802.11a/b/g Access Point

User's Guide

FCC Certifications

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

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

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

This device complies with Part 15, subpart B, subpart C, and subpart E 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 RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

CE Mark

CE Approvals:
EN 300 328
EN 301 893
EN 301 489-1/-17
EN 60950-1

Table of Content

Introduction

This is an IEEE802.11a/b/g compliant 11 Mbps & 54 Mbps Ethernet wireless Access Point. The wireless Access Point is equipped with five 10/100 M Auto-sensing Ethernet ports for connecting to LAN and also for cascading to next wireless Access Point.

This Access Point provides 64/128bit WEP encryption, WPA and IEEE802.1x which ensures a high level of security to protects users' data and privacy. The MAC Address filter prevents the unauthorized MAC Addresses from accessing your Wireless LAN. Your network security is therefore double assured.

The web-based management utility is provided for easy configuration that your wireless network connection is ensured to be always solid and hassle free.

Features

- Five LAN ports for Wireless AP cascade
- Support WPA-PSK and WPA2-PSK
- Support AP client mode
- Support data rate automatic fallback
- Automatic channel selection
- Client access control
- Support 802.1x/Radius client with, TKIP, AES and TKIP_AES encryption
- Support IAPP
- Adjustable Tx power, Tx rate, and SSID broadcast
- Allow WEP 64/128 bit

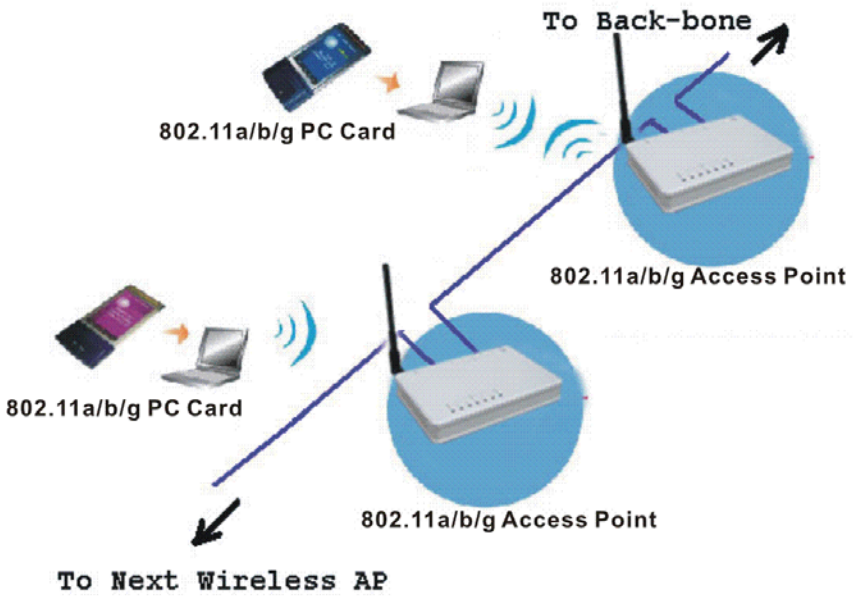
Web interface management

- Support System event log and statistics
- MAC filtering (For wireless only)
- Support wireless 802.11 SNMP management
- WatchDog timer to warm boot system

Application

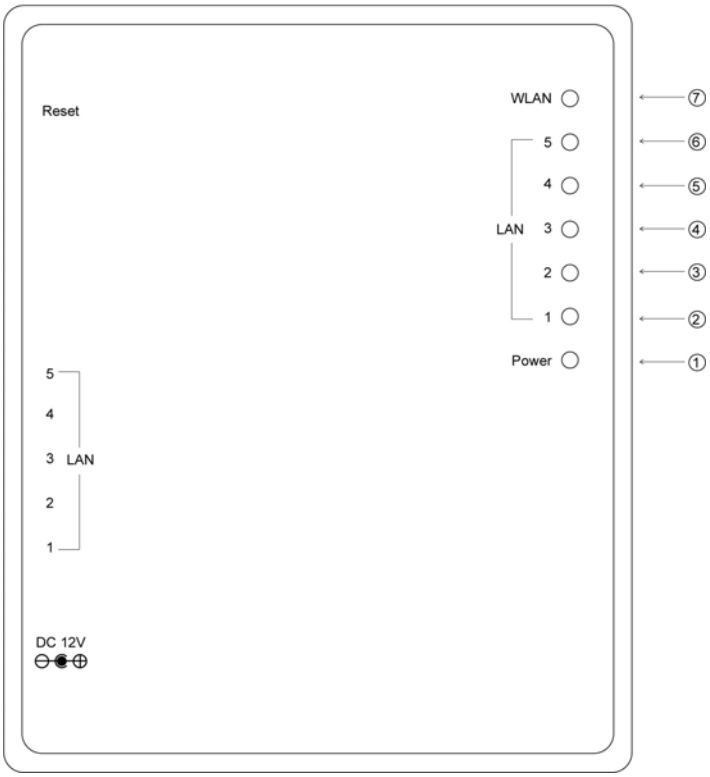
Example 1

Example 2



Parts Names and Functions

1. Front Panel: (LED Indicators)

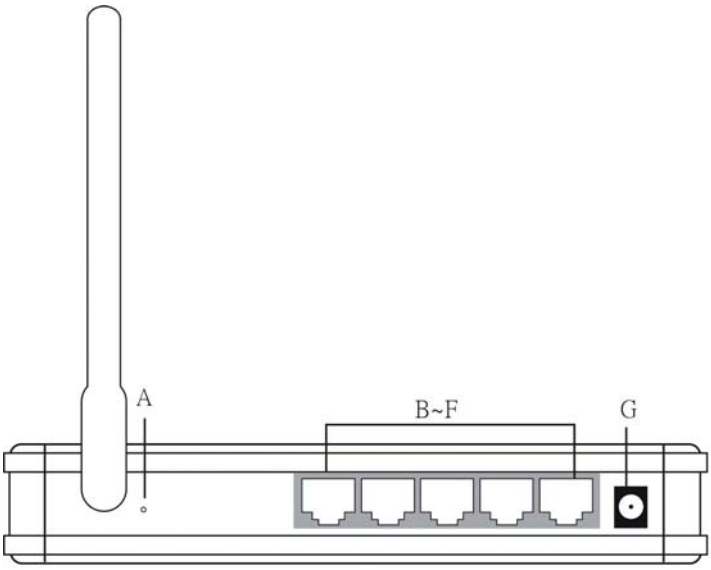


	LED Indicator	Color	Status	
			Solid	**Flashing**
1	**Power**	Yellow	Turns solid yellow when the power is applied to this device.	N/A.
2~6	**LAN**	Yellow	Turns solid Yellow when the corresponding port is connected to another network device through an Ethernet cable.	Receiving/ Sending data
7	**WLAN**	Blue	Turns solid Blue when the power is applied to this device.	Receiving/ Sending data

Table 1: LED Indicators

2. Rear Panel: Connection Ports

-

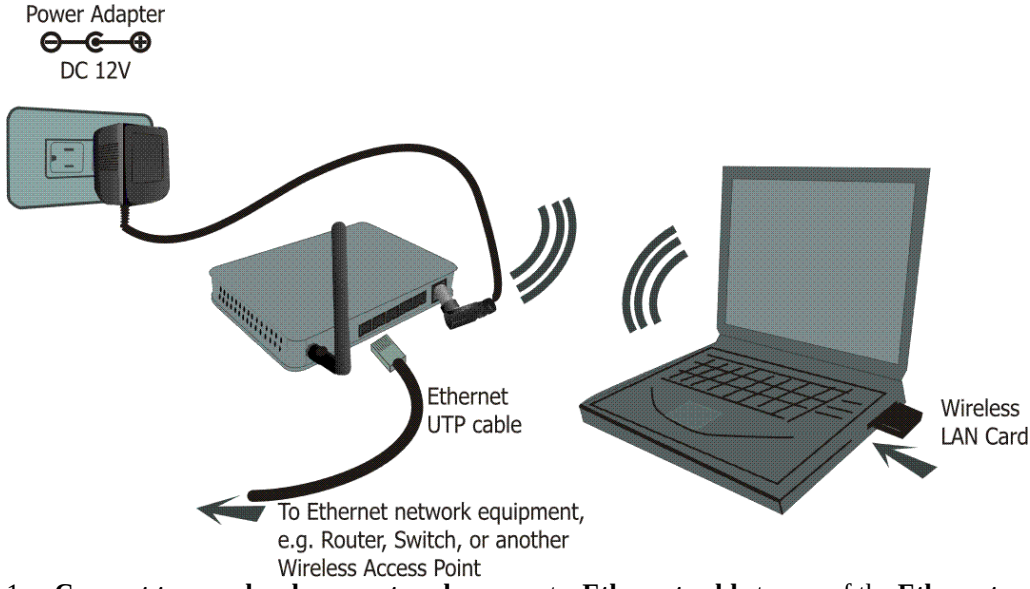


	Port/button	Functions
A	**(Factory) RESET**	Press for over 3 seconds to reboot this device. Press for over 10 seconds to restore the factory settings. Performing the Factory Reset will erase all previously entered device settings.
B~F	**LAN ports**	Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary.
G	**12V DC**	Connects the power adapter plug

Table 2: Connection Ports

Hardware Connection

Note: Before you start the hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for an Access Point is at the center of your wireless network, with line of sigh to all wireless stations. Also, the higher the antenna is placed, the better the device can perform.



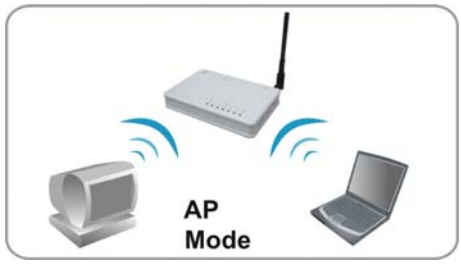
1. **Connect to your local area network:** connect a **Ethernet cable** to one of the **Ethernet** port (LAN1~LAN5) of this wireless Access Point, and the other end to a hub, switch, router, or another wireless access point.
2. **Power on the device**: connect the included AC power adapter to the wireless Access Point's power port and the other end to a wall outlet.
3. **Configure your PC:** Make sure your local PC(s) has wireless network adapter(s) installed.

