Content

Part 1: Introduction 1

1.1 About 54M Wireless Router..1

1.2 Package contents...1

1.3 Features 1

Part 2: Hardware Installation..2

2.1 Panel Layout...2

2.1.1 The Front Panel...2

2.1.2 The Rear Panel...2

2.2 The System Requirement...3

2.3 Installation Environment Requirement...3

2.4 Connection to Router...3

Part 3: Quick Installation Guide..4

3.1 TCP/IP Configuration...4

3.2 Quick Setup Wizard..5

3.3 Operation mode...11

Part 4: Configuration Guide..12

4.1 Wireless Setting...12

4.2 Wireless Basic settings..12

4.2.1 Wireless Advanced Settings...13

4.2.2 Wireless security setup...13

4.2.3 Wireless Access Control...14

4.2.4 WDS Settings..15

4.2.5 Wireless Site Survey...15

4.2.6 WPS Setting 15

4.3 TCP/IP settings..16

4.3.1 LAN Interface...16

4.3.2 WAN Interface..17

4.4

Firewall...18

4.4.1 Port

Filtering...18

4.4.2 IP

Filtering...19

4.4.3 MAC Filtering...19

4.4.4 Port Forwarding 19

4.4.5 URL Filtering...20

4.4.6 DMZ...20

4.4.7 AntiARP Cheating..21

4.5 Management...21

4.5.1 Status...21

4.5.2 Statistics...22

4.5.3 DDNS...22

4.5.4 QOS...23

4.5.5 Time Zone Setting..23

4.5.6 Denial of Service..24

4.5.7 Log...25

4.5.8 Upgrade Firmware..25

4.5.9 Save/Reload settings ……...25

4.6.0 Password setup.……...26

4.6.1 Apply Settings..……...26

Part 1: Introduction

Thank you for purchasing 54M Wireless Broadband Router. This user guide will assist you with the installation procedure.

1.1 About the 54M Wireless Router

54M Wireless Router is a hybrid design product which combines Ethernet technology and wireless access into a single stand-alone unit. The device allows you take advantages of both mobility and fast connection. All PCs whenever on wireless LAN or Ethernet LAN can share files, printers and other network resource. Moreover, all users can share single account of Internet access by having this device connect to a DSL/Cable modem.

1. Ethernet / Fast Ethernet

Ethernet is the most widely-used network access method, especially in a Local Area Network (LAN) and is defined by the IEEE as the 802.3 standard. Normally, Ethernet is a shared media LAN. All stations on the segment share the total bandwidth, which could be 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet). With a switched Ethernet, each sender and receiver has the full bandwidth. *Fast Ethernet* is defined by the IEEE 802.3u standard, a high-speed version of Ethernet with 100 Mbps transmission rate.

2. Wireless LAN

Wireless Local Area Network systems (WLAN) transmit and receive data through the air by using radio frequency (RF). This offers some advantages like mobility, ease of installation, and scalability over traditional wired systems.

***Mobility**:*

WLAN combine data connectivity with user mobility. This provides users with access to network anywhere in their organization. For example, users can roam from a conference room to their office without being disconnected from the LAN. This is impossible with wired networks.

1.2 Package contents

After carefully unpacking the shipping carton, check the contents listed below.

- 54M Wireless Broadband Router
- A power adapter
- 54M Wireless Broadband Router User Manual

If any of the listed contents are damaged or missing, please contact the retailer from whom you purchased the 54M Wireless Router for assistance.

1.3 Features

The 54M Wireless Router has the following features that make it excellent for network connections.

- Complies with IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u standards
- 1 10/100M Auto-Negotiation WAN RJ45 port, 4 10/100M Auto-Negotiation LAN RJ45 ports
- Supports Auto MDI/MDIX
- Supports Wireless Roaming, can move among different AP and no break
- Supports 54/48/36/24/18/12/9/6/11/5.5/3/2/1Mbps wireless LAN data transfer rates
- Provides 64/128 bit WEP encryption security
- Supports wireless Relay/Bridging/WDS/WDS+AP mode
- Provides WPA and WPA2 authentication and TKIP/AES encryption security
- Provides wireless LAN ACL (Access Control List) filtering
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Virtual Server, Special Application, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT

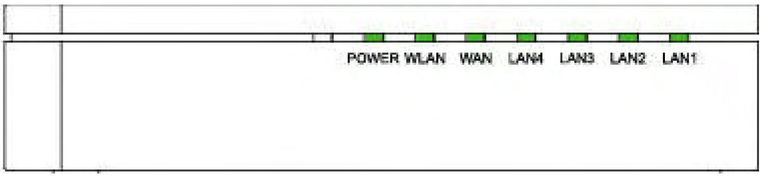
- Supports UPnP, Dynamic DNS, Static Routing,
- Supports Flow Statistics
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter
- Supports firmware upgrade
- Supports Remote and Web management

Part 2: Hardware Installation

2.1 Panel Layout

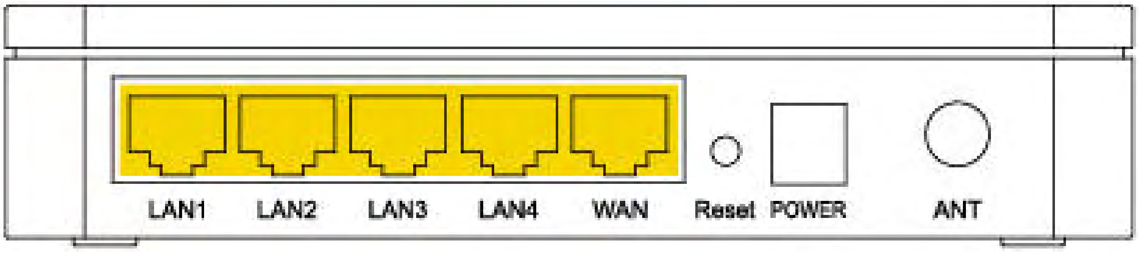
2.1.1 The Front Panel

The front panel of the 54M Wireless Router consists of several LED indicators, which is designed to indicate connections. The table describes the LED on the front panel of the router.



Name	Action	Description
Power	OFF	No Power
	ON	Power on
WAN	ON	The router is starting
	Flashing	The router is working properly
	OFF	The router has a hardware error
WLAN	OFF	The Wireless Radio function is disabled
	Flashing	The Wireless Radio function is enabled
LAN1 / 2 / 3 / 4	OFF	There is no device linked to the corresponding port
	ON	There is a device linked to the corresponding port
	Flashing	There is an active device linked to the corresponding port

2.1.2 The Rear Panel



Antenna interface	Omini Antenna with SMA connector
Power (Power Play Hole)	Plug the power jack. Note: Please use the random spin-off of power, if the use does not match the power supply, may result in damage to the router.
Reset	Factory Default Reset button
WAN	WAN port (RJ-45). Connect xDSL Modem / Cable Modem or Ethernet

LAN 1 / 2 / 3 / 4	RJ-45 interface. Computer and hub / switch connected through these ports into the LAN.

There is a way to reset the router's factory defaults

1.Use the Factory Default Reset button: First, turn on the router's power. Second, press and hold the default reset button, until the system LED lights up(about 5 seconds). Last, release the reset button and wait for the router to reboot.

Notice: Ensure the router is powered on before it restarts completely.

2.2 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector (you do not need it if you connect the router to Ethernet)
- Each PC on the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

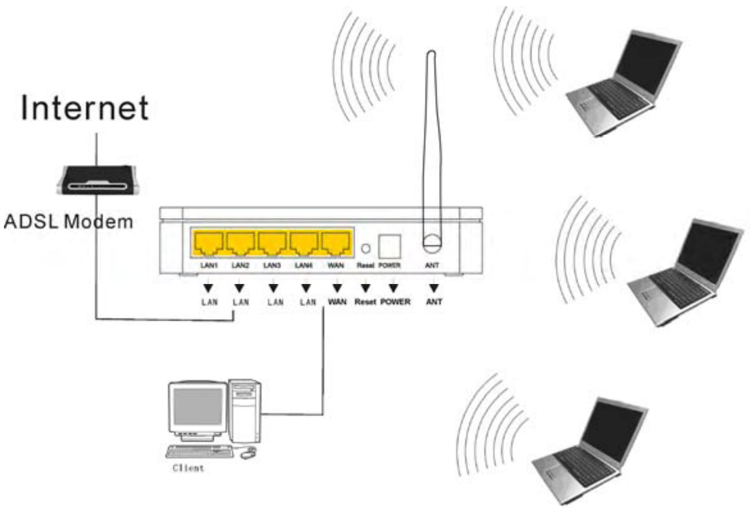
2.3 Installation Environment Requirements

- Not in direct sunlight or near a heater or heating vent
- Not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0℃~40℃
- Operating Humidity: 5%~90%RH, Non-condensing

2.4 Connection to Router

Before you install the router, you should connect your PC to the Internet through your broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

- Power off your PC(s), Cable/DSL modem, and the router.
- Locate an optimum location for the router. The best place is usually near the center of the area in which your PC(s) will wirelessly connect. The place must accord with the Installation Environment Requirements.
- Adjust the direction of the antenna. Normally, upright is a good direction.
- Connect the PC(s) and each Switch/Hub on your LAN to the LAN Ports on the router.
- Connect the DSL/Cable Modem to the WAN port on the router.
- Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
- Power on your PC(s) and Cable/DSL modem.



Part 3: Quick Installation Guide

After connected the 54M Wireless Router with your network, you should configure it. This chapter describes how to configure the basic functions of your 54M Wireless Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after successfully configured.

3.1 TCP/IP configuration

The default IP address of 54Mbps Wireless Router is 192.168.1.254, and the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN, which can be changed as you desired, as an example we use the default values for description in this guide.
Connect the local PCs to the LAN ports on the router. There are then two means to configure the IP address for your PCs.

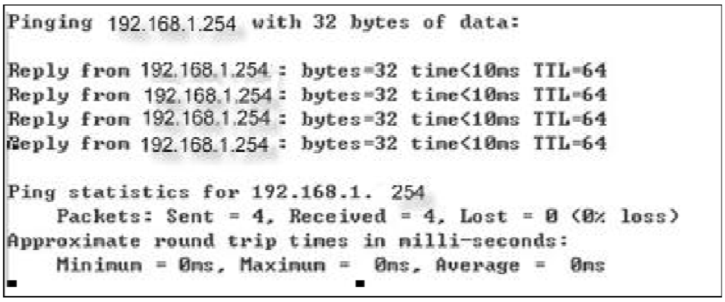
Configure the IP address manually

1. Set up the TCP/IP Protocol for your PC(s).
2. Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.254(The router's default IP address)

Obtain an IP address automatically

1.Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC(s).
2. Power off the router and PC(s). Then turn on the router, and restart the PC(s). The built-in DHCP server will assign IP addresses for the PC(s).

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC(s) and the router.
Open a command prompt, and type ping **192.168.1.254**, then press **Enter.**

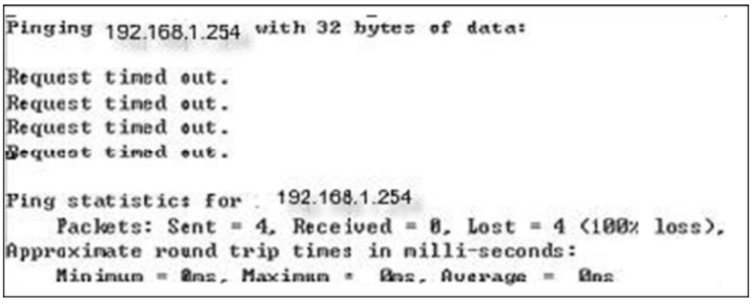


```
Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254 : bytes=32 time<10ms TTL=64
Reply from 192.168.1.254 : bytes=32 time<10ms TTL=64
Reply from 192.168.1.254 : bytes=32 time<10ms TTL=64
Reply from 192.168.1.254 : bytes=32 time<10ms TTL=64

Ping statistics for 192.168.1. 254
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

If the result displayed is similar to that shown in the top of figure, the connection between your PC and the router has been established.



```
Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for  192.168.1.254
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

If the result displayed is similar to that shown in the top of figure, it means that your PC has not connected to the router. Please check it following these steps:

1. Is the connection between your PC and the router correct?

Notice: The 1/2/3/4 LEDs of LAN port on the router and LEDs on your PC's adapter should be light on.

2.Is the TCP/IP configuration for your PC correct?

Notice: If the router's IP address is 192.168.1.254, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.253, the gateway must be 192.168.1.254

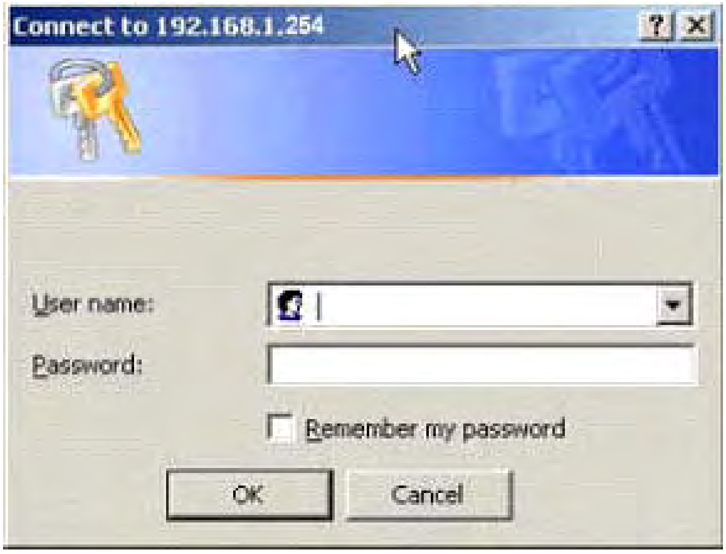
3.2 Quick Setup wizard

With a Web-based (Internet Explorer or Netscape® Navigator) utility, the 54Mbps Wireless Router is easy to configure and manage. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a web browser.

Connect to the router by typing *http://192.168.1.254* in the address field of web browser.

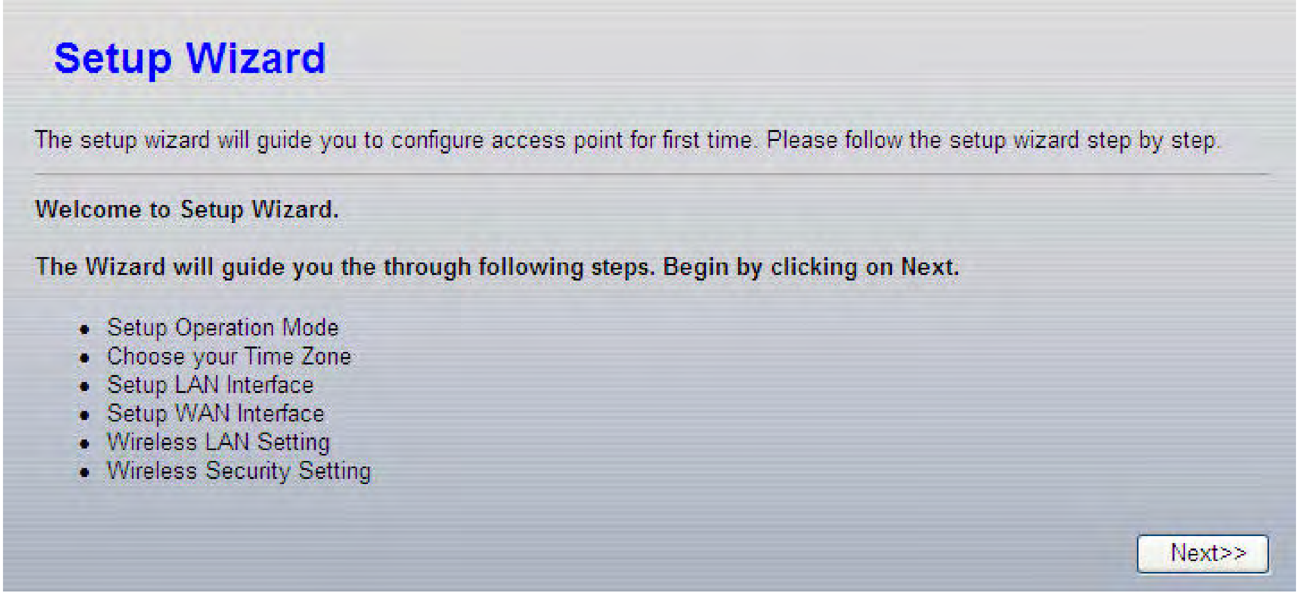
http://192.168.1. 254

After a moment, a login window will appear similar to that shown in Figure. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



NOTE:
If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.
If the User Name and Password are correct, you can configure the router using the web browser. Please click the Setup Wizard link on the left of the main menu and the Setup Wizard screen will appear.

