AAP3000 supports IEEE802.11g/b, IEEE802.1x, and IEEE 802.3/802.3u compliance devices. It is designed to meet the mobility, performance, security, interoperability, manageability, and reliability requirements in the ever demanding wireless networking application environments.

It is extremely easy and secure to configure via web browser. Its access control is achieved through the MAC address filtering and the WPA/WPA2 (Wi-Fi Protected Access) security algorithm meets the stringent security protection needs.

The AAP3000 provides WDS function which allows two geographically separated LANs to be wirelessly interlinked in addition to serving as a WLAN base station (Access Point).

The AAP3000 is designed for the ease of installation and future upgradeability with features such as automatic MDI –MDIX detection on the RJ45 LAN port and downloadable flash-upgradeable firmware.

Overall, the AAP3000 is a versatile and cost effective solution for your office, commercial or home WLAN application needs.

1.1 Features

- Compatible with WLAN 802.11g/b devices
- AP mode or AP-client mode selection
- Supports WDS (Wireless Distribution Systems)
- Supports full mobility and seamless roaming
- Supports RADIUS (Remote Authentication Dial In User Services) security function
- Enhances security through WPA (Wi-Fi Protected Access) supports of TKIP (Temporary Key Integrity Protocol) or AES (Advanced Encryption Standard) algorithm
- WEP (Wired Equivalent Privacy) supports 64/128-bit encryption
- MAC address filtering enhancement
- Login security through password protection
- Web browser user interface for easy configuration and management
- Supports event log
- Display the associated station status
- Save/Reload settings to/from file
- Downloadable firmware upgradeability
- Enhances reliable connectivity through automatic data rate fallback in noisy environment
- Auto MDI-MDIX connection

- Reset button for fast default setting recovery
- Desktop and wall/ceiling mounting
- High output allows extended range application through the third party external antenna

1.2 Specifications

- Standards: IEEE 802.11b/g (Wireless), IEEE 802.3 (Wired)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP and WPA Data Encryption
- Frequency Band: 2.400~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: CCK@11/5.5Mbps, DQPSK@2Mbps and DBPSK@1Mbps
- Radio Output Power: up to 20dBm (802.11b)
  up to 15dBm (802.11g)
- Radio Technology: Direct Sequence Spread Spectrum (DSSS)
- Antenna: External detachable dipole antenna (with RP-SMA connector)
- Connectors: 10/100Mbps RJ-45 x 1
- Power: 9VDC, 0.8A
- LEDs: Power, LAN Link/Activity, Wireless Activity
- Dimension: 26(H) x 129(W) x 78(D) mm
- Temperature:
  Operating: 32~131°F (0~55°C)
  Storage: -4~158°F (-20~70°C)
- Humidity: 10-90% (Noncondensing)
- Certification: FCC, CE

1.3 Applications

- Networking for device sharing - Remote access to corporate network information, email, file transfer and terminal emulation.
- Frequently changing environments - Retailers, manufacturers and banks that frequently rearrange the workplace and change location.
- SOHO (Small Office and Home Office) users - SOHO users need easy and quick installation of a small computer network functions.
- Inter-building connection - The wireless building-to-building network installs quickly, requires no monthly lease fees, and provides the flexibility to reconfigure easily.
- Typical applications include hard-to-wire buildings, campuses, hospitals/medical offices, warehouse, security huts, exhibition centers, etc.
- Temporary LANs for special projects or occasions - Auditors require workgroups at customer sites. Trade shows, exhibitions, retailers, airline, and shipping companies need additional workstations for the peak periods of data traffic.

1.4 Safety Notification

Your Wireless AP should be placed in a safe and secure location. To ensure proper operation, please keep the unit away from water and other damaging elements. Please read the user manual thoroughly before you install the device. The device should only be repaired by authorized and qualified personnel.

- Please do not try to open or repair the device yourself.
- Do not place the device in a damp or humid location, i.e. a bathroom.
- The device should be placed in a sheltered and non-slip location within a temperature range of 0 to +40 Celsius degree.
- Please do not expose the device to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

1.5 Operation Mode

The AAP2000 supports four operation modes:

- AP mode
- AP Client mode
- Repeater mode
- Bridge mode

1.5.1 AP (Access Point) Mode

The AP mode is a typical "Infrastructure mode". The WLAN station (e.g. Note Book with WLAN card) can access the LAN/Internet via the AP. The following shows a typical configuration.

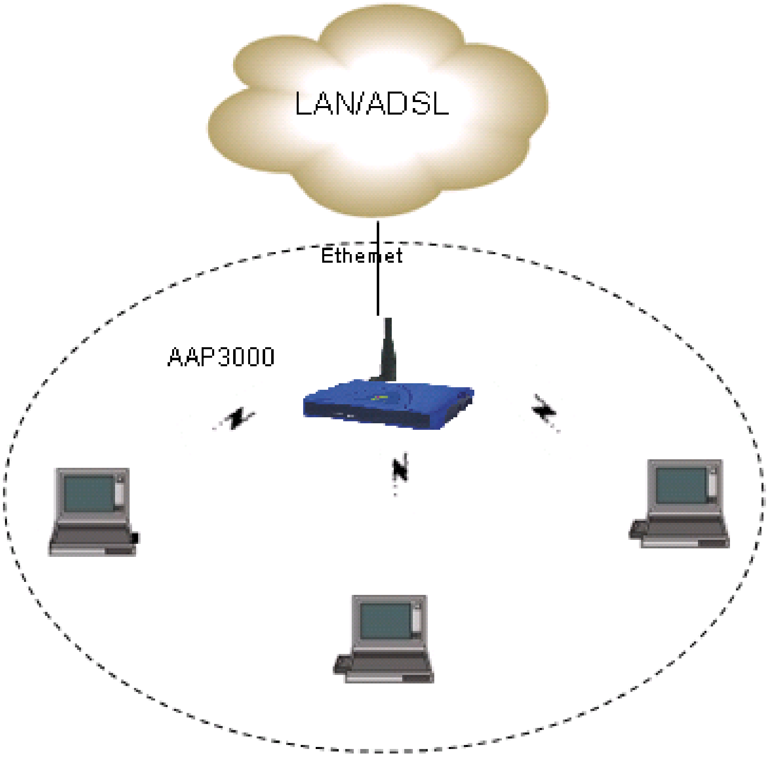


Figure 1-1 AP mode configuration example

1.5.2 AP Client:

The AAP2000 can be configured as an AP client to access other AP. In this operating mode, the device will be used as a wireless NIC. The following shows the possible configuration:

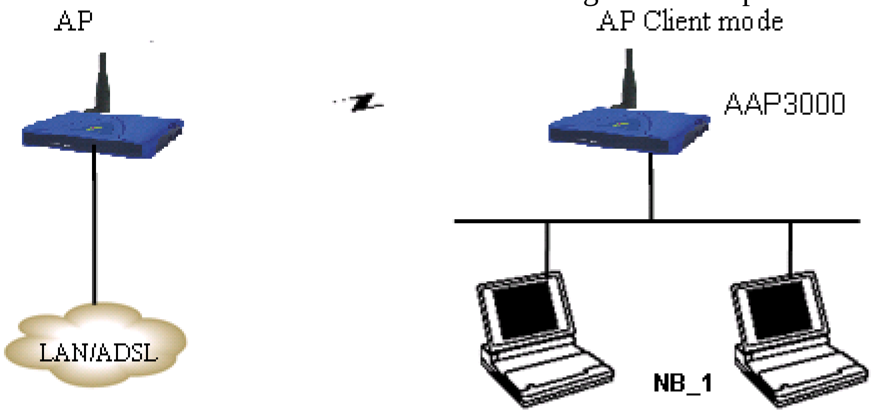


Figure 1-2 AP-client mode configuration example

The NB_1 can access the LAN/WAN at the left side via the AP Client which acts as wireless NIC station.

1.5.3 Repeater Mode

This mode allows the AP to keep the AP function role and at the same time establishing a connection with other 802.11g AP to extend your wireless network. The following shows the possible configuration:

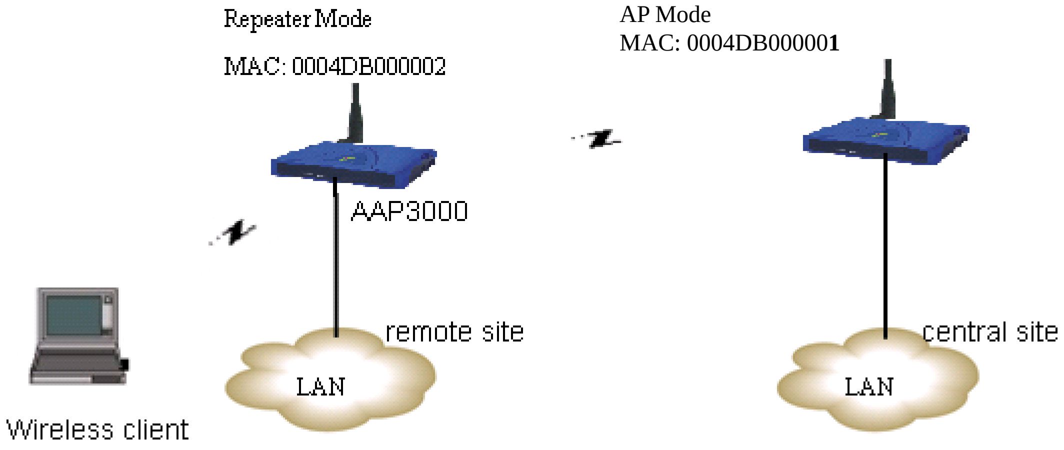


Figure 1-3 Repeater mode configuration example

1.5.4 Bridge Mode

As shown in the following configuration, the two AP are linked to each other via the wireless connection. Each AP can use its LAN port to connect to one LAN. So, the two wired Ethernet Network are linked together logically by a pair of wireless bridges. Once AAP3000 has been set into the bridge mode, The AAP3000's Access Point function is disabled.

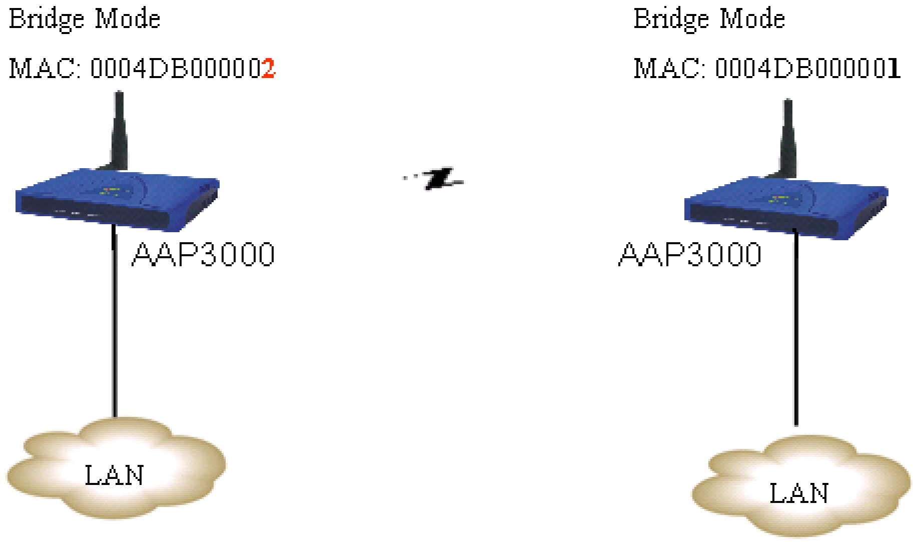


Figure 1-4 Bridge mode configuration example

2 Installation

2.1 Package Contents

The product package should contain the following items:

- 802.11g/b Access Point
- Power Adapter
- Quick Install Guide
- CD-ROM (User manual)
- Antenna
- Cat5 Ethernet cable
- four pads in a plastic bag

If any of the parts are incorrect, missing, or damaged, please contact your vendor. Retain the carton and the original packing materials in case you need to return the product.