About the Operation Modes

This device provides four operational applications with **AP, Bridge, Client (Ad-hoc), Client (Infrastructure) and Repeater** modes, which are mutually exclusive.
This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can use the web-based utility provided by the manufacturer as described in the following sections.

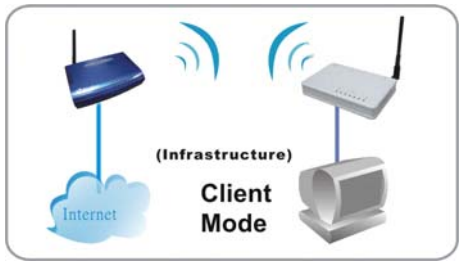
AP Mode

When acting as an access point, this device connects all the stations (PC/notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the Access Point has the Internet connection.



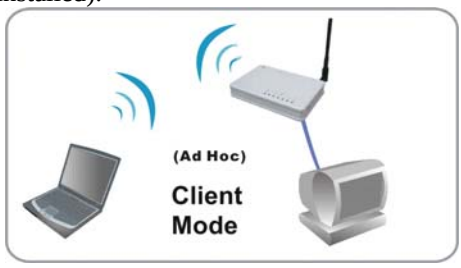
Client Mode (Infrastructure)

If set to Client (Infrastructure) mode, this device can work like a wireless station when it's connected to a computer so that the computer can send packets from wired end to wireless interface.



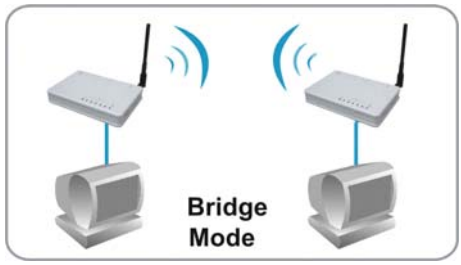
Client Mode (Ad-hoc)

If set to the Client (Ad-hoc) mode, this device can work like a wireless station when it is connected to a computer so that the computer can send packets from wired end to wireless interface. You can share files and printers between wireless stations (PC and laptop with wireless network adapter installed).



Bridge Mode

You will be able to connect two wireless LANs together under the Bridge mode. This only works with another wireless a/b/g Access Point. If enabled you must enter the MAC address of that wireless a/b/g Access Point.



Repeater

You will be able to repeat the wireless signal of the root access point. When enabled you must enter the MAC address of the root access point.

WISP (Client Router) mode

In WISP mode, the AP will behave just the same as the Client mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WISP subscriber can share the WISP connection without the need for extra router.

WISP + Universal mode

In WISP + Universal mode, the AP can also send wireless signal to LAN side, i.e. the AP can connect with the remote WISP AP and the indoor wireless device, and then provide IP sharing capability all at the same time. However, the output power will be cut down while it is being distributed to two wireless sides.

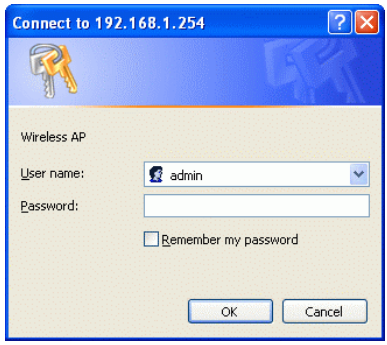
Configuration

Login

1. Start your computer. Connect an Ethernet cable between your computer and the wireless Access Point.
2. Make sure your wired station is set to the same subnet as the wireless Access Point, i.e. 192.168.1.254
3. Start your WEB browser. In the *Address* box, enter the following:

HTTP://192.168.1.254

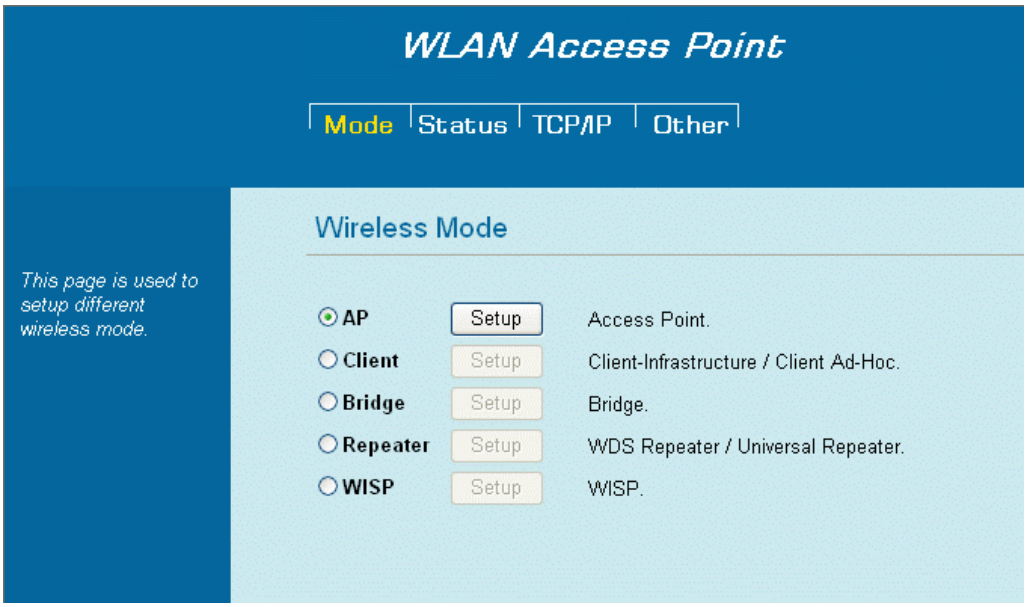
4. Enter **admin** in the Username column when you are prompted the login screen. No password is required for the default setting.



Configuration via Web

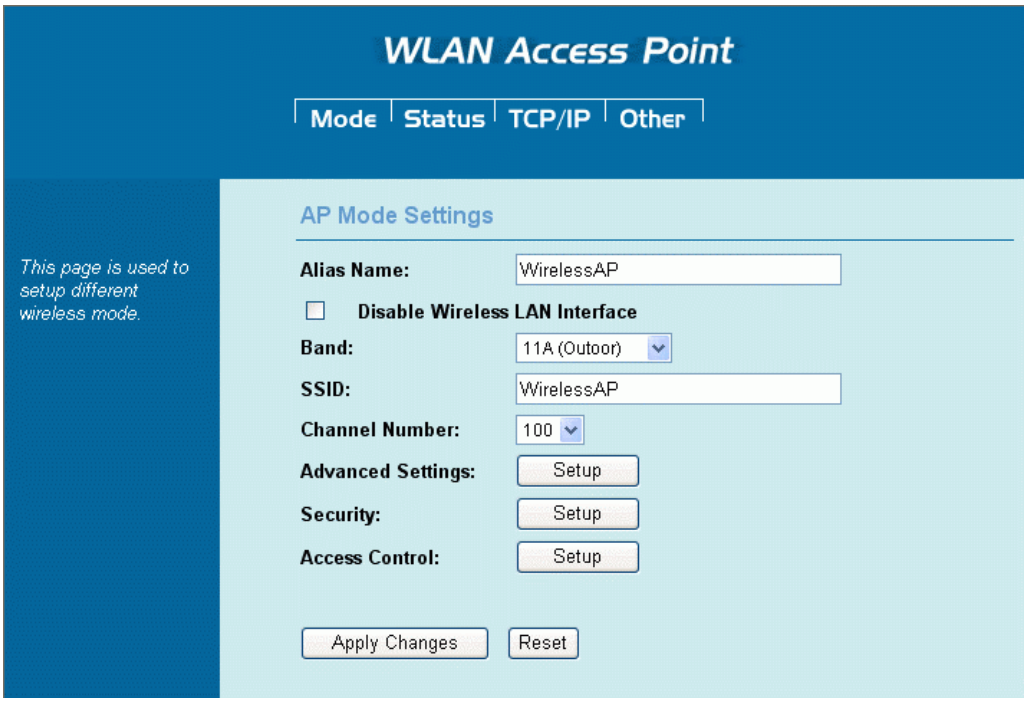
Wireless Mode

Select a wireless mode and then click the **Setup** button to enter its configuration page.



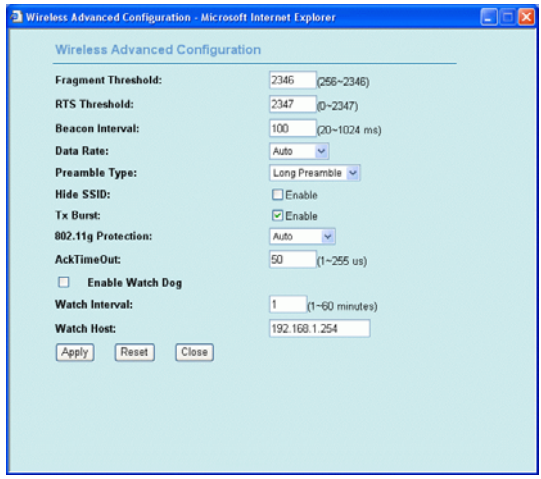
Wireless Mode	
AP	When acting as an access point, this device connects all the stations (PC/notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the Access Point has the Internet connection.
Client	If set to Client (Infrastructure) mode, this device can work like a wireless station when it's connected to a computer so that the computer can send packets from wired end to wireless interface. If set to the Client (Ad-hoc) mode, this device can work like a wireless station when it is connected to a computer so that the computer can send packets from wired end to wireless interface. You can share files and printers between wireless stations (PC and laptop with wireless network adapter installed).
Bridge	The WDS (Wireless Distributed System) function lets this access point act as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools …etc. This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.
Repeater	When set to Wireless Repeater mode, the Wireless Repeater is able to talk to one remote access point within its range and retransmit its signal.
WISP	In WISP mode, the wireless AP function is basically the same as in the client mode. Only the router function is added between the wireless WAN side and the Ethernet LAN side. Therefore the WISP subscriber can share the WISP connection without the need of an extra router.