Click **Setup Wizard**, the **Setup Wizard** will appear



Setup Wizard

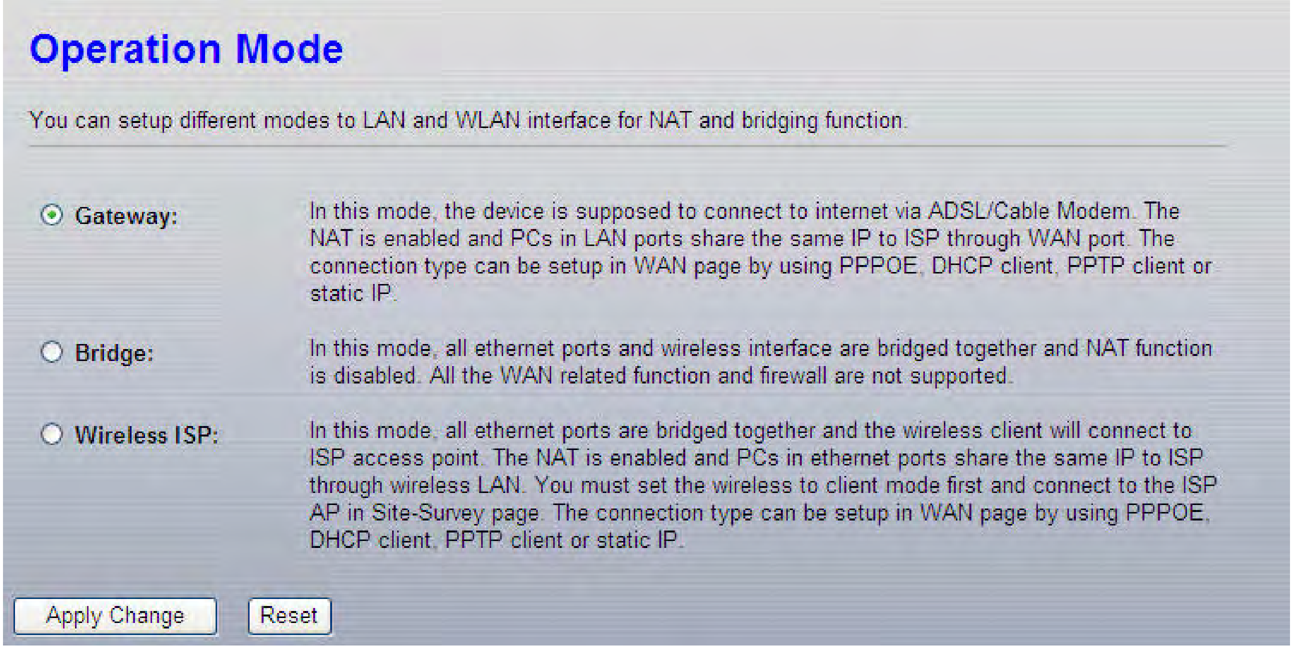
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

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

- Setup Operation Mode
- Choose your Time Zone
- Setup LAN Interface
- Setup WAN Interface
- Wireless LAN Setting
- Wireless Security Setting

The router supports three modes: gateway, bridge, wireless ISP. You can setup different modes to LAN and WLAN interface for NAT and bridging function.



Operation Mode

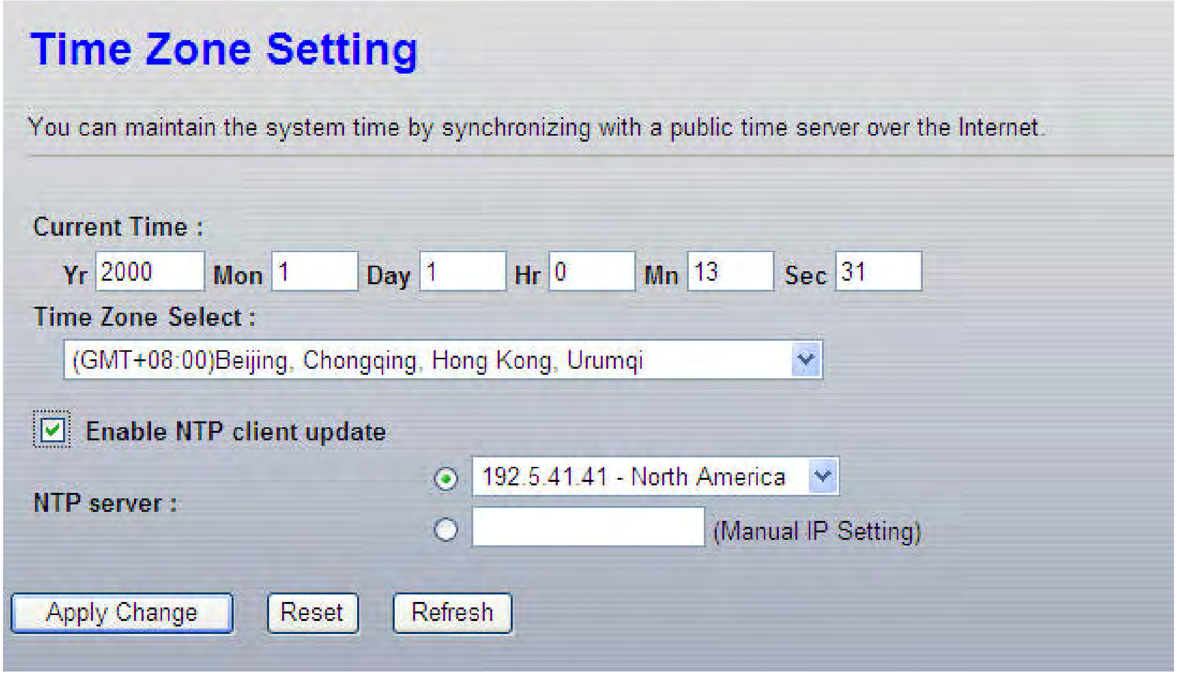
You can setup different modes to LAN and WLAN interface for NAT and bridging function.

● **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

○ **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Click **next**, **Time Zone Setting** will appear. You can select the time zone what you need.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time :

Yr 2000 Mon 1 Day 1 Hr 0 Mn 13 Sec 31

Time Zone Select :

(GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi

☑ Enable NTP client update

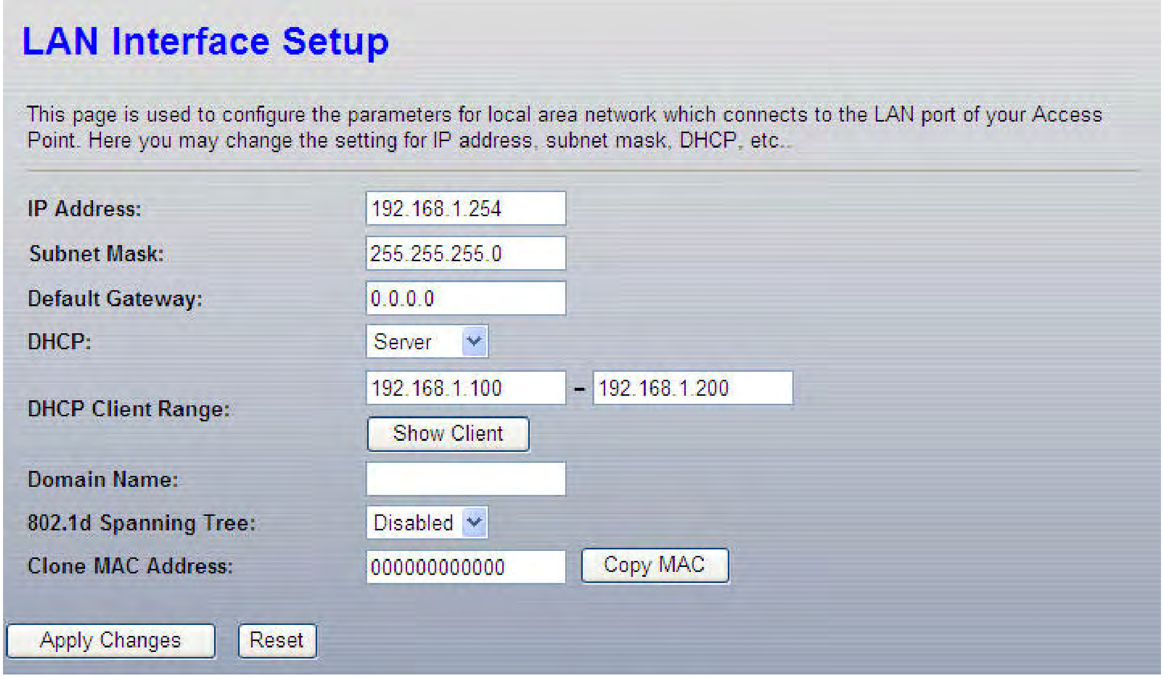
NTP server :

● 192.5.41.41 - North America

○ (Manual IP Setting)

Click **next**, **LAN Interface setup** will appear. In this page, you can set IP address, Subnet Mask.
IP Address - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.254).
Subnet Mask -An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Notice : **The same to all PCs' Subnet Mask with router in you LAN.**

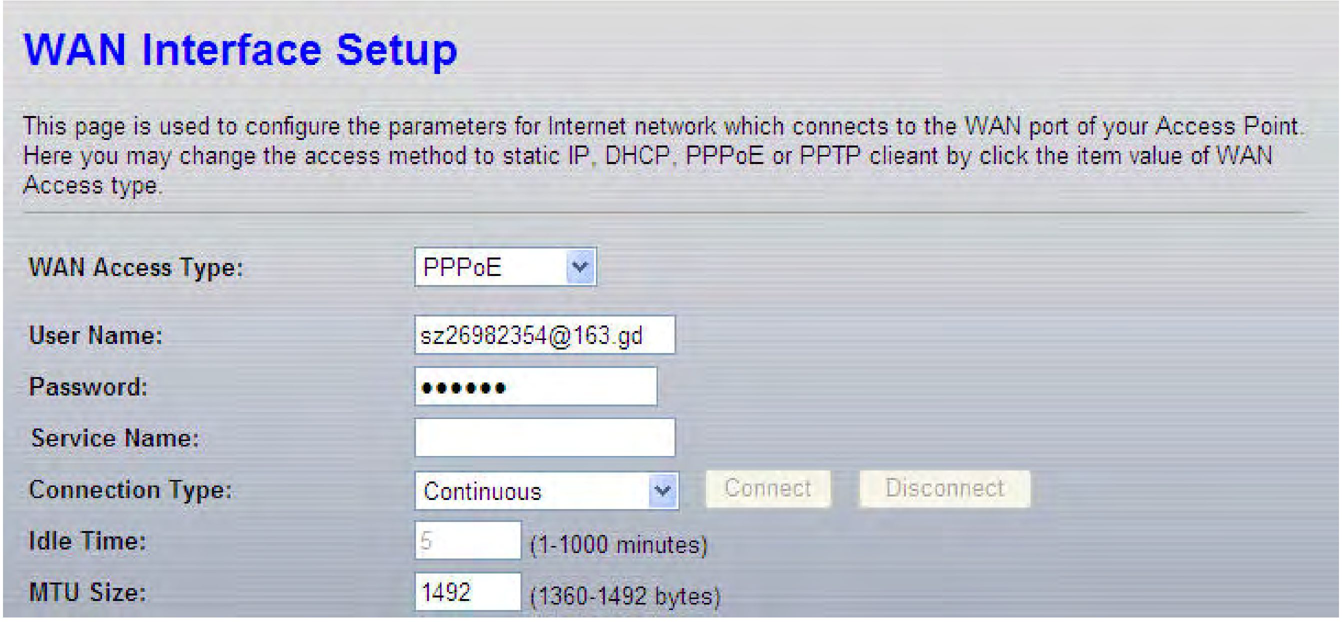


LAN Interface Setup

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 address, subnet mask, DHCP, etc..

IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.1.100 – 192.168.1.200
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Click next, WAN Interface will appear. In this page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.
WAN Access Type: Here you can select the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
User Name and **Password -** Enter the **User Name** and **Password** provided by your ISP.
Services name: Default is blank.



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP clieant by click the item value of WAN Access type.

WAN Access Type: PPPoE

User Name: sz26982354@163.gd

Password: ●●●●●●

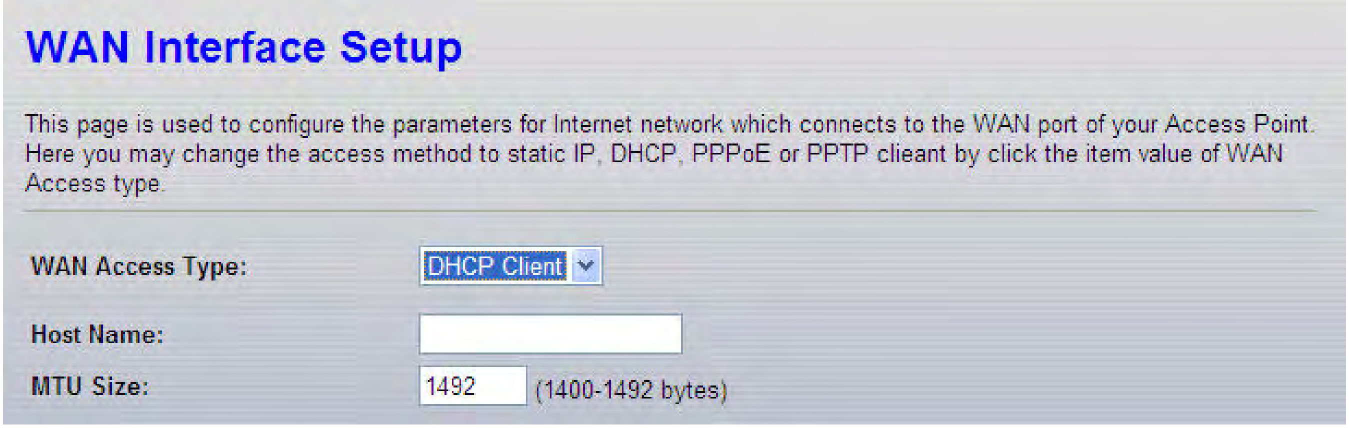
Service Name:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1492 (1360-1492 bytes)

If you choose " **DHCP Client**", the router will automatically receive the IP parameters from your ISP no need to enter any parameters.