2.2 The AAP3000's Front

On the AAP3000's front panel there are LED lights that inform you of the AAP3000's current status. Below is an explanation of each LED.

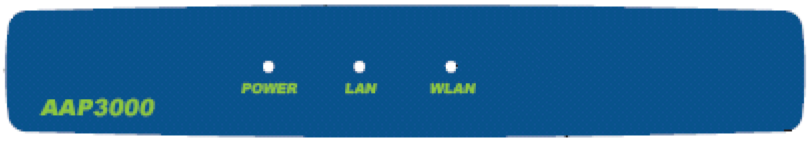


Figure 2-1 Front Panel

LED	Color	Status	Description
Power	Green	Lit Off	Power is supplied. No Power.
Wireless Activity	Green	Flash Off	Antenna is transmitting or receiving data. Antenna is not transmitting or receiving data.
LAN Link/Activity	Green	On Flash Off	A valid link is established. It is transmitting or receiving data. No link is established.

2.3 The AAP3000’s Rear Panel

AAP3000’s connection ports are located on the back panel. Below is the description of each connection port.

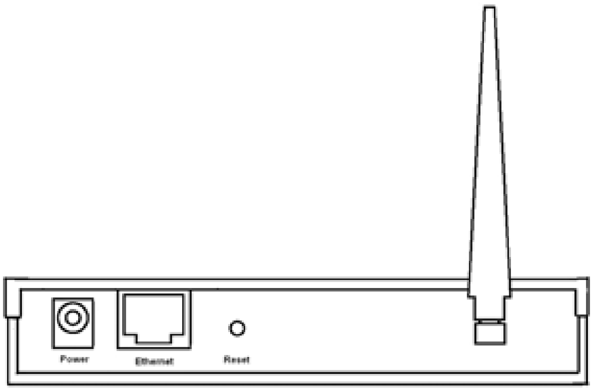


Figure 2-2 Rear Panel

- DC Adapter Port
  Insert the power jack of the power adapter into this port.
- LAN Port
  The AAP3000’s LAN port is where you connect to your LAN’s network devices.
- Reset
  The Reset button allows you to do one thing.

  If problems persist or you experience extreme problems or you forgot your password, press the reset button for longer than 10 seconds and the AAP3000 will reset itself to the factory default settings and the AAP3000 will re-boot itself. (Warning: your original configurations will be replaced with the factory default settings).

2.4 Default Settings

The following table shows the AAP3000 default settings.

Items	Default Setting
IP Address	**192.168.1.251**
User Name/Password	**admin/admin**
IP Subnet Mask	**255.255.255.0**
SSID	**Aboundi**
RF channel	**6**
Mode	**11b/g**
WEP	**Disabled**

2.5 Connect to a Network

2.5.1 Locate an optimum location for the AAP3000.

The best location for your AAP3000 is usually at the center of your wireless network, with line of sight to all of your mobile stations.

2.5.2 Connect the AAP3000 to your router, hub or switch.

Connect one end of standard UTP cable to the AAP3000's LAN Port and connect the other end of the cable to a switch, a router or a hub. The AAP3000 will then be connected to your existed wired LAN Network.

2.5.3 Connect the DC Power Adapter to the AAP3000's Power Socket.

Plug the power adapter into the power inlet on the AAP3000, and the other end into a power outlet. Check the **Power** LED on the front panel to make sure it is on. **Warning:** Use only power adapter supplied with the AAP3000; otherwise, the AAP2000 may be damaged.

The Hardware Installation is complete

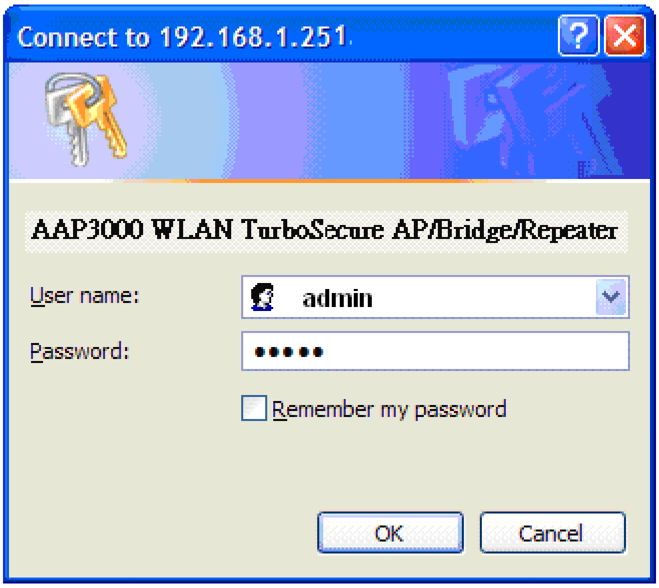
3 Configuring this Wireless Assess Point

3.1 Configuring the AAP3000

This **AAP3000** provides web-based configuration tool allowing you to configure from wired or wireless stations. Follow the instructions below to get started configuration.

From Wired Station

1. Make sure your wired station is in the same subnet with the AAP3000.
   The default IP Address and Sub Mask of the AAP3000 is:
   Default IP Address: 192.168.1.251
   Default Subnet: 255.255.255.0
2. Enter **http://192.168.1.251** from Web Browser to get into the AAP3000’s configuration tool.
3. A screen will be popped up and request you to enter user name and password. The default user name and password is as follows.
   User Name: admin
   Password: admin
   Enter the default user name and password, then press **OK** button directly.



Connect to 192.168.1.251

AAP3000 WLAN TurboSecure AP/Bridge/Repeater

User name: admin

Password: •••••

□ Remember my password

Figure 3-1 default setting

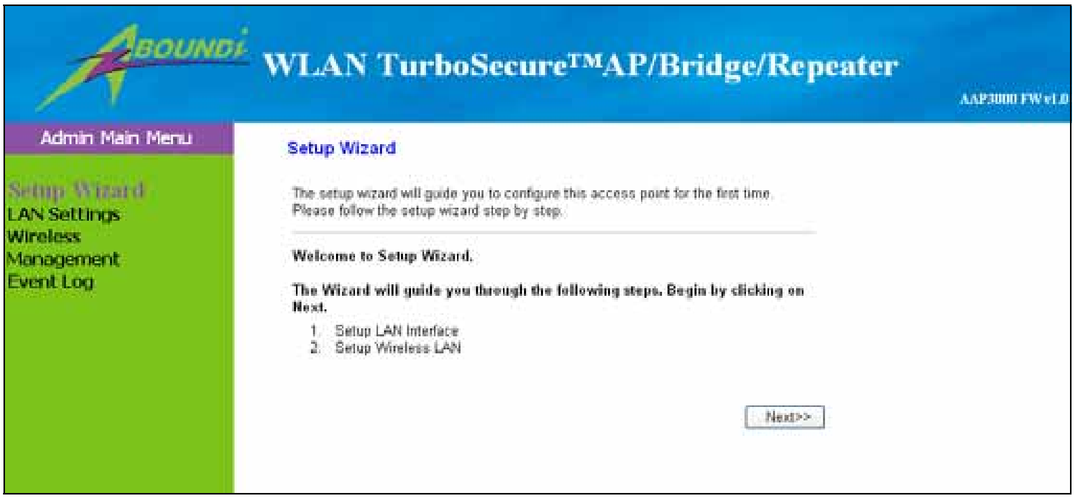
4. You can start configuring the Access Point.

From Wireless Station

1. Make sure your wireless station is in the same subnet with the AAP3000. Please refer to the **step 1** above for configuring the IP Address and Sub Mask of the wireless station.
2. Connect to the AAP3000.
   The AAP3000's default SSID is "**Aboundi**" and the WEP Encryption function is disabled. Make sure your wireless station is using the same SSID as the AAP3000 and associate your wireless station to the AAP3000.
3. Enter **http://192.168.1.251** from Web Browser to get into the AAP3000's configuration tool.
4. Enter the user name and password and then press **OK** button and you are available to configure the AAP3000 now.

3.2 Setup Wizard

After successfully accessing to the configuration web page, the setup status will be shown as in the figure below.



Setup Wizard

The setup wizard will guide you to configure this access point for the first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you through the following steps. Begin by clicking on Next.

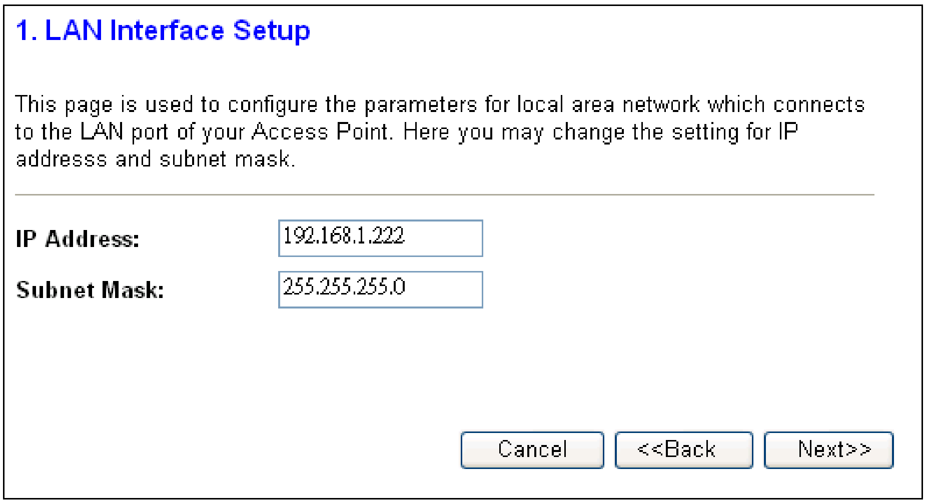
1. Setup LAN Interface
2. Setup Wireless LAN

Figure 3-2 Setup Wizard

This AAP3000 has a Setup Wizard to help you easily configure its settings.

3.2.1 LAN Interface Setup

The first step click "**Next**" button in Setup Wizard is LAN interface Setup. Users can change LAN IP address and Subnet Mask here. Most Users will not need to change these values.



1. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss and subnet mask.