AP Mode



AP Mode Settings	
Alias Name	Display the name of this device.
Disable Wireless LAN Interface	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another, therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication.

-

	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Advanced Settings	 **Fragment Threshold**: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your 802.11g Wireless LAN PC Card often transmit 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 Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the 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 Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect "hidden station", this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame of the requested transmission. 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**. **Warning:** Enabling RTS Threshold will cause redundant

network overhead that could negatively affect the throughput performance instead of providing a remedy.

This value should remain at its default setting of **2347**. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.

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 access point).

Inactivity Time:

Data Rate: By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, 11or 54 Mbps. For most networks the default setting is **Auto** which is the best choice. When **Auto** is enabled the transmission rate will select the optimal rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.

Preamble Type: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. (**Note**: If you want to change the Preamble type into **Long** or **Short**, please check the setting of AP)

Broadcast SSID: **Enable**: This wireless AP will broadcast its SSID to stations.

Disable: This wireless AP will not broadcast its SSID to stations. If stations want to connect to this wireless AP, this AP's SSID should be known in advance to make a connection.

IAPP: IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station's security context between current access point (AP) and new AP during handoff period.

802.11g Protection: The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operations. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance.

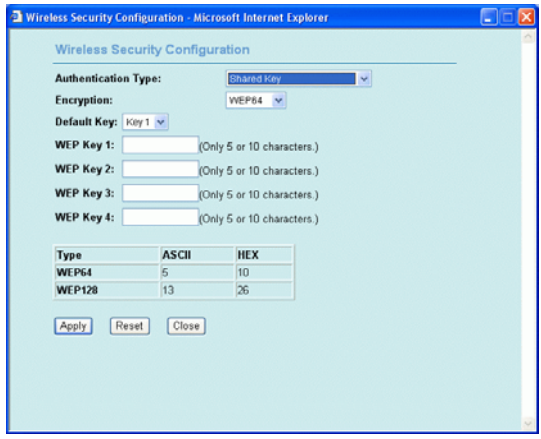
Tx Power level: Select the Tx Power Level from the pull-down men including **Highest (~16dBm)**, **High (~15dBm)**, **Middle (~13dBm)**, **Low (~10dBm)** and **Lowest (~3dBm)**.

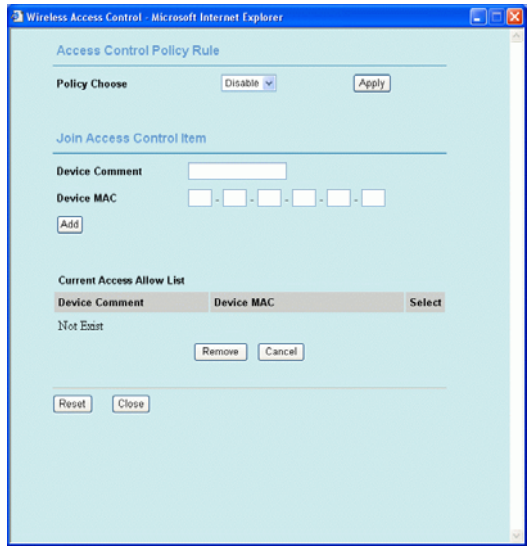
Enable WatchDog: Check to enable the WatchDog function.

Watch Interval: Set the **Watch Interval** in from **1** to **60** minutes.

Watch Host: Set the **Watch Host** in this column.

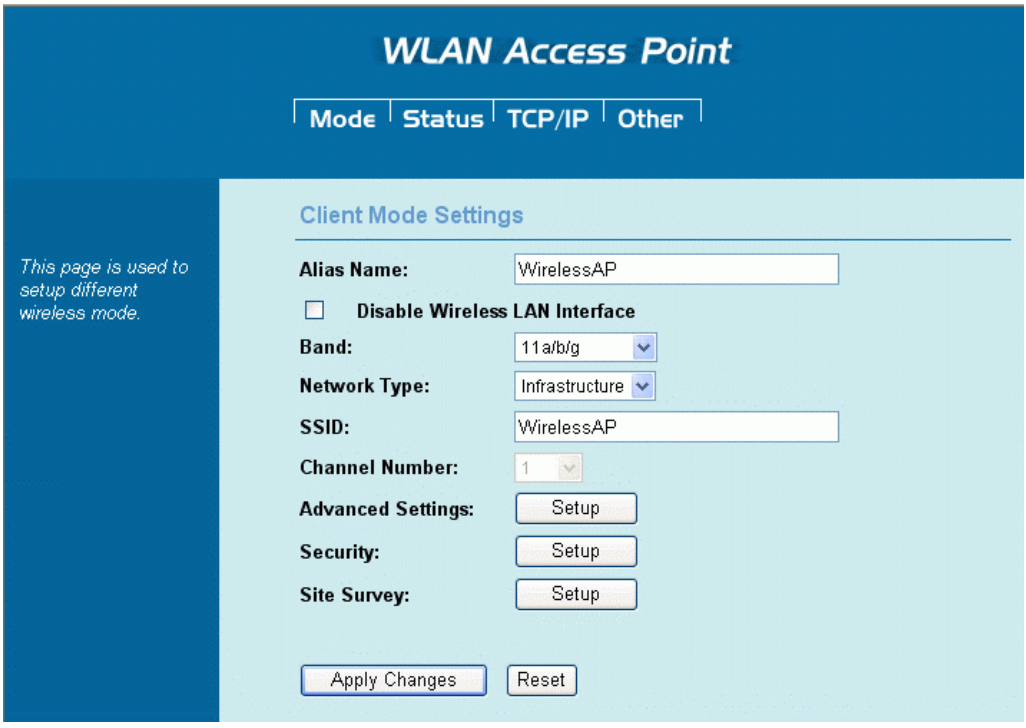
Ack Timeout: When a packet is sent out from one wireless station to the other, it will wait for an Acknowledgement frame from the remote station. If the ACK is NOT received within that timeout

	period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the ACK Window to timeout on lost packets. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. **Set Default**: Click to restore the current settings to the default ones. **Apply Changes**: Click to save and apply the current setting. **Reset**: Click to clear and reset the current settings.
Security	Click the **Setup** button to enter the Security setup page.  **Authentication**: Select an Authentication from the pull-down list including **Open system or Shared Key**, **Open System, Open System with 802.1x**, **Shared Key**, **WPA-RADIUS**, **WPA-PSK**, **WPA2-RADIUS and WPA2-PSK.** **Encryption**: Select the type of encryption from the pull-down list either non or WEP. **Use 802.1x Authentication**: Select **64bit** or **128bit** Encryption. Select **HEX** if you are using hexadecimal numbers (**0-9, or A-F**). Select **ASCII** if you are using ASCII characters (**case-sensitive**). **Ten hexadecimal digits** or **five ASCII characters** are needed if **64-bit WEP** is used; **26 hexadecimal digits** or **13 ASCII characters** are needed if **128-bit WEP** is used. **Pre-Shared Key Format**: Select Passphrase or Hex (64 characters) **Pre-Shared Key**: Pre-Shared-Key serves as a password. Users may key in a 8 to 63 characters string to set the password or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end. There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended. **Group Key Life Time**: Enter the number of seconds that will elapse before the group key change automatically. The default is

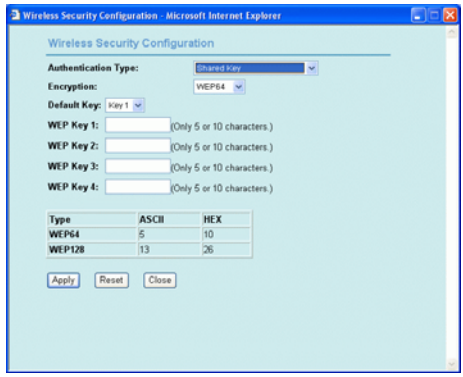
	86400 seconds. **Enable Pre-Authentication**: The two most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Preauthentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network. **Authentication RADIUS Server**: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information. **Port**: Enter the RADIUS Server's port number provided by your ISP. The default is **1812**. **IP Address:** Enter the RADIUS Server's IP Address provided by your ISP. **Password:** Enter the password that the AP shares with the RADIUS Server. **Enable Accounting**: Check to enable this function. **Accounting RADIUS Server**: **Port**: Enter the RADIUS Server's port number provided by your ISP. The default is **1812**. **IP Address:** Enter the RADIUS Server's IP Address provided by your ISP. **Password:** Enter the password that the AP shares with the RADIUS Server. **Apply Changes**: Click to save and apply the current settings. **Reset**: Click to clear and reset the current settings.
Access Control	Click to enter the Access Control screen.  **Wireless Access Control Mode:** Select the Access Control Mode

	from the pull-down menu. • **Disable**: Select to disable Wireless Access Control Mode. • **Allow Listed**: Only the stations shown in the table can associate with the AP. **Deny Listed**: Stations shown in the table won't be able to associate with the AP. **MAC Address:** Enter the MAC Address of a station that is allowed to access this Access Point. **Comment:** You may enter up to 20 characters as a remark to the previous MAC Address. **Apply Changes:** Press to save the new settings on the screen. **Reset:** Press to discard the data you have entered since last time you press Apply Change. **Delete Selected:** To delete clients from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**. **Delete All:** To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox. **Reset:** If you have made any selection, press **Reset** will clear all the select mark.
Apply Changes	Click to save the current settings.
Reset	Click to reset this page.

Client Mode



Client Mode Settings	
Alias Name	Display the name of this device.
Disable Wireless LAN Interface	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Network type	Select a network type from the pull-down menu.
SSID	The SSID differentiates one WLAN from another, therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Enable MAC Clone (Single Ethernet Client)	If your ISP restricts service to PCs only, use the MAC Clone feature to copy a PC Media Access Control (MAC) address to your router. This procedure will cause the router to appear as a single PC, while allowing online access to multiple computers on your network.
Security	Click the Setup button to enter the Security configuration page.