WAN Interface Setup

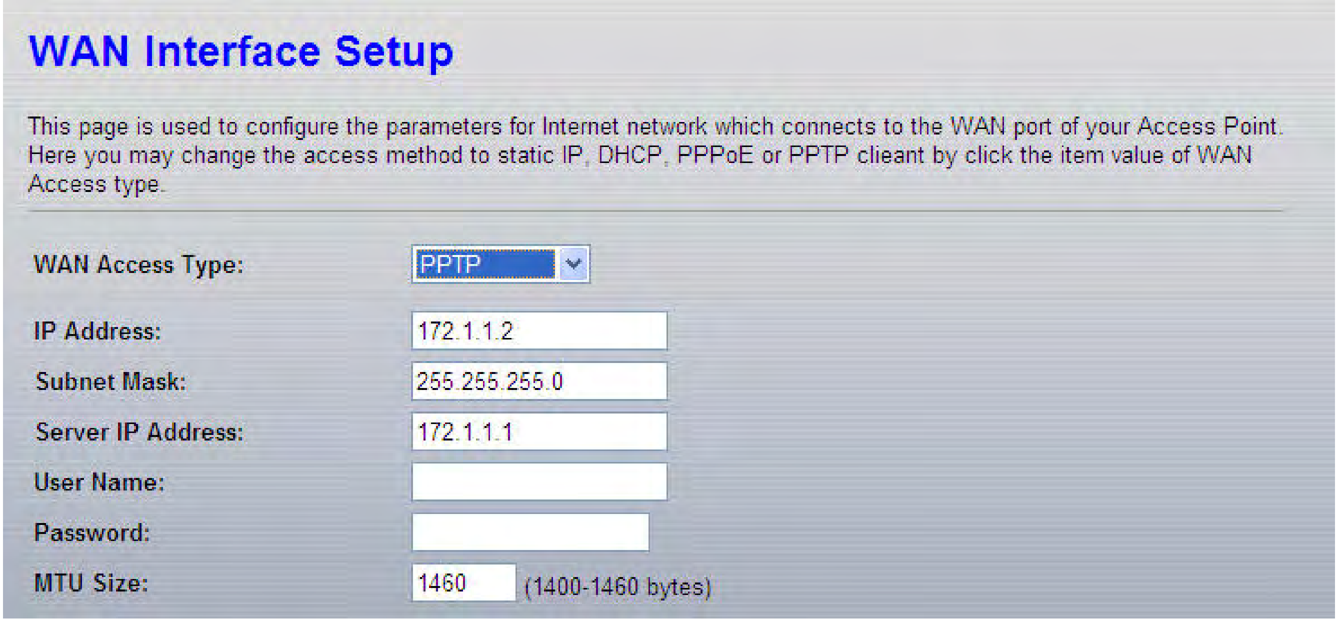
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP clieant by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1492 (1400-1492 bytes)

If you Choose "**PPTP**", the Static IP settings page will appear, shown in the figure.



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP clieant by click the item value of WAN Access type.

WAN Access Type: PPTP

IP Address: 172.1.1.2

Subnet Mask: 255.255.255.0

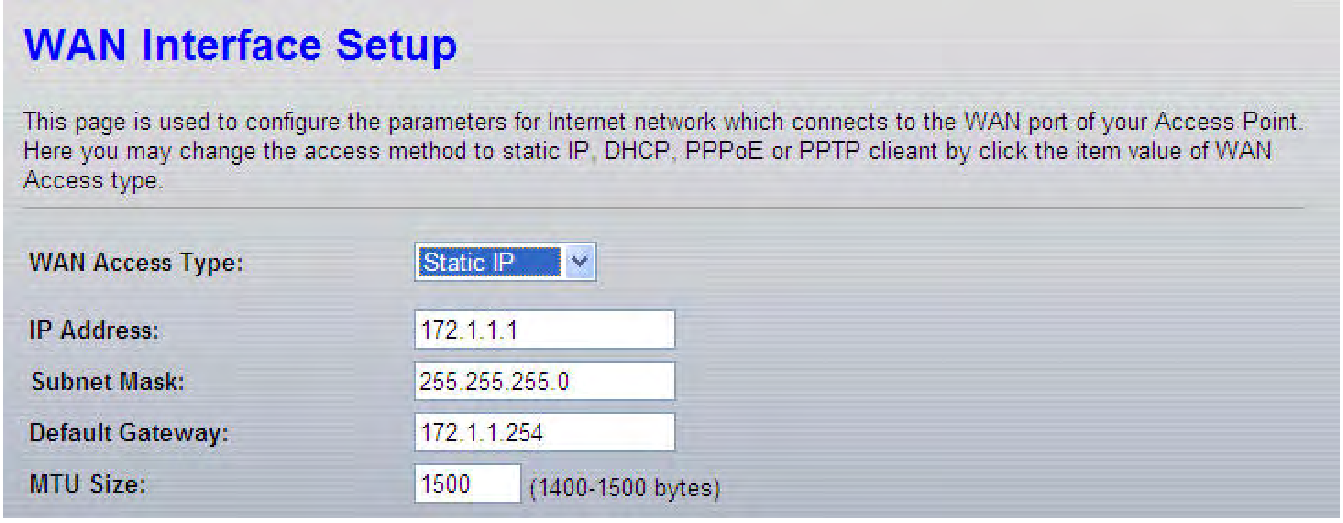
Server IP Address: 172.1.1.1

User Name:

Password:

MTU Size: 1460 (1400-1460 bytes)

You can get IP Address Subnet Mask, server IP Address, User Name and Password from your ISP
If you Choose "**Static IP**", the Static IP settings page will appear, showed in figure.



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP clieant by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254
MTU Size:	1500 (1400-1500 bytes)

Note: The IP parameters should have been provided by your ISP.

IP Address - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.

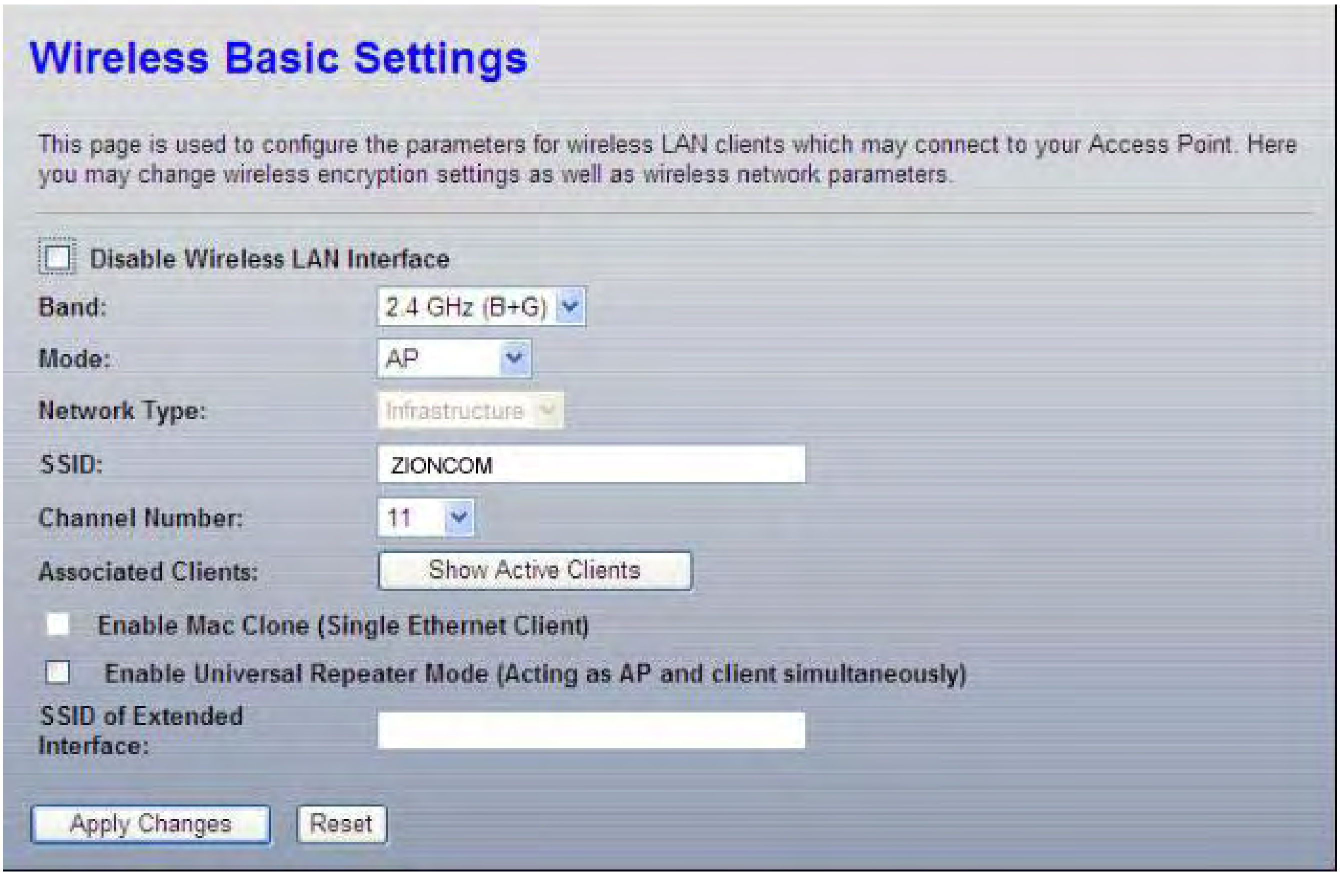
Subnet Mask - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0

Default Gateway - Enter the gateway into the box if required.

DNS - Enter the DNS Server IP address into the boxes if required.
Click next, wireless basic setting will appear.

【This page is used to configure these parameters】

Band - Indicates the current mode (2.4GHz(G)-54Mbps (802.11g), 2.4GHz(B)11Mbps (802.11b)). 2.4GHz(G+B), which allows both 802.11g and 802.11b wireless stations to connect to the router.
Mode- Default is AP, you can select Client, WDS, AP+WDS
Network Type- Default is Infrastructure, when mode is client, Network Type may be AD-HOC
SSID - Enter a value of up to 32 characters. The same name (SSID) must be signed to all wireless devices in your network. The default SSID is ZIONCOM, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive.
Channel – From 1 to 13.This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.



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: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: ZIONCOM

Channel Number: 11

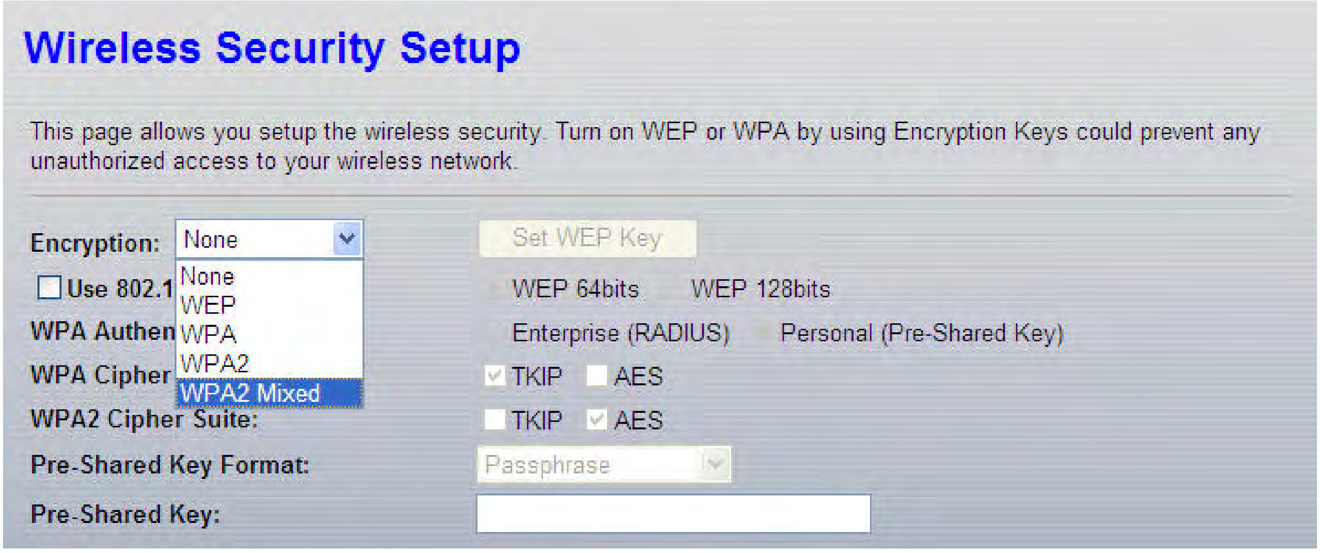
Associated Clients: Show Active Clients

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

Click next, Wireless Security Setup will appear. This page allow you setup the security. You can select None WEP WPA(TKIP),WPA2(AES),WPA2 Mixed.



Wireless Security Setup

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

Encryption: None

□ Use 802.1 — WEP 64bits WEP 128bits

WPA Authen — Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA Cipher — ☑ TKIP □ AES

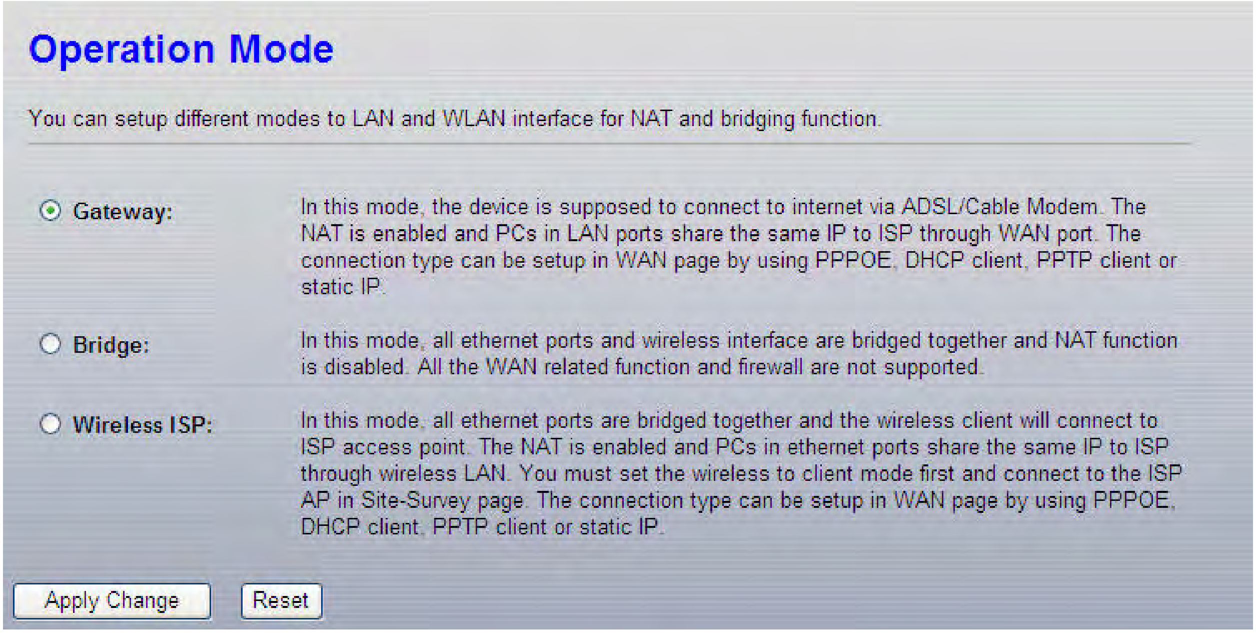
WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Click” finished”, you will find the page show set succeeded.
Notice: If you change the parameters of wireless, the router will reboot automatically.