IP Address: 192.168.1.222

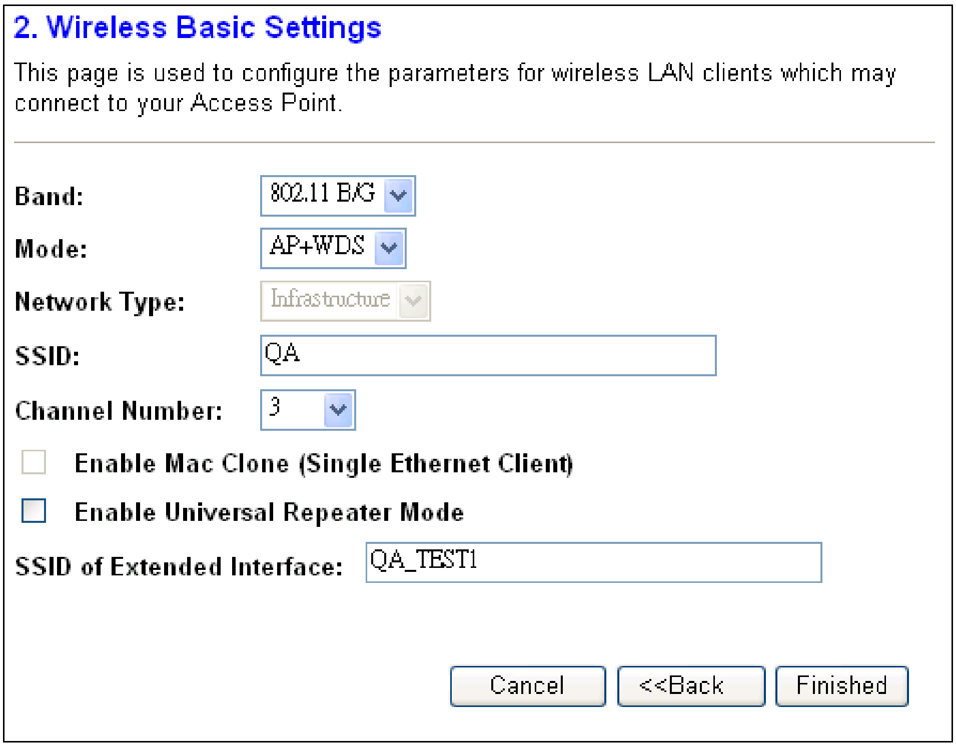
Subnet Mask: 255.255.255.0

Figure 3-3 LAN Interface Setup

After typing in the IP Address and Subnet Mask, click "**Next**" button. You will enter the Wireless Basic Settings page.

3.2.2 Wireless Basic Settings

Following LAN interface setup is the Wireless basic settings page. Users can setup the items below:



2. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band: 802.11 B/G

Mode: AP+WDS

Network Type: Infrastructure

SSID: QA

Channel Number: 3

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode

SSID of Extended Interface: QA_TEST1

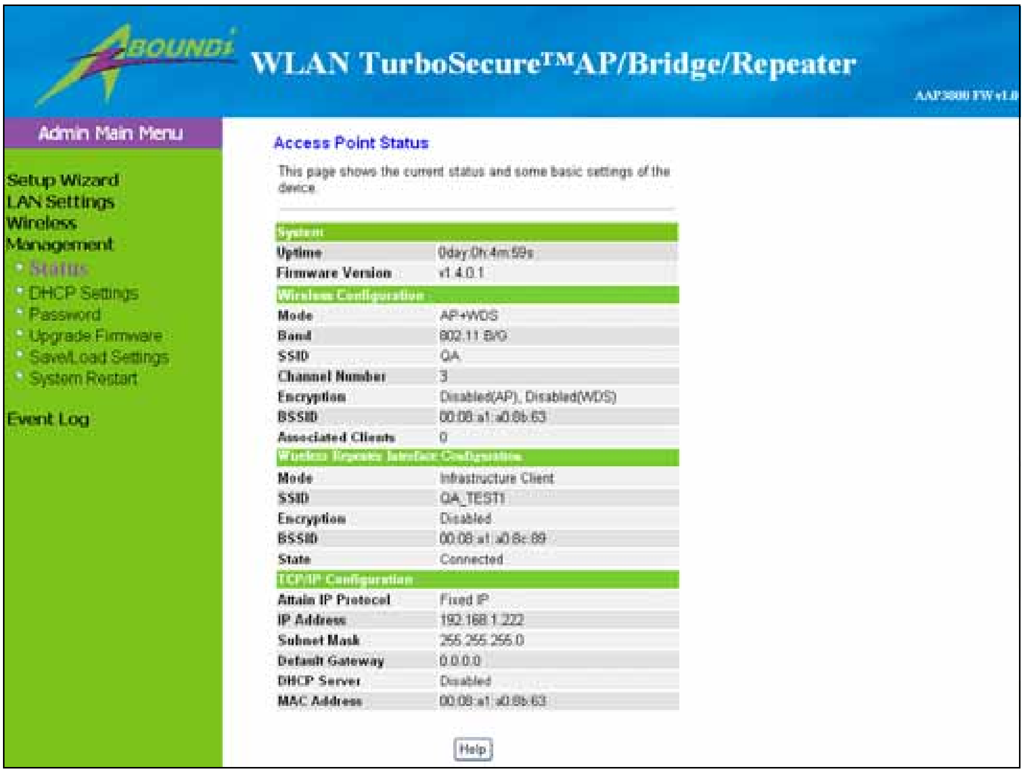
Figure 3-4 Wireless Basic Settings

1. Operating band: 802.11B/G, 802.11G or 802.11B.
2. Operating mode: AP, Client, WDS, and AP+WDS.
3. Network type: when operating mode is "Client" mode, users can select the network type as "infrastructure" or "Adhoc".
4. SSID: The SSID differentiates one WLAN from another, therefore, all wireless access points/routers and all wireless devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters.
5. Channel Number: The number of channels supported depends on the region of this Wireless Access Point. All stations communicating with this Wireless Access Point must use the same channel. (**Note: not supported in client mode**)
6. Enable Mac clone: when operating mode is "Client" mode and only one Ethernet client exists, users can enable this Mac clone feature to connect with the wireless station easily.
7. Enable Universal Repeater Mode: when choose the repeater mode, the AAP3000 will to be repeater function only.

After all items are set, click **"Finished"** button.

3.3 Status

The status screen is shown in the figure below.



Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:4m:59s
Firmware Version	v1.4.0.1
Wireless Configuration	
Mode	AP+WDS
Band	802.11 B/G
SSID	QA
Channel Number	3
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:08:a1:a0:8b:63
Associated Clients	0
Wireless Repeater Interface Configuration	
Mode	Infrastructure Client
SSID	QA_TEST1
Encryption	Disabled
BSSID	00:08:a1:a0:8c:89
State	Connected
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.222
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:08:a1:a0:8b:63

Figure 3-5 Status

This status page provides a brief read-only report for System, Wireless Configuration and TCP/IP Configuration status. The data displayed may be changed depending on your current configuration.

3.3.1 System status

This system status includes:
Uptime and firmware version.

3.3.2 Wireless Configuration

This Wireless Configuration status includes:
Mode, Band, SSID, Channel Number, Encryption, BSSID, and Associated Clients.

3.3.3 Wireless Repeater Interface Configuration

This Wireless Configuration status includes:
Mode, SSID, Encryption, BSSID, and State.

3.3.4 TCP/IP Configuration status

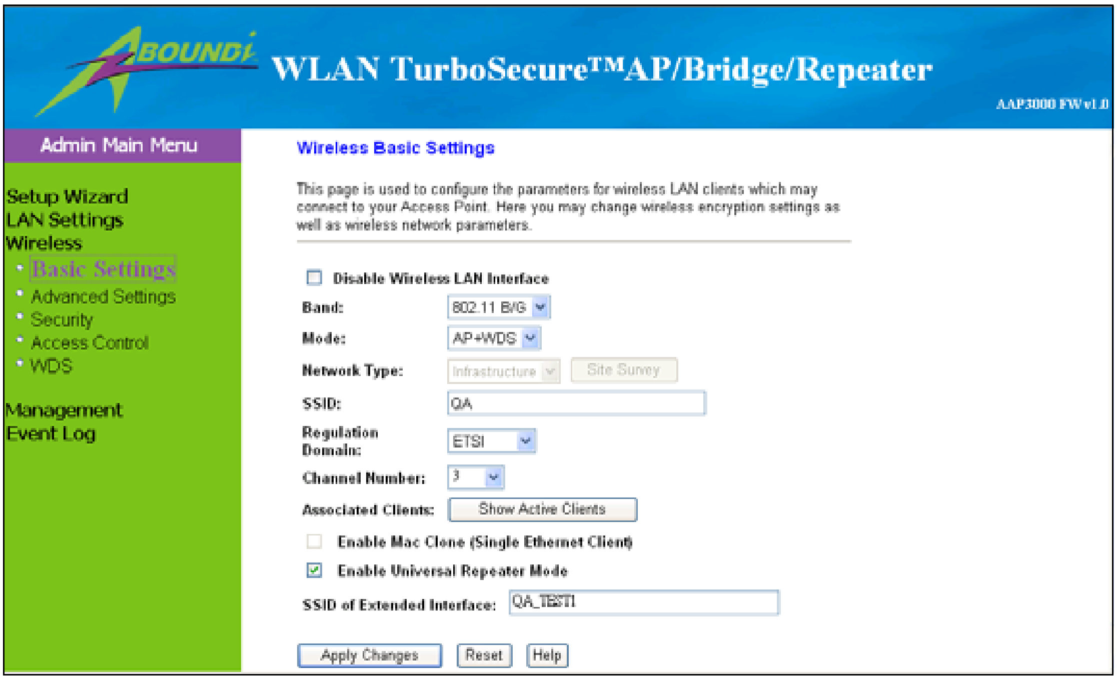
This TCP/IP Configuration status includes:
Attain IP Protocol, IP Address, Subnet Mask, Default Gateway, and MAC Address.

3.4 Wireless

3.4.1 Basic Settings

The wireless basic settings include Band, Mode, SSID and Channel Number.