Authentication: Select an Authentication from the pull-down list including **Open system or Shared Key**, **Open System**, **Shared Key**, **WPA-PSK and WPA2-PSK.**

Encryption: Select either **Non** or **WEP**.

Pre-Shared Key Format: Pre-Shared-Key serves as a password. Users may key in a 1 to 63 characters string to set the password or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

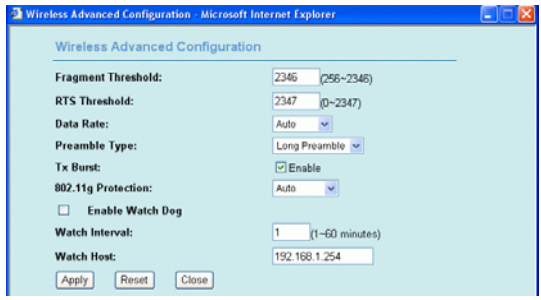
There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.

Pre-Shared Key:

Group Key Life Time: Enter the number of seconds that will elapse before the group key change automatically. The default is 86400 seconds.

Advanced Settings

Click the Setup button to enter the Advanced Settings page.



Fragment Threshold: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your 802.11g Wireless LAN PC Card often transmit 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 Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data

transmission with the 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 Access Point. The collision will most certainly result in a loss of messages for both stations.

Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect "hidden station", this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame of the requested transmission.

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**.

Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

This value should remain at its default setting of **2347**. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.

Data Rate: By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, 11or 54 Mbps. For most networks the default setting is **Auto** which is the best choice. When **Auto** is enabled the transmission rate will select the optimal rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.

Preamble Type: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. (**Note**: If you want to change the Preamble type into **Long** or **Short**, please check the setting of AP)

Tx Burst: Click to enable the Tx burst mode.

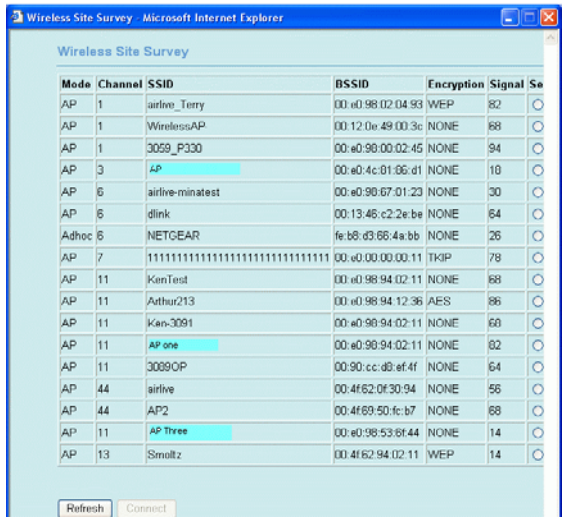
802.11g Protection: The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operations. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance.

Enable WatchDog: Check to enable the WatchDog function.

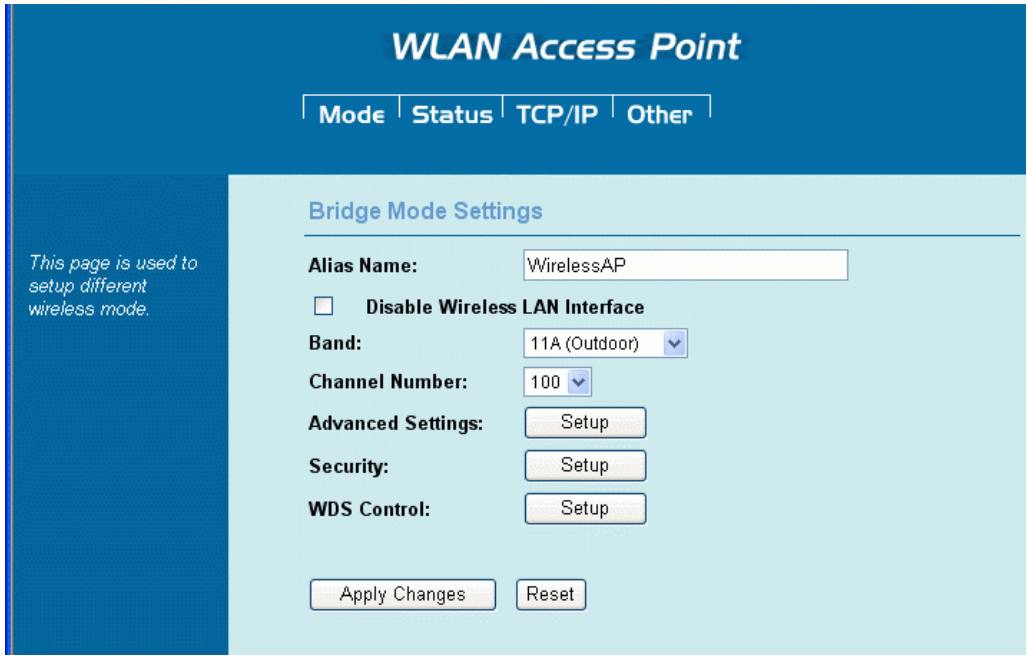
Watch Interval: Set the **Watch Interval** in from **1** to **60** minutes.

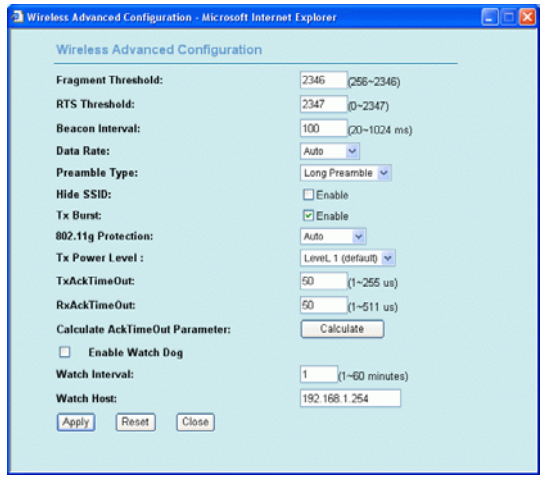
Watch Host: Set the **Watch Host** in this column.

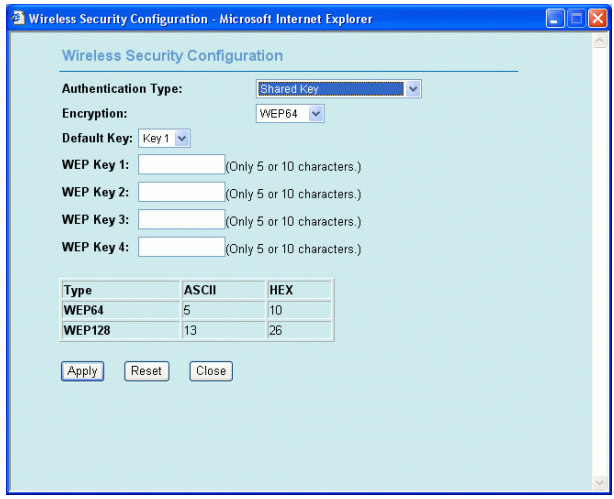
-

	Apply Changes: Click to save and apply the current setting. **Reset**: Click to clear and reset the current settings. **Close**: Click to exit this configuration window.
Site Survey	Site survey displays all the active Access Points and IBSS in the neighborhood. 
Apply Changes	Click to save the current settings.
Reset	Click to reset this page.

Bridge Mode



Bridge Mode Settings	
Alias Name	Display the name of this device.
Disable Wireless LAN Interface	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Advanced Settings	Please refer to the advanced settings of AP Mode. 
Security	Click the Setup button to enter the WDS Security configuration page.



Encryption: Select he encryption type from the pull-down menu, including None, WEP64 bits, WPA (TKIP) and WPA (AES).

WEP Key Format: Select **HEX** if you are using hexadecimal numbers (**0-9, or A-F**). Select **ASCII** if you are using ASCII characters (**case-sensitive**).

Ten hexadecimal digits or **five ASCII characters** are needed if **64-bit WEP** is used; **26 hexadecimal digits** or **13 ASCII characters** are needed if **128-bit WEP** is used.

WEP Key: Enter the WEP key in this column

Pre-Shared Key Format: Select the Pre-Shared Key from the pull-down menu

Pre-Shared Key: Pre-Shared-Key serves as a password. Users may key in 8 to 63 characters a string to set the password or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

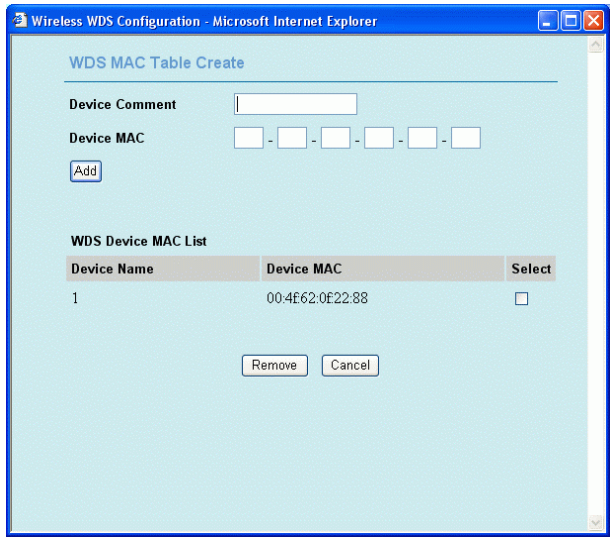
There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.

Apply Changes: Click to save and apply the current settings.