3.3 Operation mode



Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

● Gateway: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

○ Bridge: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ Wireless ISP: In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

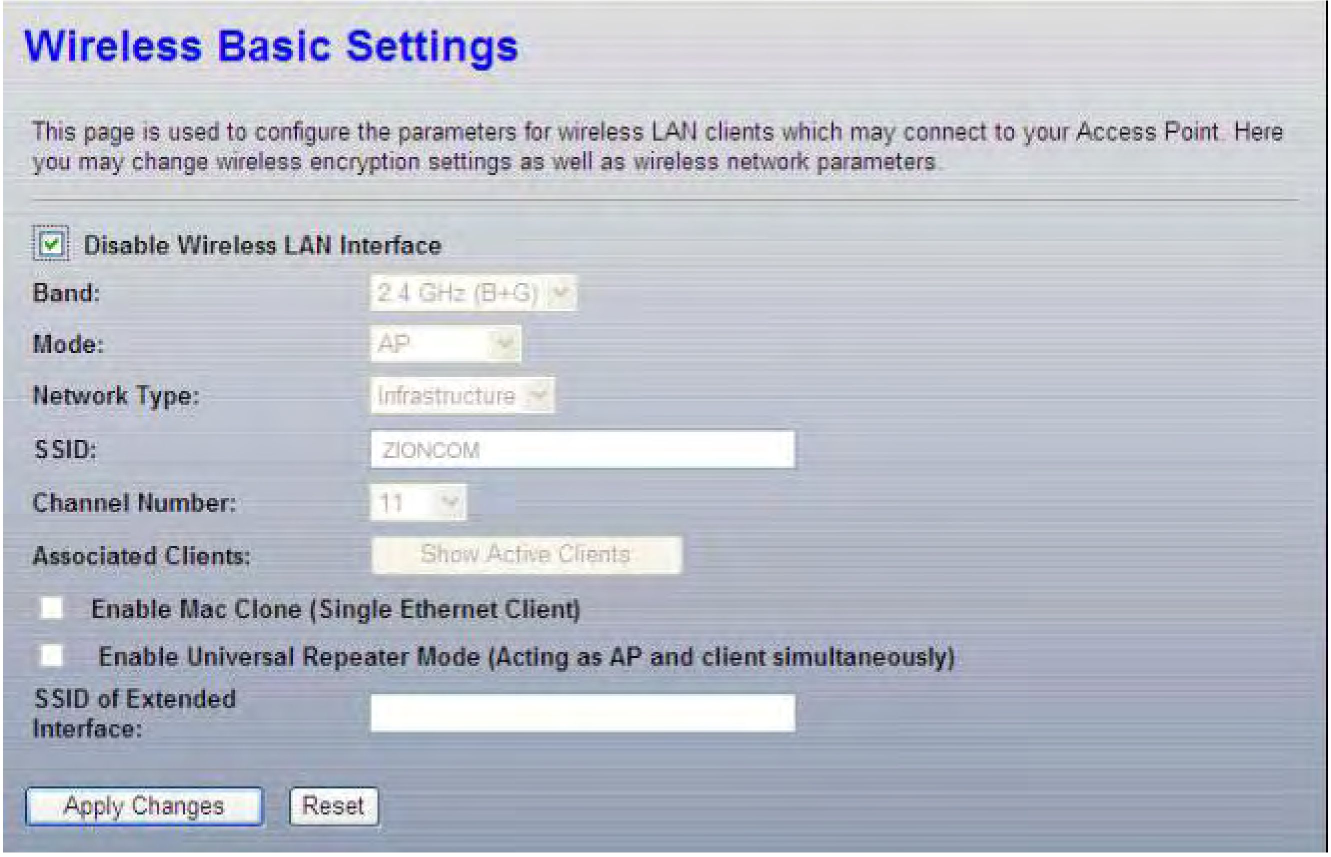
Gateway: (default) In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Bridge: In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP: In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Part 4: Configuration Guide

4.1 Wireless Setting

it contains Wireless Basic settings, Advance Settings, security, Access Control, WDS Settings, Site Survey.

4.2 Wireless Basic settings



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: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: ZIONCOM

Channel Number: 11

Associated Clients:

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

Band: Indicates the current mode (2.4GHz(G)-54Mbps (802.11g), 2.4GHz(B)11Mbps (802.11b)). 2.4GHz(G+B), which allows both 802.11g and 802.11b wireless stations to connect to the router.

Mode: Default is AP, you can select Client, WDS, AP+WDS

Network Type: Default is Infrastructure, when mode is client, Network Type should be setting AD-HOC

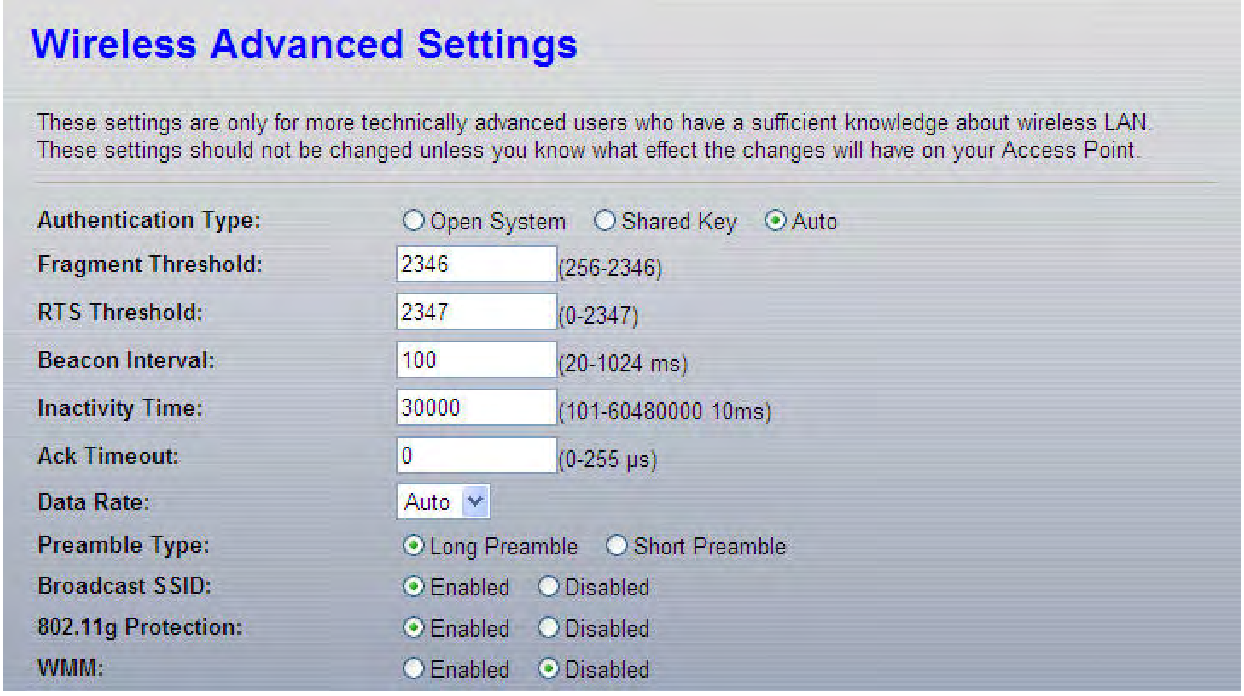
SSID: Enter a value of up to 32 characters. The same name (SSID) must be signed to all wireless devices in your network. The default SSID is ZIONCOM, but It is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive.

Channel: From 1 to 13.This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Associated Client: click show active client, you can check the list of wireless client.

Enable MAC Clone: it only adapts to wireless client.

4.2.1 Wireless Advanced Settings



Wireless Advanced Settings

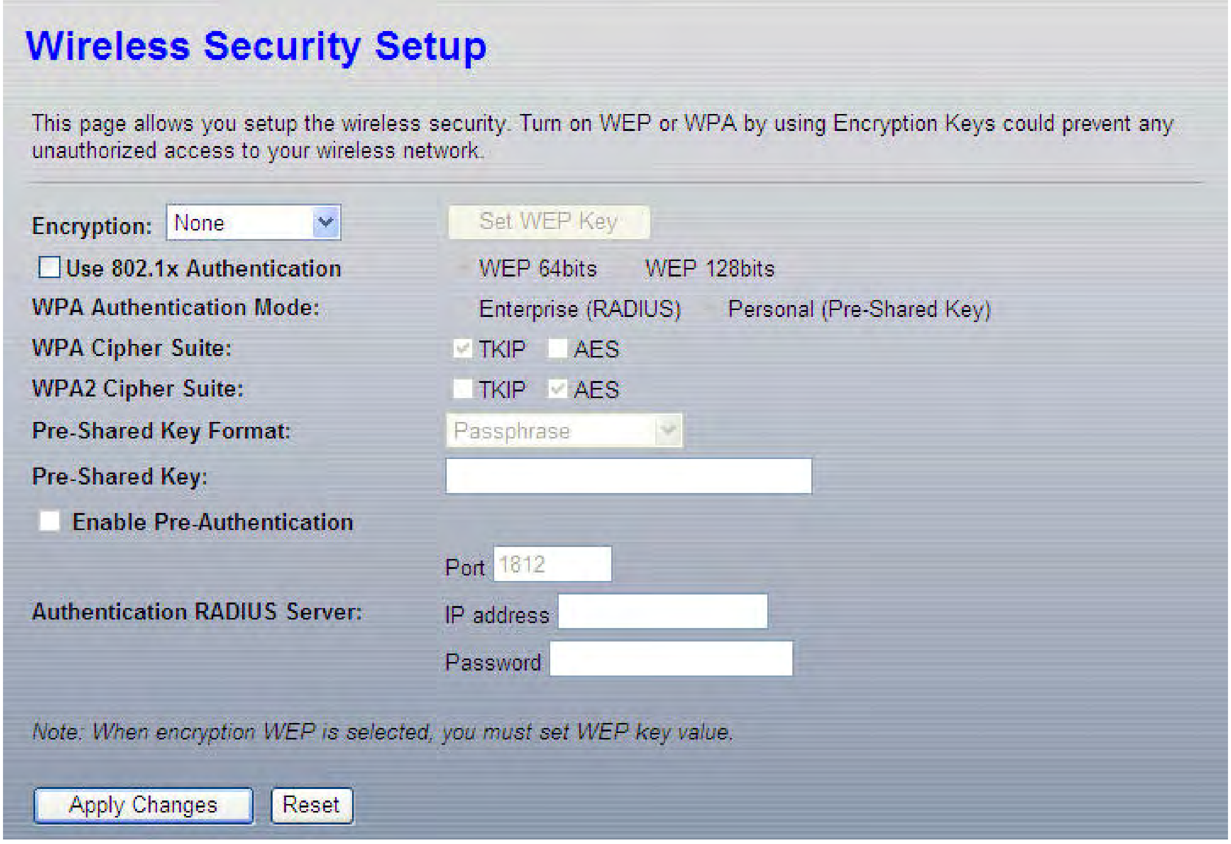
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Inactivity Time:	30000 (101-60480000 10ms)
Ack Timeout:	0 (0-255 µs)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
802.11g Protection:	● Enabled ○ Disabled
WMM:	○ Enabled ● Disabled

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

4.2.2 Wireless security setup

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



Wireless Security Setup

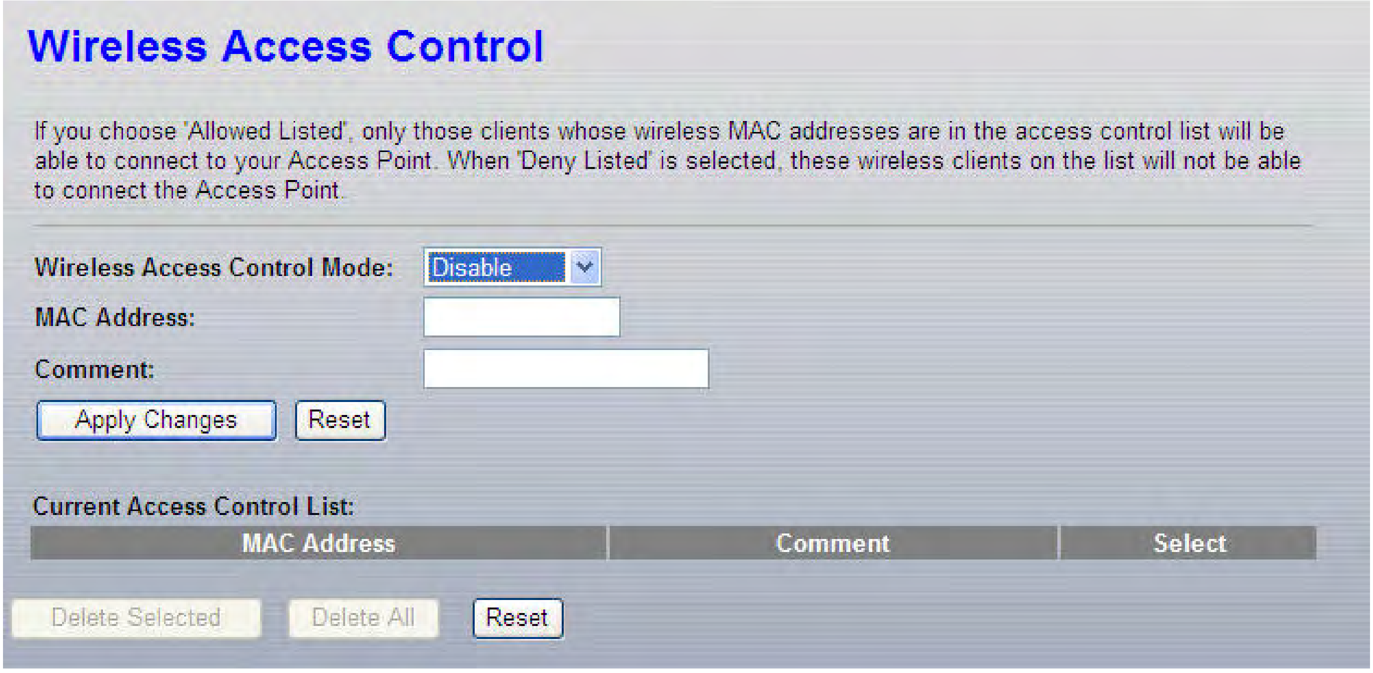
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: None	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:	Passphrase
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.

Encryption: you can select None,WEP,WPA,WPA2, WPA2 Mixed
WEP: Wired Equivalent Protocol.
WPA:(WI-FI Protected Access Wi-Fi) WPA is an intermediate solution for the security issues. It uses Temporal Key Integrity Protocol (TKIP) to replace WEP.
TKIP: TKIP is a compromise on strong security and possibility to use existing hardware. It still uses RC4 for the encryption like WEP, but with per-packet RC4 keys. In addition, it implements replay protection, keyed packet authentication mechanism (Michael MIC).
WPA Authentication Mode: Keys can be managed using two different mechanisms. WPA can either use an external authentication server (e.g., RADIUS) and EAP just like IEEE 802.1X is using or pre-shared keys without need for additional servers. Wi-Fi calls these "WPA-Enterprise" and "WPA-Personal", respectively. Both mechanisms will generate a master session key for the Authenticator (AP) and Supplicant (client station).
802.1X: The original security mechanism of IEEE 802.11 standard was not designed to be strong and has proven to be insufficient for most networks that require some kind of security. Task group I (Security) of IEEE 802.11 working group has worked to address the flaws of the base standard and in practice completed its work in May 2004. The IEEE 802.11i amendment to the IEEE 802.11 standard was approved in June 2004 and published in July 2004.
WPA Cipher suite/WPA2 Cipher suite: The encryption piece of WPA and WPA2 mandates the use of TKIP or, because it's considered to be more secure than TKIP, preferably AES encryption.
Pre-Shared Key Format: You can select PASSPHRASE or HEX(64 CHARACTERS).
Pre-Shared Key: You can input 128 characters key.
Authentication RADIUS Server: input Port and IP Address and Password.

4.2.3 Wireless Access Control



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 the Access Point.

Wireless Access Control Mode: Disable

MAC Address:

Comment:

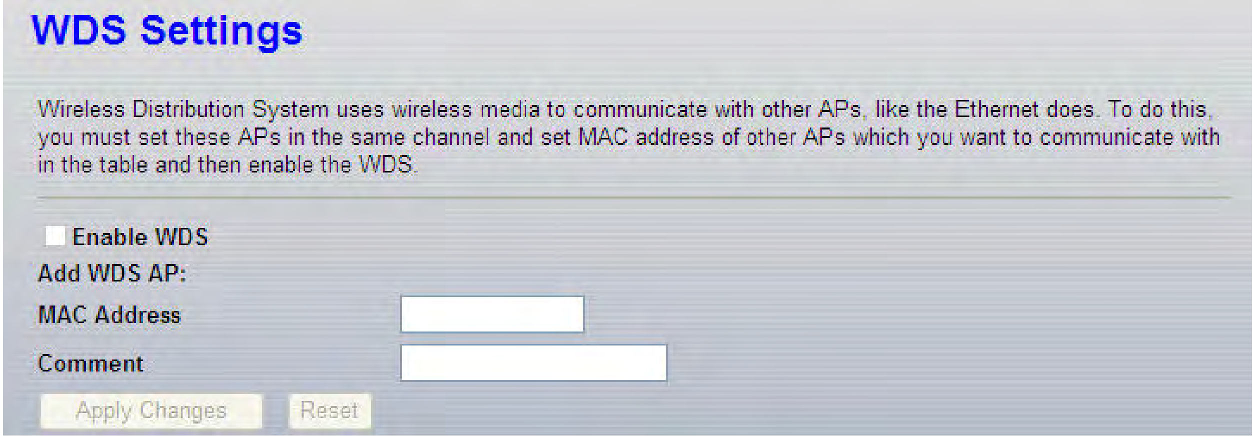
Current Access Control List:

MAC Address	Comment	Select

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 the Access Point.

4.2.4 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 other APs 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 other APs which you want to communicate with in the table and then enable the WDS.