- Disable Wireless LAN Interface: check or uncheck (Enable or Disable).
- Band: This Wireless Access Point can support three RF band: 802.11B/G, 802.11G and 802.11B.
- Mode: This Wireless Access Point supports four operating modes: AP, client, WDS, and AP+WDS.
- Network Type: when operating mode is Client mode, users can select the network type as "Infrastructure" or "Adhoc" mode.
- SSID: The SSID differentiates one WLAN from another, therefore, all wireless access points/routers and all wireless devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters.
- Channel Number: The number of channels supported depends on the region of this Wireless Access Point. All stations communicating with this Wireless Access Point must use the same channel.
- Associated Clients: When you click the "Show Active Client" button, it will show all the clients already associating this Wireless Access Point, see the "Active Wireless Client Table", only valid for AP mode and AP+WDS mode.
- Enable Mac clone: when operating mode is Client mode and only one Ethernet client exists, users can enable this Mac clone feature to connect with wireless station easily.
- Enable Universal Repeater Mode: when choose the repeater mode, the AAP3000 will to be repeater function only.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 802.11 B/G

Mode: AP+WDS

Network Type: Infrastructure

SSID: QA

Regulation Domain: ETSI

Channel Number: 3

Associated Clients: Show Active Clients

□ Enable Mac Clone (Single Ethernet Client)

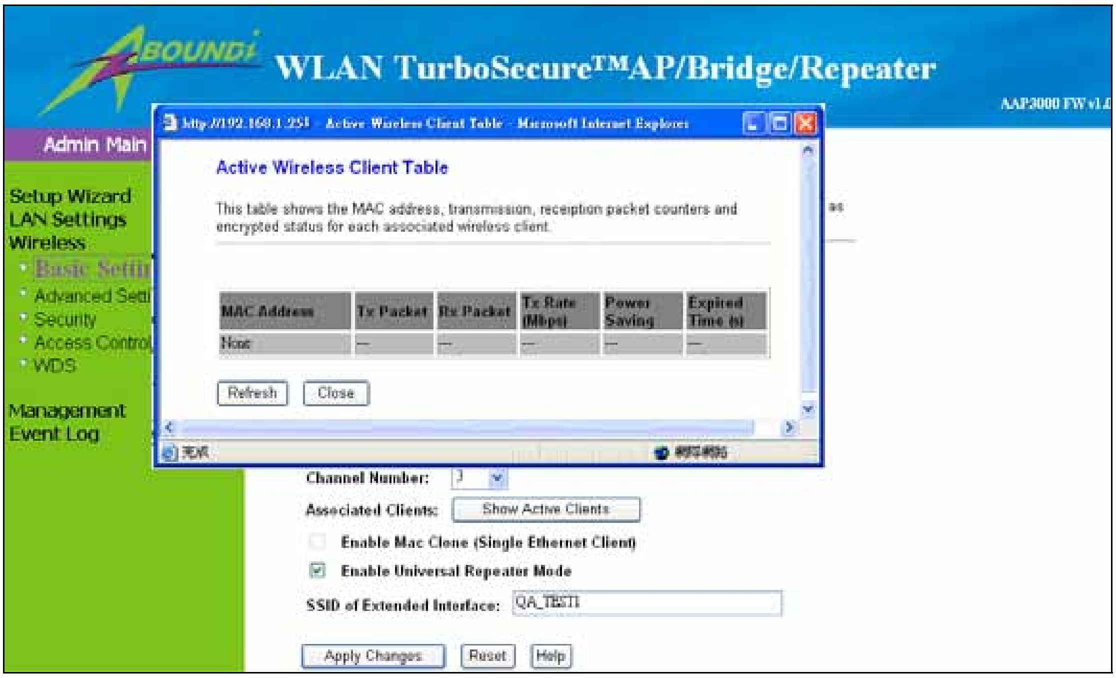
☑ Enable Universal Repeater Mode

SSID of Extended Interface: QA_TEST1

Figure 3-6 Wireless Basic Settings

Click "**Apply Changes**" button when you finish your settings or click "**Reset**" to undo your changes.

In the figure above, click "**Show Active Clients**" button while there are wireless clients connected to this Wireless Access Point. You will see the figure below to show the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client. Click "**Refresh**" button to show the latest information



http://192.168.1.251 - Active Wireless Client Table - Microsoft Internet Explorer

Active Wireless Client Table

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

Channel Number: 3

Associated Clients: Show Active Clients

□ Enable Mac Clone (Single Ethernet Client)

☑ Enable Universal Repeater Mode

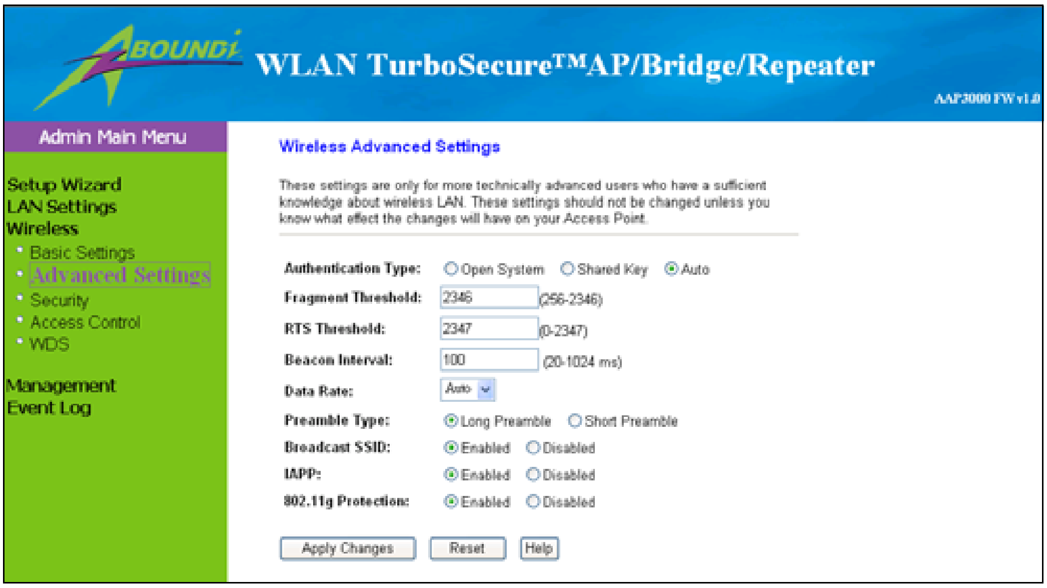
SSID of Extended Interface: QA_TEST1

Figure 3-7 Active Wireless Client Table

3.4.2 Advanced Settings

In Advanced Settings page, more 802.11 related parameters are tunable.

- Authentication Type: There are three Authentication Type- Open System, Shared Key, and Auto
- Fragment Threshold: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If a wireless client often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346.
- RTS Threshold: RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. “Hidden Node” is a situation in which two stations are within range of the same wireless access point/router, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Wireless Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Wireless Access Point. The collision will most certainly result in a loss of messages of both stations. If the “Hidden Node” problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. The default value is 2347.
- Beacon Interval: Beacon interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the wireless router).
- Data Rate: By default, it selects the highest rate for transmission.
- Preamble Type: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a “noisy” network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired.
- Broadcast SSID: Select enabled to allow all the wireless stations to detect the SSID of this wireless router.
- IAPP: The Inter-Access Point Protocol (IAPP) can extend multi-vendor interoperability to the roaming function.
- 802.11g Protection: there are CCK and OFDM modulation scheme using for 802.11b and 802.11g respectively, the packet collision will increase when these two kind devices exist at the same time. We need to enable the Protection mode to increase the performance.



Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type: ○ Open System ○ Shared Key ● Auto

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Data Rate: Auto

Preamble Type: ● Long Preamble ○ Short Preamble

Broadcast SSID: ● Enabled ○ Disabled

IAPP: ● Enabled ○ Disabled

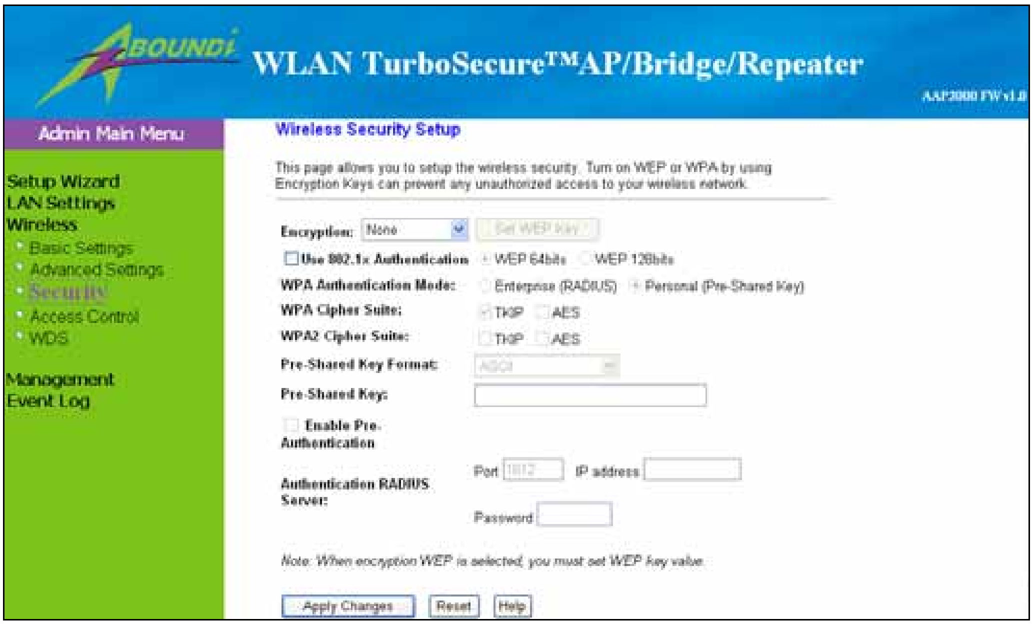
802.11g Protection: ● Enabled ○ Disabled

Figure 3-8 Wireless Advanced Settings

3.4.3 Security

Here you can configure the security of your wireless network. Selecting different method will enable you to have different level of security. Please note that using any encryption may be a significant degradation of the data throughput on the wireless link.

- Note: If no encryption is selected, users can enable the 802.1x Authentication and set the RADIUS server authentication parameters – port, IP address and Password.



Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption: None

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP □ AES

Pre-Shared Key Format: ASCII

Pre-Shared Key:

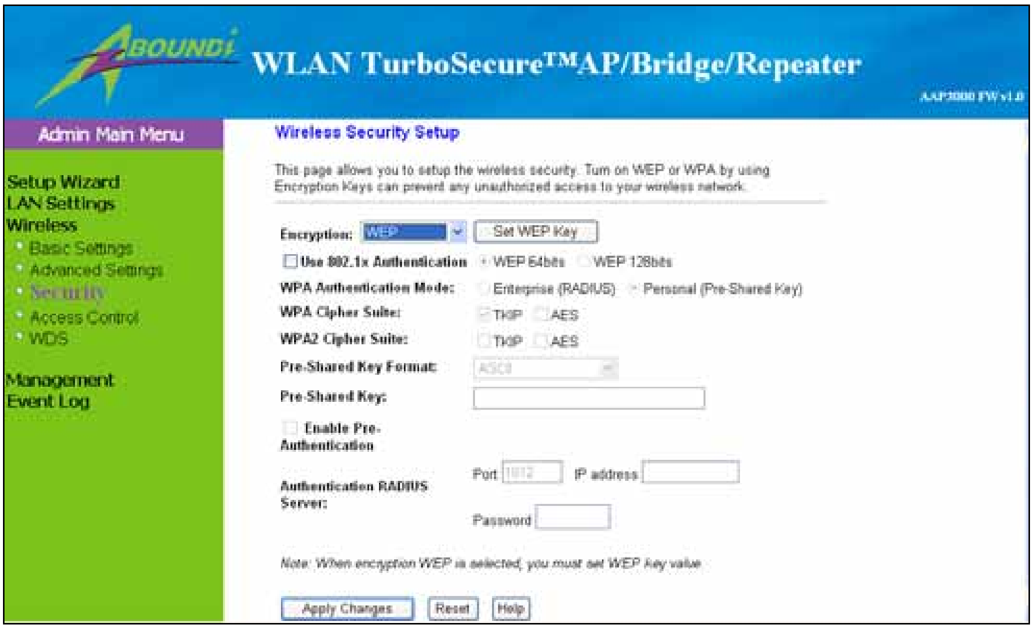
□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

Figure 3-9 Wireless Security Setup--None

- WEP: Wired Equivalent Privacy. When you press the "Set WEP Key", you may choose either 64-bit or 128-bit as the encryption key and Select ASCII or Hex as the format of input value. All the four WEP keys are set identical. You can enable the 802.1x Authentication and set the RADIUS server authentication parameters – port, IP address and Password.



Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption: WEP | Set WEP Key

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP □ AES

Pre-Shared Key Format: ASCII

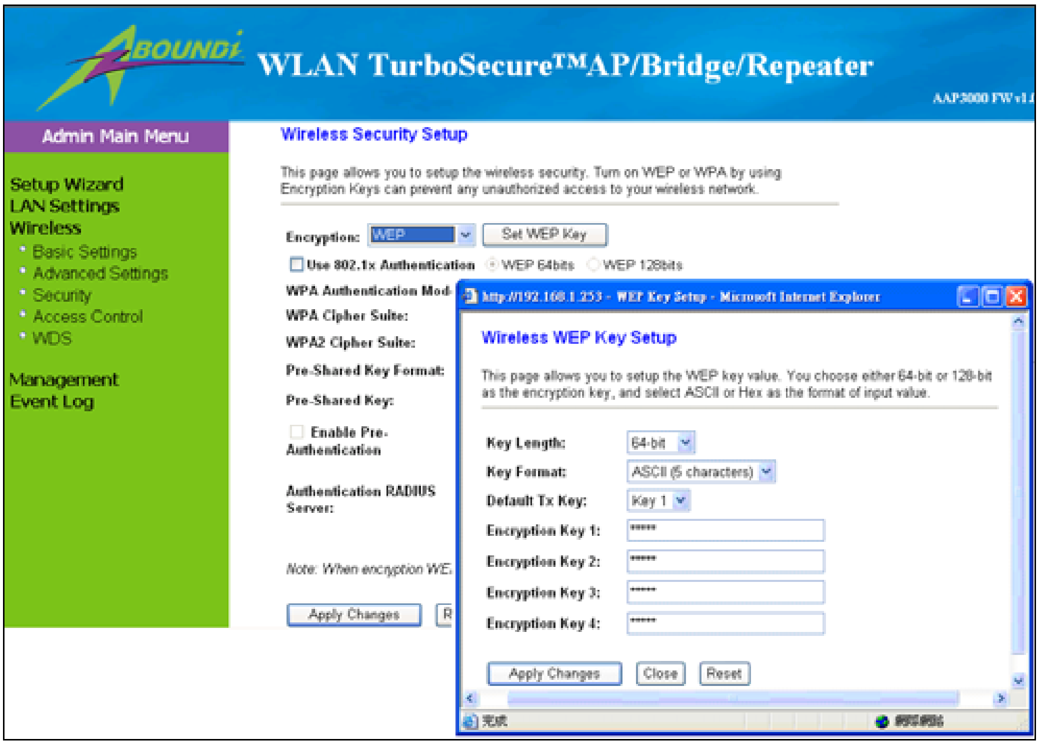
Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

Note: When encryption WEP is selected, you must set WEP key value

Figure 3-10 Wireless Security Setup--WEP



Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption: WEP | Set WEP Key

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

http://192.168.1.253 - WEP Key Setup - Microsoft Internet Explorer

Wireless WEP Key Setup

This page allows you to setup the WEP key value. You choose either 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length: 64-bit

Key Format: ASCII (5 characters)

Default Tx Key: Key 1

Encryption Key 1: *****

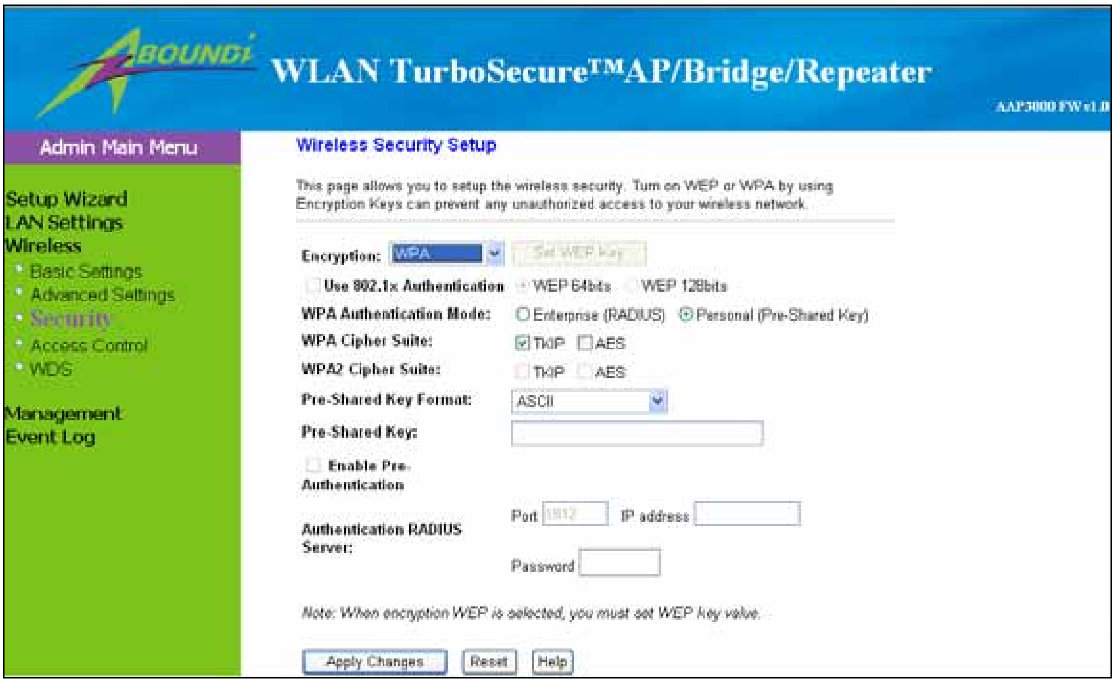
Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

Figure 3-11 Wireless WEP Key Setup

- WPA: Wi-Fi Protected Access. There are three encryption modes – TKIP, AES and Mixed.
- TKIP: Temporal Key Integrity Protocol
- AES: Advanced Encryption Standard
- Mixed: WPA2 Mixed mode operation permits the coexistence of WPA and WPA2 clients on a common SSID. WPA2 Mixed Mode is a Wi-Fi Certified feature. During WPA2 Mixed Mode, the access point advertises the encryption ciphers (TKIP, CCMP, other) that are available for use. The client selects the encryption cipher it would like to use and the selected encryption cipher is used for encryption between the client and access point once it is selected by the client. The access point must support WPA2 Mixed Mode to use this option.
- There are two authentication modes – WPA enterprise By RADIUS server and WPA personal pre-shared key.
- RADIUS: When user chooses RADIUS authentication, there are three parameters of RADIUS server being set – Port, IP address and Password.
- Pre-Shared Key: When user chooses Pre-Shared Key authentication, there are two types of input format – ASCII and Hex.
- Enable Pre-Authentication: only valid for AES and Mixed mode.



Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption: WPA [Set WEP Key]

☐ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP ☐ AES

WPA2 Cipher Suite: ☐ TKIP ☐ AES

Pre-Shared Key Format: ASCII

Pre-Shared Key:

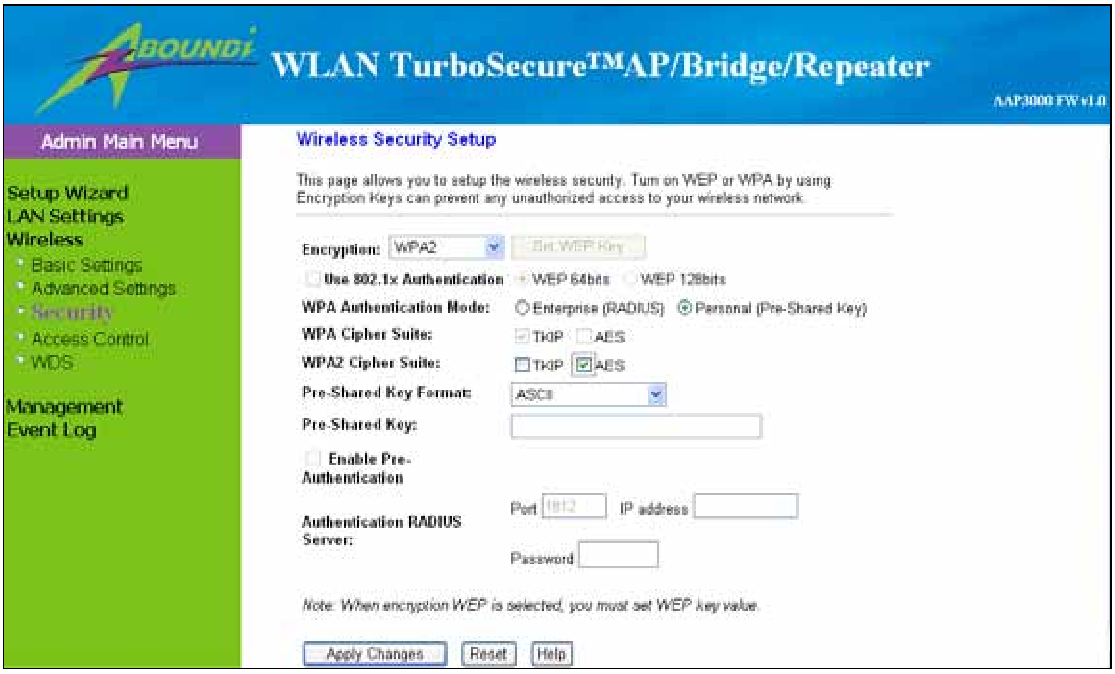
☐ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address
Password

Note: When encryption WEP is selected, you must set WEP key value.

[Apply Changes] [Reset] [Help]

Figure 3-12 Wireless Security Setup--WPA



Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption: WPA2

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: ASCII

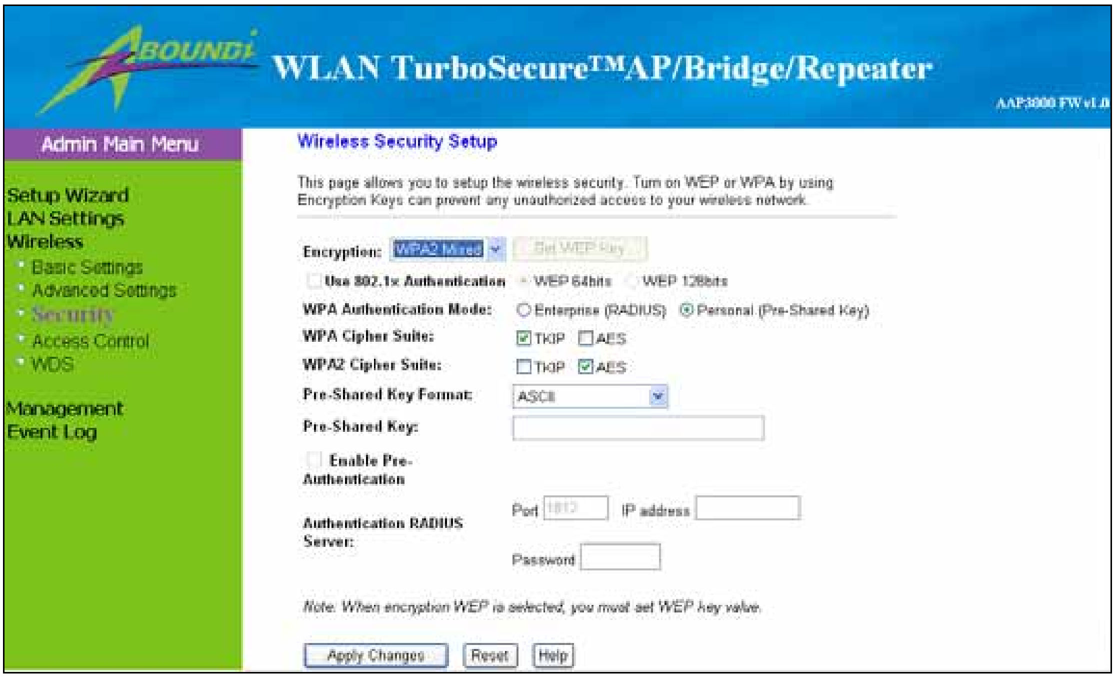
Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

Figure 3-13 Wireless Security Setup--WPA2



Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption: WPA2 Mixed

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: ASCII

Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

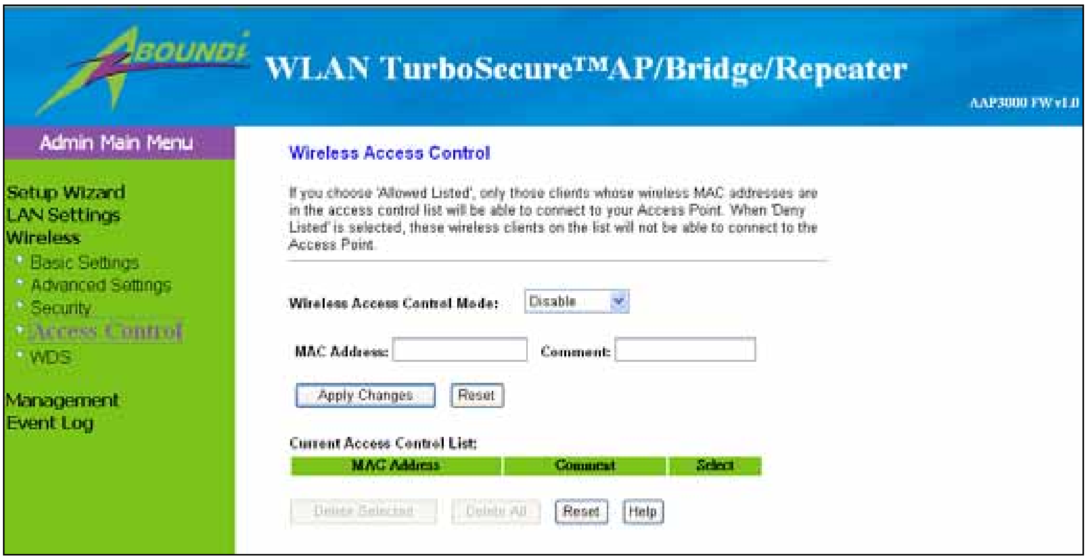
Note: When encryption WEP is selected, you must set WEP key value.

Figure 3-14 Wireless Security Setup--WPA2 Mixed

1.1.1

3.4.4 Access control

There are three types of access control options: Disable, Allow Listed and Deny Listed. If you choose "Allow Listed", only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When "Deny Listed" is selected, these wireless clients on the list will not be able to connect to the Access Point. Users can add new MAC address with simple comment and then press "Apply Changes" button. To delete a MAC, select its corresponding Select checkbox and press "Deleted Selected" button.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect to the Access Point.

Wireless Access Control Mode: Disable

MAC Address: Comment:

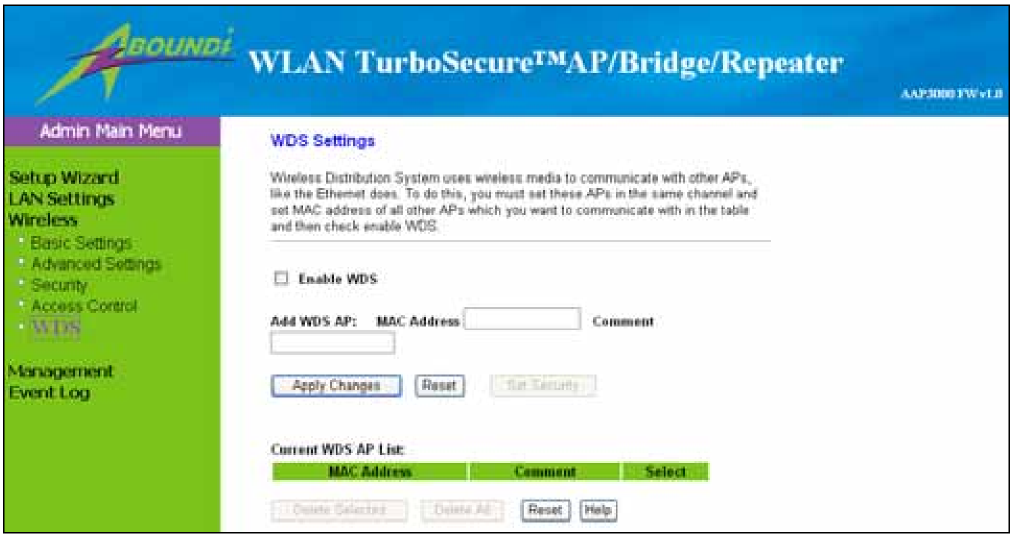
Current Access Control List:

MAC Address	Comment	Select

Figure 3-15 Wireless Access Control

3.4.5 WDS

When you enable the WDS feature selected in the Basic Settings. This Wireless Distribution System (WDS) feature will set this AAP3000 in "Bridge Mode". Two Wireless Access Points in bridge mode can communicate with each other through wireless interface. To do this, you must set these Access Points in the same channel and set MAC address of all other Access Points which you want to communicate with in the table and then enable the WDS.



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of all other APs which you want to communicate with in the table and then check enable WDS.

☐ Enable WDS

Add WDS AP: MAC Address Comment

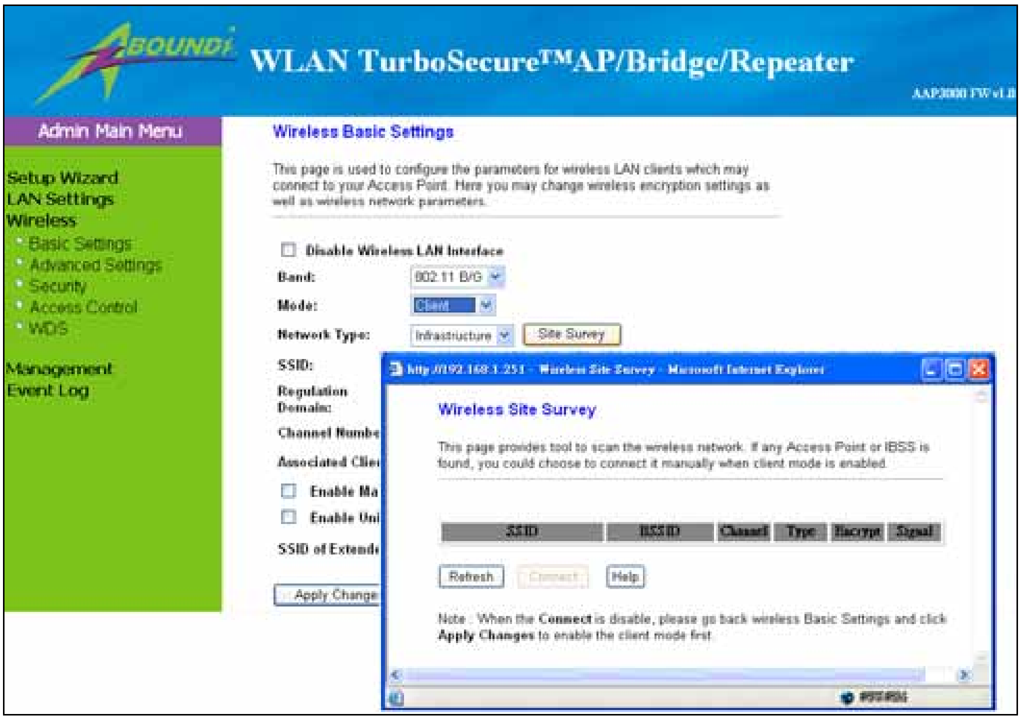
Current WDS AP List:

MAC Address	Comment	Select

Figure 3-16 WDS Settings

3.4.6 Site Survey

This Wireless Site Survey tool will scan the wireless network. Click "**Refresh**" button to search for available Access Point or IBSS. If any Access Point or IBSS is found, you may choose to connect it manually when client mode is enabled.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ **Disable Wireless LAN Interface**

Band: 802.11 B/G

Mode: Client

Network Type: Infrastructure

SSID:

Regulation Domain:

Channel Numbe

Associated Clie

□ **Enable Ma**

□ **Enable Uni**

SSID of Extende

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal

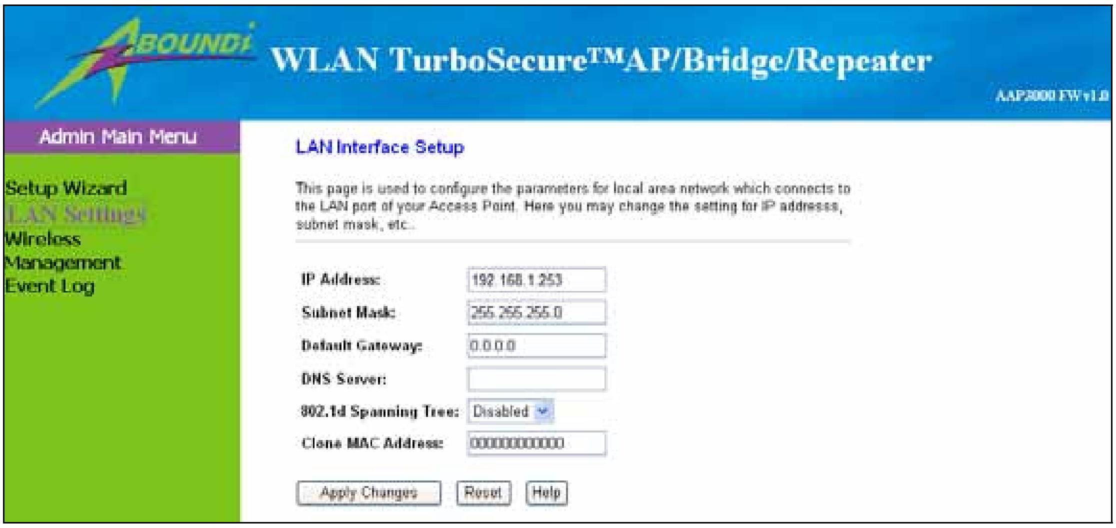
Note : When the **Connect** is disable, please go back wireless Basic Settings and click **Apply Changes** to enable the client mode first.

Figure 3-17 Wireless Site Survey

3.5 TCP/IP Settings

TCP/IP Settings allows you to configure the parameters for local area network which connects to the LAN port of your Access Point.

- IP Address: Enter IP address for this Access Point.
- Subnet Mask: Enter the subnet mask for this Access Point.
- Default Gateway: Enter Default Gateway for this Access Point.
- DHCP: There are three options for DHCP – Disabled, Client and Server.
- DHCP Client Range: you can define the IP range for DHCP clients. You can click the "Show Client" button to display the current active DHCP clients.
- DNS Server: It will active when the DHCP Server is enabled.
- 802.1d Spanning Tree: On LAN side, it supports Spanning Tree Protocol to avoid physical loop problem.
- Clone MAC Address: You can assign a new MAC address for external DHCP server to be cloned.



LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, etc..

IP Address: 192.168.1.253

Subnet Mask: 255.255.255.0

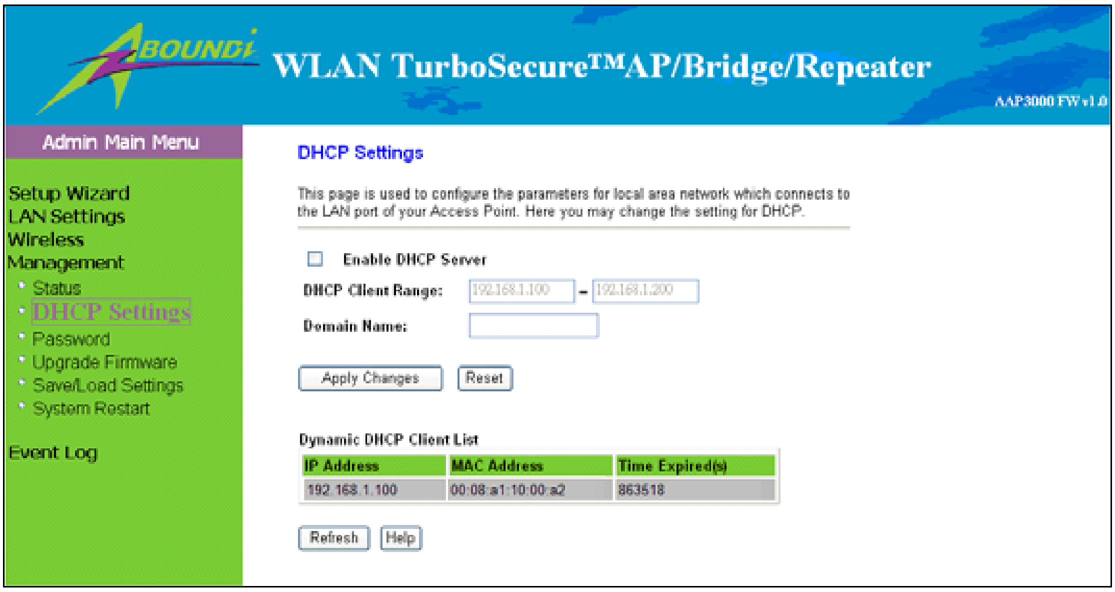
Default Gateway: 0.0.0.0

DNS Server:

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

Figure 3-18 LAN Interface Setup



DHCP Settings

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for DHCP.

□ Enable DHCP Server

DHCP Client Range: 192.168.1.100 - 192.168.1.200

Domain Name:

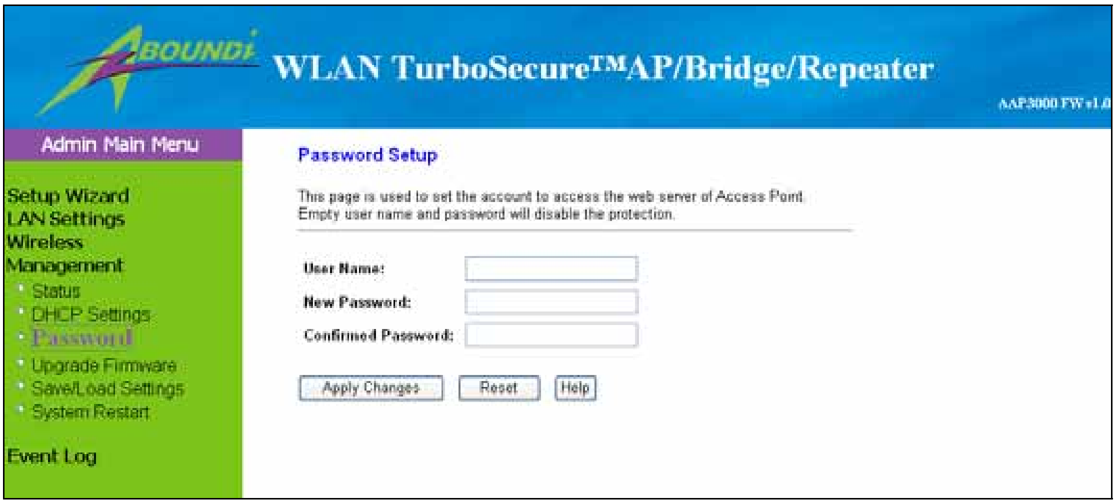
Dynamic DHCP Client List

IP Address	MAC Address	Time Expired(s)
192.168.1.100	00:08:a1:10:00:a2	863518

Figure 3-19 DHCP Settings

3.6 Password

You can change login ID and Password here. The default Login ID and Password is "**admin**" with password "**admin**".



Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

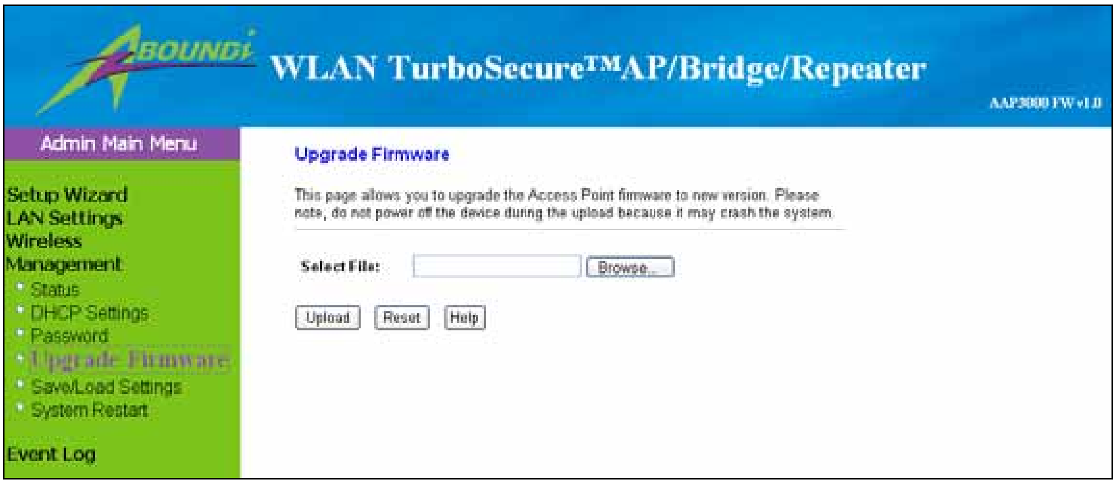
New Password:

Confirmed Password:

Figure 3-20 Password Setup

3.7 Upgrade Firmware

This Wireless Access Point allows you to easily upgrade its firmware.
Select File: click on Browse button to select the firmware and then click on the Upload button.
After firmware upgrade is completed, this AAP3000 will restart.
Note: Do not power off this Wireless Access Point while firmware is being upgraded.



Upgrade Firmware

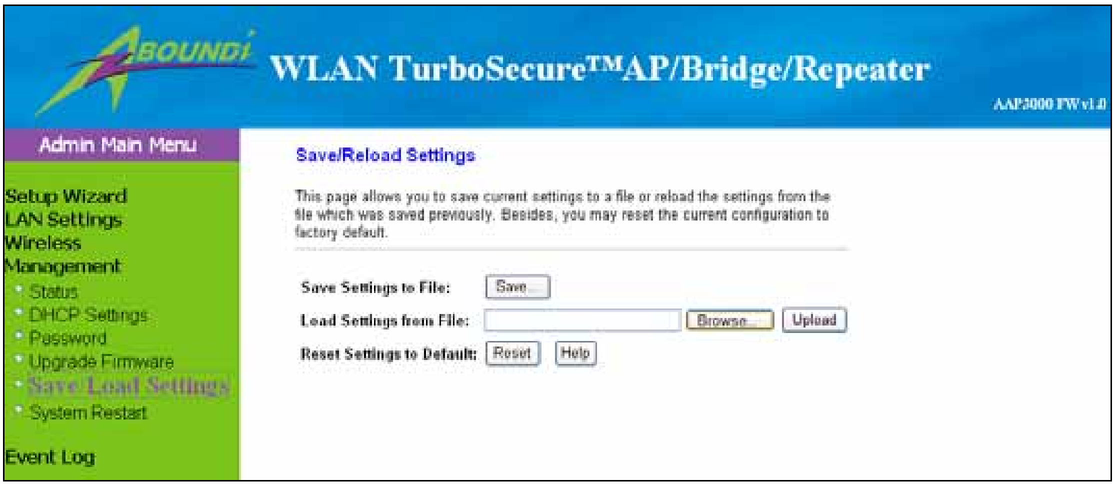
This page allows you to upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

Figure 3-21 Upgrade Firmware

3.8 Save/Reload Settings

You can reset this AAP3000 back to its default settings by clicking on Reset button, and then press OK button to confirm your decision.
Note: you can also hold down the reset button on this AAP3000's panel for more than 10 seconds to reset its default settings back to factory default.



Save/Reload Settings

This page allows you to save current settings to a file or reload the settings from the file which was saved previously. Besides, you may reset the current configuration to factory default.

Save Settings to File:

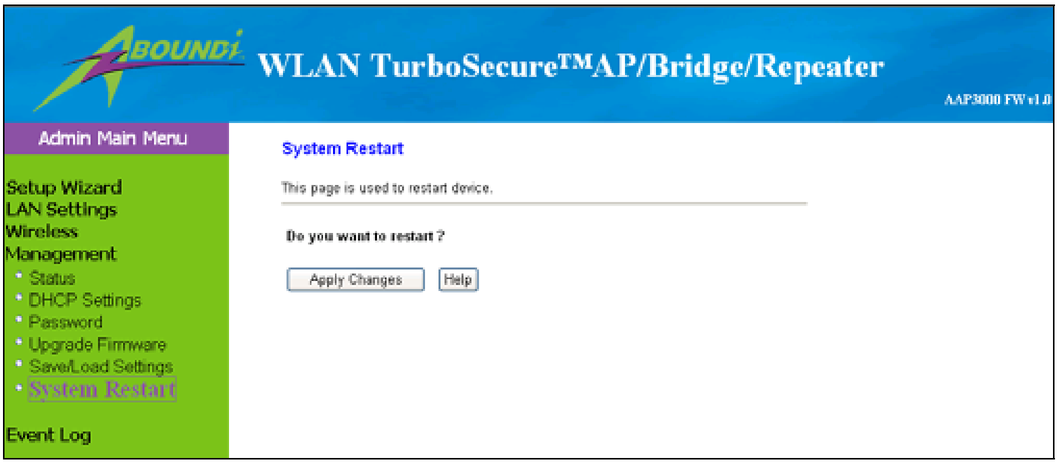
Load Settings from File:

Reset Settings to Default:

Figure 3-22 Save/Reload Settings

3.9 System Restart

You can restart the AAP3000 system should any problem exist. The restart function essentially Re-boots your AAP3000's system. In the event that the system stops responding correctly or in some way stops functioning, you can perform a restart. **Your settings will not be changed**. To perform the restart, click on the **Apply** button. You will be asked to confirm your decision. Once the restart process is complete you may start using the AAP3000 Point again.



System Restart

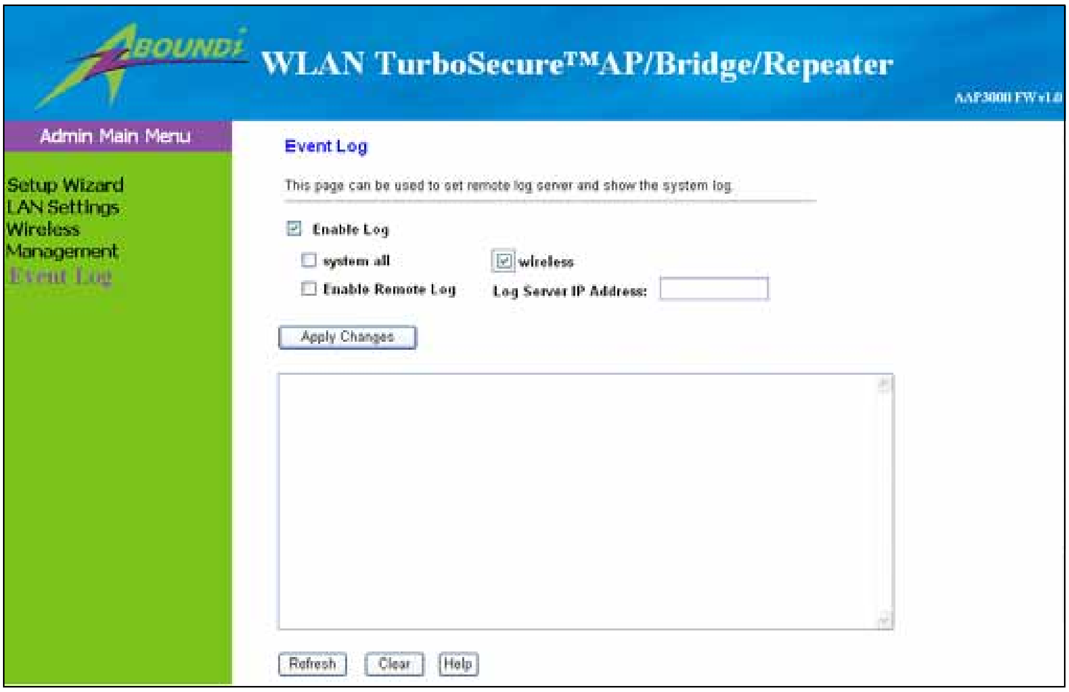
This page is used to restart device.

Do you want to restart ?

Figure 3-23 System Restart

3.10 Event Log

You can enable Log data either from wireless or from the whole system.



Event Log

This page can be used to set remote log server and show the system log.

☑ Enable Log

□ system all ☑ wireless

□ Enable Remote Log Log Server IP Address:

Figure 3-24 Event Log

4 .Troubleshooting

a). My Wireless AP will not turn on.

No LED’s light up.

Cause:

- The power is not connected.

Resolution:

- Connect the power adapter to your AP and plug it into the power outlet.

Note: Only use the power adapter provided with your AP. Using any other adapter may damage your AP.

b). LAN Connection Problems:

I can’t access my AP.

Cause:

- The unit is not powered on.
- There is not a network connection.
- The computer you are using does not have a compatible IP Address.

Resolution:

- Make sure your AP is powered on.
- Make sure that your computer has a compatible IP Address. Be sure that the IP Address used on your computer is set to the same subnet as the AP. For example, if the AP is set to 192.168.1.250, change the IP address of your computer to 192.168.1.15 or another unique IP address that corresponds to the 192.168.1.X subnet.
  Use the Reset button located on the rear of the AP to revert to the default settings.

I can’t connect to other computers on my LAN.

Cause:

- The IP Addresses of the computers are not set correctly.
- Network cables are not connected properly.
- Windows network settings are not set correctly.

Resolution:

- Make sure that each computer has a unique IP address. And the IP must be in the same subnet as the AP.
- Make sure that the Link LED is on. If it is not, try a different network cable.
- Check each computer for correct network settings.

c). Wireless Troubleshooting

I can't access the Wireless AP from a wireless network card

Cause:

- Out of range.
- IP Address is not set correctly.

Resolution:

- Make sure that the Mode, SSID, Channel and encryption settings are set the same on each wireless adapter.
- Make sure that your computer is within range and free from any strong electrical devices that may cause interference.
- Check your IP Address to make sure that it is compatible with the Wireless AP.

d). Lost or forgot Administrator password.

- Reset system setting (by holding **Reset** button down for 10 seconds) into factory default, this will restore administrator password to **admin/admin**.
- Re-configure your AP according to your previous setting.

Warning: When you reset the AP device, the configuration settings will also be reset to the factory default. Make sure you have written down the AP settings for record.

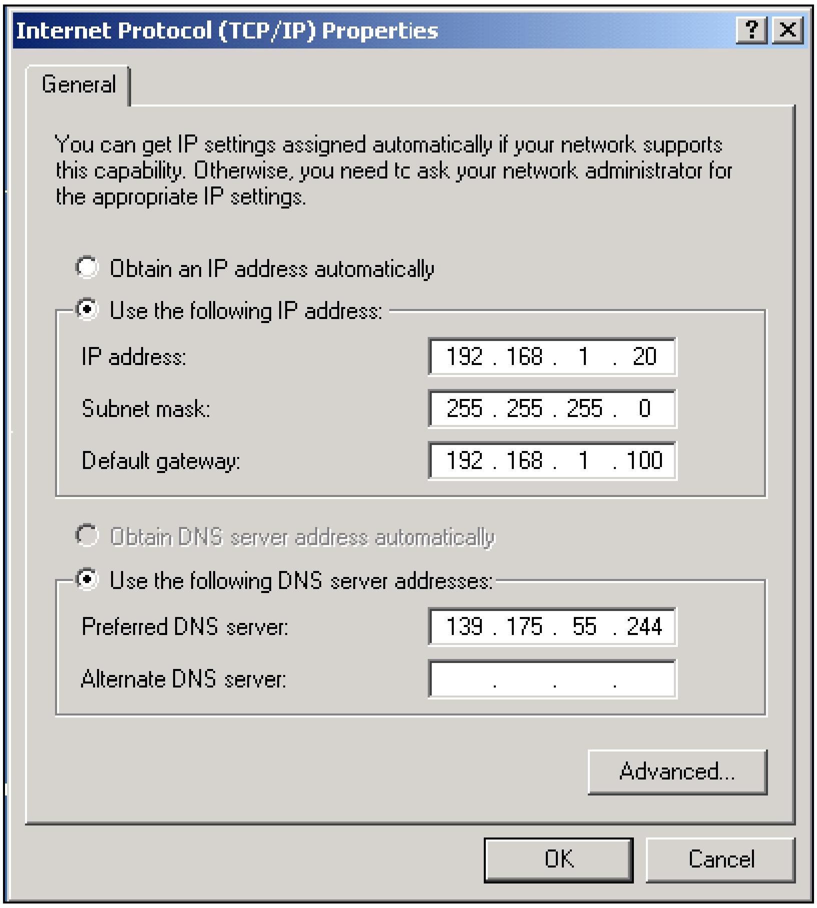
Appendix A

Configure PC's IP address manually

(a). Select **IP Address** tab, and then choose **Specify an IP Address**. Type in your customized IP address (the default IP address of this product is 192.168.1.251. So you can type in an IP Address such as 192.168.1.xxx.). Set the Subnet Mask as 255.255.255.0.

(b). Click **Gateway** tab, and add IP address of the router (e.g. the AP's IP Address is 192.168.1.251).

(c). Change to **DNS Configuration** tab; enable DNS and add DNS values provided by your ISP into **DNS Server Search Order** (See Figure A-1).



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need tc ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 100

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 139 . 175 . 55 . 244

Alternate DNS server: . . .

Figure A-1 DNS Configuration tab

(d). Click **OK** to finish.

Appendix B

Technical information

General:

• Standard Compliance: IEEE 802.11g/b, IEEE 802.3af, IEEE 802.3, IEEE 802.3u, IEEE 802.1x
• Security: WEP 64 and 128 Bit Encryption, WPA, IEEE802.1x

LAN Interface:

• LAN Port Connection (RJ45): 10/100 Mbps auto-sensing, MDI- MDIX auto-sensing

WLAN Radio:

• Frequency Band: 2.4 ~ 2.4835 GHz
• Spread Spectrum Technology: DSSS (Direct Sequence Spread Spectrum)
• Modulation: DBPSK for 1 Mbps, DQPSK for 2 Mbps, CCK for 5.5 /11 Mbps,
OFDM for 6/9/12/18/24/36/48/54 Mbps
• Data Rate: up to 54Mbps with Auto Fallback
• Radio Output Power (Typical): up to 20 dBm (802.11b)
up to 19 dBm (802.11g)
• Receive Sensitivity (Typical @BER < 10E-5): -80 dBm @ 11 Mbps
(Typical @BER < 10E-5):-65 dBm @ 54 Mbps
• Operating range: Open environment: Up to 300m, Office environment: 30 ~ 100m

Management:

• Web-Based management (single log-in with timeout protection)

Maximum Users:

• Up to 64 wireless users per channel

Mechanical:

• Antenna Connector: RSMA for external antenna
• Antenna type: External Dipole Antenna
• LED Indicators: LAN, WLAN, Power,
• Dimension: 26(H) × 129(W) × 78(D)mm
• Weight: 300g / 10.6 oz
• Mounting: Desktop, ceiling or wall-mounted hardware included
• Power Adapter: 9 VDC, 0.8A output

Environmental:

• Temperature: Operating: 0 to +55°C / 32 to 131°F
Storage: -20 to +70°C / -4 to +158°F
• Humidity: 0 ~ 90% (non-condensing)

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.

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.

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

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.

Adapter
Pluggable equipment, the socket-outlet shall be installed near the equipment and shall be easily accessible.