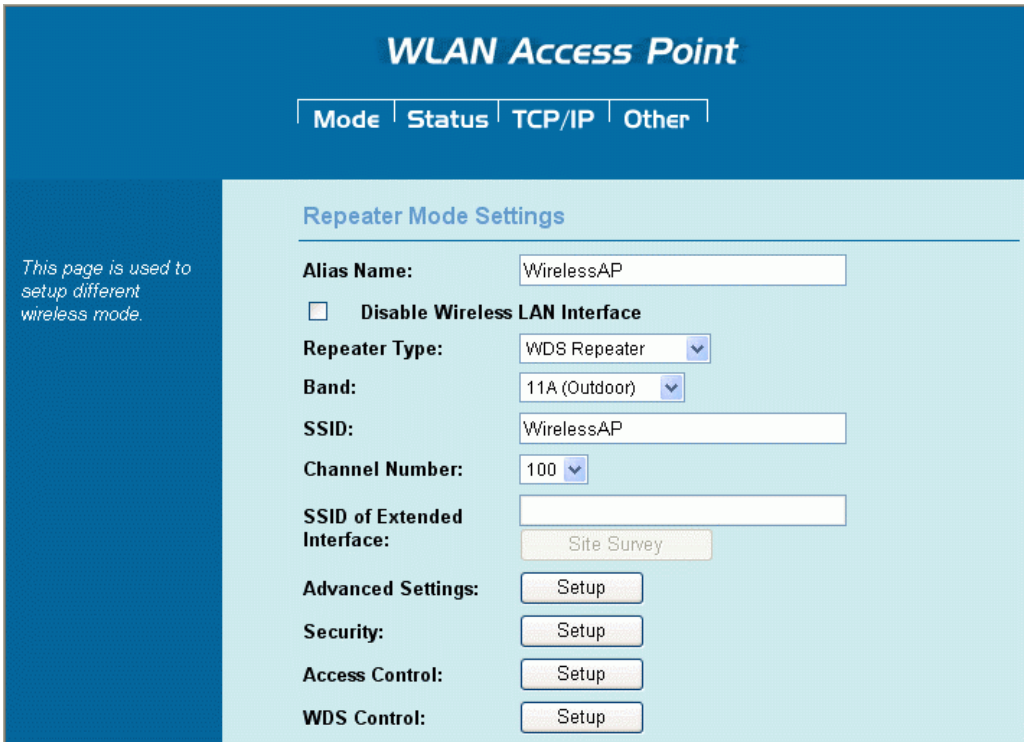
Close: Click to close this configuration window.

Reset: Click to clear and reset the current settings.

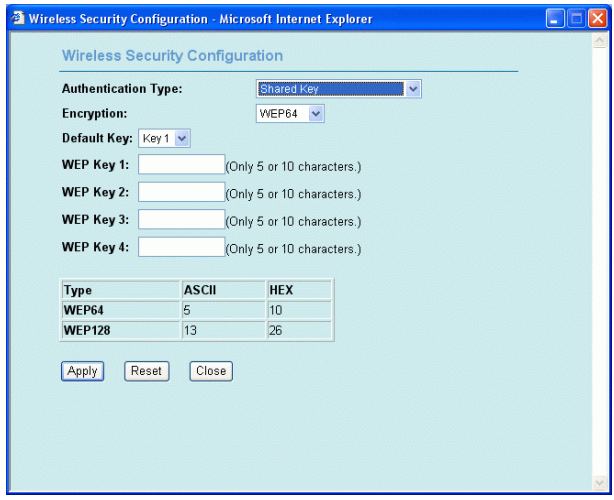
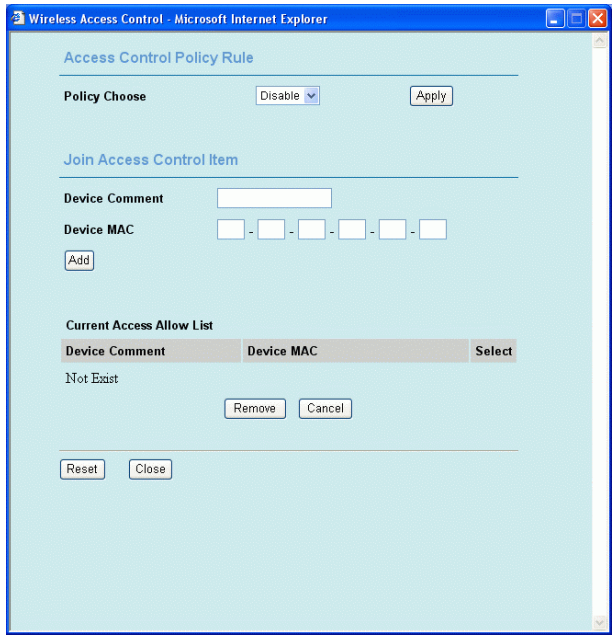
WDS Control	

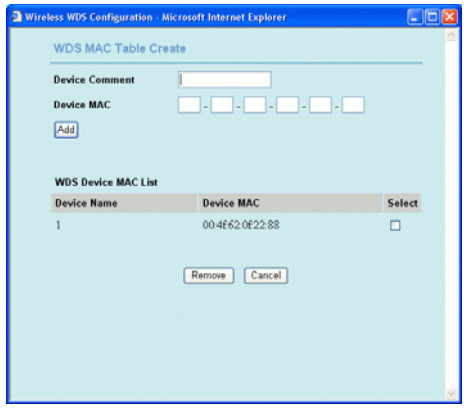
	 **Device Comment:** Enter a comment or description for the AP MAC Address. **Device MAC:** Enter the AP MAC address in this column, the maximum input is 12 digits. **Add:** Click to add a new MAC address. **WDS Device MAC List:** This table displays you the AP MAC information. **Remove**: Select a device name and then click the Remove button to delete. **Cancel**: Click to abort selecting.
Apply Changes	Click to save the current settings.
Reset	Click to reset this page.

Repeater Mode

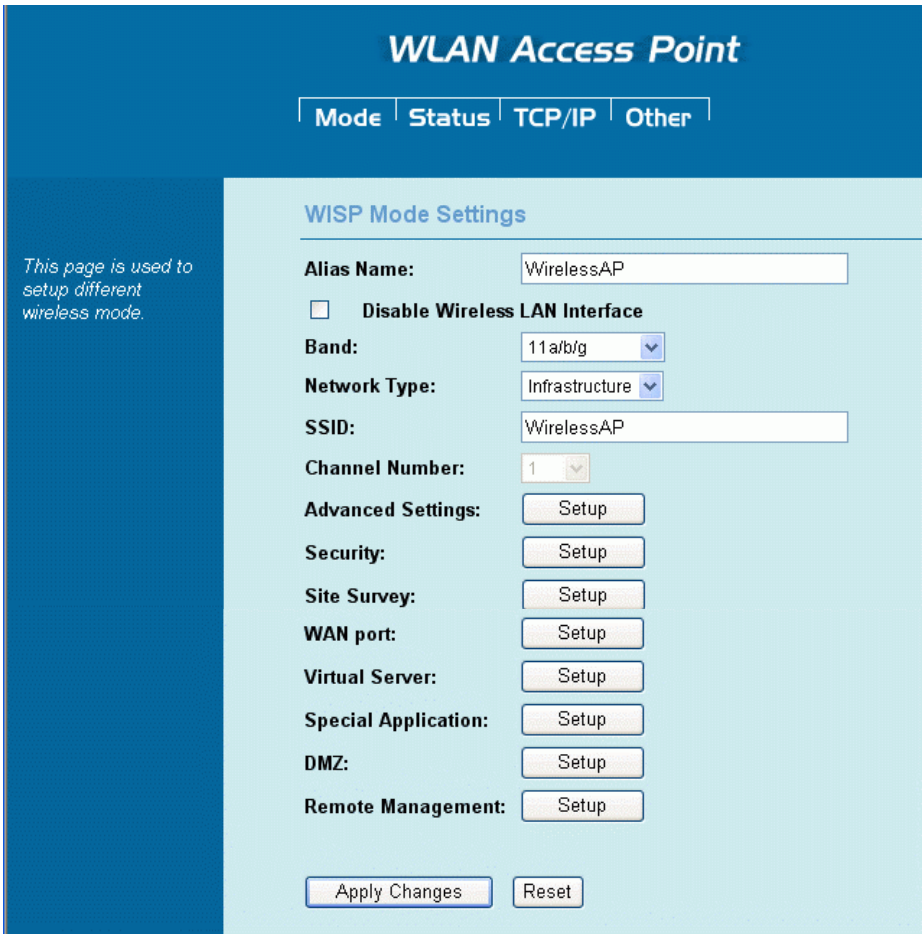


Repeater Mode Settings	
Alias Name	Display the name of this device.
Disable Wireless LAN Interface	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Repeater Type	Select WDS Repeater or Universal Repeater from the pull-down menu.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	Displays the wireless network name.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point

	must use the same channel.
SSID of Extended Interface	When the Universal Repeater is enabled, the SSID of other AP must be entered in this field.
Advanced Settings	Click to enter the Advanced Settings screen. For the detailed settings, please refer to the Advanced setting described previously.
Security	Click the Setup button to enter the security configuration page. For the detailed Settings, please refer to the Security settings in the AP mode. 
Access Control	Click to enter the Access Control screen.  **Wireless Access Control Mode:** Select the Access Control Mode from the pull-down menu. • **Disable**: Select to disable Wireless Access Control Mode. • **Allow Listed**: Only the stations shown in the table can

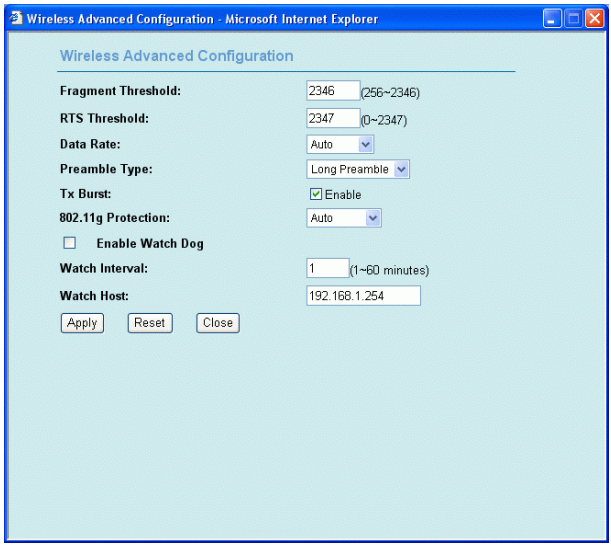
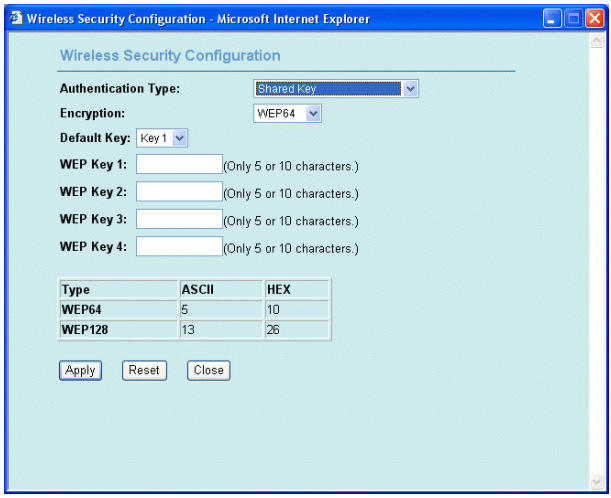
	associate with the AP. **Deny Listed**: Stations shown in the table won't be able to associate with the AP. **MAC Address:** Enter the MAC Address of a station that is allowed to access this Access Point. **Comment:** You may enter up to 20 characters as a remark to the previous MAC Address. **Apply Changes:** Press to save the new settings on the screen. **Reset:** Press to discard the data you have entered since last time you press Apply Change. **Delete Selected:** To delete clients from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**. **Delete All:** To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox. **Reset:** If you have made any selection, press **Reset** will clear all the select mark.
WDS Control	 Device Comment: You may enter up to 20 characters as a remark to the previous MAC Address. Device MAC: Enter the MAC Address of a station that is allowed to access this Access Point. Add: Click to add the MAC address into the WDS Device MAC List. Remove: Click the Remove button after selecting the item you want to delete. Cancel: Click to abort selecting.
Reset	Click to clear and reset the current settings.

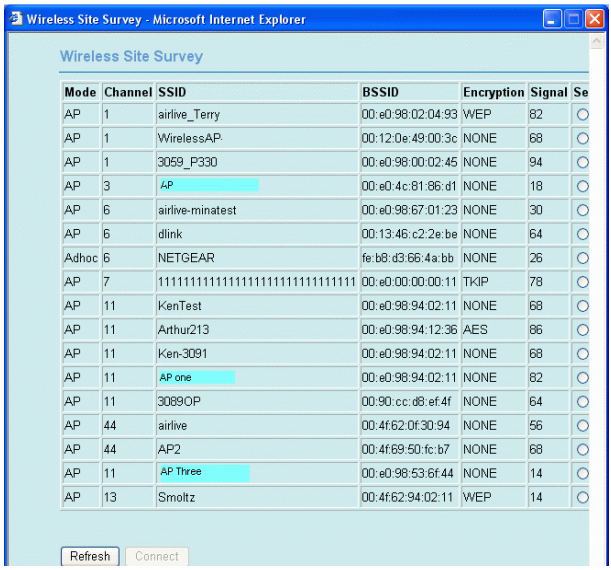
WISP



WISP Mode Settings	
Alias Name	Displays the alias name of this device.
Disable Wireless LAN Interface	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Network type	Select the network type from the pull-down menu.
SSID	Displays the wireless network name.
Channel number	Select which channel to be located (from 1 to 13).
Advanced Settings	Click to enter the advanced settings screen.

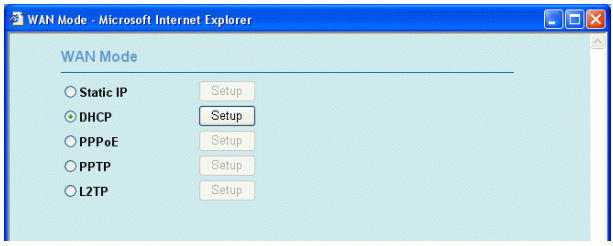
-

	
Security	Click to enter the security configuration screen. 
Site Survey	Site survey displays all the active Access Points and IBSS in the neighborhood.



WAN Port

Click to enter the WAN Port setup screen.



WAN Access Type: Select the WAN access type (Static IP, DHCP, PPPoE and PPTP) from the pull-down menu.

DNS1~3: Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es).
DNS 1 and DNS 2 servers are optional. You can enter another DNS server's IP address as a backup. DNS 1 and DNS 2 servers will be used when the DNS 1 server fails.

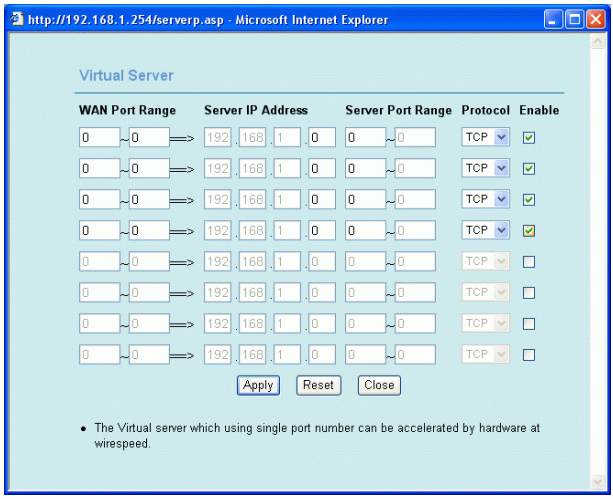
Clone MAC Address: Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.

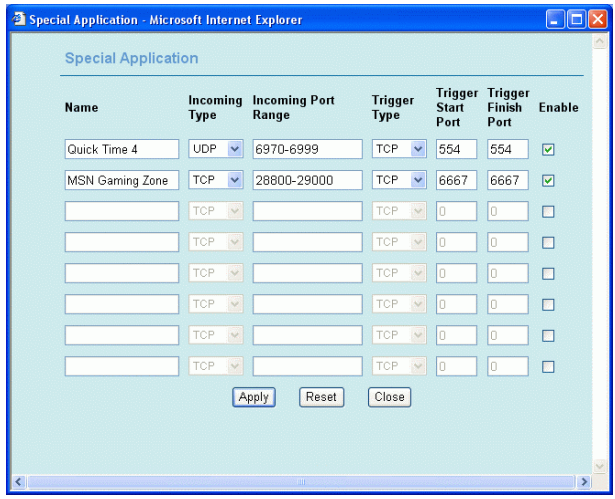
Save: Click to save and apply the current settings.

Reset: click to clear and reset the current settings.

Virtual Server

Click to enter the Virtual Server screen.

	 **Enable Virtual Servers**: Check to enable the Virtual Server function. **Servers**: You can set up a local server with specific port number that stands for the service (e.g. web (80), FTP (21), Telnet (23)). When this device receives an incoming access request for this specific port, it will be forwarded to the corresponding internal server. You can add virtual servers by either port numbers or by names. Maximum 24 Server entries are allowed and each port number can only be assigned to one IP address. **Local IP Address**: Enter the Local Server's IP address. **Protocol**: Select the protocol (TCP, UDP or Both) used to the remote system or service. **Port Range**: For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields. **Description**: You may key in a description for the local IP address. **Save**: Click to save and apply the current settings. **Reset**: Click to clear and rest the current settings. **Current Virtual Servers table**: Shows the current virtual servers information.
Special Application	Click to enter the Special Application screen.



Name: Enter the application name.

Incoming Type Click the down arrow ▼ to select the incoming application type (TCP or UDP)

Incoming Start Port Type a port number or the starting port number in a range of port numbers.

.

Incoming Finish Port: Type a port number or the ending port number in a range of port numbers.

Trigger Type Click the down arrow ▼ to select the trigger type (TCP or UDP)

Trigger Start Port: Enter a port number as the starting outbound port for the special application defined in the preceding field.

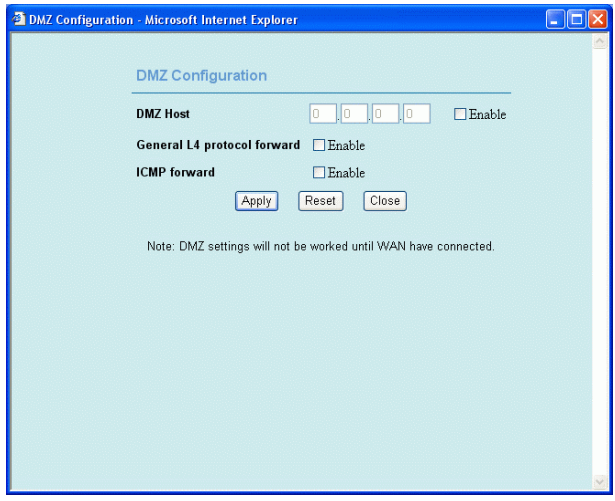
Trigger Finish Port: Enter a port number as the ending outbound port for the special application defined in the preceding field.

Save: Click to save and apply the current settings.

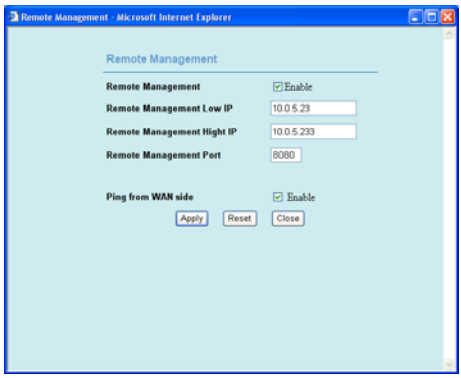
Reset: Click to clear and reset the current settings.

DMZ

Click to enter the DMZ screen.

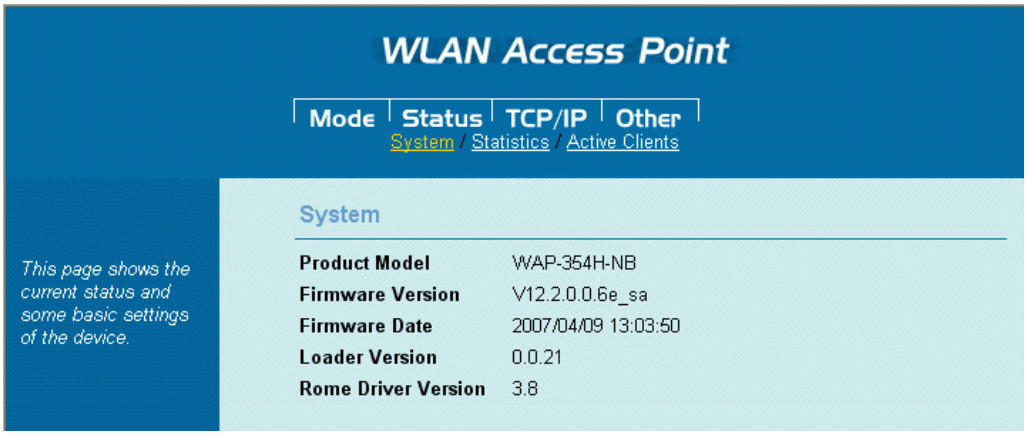


Enable DMZ**:** If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that

	some applications/software, especially Internet / online game can have two-way connections. **DMZ Host IP Address:** Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above. **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly. **Save:** After completing the settings on this page, click **Save** to save the settings. **Reset:** Click **Reset** to restore to default values.
Remote Management	 Remote Management: Check to enable the remote management function. Remote Management Low IP: Enter the minimum IP address, e.g. 10.0.5.23 Remote Management High IP: Enter the minimum IP address, e.g. 10.0.5.233 Remote Management Port: Enter the remote management port number, e.g., 8080. Ping from WAN side: place a check in front of the Enable item to activate this function. Apply: click to save the current settings. Reset: click to clear the current settings. Close: click to exit this page.
Apply Changes	Click to save the current settings.
Reset	Click to reset this page.

Status

System Data



System	
Product Model	Shows the product model name.
Firmware Version	The current version of the firmware installed in this device.
Firmware Date	Shows the firmware date.
Loader Version	The SSID differentiates one WLAN from another, therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.
Rome Driver Version	Shows the Rome driver version.

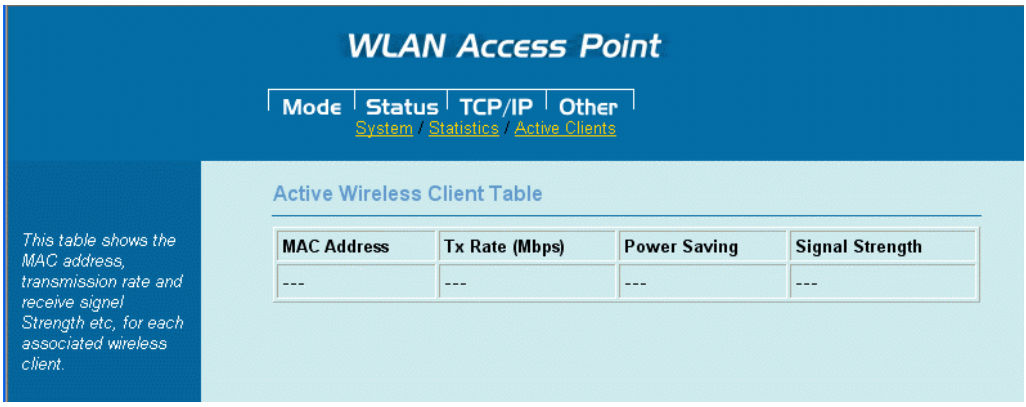
Statistics

Shows the current wireless LAN and Ethernet LAN/WAN statistics table in this screen.

Refresh	Click to refresh the statistics table.

Active Clients

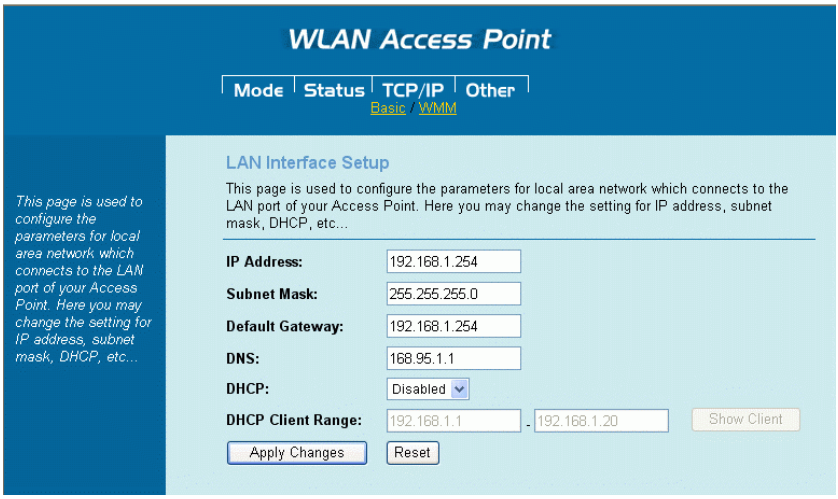
Displays the wireless clients that are currently connecting with this wireless Access Point.



Refresh	Click to refresh the Active Wireless Client table.

TCP/IP

Basic



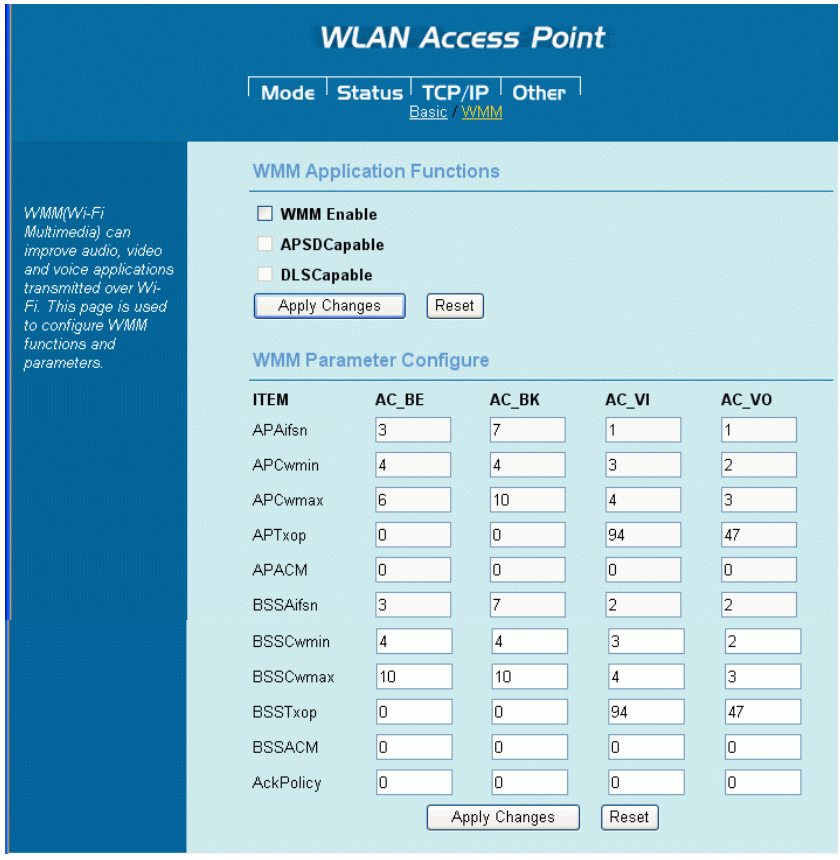
IP Address	Shows the default IP address of this Wireless AP.
Subnet Mask	Shows the default Subnet Mask.
Default Gateway	Shows the default gateway.
DNS	Shows the default DNS address.
DHCP	**Disable**: Select to disable this Router to distribute IP Addresses (Disabled) **Server**: Select to enable this Router to distribute IP Addresses

-

	(DHCP Server). And the following field will be activated for you to enter the starting IP Address
DHCP Client Range	**The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 192.168.1.1 should work for most cases.** • Maximum: **253**. Default value 253 should work for most cases. *Note: If "Continuous IP address poll starts" is set at 192.168.1.1 and the "Number of IP address in pool" is 253, the device will distribute IP addresses from 192.168.1.1 to 192.168.1.253 to all the computers in the network that request IP addresses from DHCP server (Router)*
Apply Changes	After completing the settings on this page, click to save the settings.
Reset	Click to restore to default values.

WMM

WMM™ Quality of Service is a mechanism that assists to handle many applications happening at a time, e.g., video, multimedia streaming, and VoIP phones, to meet a higher quality in congested networks. WMM™ Quality of Service is based upon a subset of the IEEE 802.11e standard.

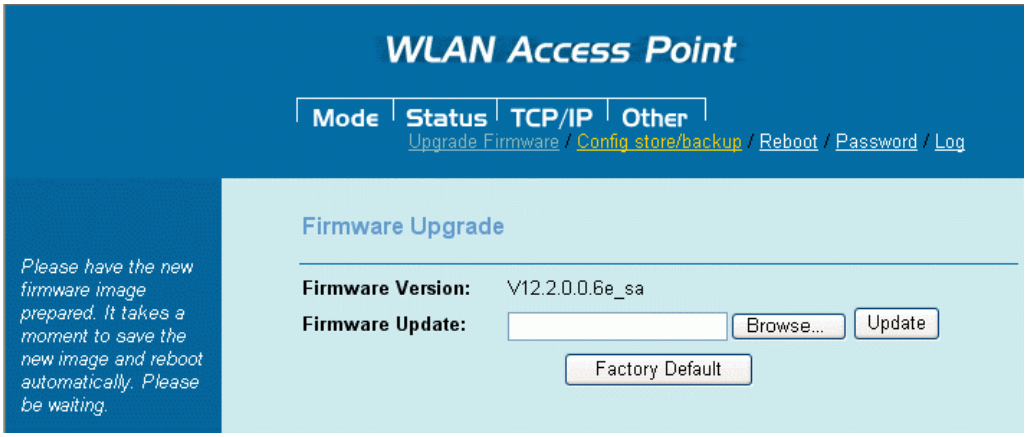


WMM Application Functions	
WMM Enable	If you have other devices on your network that support WMM, Select **Enabled**. Otherwise, keep it disabled.
APSDCapable	Automatic Power Save Delivery is a more efficient power management method than legacy 802.11 Power Save Polling. Most newer 802.11 STAs already support a power management mechanism similar to APSD.
DLSCapable	Direct Link Setup allows direct STA-to-STA frame transfer within a BSS. This is designed for consumer use, where STA-to-STA transfer is more commonly used.
Apply Changes	Click to save the current settings.
Reset	Click to clear the current changes.
WMM Parameter Configure	There are two categories of parameters：APAifsn, APCwmin, APCwmax, APTxop, APACM are the parameters for configuring AP. BSSAifsn, BSSCwmin, BSSCwmax, BSSTxop, BSSACM are for configuring Station **AC:** Access Category **AC_BE**：Best Effort (high priority) **AC_BK**：Background (low priority) **AC_VI**：Video (video first) **AC_VO**：Voice (voice first) If you want to alter any of the parameters above, please refer to the instructions of your WMM products. Instructions of the parameters of WMM Aifsn：Arbitrary Inter-Frame Space Number **The back-off timing for each access category consists of a fixed period called the** Arbitrary Inter-Frame Space Number **followed by a random period called the** Contention Window (CW), **both specified in multiples of the slot time. If the service you are using is VI or VO, the value of the parameters of AC_VI or AC_VO should be smaller. If the service is E-Mail or Web, the value of the parameters of AC_BE or AC_BK should be greater.** Cwmin：Contention Window-Min. Cwmax：Contention Window-Max. **The maximum and the minimum value of Contention Window both affect the back-off timing of WMM access category. In AC_VI and AC_VO, the difference between the maximum and minimum value should be smaller, however, in AC_BE and AC_BK the difference between the maximum and minimum value should be greater.** Txop：Transmission Opportunity **Txop can optimize the configuration of WMM access. Those which need prior WMM access, such as AC_VI and AC_VO, need greater value of parameters.**

	ACM：Admission Control Mandatory **ACM only takes effect on AC_VI and AC_VO. When you set the value as 0, it means that the ACM is controlled by the connecting AP. If you set the value as 1, it means that the Client is in charge.** Ackpolicy：Acknowledgement Policy **When the WMM packets be delivered, it will also send a request back. If you set the value as 0, it means that the system do not want to answer the request. If the value is 1, it means that the system will reply the request. If the system does not reply the request, WMM might have better efficiency.**
Apply Changes	Click to save the current settings.
Reset	Click to clear the current changes.

Other

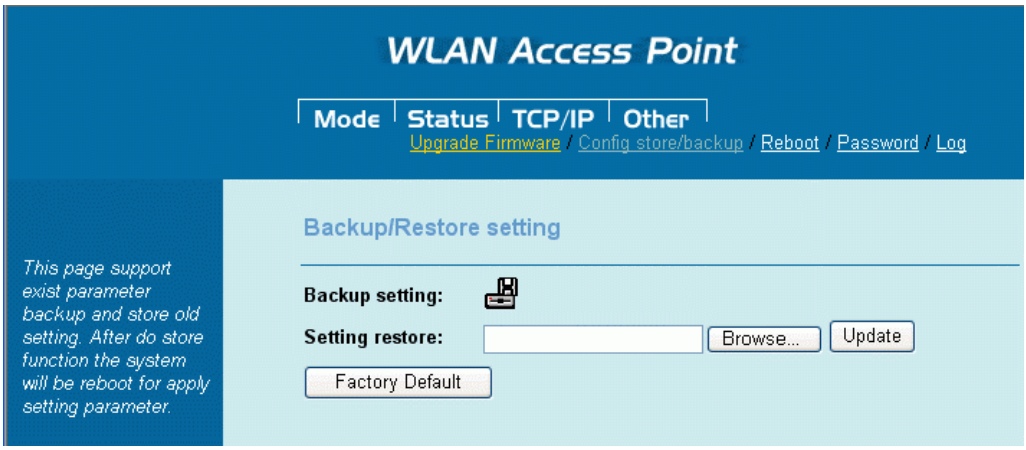
Upgrade Firmware



Upgrade Firmware	
Browse	Click the **Browse** button, find and open the firmware file (the browser will display to correct file path).
Upload	Click the **Upload** button to perform.
Reset	Clic the Reset button to restore default values.

Config store/backup

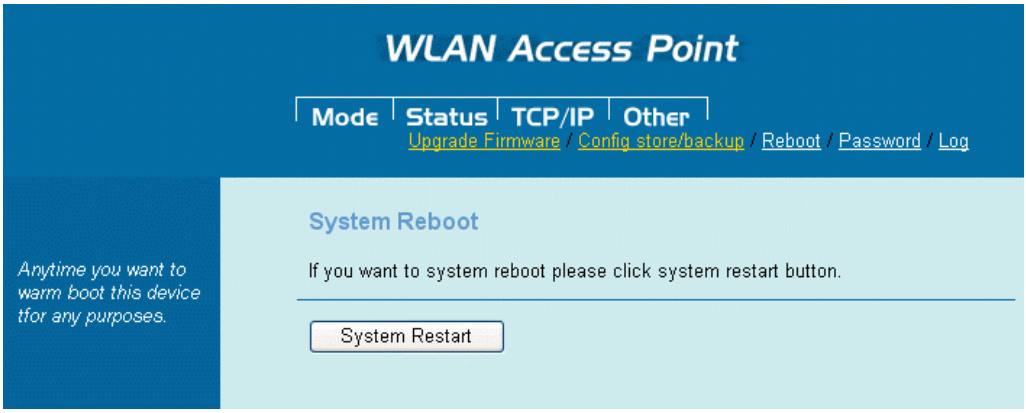
This function enables users to save the current configurations as a file to your computer.



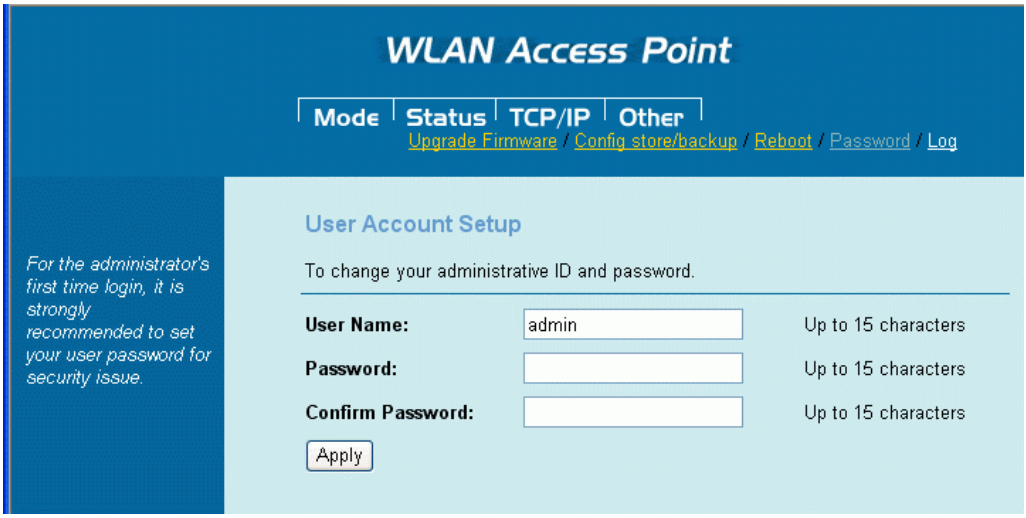
Click the Backup setting icon  to save your current configuration as a file. Users are able to save different versions of configuration files and alter the desired version as they wish. By clicking **Browse**, users can select a file from the computer and then clicking **Update** to start processing. Click **Factory Default** enables users to restore the current configuration to the default settings.

Reboot

Click the Reboot button to reboot the hardware system.



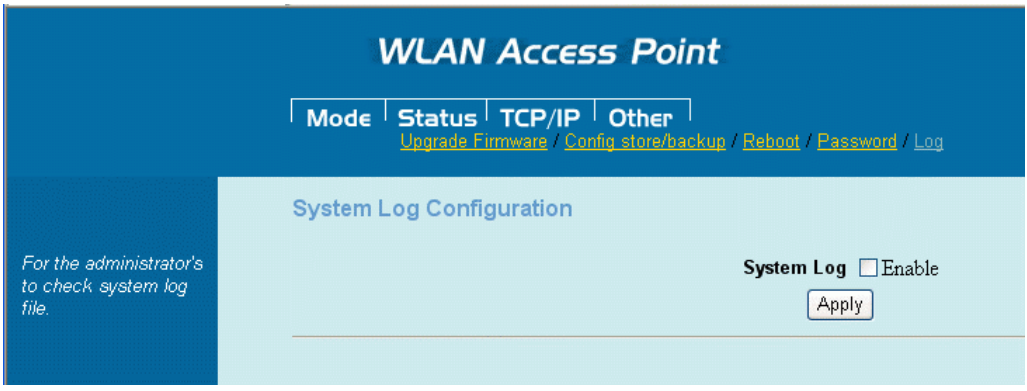
Password



Password Setup	
User Name	Maximum input is 36 alphanumeric characters (case sensitive)
Password	Key in the password you wish to set.
Confirmed Password	Key in the password again to confirm.
Apply Change	After completing the settings on this page, click the **Apply Change** button to save the settings.

Log

The Logs record various types of activity on the Wireless Router. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.



Place a check in front of the Enable item, and then click **Apply** to enable this function. The System log information will appear below right after click the Apply button.