☐ Enable WDS

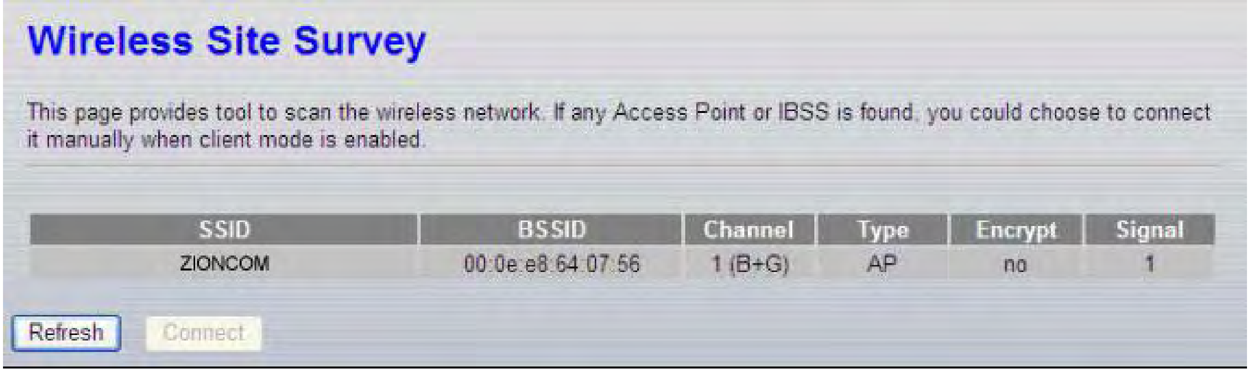
Add WDS AP:

MAC Address

Comment

4.2.5 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.

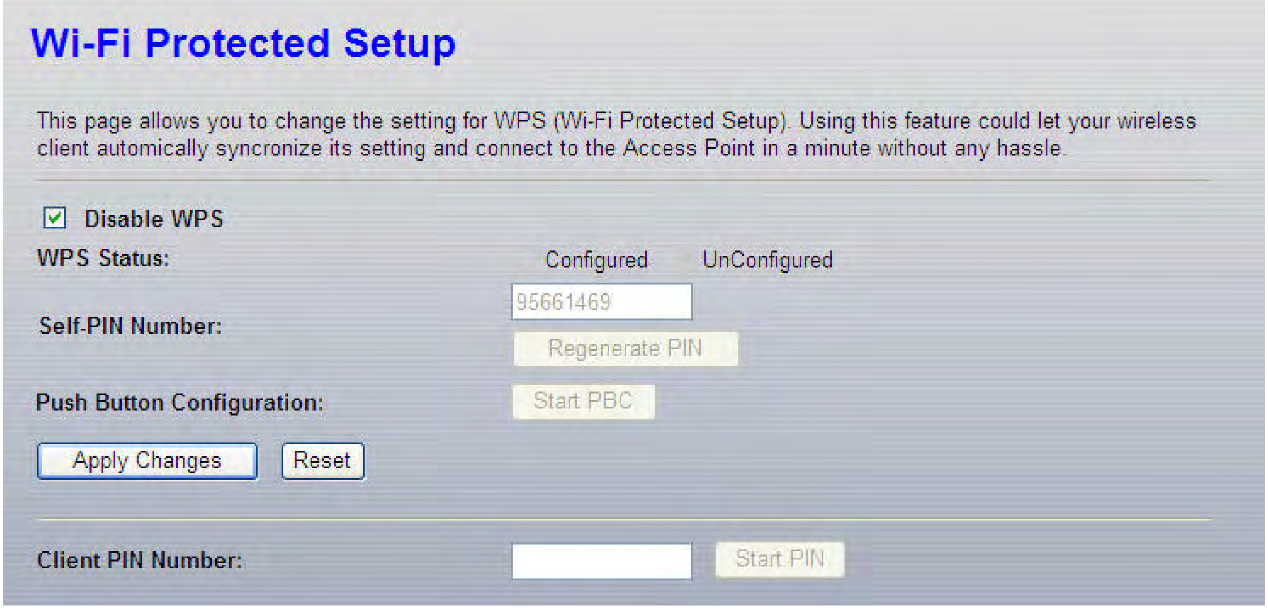


Wireless Site Survey

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
ZIONCOM	00:0e:e8:64:07:56	1 (B+G)	AP	no	1

4.2.6 WPS Setting



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☑ Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number: 95661469

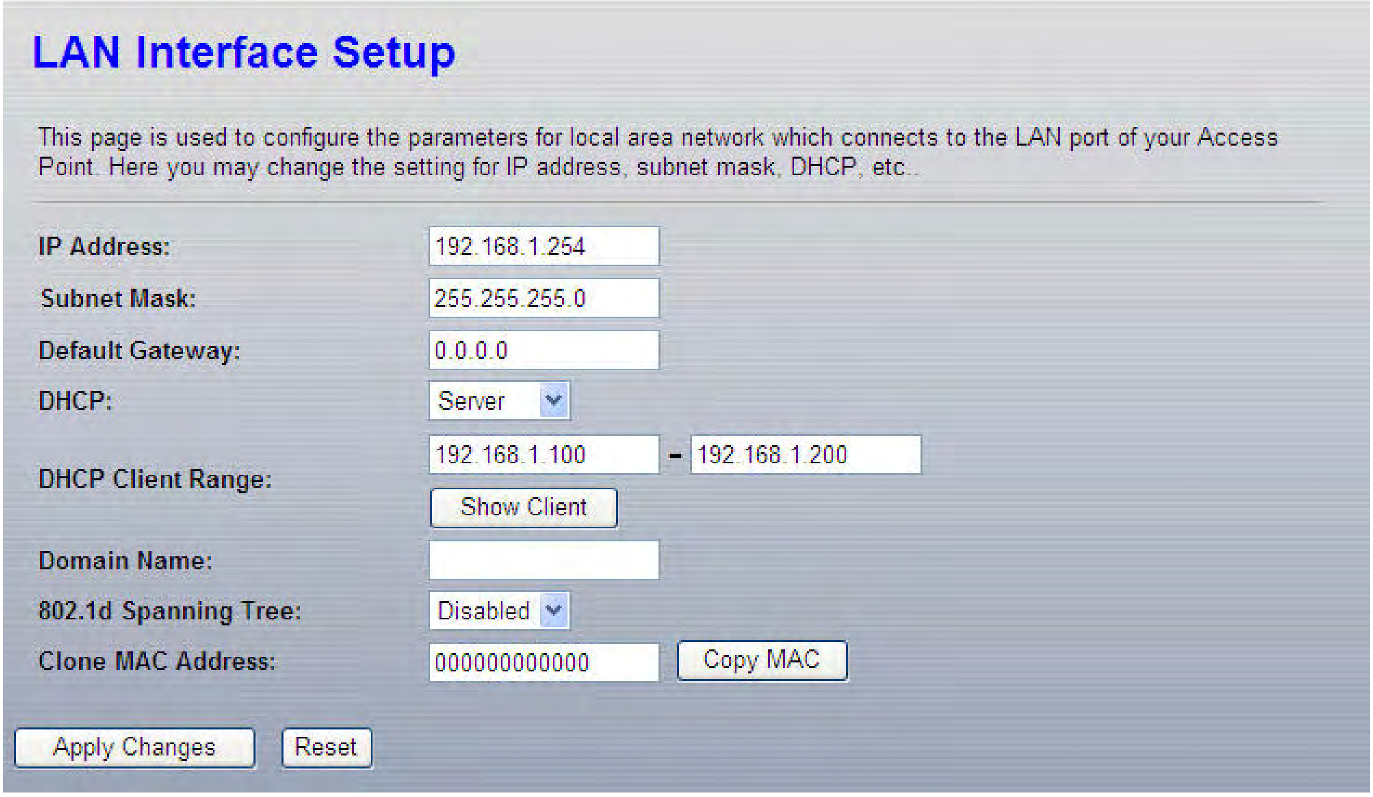
Push Button Configuration:

Client PIN Number:

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

4.3 TCP/IP Setting

4.3.1 LAN Setting LAN Interface setup



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 address, subnet mask, DHCP, etc..

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Server

DHCP Client Range: 192.168.1.100 - 192.168.1.200

Domain Name:

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

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 address, subnet mask, DHCP, etc..

MAC Address - the physical address of the router, as seen from the LAN. The value can't be changed.

IP Address - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.254).

Subnet Mask - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

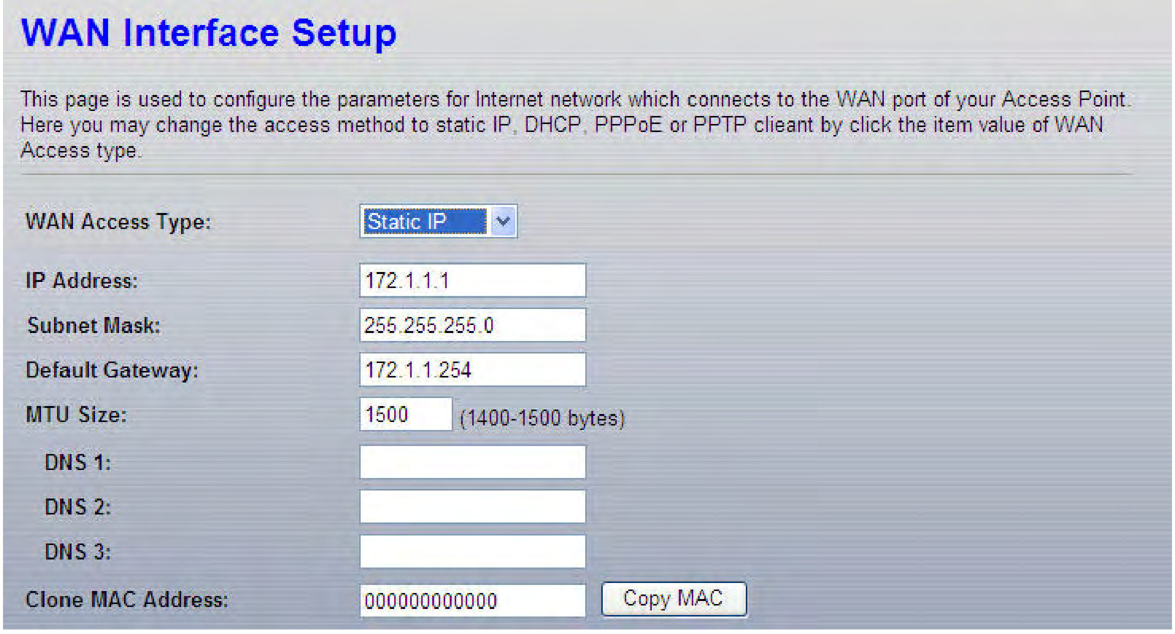
DHCP: You can select None, Client, Serve. The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN.

DHCP Client Range: This field specifies the first of the addresses in the IP address pool.

802.1d Spanning Tree: The IEEE 802.1D Spanning Tree Algorithm (STA) ,loop prevention and redundant link configuration. You can select disabled or enabled. if your mode was set WDS or AP+WDS, this item should be set “enable”

Clone MAC Address: you can enter a MAC, then click clone.

4.3.2WAN Interface



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP clieant by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

MTU Size: 1500 (1400-1500 bytes)

DNS 1:

DNS 2:

DNS 3:

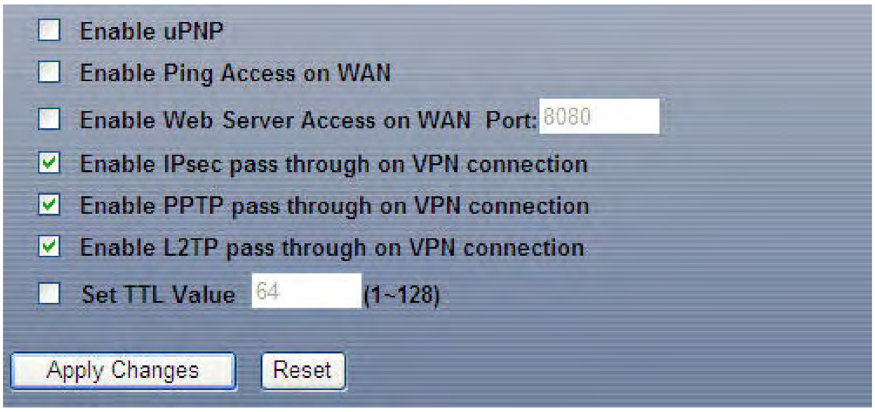
Clone MAC Address: 000000000000

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type, User name, password, Service:

you can refer to 3.2 Quick Installation Guide.

Connection Type: you can select continue , connect on demand, manual.
Idle time: when connection type is connect on demand, you can set idle time.
MTU Size: The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1492 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
DNS: You can select Attain DNS Automatically or Set DNS Manually
Clone MAC Address: if you want clone, input MAC Address



□ Enable uPNP

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN Port: 8080

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

□ Set TTL Value 64 (1~128)

Enable UpnP: The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

Enable L2TP pass through on VPN connection:

Enable IPsec pass through on VPN connection:

Enable PPTP pass through on VPN connection:

4.4 Firewall

4.4.1 Port Filtering

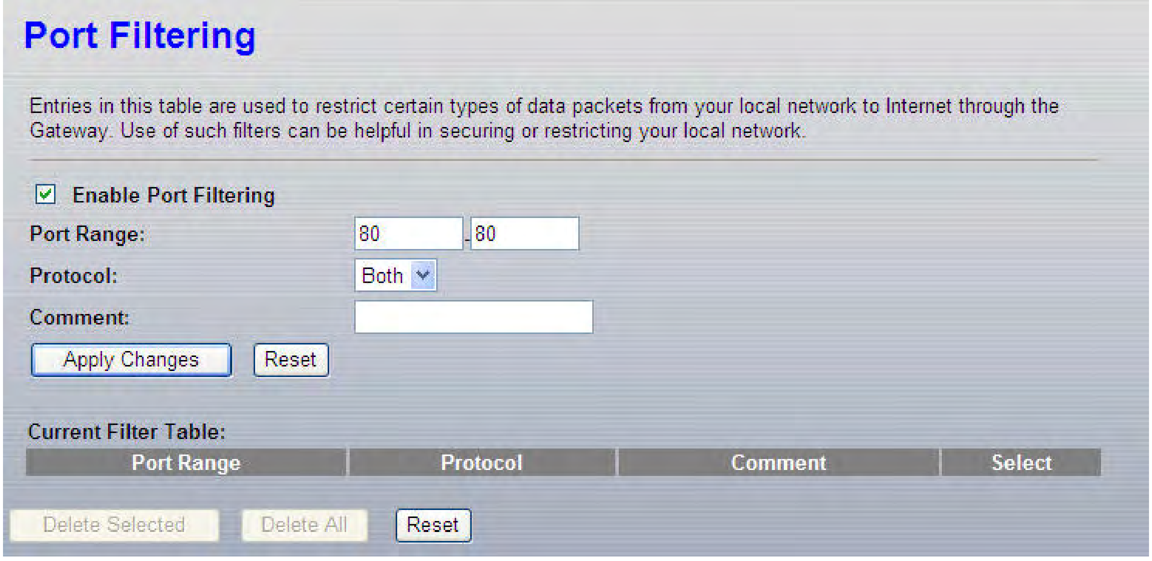
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port filtering: select it, you can modify port filter.

Port range: input the filter port, for example 20-220

Protocol: you can select both, TCP and UDP

Current filter table: The list of port filter.



Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable Port Filtering

Port Range: 80 - 80

Protocol: Both

Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select

4.4.2 IP Filtering

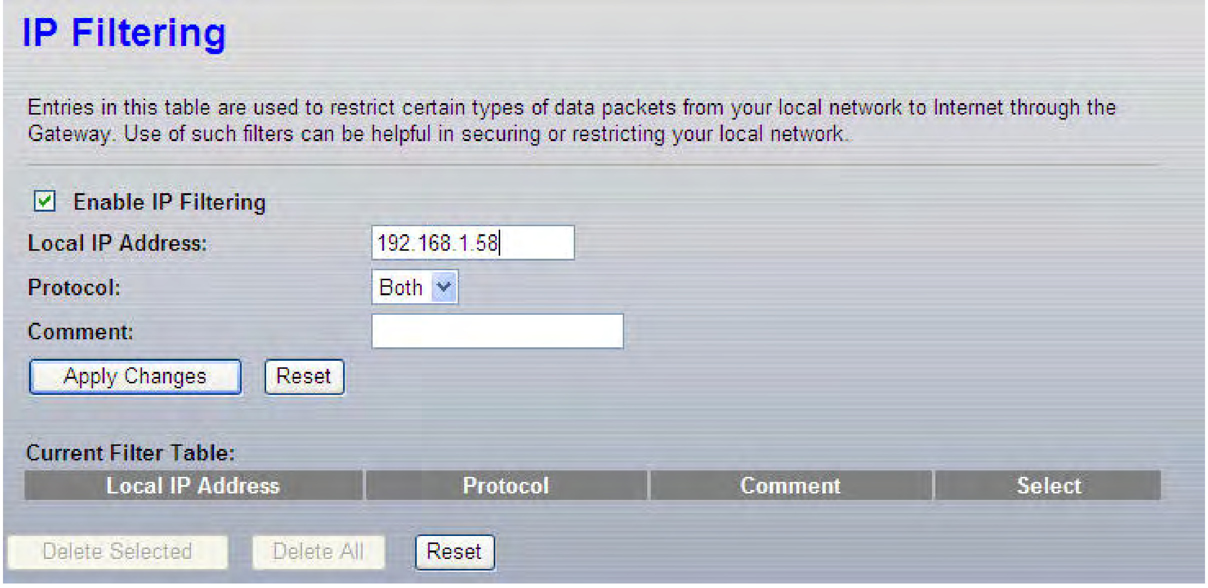
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering: select it, you can modify IP filter.

Local IP Address: Input the IP Address, for example:192.168.1.23.

Protocol: you can select both TCP,UDP

Current Filter table: The list of IP filter.



IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable IP Filtering

Local IP Address: 192.168.1.58

Protocol: Both

Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select

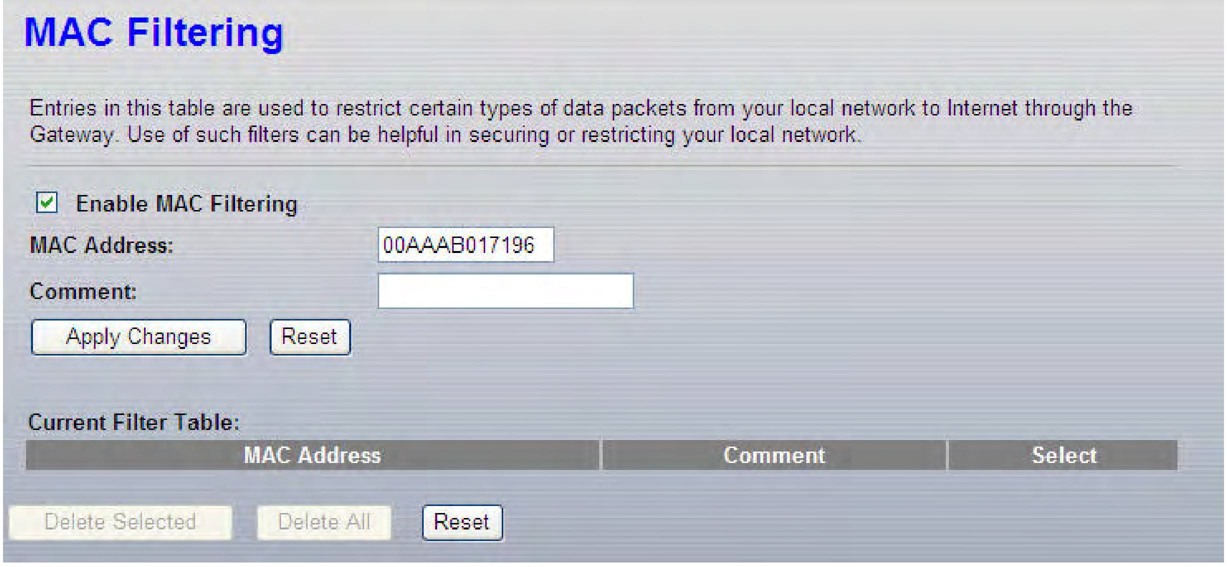
4.4.3 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network

Enable MAC Filtering: select it, you can modify MAC filter.

MAC Address: Type the MAC Address, for example:00:e0:4e:3f:2d:c5.

Current Filter table: The list of MAC filter.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable MAC Filtering

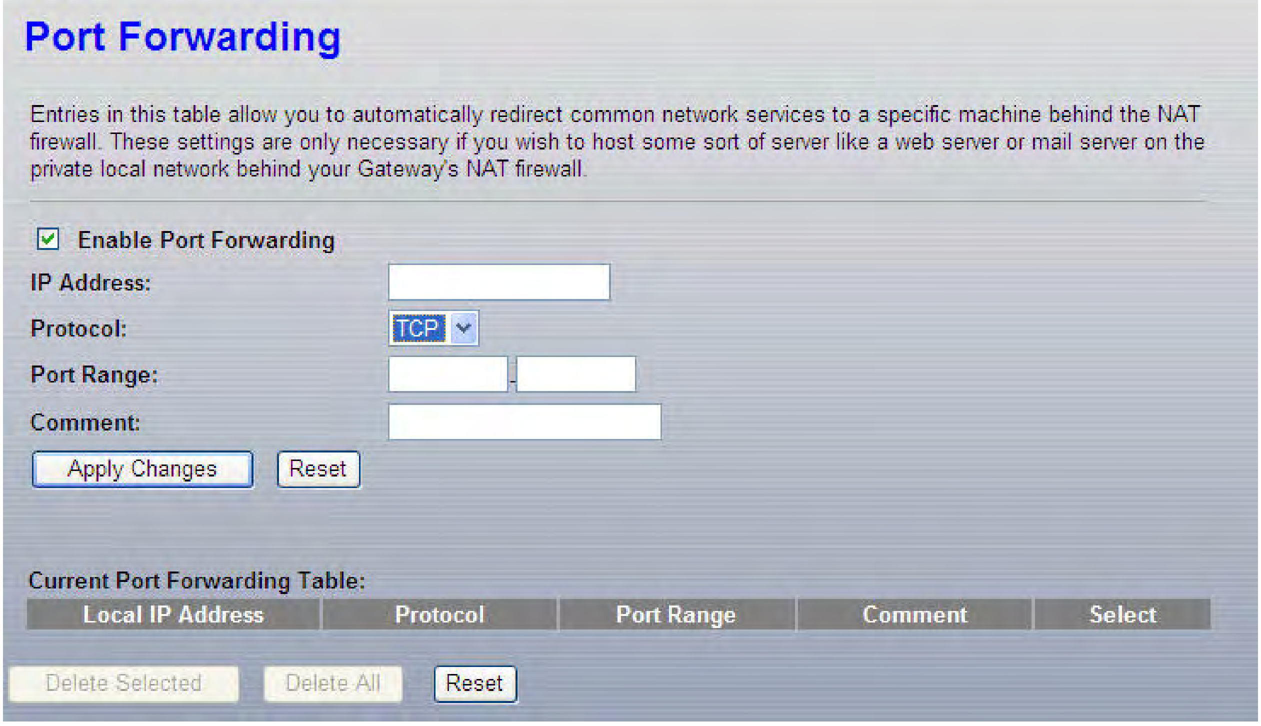
MAC Address: 00AAAB017196

Comment:

Current Filter Table:

MAC Address	Comment	Select

4.4.4 Port Forwarding



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☑ Enable Port Forwarding

IP Address:

Protocol: TCP

Port Range: -

Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable MAC Address: select it, you can modify MAC Address Filtering..

IP Address: The IP Address of the PC running the service application

Protocol - The protocol used for this application, either **TCP**, **UDP**, or **both** (all protocols supported by the router).

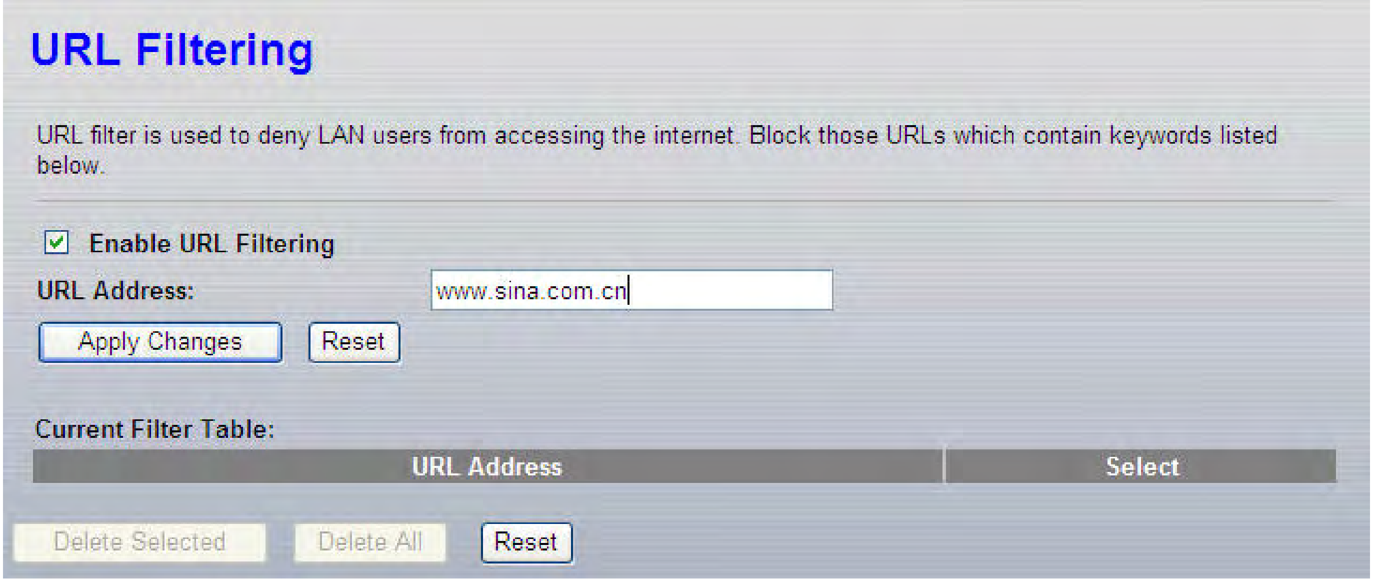
Port Range- The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is Start port, YYY is End port).

Current Port Forward Table: port forward services already list.

4.4.5 URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Enable URL : select it, you can edit URL, For example: www.xxx.com. Click apply changes.



URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

☑ Enable URL Filtering

URL Address: www.sina.com.cn

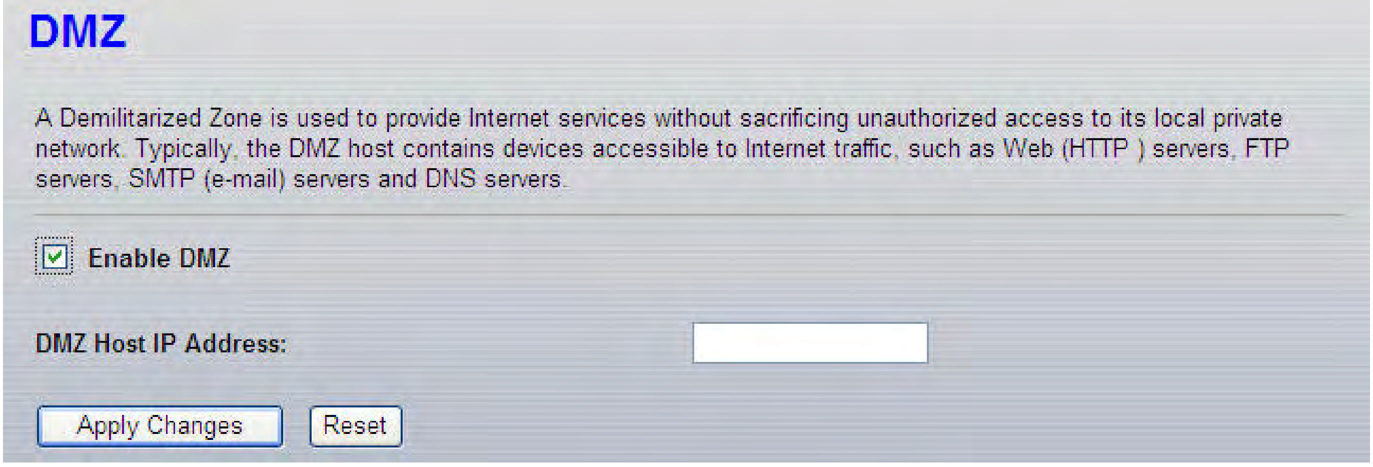
4.4.6 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet game or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function.

DMZ Enable: Select it, DMZ can be editted.

DMZ Host IP Address: input IP Address, for example 192.168.1.34.

Click **apply changes**, complete set DMZ.



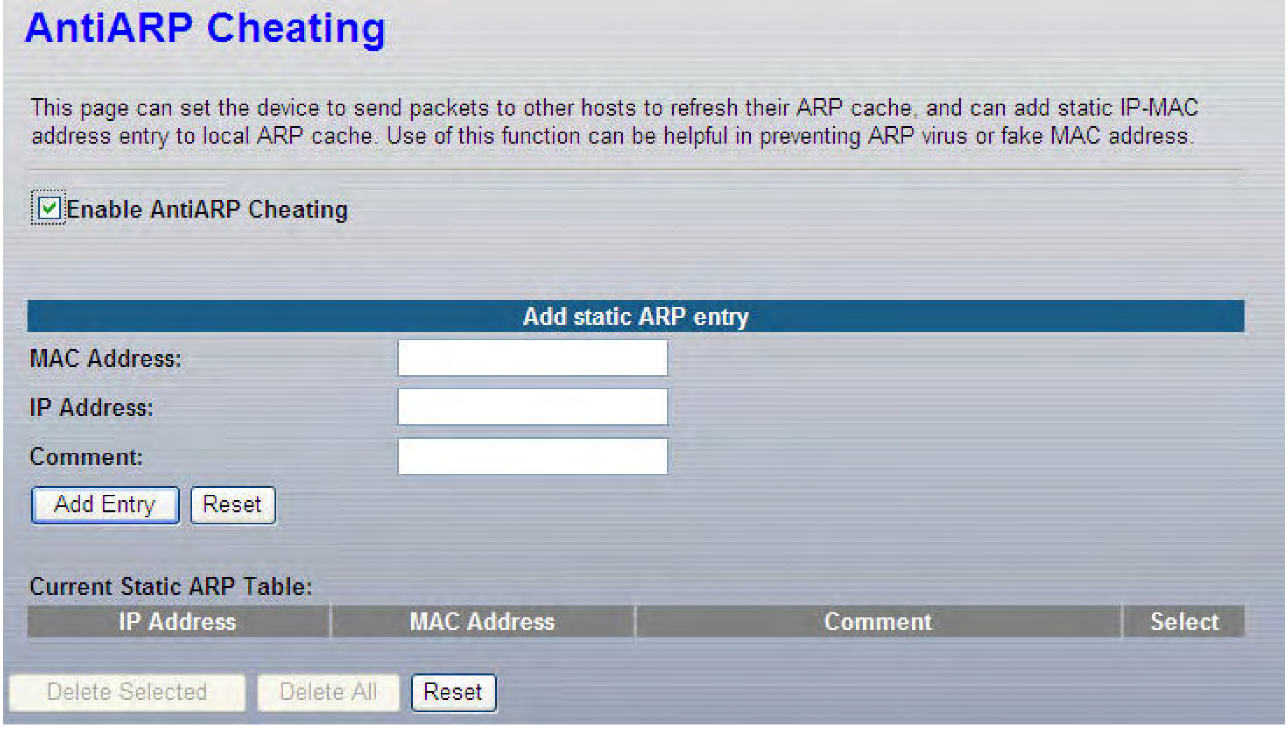
DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

☑ Enable DMZ

DMZ Host IP Address:

4.4.7 AntiARP Cheating



AntiARP Cheating

This page can set the device to send packets to other hosts to refresh their ARP cache, and can add static IP-MAC address entry to local ARP cache. Use of this function can be helpful in preventing ARP virus or fake MAC address.

☑ Enable AntiARP Cheating

Add static ARP entry	
MAC Address:	
IP Address:	
Comment:	

Current Static ARP Table:

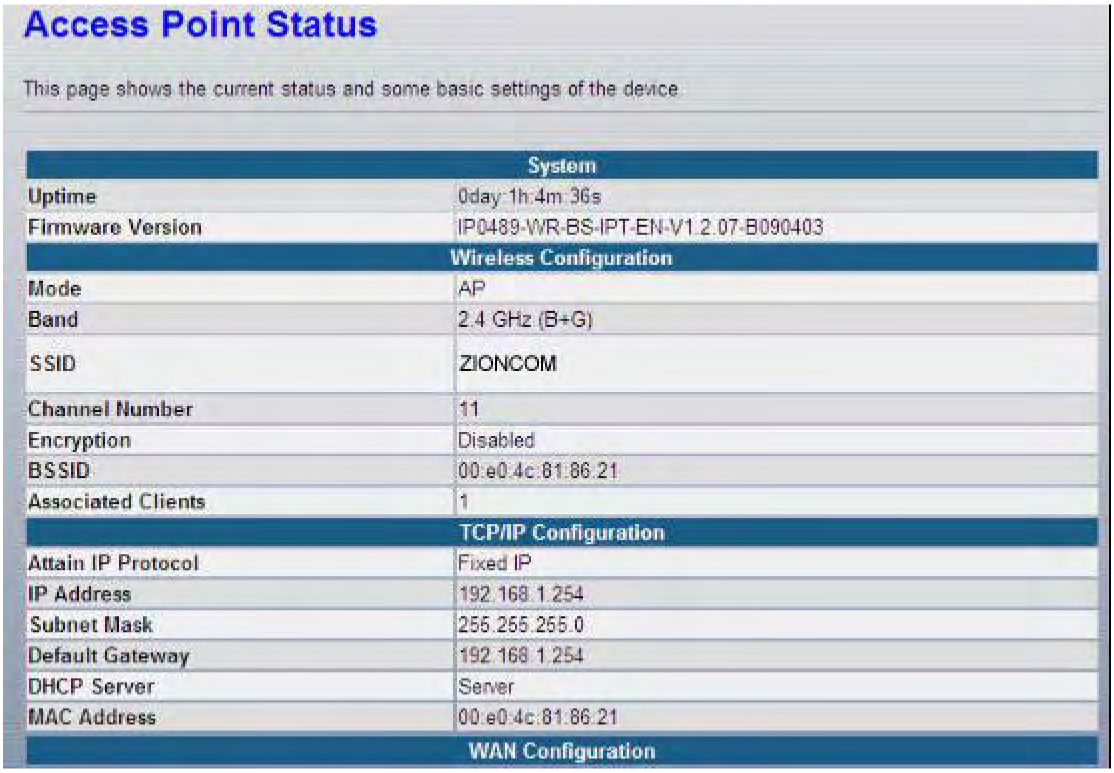
IP Address	MAC Address	Comment	Select

This page can set the device to send packets to other hosts to refresh their ARP cache, and can add static IP-MAC address entry to local ARP cache. Use of this function can be helpful in preventing ARP virus or fake MAC address

4.5 Management

4.5.1 Status

This page shows the current status and some basic settings of the device. You can check system Information, LAN Interface Information, WAN Interface Information.



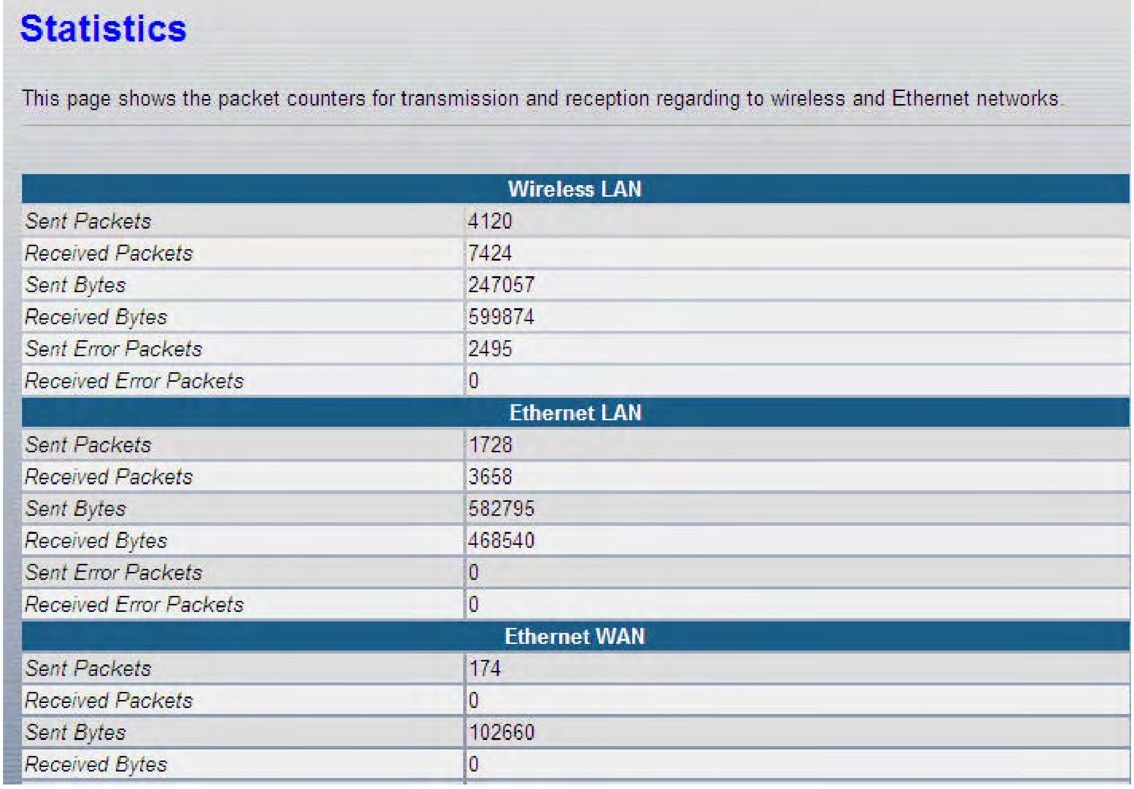
Access Point Status

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

System	
Uptime	0day:1h:4m:36s
Firmware Version	IP0489-WR-BS-IPT-EN-V1.2.07-B090403
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	ZIONCOM
Channel Number	11
Encryption	Disabled
BSSID	00:e0:4c:81:86:21
Associated Clients	1
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Server
MAC Address	00:e0:4c:81:86:21
WAN Configuration	

4.5.2 Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

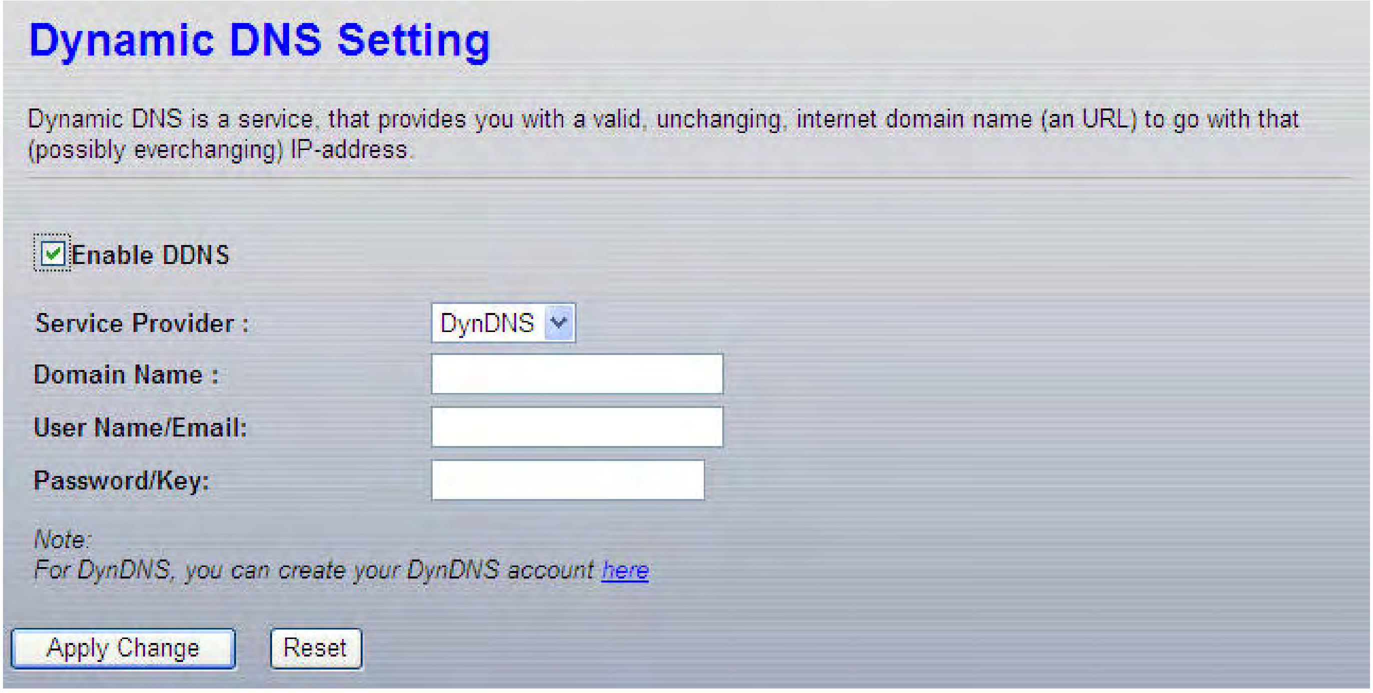


Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	
Sent Packets	4120
Received Packets	7424
Sent Bytes	247057
Received Bytes	599874
Sent Error Packets	2495
Received Error Packets	0
Ethernet LAN	
Sent Packets	1728
Received Packets	3658
Sent Bytes	582795
Received Bytes	468540
Sent Error Packets	0
Received Error Packets	0
Ethernet WAN	
Sent Packets	174
Received Packets	0
Sent Bytes	102660
Received Bytes	0

4.5.3 DDNS



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☑ Enable DDNS

Service Provider :	DynDNS
Domain Name :	
User Name/Email:	
Password/Key:	

Note:
For DynDNS, you can create your DynDNS account here

Dynamic DNS is a service that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly ever changing) IP-address. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for

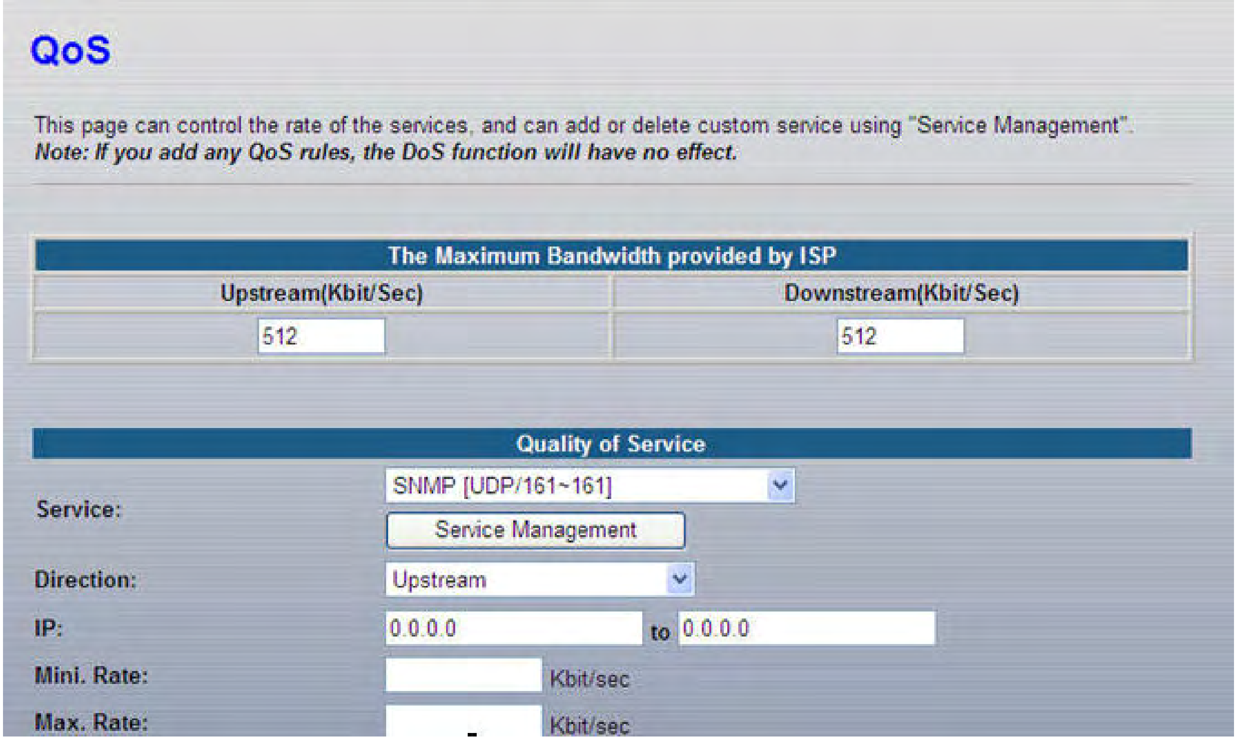
DDNS service providers such as www.zioncom.net . The Dynamic DNS client service provider will give you a password or key.
To set up for DDNS, follow these instructions:

1. Type your **service provider.**
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. **Domain Name -** the domain names are displayed here. Click **Apply Changes** to logout the DDNS service.

4.5.4 QOS

This page can control the rate of the services and can add or delete custom service using "Service Management "

Note : if you and QOS rules, the DOS function will have no effect



QoS

This page can control the rate of the services, and can add or delete custom service using "Service Management".
Note: If you add any QoS rules, the DoS function will have no effect.

The Maximum Bandwidth provided by ISP	
Upstream(Kbit/Sec)	Downstream(Kbit/Sec)
512	512

Quality of Service

Service: SNMP [UDP/161~161]

Direction: Upstream

IP: 0.0.0.0 to 0.0.0.0

Mini. Rate: Kbit/sec

Max. Rate: Kbit/sec

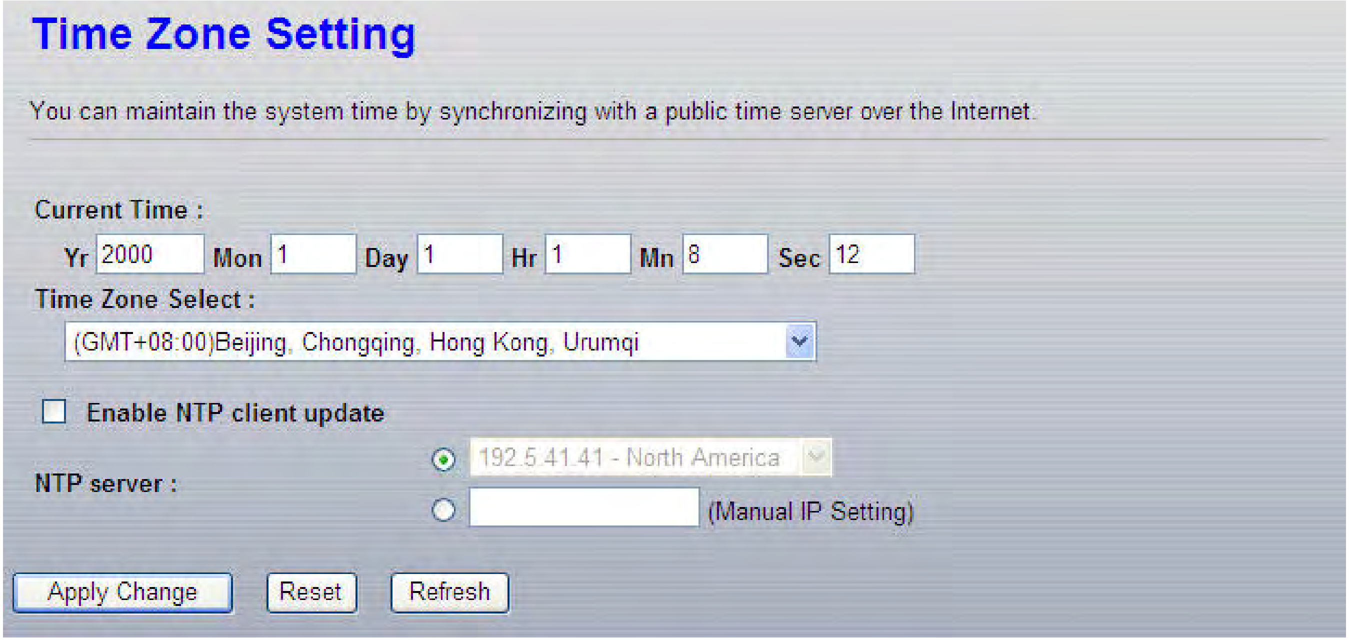
- Upstream：Please enter the router through the WAN port want to upload speed provided.
- Downstream：Please enter the router through the WAN port wish to provide download speeds.
- Service：Please enter the transport layer protocol type.
- IP：Please enter the internal host address range, when all is empty or "0", said the domain is invalid.
- Uplink, download. Please bandwidth control parameters as described in the list of rules to set up.

4.5.5 Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current time: type the date and time.

Time Zone Select: Select your local time zone from this pull down list.
Enable NTP client update: select it, you can get the time from **NTP.**
NTP server : select a server from list.
Click the Apply changes.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time :

Yr 2000 Mon 1 Day 1 Hr 1 Mn 8 Sec 12

Time Zone Select :

(GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi

☐ Enable NTP client update

NTP server : ● 192.5.41.41 - North America

○ (Manual IP Setting)

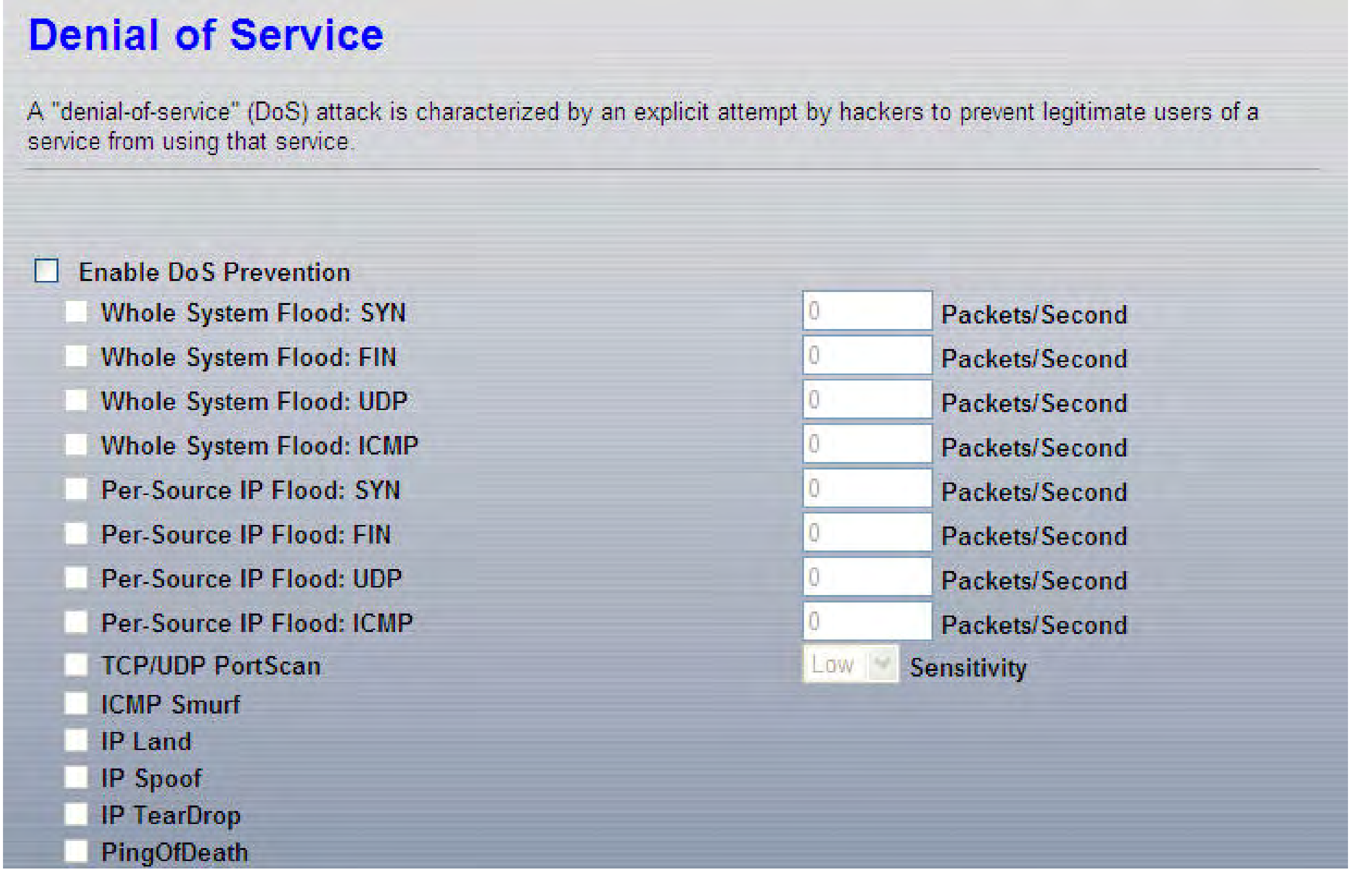
4.5. 6 Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Enable DOS Prevention: select it, you can modify DOS Prevention.

Enable Source IP Blocking: you can input source IP Blocking time

Click apply changes, DOS take effect.



Denial of Service

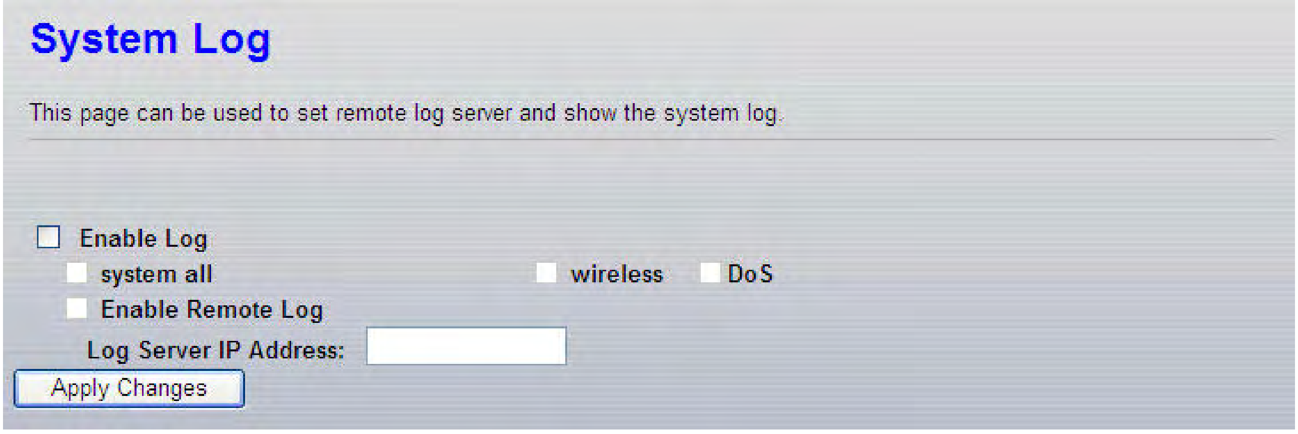
A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☐ Enable DoS Prevention

☐ Whole System Flood: SYN	0	Packets/Second
☐ Whole System Flood: FIN	0	Packets/Second
☐ Whole System Flood: UDP	0	Packets/Second
☐ Whole System Flood: ICMP	0	Packets/Second
☐ Per-Source IP Flood: SYN	0	Packets/Second
☐ Per-Source IP Flood: FIN	0	Packets/Second
☐ Per-Source IP Flood: UDP	0	Packets/Second
☐ Per-Source IP Flood: ICMP	0	Packets/Second
☐ TCP/UDP PortScan	Low	Sensitivity
☐ ICMP Smurf		
☐ IP Land		
☐ IP Spoof		
☐ IP TearDrop		
☐ PingOfDeath		

4.5.7 Log

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

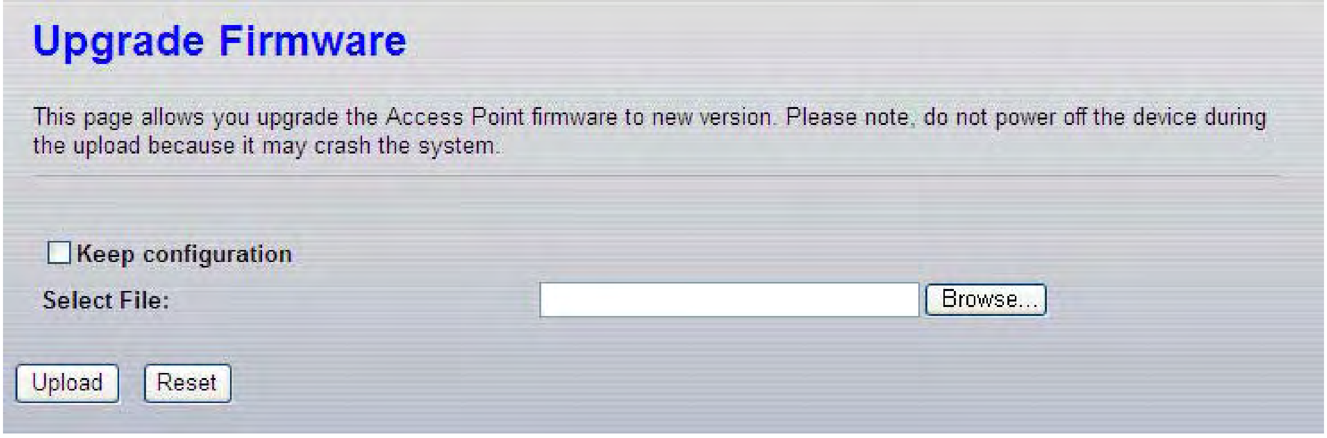


System Log

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

4.5.8 Upgrade Firmware

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

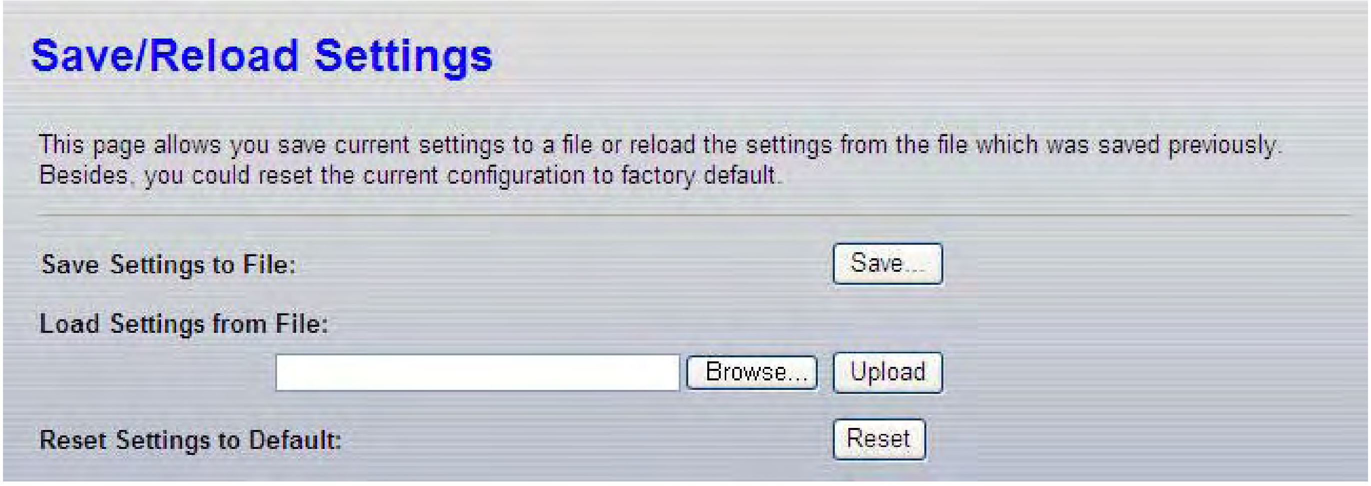


Upgrade Firmware

This page allows you 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.

4.5.9 Save/Reload settings

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

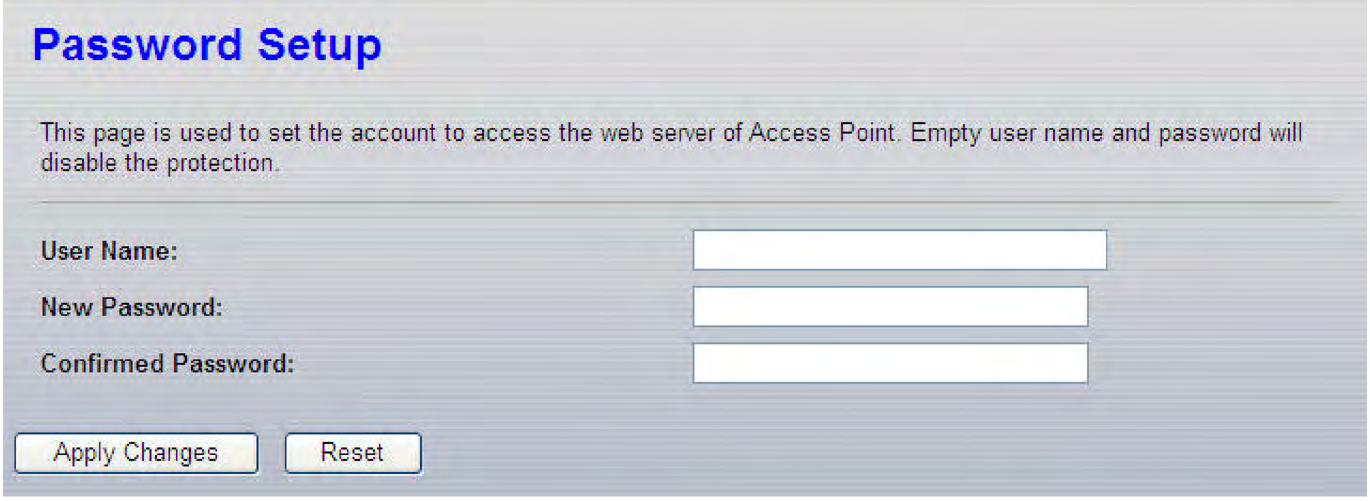


Save/Reload Settings

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

4.6.0 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 function



Password Setup

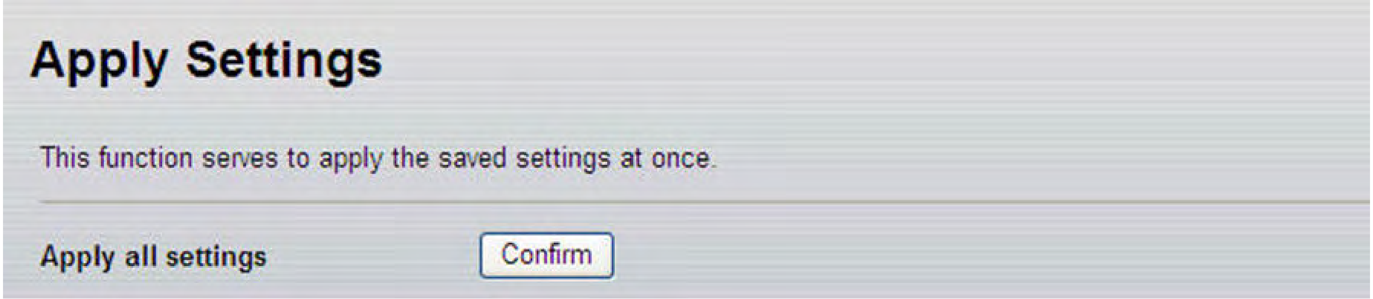
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

4.6.1 Apply Settings



Apply Settings

This function serves to apply the saved settings at once.

Apply all settings

This function serves to apply the saved setting at once.

FCC 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 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.

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

FCC Radiation Exposure Statement

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

This equipment 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.

Caution!

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment.