EnGenius

ECB-1220R

Wireless Client Bridge /AP/Router/Client Router

User's Manual

Version: 1.1

Table of Contents

1 INTRODUCTION 5

FEATURES & BENEFITS 5
PACKAGE CONTENTS 7
UNIT DESCRIPTION 7
SYSTEM REQUIREMENTS 8
APPLICATIONS 8
NETWORK CONFIGURATION 9
a) Ad-hoc (peer-to-peer) Mode 9
b) Infrastructure Mode 10

2 UNDERSTANDING THE HARDWARE 11

HARDWARE INSTALLATION 11
IP ADDRESS CONFIGURATION 11

3 CLIENT BRIDGE/ROUTER & ROUTER/ AP 13

BRIDGE/BRIDGE ROUTER TO ACCESS POINT 13
ACCESS POINT TO BRIDGE/BRIDGE ROUTER 13

4 ACCESS POINT/ROUTER MODE – CONFIG 14

LOGGING IN 14
MANAGEMENT 16
MANAGEMENT (ROUTER *MODE*) 17
OPERATION MODE 17
STATUS 19
STATISTICS 20
DYNAMIC DNS (ROUTER *MODE)* 21
TIME ZONE SETTING (ROUTER *MODE*) 22
DENIAL OF SERVICE (DOS) (ROUTER *MODE*) 23
LOG 23
UPGRADE FIRMWARE 24
SAVE / RELOAD SETTINGS, RESET TO DEFAULT 25
PASSWORD 26
TCP/IP SETTINGS 26
LAN INTERFACE 27
4.3.2 SNMP SETTINGS 27
WLAN INTERFACE (ROUTER *MODE*) 28
PPPOE 30
PPTP (POINT-TO-POINT TUNNELING PROTOCOL) (ROUTER *MODE*) 31
WIRELESS 33
BASIC SETTINGS (INFRASTRUCTURE, ADHOC) 34
ADVANCED SETTINGS 35
SECURITY 36
ENCRYPTION DISABLED 37
WEP 64-BIT / 128-BIT 38
WPA / WPA2 PASSPHRASE 39
WPA / WPA2 RADIUS AUTHENTICATION 40
WIRELESS DISTRIBUTION SYSTEM 40
FIREWALL 41
MAC ADDRESS FILTER 43
PORT FORWARDING 43
WEB SITE FILTER 44
DMZ 45

4 CLIENT BRIDGE/ROUTER MODE – CONFIG 46

LOGGING IN 46
MANAGEMENT 48
OPERATION MODE 49
STATUS 50
STATISTICS 51
LOG 51
UPGRADE FIRMWARE 52
SAVE / RELOAD SETTINGS, RESET TO DEFAULT 52
PASSWORD 53
TCP/IP SETTINGS 54
LAN INTERFACE 54
STATIC IP ADDRESS 55
DHCP CLIENT 55
DHCP SERVER 56
SNMP SETTINGS 57
CLIENT BRIDGE ROUTER 58
WLAN INTERFACE 58
PPPOE 59
WIRELESS 61
BASIC SETTINGS 61
ADVANCED SETTINGS 62
SECURITY 64
ENCRYPTION DISABLED 64
WEP 64-BIT / 128-BIT 65
WPA / WPA2 / WPA2 MIXED PASSPHRASE 66
WIRELESS SITE SURVEY 67

APPENDIX A – FCC INTERFERENCE STATEMENT 68

APPENDIX B – IC STATEMENT 69

Revision History

Version	Date	Notes
1.0	March 21, 2008	Created
1.1	March 22, 2008	Chapters added

1 Introduction

The Wireless Client Bridge/AP/Router/Bridge Router device operates seamlessly in the 2.4 GHz frequency spectrum supporting the 802.11b (2.4GHz, 11Mbps) and faster 802.11g (2.4GHz, 54Mbps) wireless standards. It's the best way to add wireless capability to your existing wired network, or to add bandwidth to your wireless installation.

ECB-1220R has high transmitted output power and high receivable sensitivity. High output power and high sensitivity can extend range and coverage to reduce the roaming between APs to get more stability wireless connection. It also can reduce the expense of equipment in the same environment.

To protect your wireless connectivity, it can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA/WPA2. The MAC address filter lets you select exactly which stations should have access to your network. User isolation function can protect the private network between client users.

This chapter describes the features & benefits, package contents, applications, and network configuration.

Features & Benefits

Features	Benefits
Client Bridge/AP/Router/Client Router	
High Speed Data Rate Up to 54Mbps	**Capable of handling heavy data payloads such as MPEG video streaming**
High Output Power Solution	**Excellent output power spreads the operation distance**
IEEE 802.11b/g Compliant	**Fully Interoperable with IEEE 802.11b/IEEE802.11g compliant devices**

SNMP Remote Configuration Management	**Help administrators to remotely configure or manage the Access Point easily.**
Point-to-point, Point-to-multipoint Wireless Connectivity	**Let users transfer data between two buildings or multiple buildings**
DoS (Denial of Service) protection	**Prevent from well-known DoS attack**
Built-in 4-port Switch automatically detects cable type	**Easy local connectivity**
Web-based configuration	**Simple and intuitive network management**
Firmware change via the Web-based configuration screen	**Allow easy upgrade/restore/dump system configuration via web interface**
System log	**Logging critical event according to network manager's criteria**
WPA2/WPA/ IEEE 802.1x support	**Powerful data security**
DHCP Client/ Server	**Simplifies network administration**
Universal Repeater	**The easiest way to expand your wireless network's coverage**
Keep personal setting	**Keep the latest setting when firmware upgrade**
Router/AP Mode	
NAT Router	**Multiple computer Internet Access, also act as natural firewall**
UPnP(Universal Plug and Play)	**Friendly to special application e.g. instant messenger, VoIP**
Port forwarding	**Set up application server (FTP, Web, Email, …) on LAN**
Access control	**WLAN-to-WAN access control (allow/disallow), prevent users from access unwanted content**
Firewall	**Prevent malicious access from Internet**
Hide SSID	**Avoids unallowable users sharing bandwidth, increases efficiency of the network**
WDS (Wireless Distributed System)	**Make wireless AP and Bridge mode simultaneously as a wireless repeater**
MAC address filtering	**Ensures secure network connection**

User isolation support	**Protect the private network between client users.**
Client Router mode	
PPPoE function support	**Easy to access internet via ISP service authentication**

Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- One Wireless Client Bridge Unit
- One Switching Power Adapter (12V/ 1.25A)
- One CAT5 UTP Cable
- One CD-ROM with User's Manual

Unit Description

System Requirements

The following are the minimum system requirements in order configure the device.

- PC/AT compatible computer with Ethernet interface.
- Operating system that supports HTTP web-browser

Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
   There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
b) **Temporary workgroups**
   Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
c) **The ability to access real-time information**
   Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
d) **Frequently changed environments**
   Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
e) **Small Office and Home Office (SOHO) networks**
   SOHO users need a cost-effective, easy and quick installation of a small

network.

f) Wireless extensions to Ethernet networks

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) Wired LAN backup

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

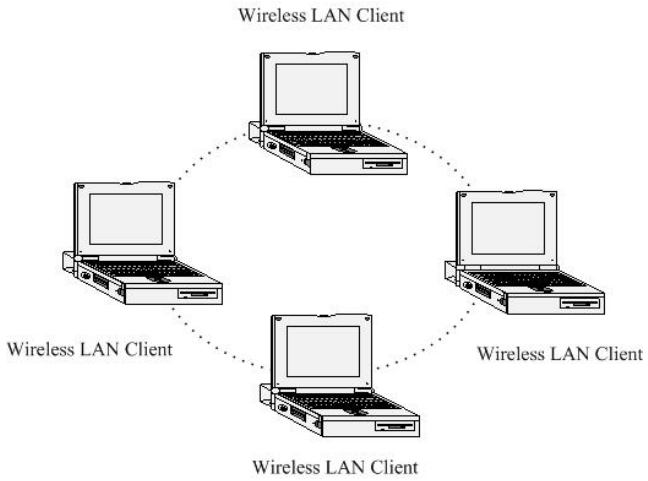
Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
b) Infrastructure for enterprise LANs.

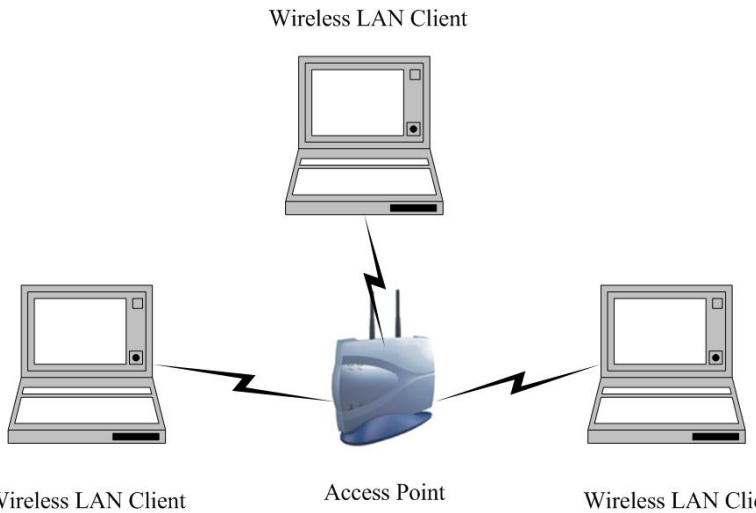
a) Ad-hoc (peer-to-peer) Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



2 Understanding the Hardware

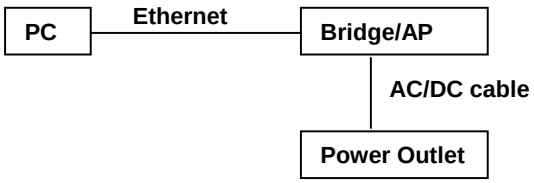
Hardware Installation

1 Place the unit in an appropriate place after conducting a site survey.

2 Plug one end of the Ethernet cable into the RJ-45 port of the device and another end into your PC/Notebook.

3 Insert the DC-inlet of the power adapter into the port labeled "DC-IN" and the other end into the power socket on the wall.

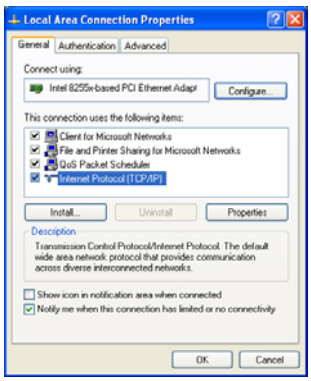
This diagram depicts the hardware configuration



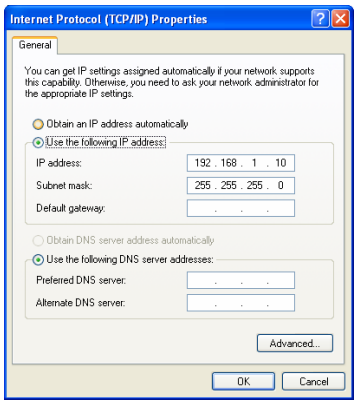
IP Address Configuration

This device can be configured as a Client Bridge or Access Point. The default IP address of the device is **192.168.1.1** or **192.168.1.2**. In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook.



3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.

For Example: Device IP address: 192.168.1.1
PC IP address: 192.168.1.10
PC subnet mask: 255.255.255.0

4. Click on the **OK** button to close this window, and once again to close LAN properties window.

3 Client Bridge/Router & Router/ AP

This device can be configured as a Bridge or Access Point. The default IP address of the device is **192.168.1.1** in Client Bridge /Client Router mode. The default IP address of the device is **192.168.1.2** in AP/Router mode. This chapter will describe the steps to switch from Bridge to Access Point and Access Point to Bridge.

Bridge/Bridge Router to Access Point

1 Enter the default IP address (192.168.1.2) of the bridge into the address bar of the web-browser.

2 By default, a user name and password has not been configured. If you have configured a user name and password, please enter them into the field to continue

3 Once you have logged in, click on the **Operation Mode** link under the **Management** menu.

4 Since this device is currently in Bridge mode, the **Bridge** radio button will be selected by default.

5 Select the **AP** radio button to and then click on the **Apply Change** to switch the operation mode to Access Point.

6 Wait for about 1 minute and the device will automatically restart into Access Point mode.

Access Point to Bridge/Bridge Router

1 Enter the default IP address (192.168.1.1) of the bridge into the address bar of the web-browser.

2 By default, a user name and password has not been configured. If you have configured a user name and password, please enter them into the field to continue

3 Once you have logged in, click on the **Operation Mode** link under the **Management** menu.

4 Since this device is currently in Access Point mode, the **AP** radio button will be selected by default.

5 Select the **Bridge or Bridge Router** radio button to and then click on the **Apply Change** to switch the operation mode to Bridge.

6 Wait for about 1 minute and the device will automatically restart into Bridge mode.

4 Access Point/Router Mode – Config

Logging In

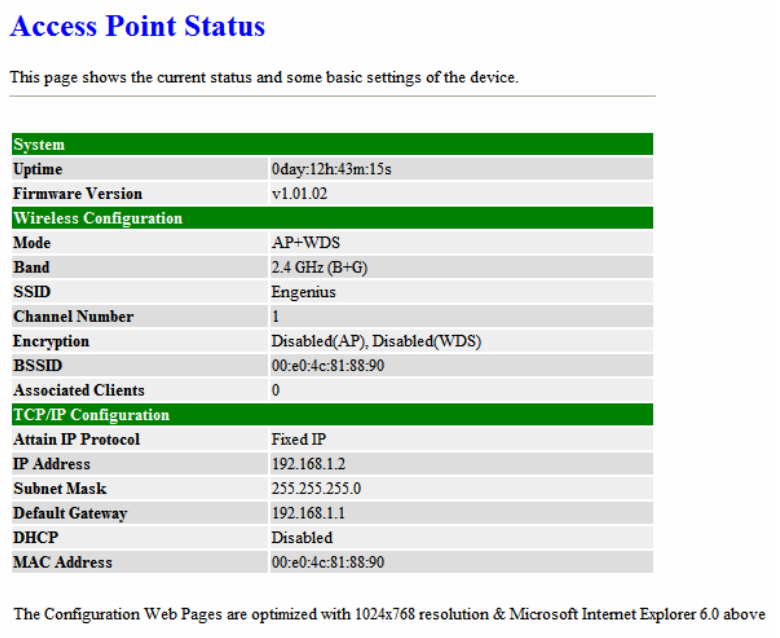
- To configure the AP through the web-browser, type IP address (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.

- Make sure that the ECB-1220R and your computers are on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- Username：**admin**; Password：**admin**

- After logging in you will graphical user interface (GUI) of the bridge. The navigation drop-down menu on left is divided into three main sections:

1. **Management**: This includes operation mode, status, statistics, logs, upgrade firmware, save/reload settings, and password.
2. **TCP/IP Settings**: This includes the configuration of the LAN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
3. **Wireless**: This includes the basic, advanced, security and site-survey settings for the wireless interface.

- The Bridge status page is also displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.



Access Point Status

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

System	
Uptime	0day:12h:43m:15s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	1
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:e0:4c:81:88:90
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP	Disabled
MAC Address	00:e0:4c:81:88:90

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

- **System**
  - **Uptime:** Duration of time since the device was last reset.
  - **Firmware version**: Version of the firmware that is currently loaded on the device.
- **Wireless Configuration**:

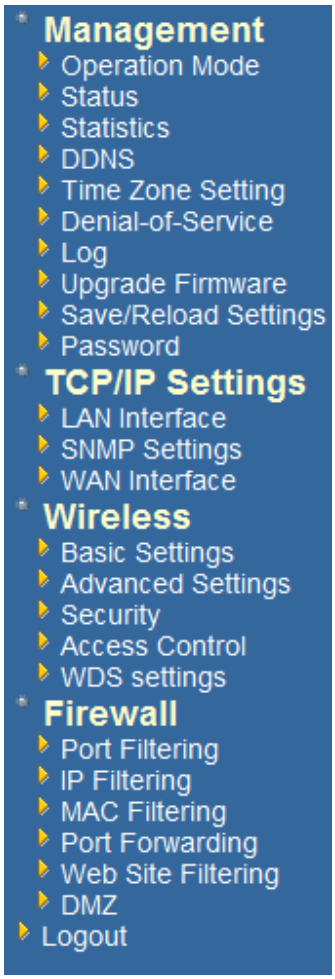
- **Mode**: Wireless configuration mode such as Client Bridge, AP, or WDS.
- **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
- **SSID**: The name used to identify the wireless network.
- **Channel Number**: The channel used to communicate on the wireless network.
- **Encryption**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
- **BSSID**: The MAC address of the SSID.
- **State**: The current state of the bridge. It may be scanning or associated or disabled.
- **Signal Strength**: The signal strength of the wireless device.
- **Noise Level**: The level of interference.

- **TCP/IP Configuration:**
  - **Attain IP Protocol**: The IP address setting may be fixed or static.
  - **IP Address**: Displays the current IP address of the LAN port.
  - **Subnet Mask**: Displays the current subnet mask for the IP address.
  - **Default Gateway**: Displays the default gateway for the device.
  - **DHCP**: Displays the DHCP setting.
  - **MAC Address**: Displays the MAC address of the device.

Management

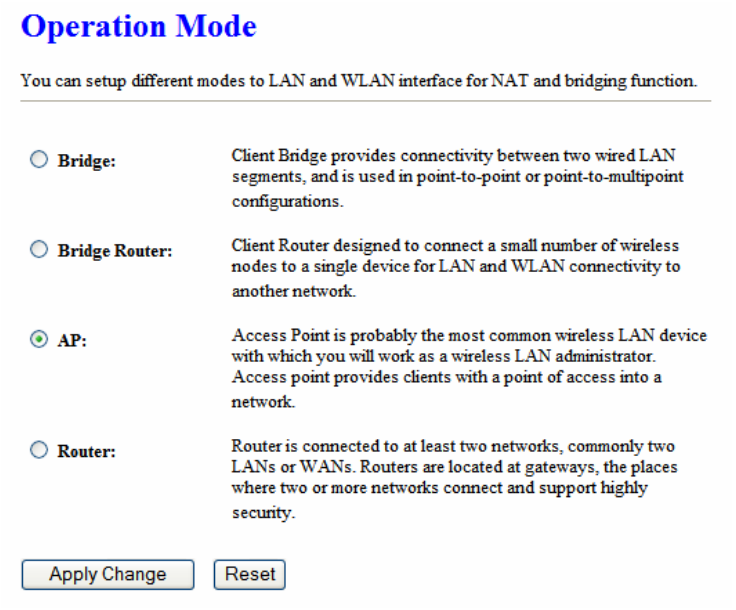
- Click on the **Management** link on the navigation drop-down menu. You will then see five options: operation mode, status, statistics, log, upgrade firmware, save/reload settings, and password. Each option is described below.

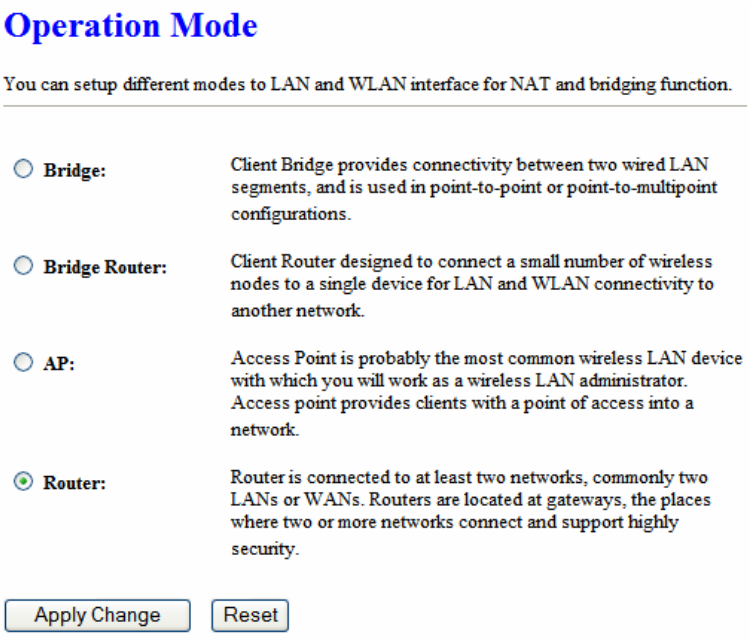
Management (Router *mode*)



Operation Mode

- Click on the **Operation Mode** link under the **Management** menu. The **Operation Mode** allows you to switch from Client Bridge to Access Point mode/Router Mode.



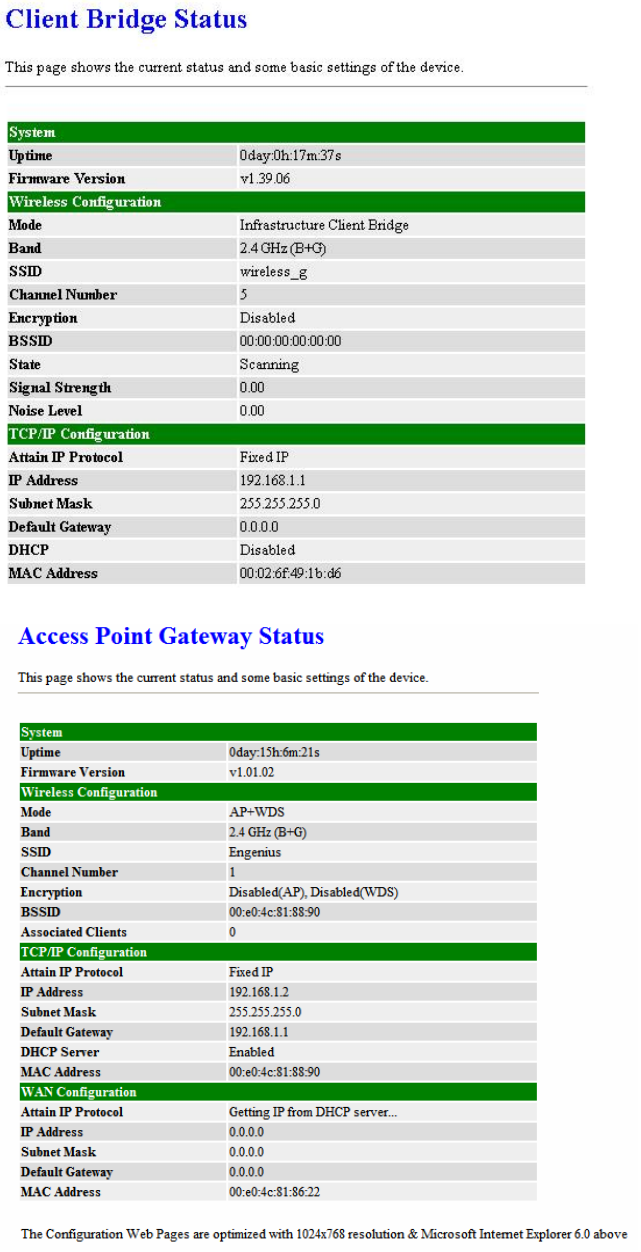


- Select the AP, Bridge or Bridge Router and then click on the Apply Change button.
- Please wait and the n enter the spec ified IP address into the web- browser. The previous settings will be retained in AP mode. .

▪ Refer to **Chapter 5** to learn how to configure this device in Access Point mode.

Status

- Click on the **Status** link under the **Management** menu. The **Status** page is the first page that is displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.



Client Bridge Status

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

System	
Uptime	0day:0h:17m:37s
Firmware Version	v1.39.06
Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	wireless_g
Channel Number	5
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
Signal Strength	0.00
Noise Level	0.00
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:02:6f:49:1b:d6

Access Point Gateway Status

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

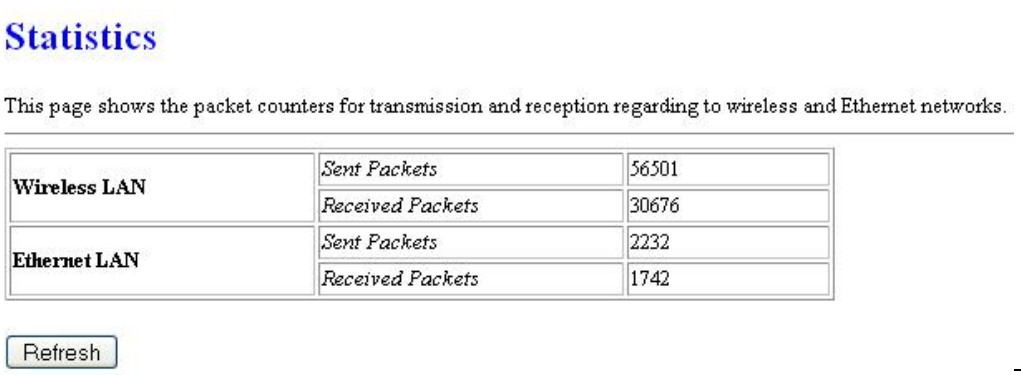
System	
Uptime	0day:15h:6m:21s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	1
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:e0:4c:81:88:90
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:88:90
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:86:22

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

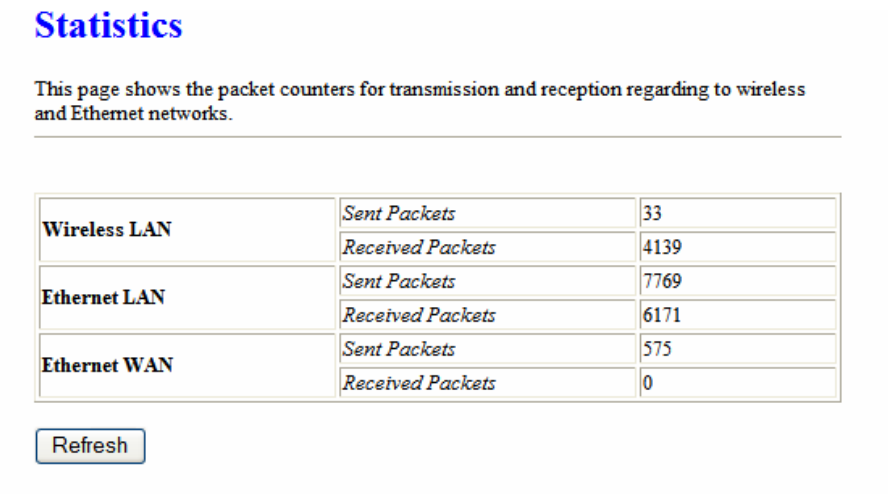
- **System**
  - **Uptime:** Duration of time since the device was last reset.
  - **Firmware version**: Version of the firmware that is currently loaded on the device.
- **Wireless Configuration**:
  - **Mode**: Wireless configuration mode such as Client Bridge, AP, or WDS.
  - **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
  - **SSID**: The name used to identify the wireless network.
  - **Channel Number**: The channel used to communicate on the wireless network.
  - **Encryption**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
  - **BSSID**: The MAC address of the SSID.
  - **State**: The current state of the bridge. It may be scanning or associated or disabled.
  - **Signal Strength**: The signal strength of the wireless device.
  - **Noise Level**: The level of interference.
- **TCP/IP Configuration:**
  - **Attain IP Protocol**: The IP address setting may be fixed or static.
  - **IP Address**: Displays the current IP address of the LAN port.
  - **Subnet Mask**: Displays the current subnet mask for the IP address.
  - **Default Gateway**: Displays the default gateway for the device.
  - **DHCP**: Displays the DHCP setting.
  - **MAC Address**: Displays the MAC address of the device.

Statistics

- Click on the **Statistics** link under the **Management** menu. This page displays the number of sent and received packets on the Ethernet and Wireless interface.



Additional WAN traffic information under **Router Mode**



Statistics

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

Wireless LAN	*Sent Packets*	33
	Received Packets	4139
Ethernet LAN	*Sent Packets*	7769
	Received Packets	6171
Ethernet WAN	*Sent Packets*	575
	Received Packets	0

Refresh

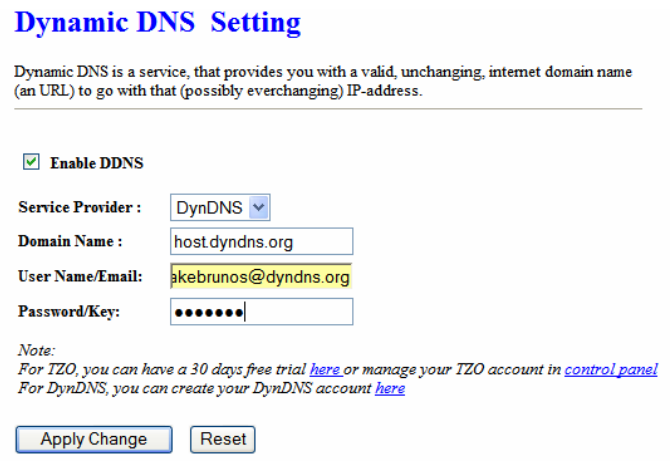
- Since the packet counter is not dynamic, you must click on the **Refresh** button for the most recent statistics.

Dynamic DNS (Router *mode)*

Allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your host name to connect to your server, no matter what your IP address is.

- **Enable Dynamic DNS**: Place a check in this box to enable the DDNS feature.
- **Service Address**: Select a DDNS service provider from the drop-down list. DynDNS is a free service while TZO offers a 30 day free trial.
- **Host Name**: Specify the website URL.
- **User Name**: Specify the user name for the DDNS service.
- **Password**: Specify the password for the DDNS service and verify it once again in the next field.

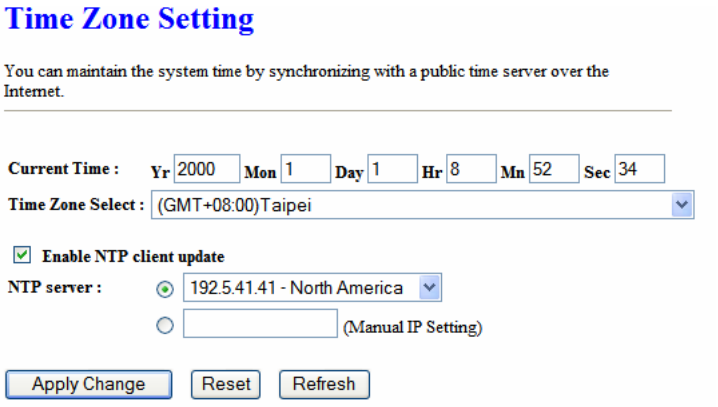
- **Timeout**: Specify the time between periodic updates to the Dynamic DNS, if the dynamic IP address has not changed. The timeout period is entered in hours.
- Cli ck on the **Save Settings** button once you have modified the settings.



Time Zone Setting (Router *mode*)

Click on the **Time** link in the navig ation menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by synchronizing with a time server.

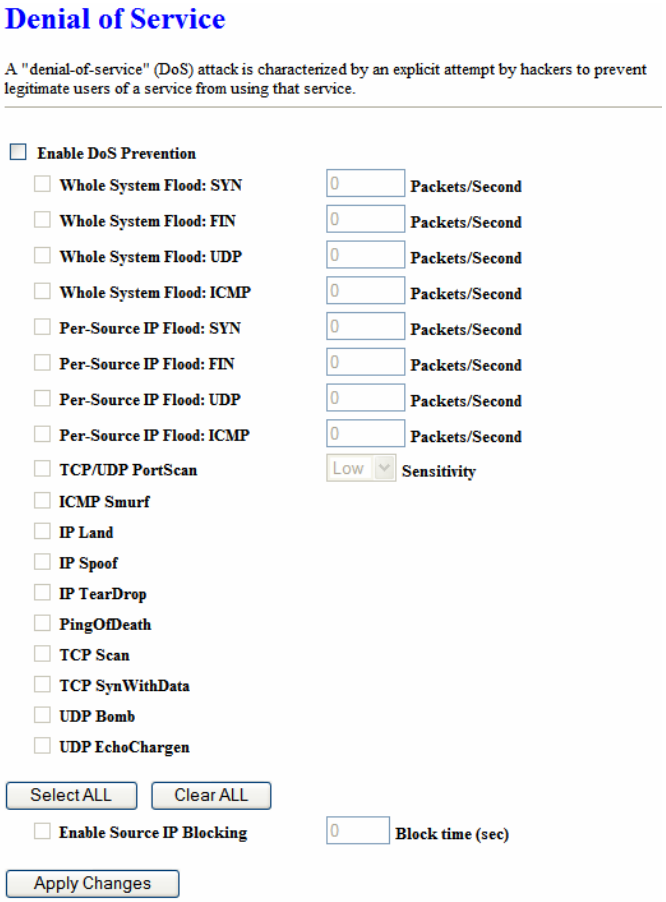
Note: If the device losses power for any reason, it wi ll not be able to keep its clock running, an d w ill no t display the correct time on ce t he device has be en r estarted. Therefore, you must re-enter the correct date and time.



- **Current Time**: Displays the current time on the device.
- **Time Zone**: Select your time zone from the drop-down list.
- **Enable NTP Server**: Place a check in this box if you would like to synchronize the device's clock to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.
- **NTP Server Used**: Specify the NTP server or select one from the drop-down list.
- Click on the **Apply Change** button once you have modified the settings.

Denial of Service (DoS) (Router *mode*)

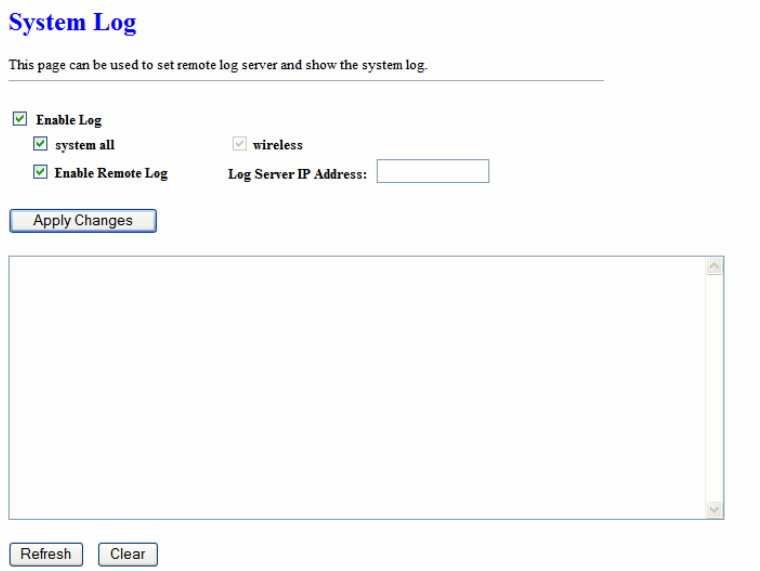
DoS attack is an attempt by hackers to block services for legitimate users of a PC/Network. Check the kind of specific protection you need.



Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be

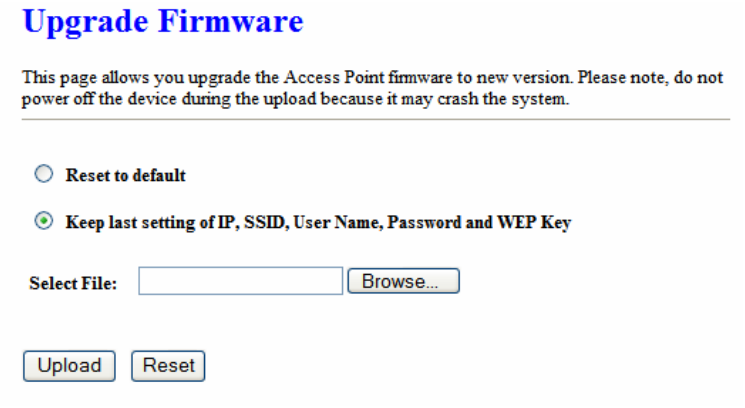
referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.



- In order for the log to record all the events, you must first place a check in the **Enable Log** or **Enable Remote Log (Log Server required)** check box.
- Select **system all** or **wireless** depending on the type of events you want recorded.
- Since the log is not dynamic, you must click on the **Refresh** button for the most recent events, or click on the **Clear** button to clear the log.
-

Upgrade Firmware

- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.

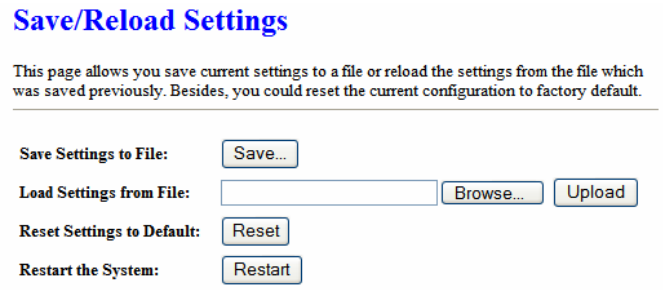


- Click on the Browse button and then select the appropriate firmware and then clic k on the **Upload** button.
- Clic k on **Reset to Default** to restore the device to factory default settings.

Note: The upgrade process may take abo ut 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

Save / Reload Settings, Reset to Default

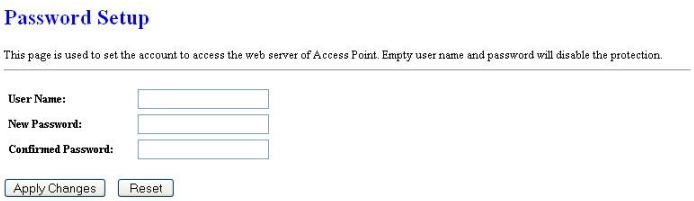
- Click on the **Save / Reload Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local dis k or load settings on t o the dev ice f rom a local disk. This feature is very handy for administrators who have several devices that need to be configured with the sam e settings.
- This page also allows you to reset the device to its factory default settings.



- Click on the **Save** button to save the current settings to a file on the local disk.
- Click on the **Browse** button to select the settings file and then click on the Upload button to load the previously saved settings.
- Click on the **Reset** button to reset the device to its factory default settings. Click **Restart** to reboot the device.

Password

- Click on the **Password** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password. For security reasons it is highly recommended that you create a user name and password.



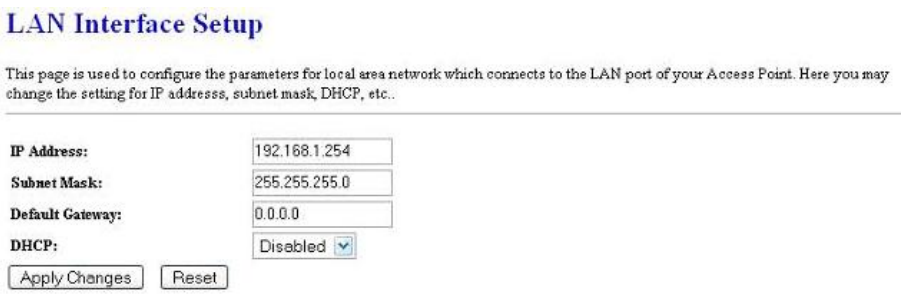
- Enter a **user name** into the first field.
- Enter a password into the **New Password** field and then re-type the password into the **Confirmed Password** field. Then click on the **Apply Changes** button.
- By clicking on the **Reset** button, the user name and password fields will become blank indicating that the username and password has been disabled.

TCP/IP Settings

- Click on the **TCP/IP Settings** link on the navigation drop-down menu. You will then see the LAN Interface and SNMP option. The options are described in detail below.

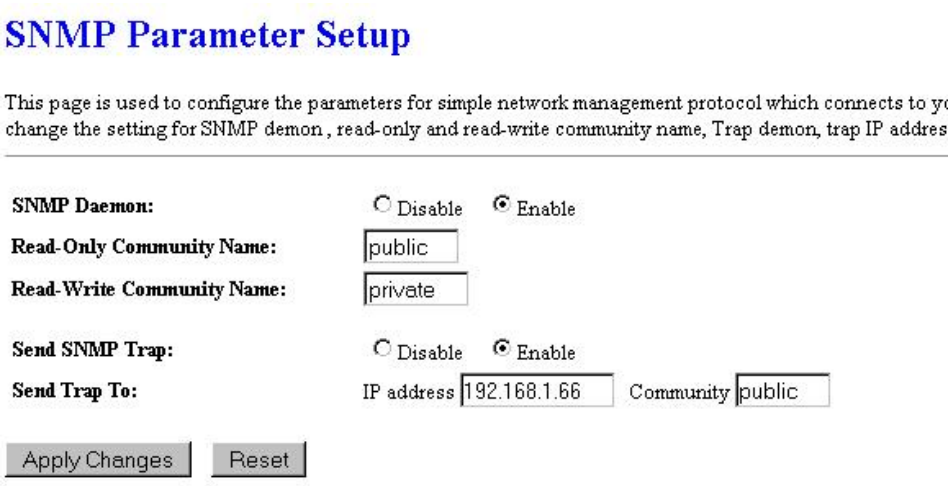
LAN Interface

- Click on the **LAN Interface** link under the **TCP/IP Settings** menu. Using this option you may change the IP address of the device as well as toggle the DHCP setting.



- **IP Address**: Enter the IP address.
- **Subnet Mask**: Enter the subnet mask for the IP address.
- **Default Gateway**: Enter the IP address for the default gateway.
- **DHCP**: If this device is a DHCP client and will receive its IP settings from a DHCP server, then select **Enabled** from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is **disabled**, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.3.2 SNMP Settings



- **Read-Only Community Name**: Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap**: Select **Enable** if you would like to receive SNMP traps.
- **Send Trap To**: Specify the IP address that would receive the SNMP traps.
- **Trap Community Name**: Specify the password for the SNMP trap community.
- Click on the **Save Settings** button once you have modified the settings.

WLAN Interface (Router *mode*)

DHCP Connection (Dynamic IP address) – Choose this connection type if your ISP provides you the IP address. Most cable modems use this type of connection.

PPPoE (Point-to-Point Protocol over Ethernet) – Choose this option if your internet connection requires a user name and password. Most DSL modems use this type of connection.

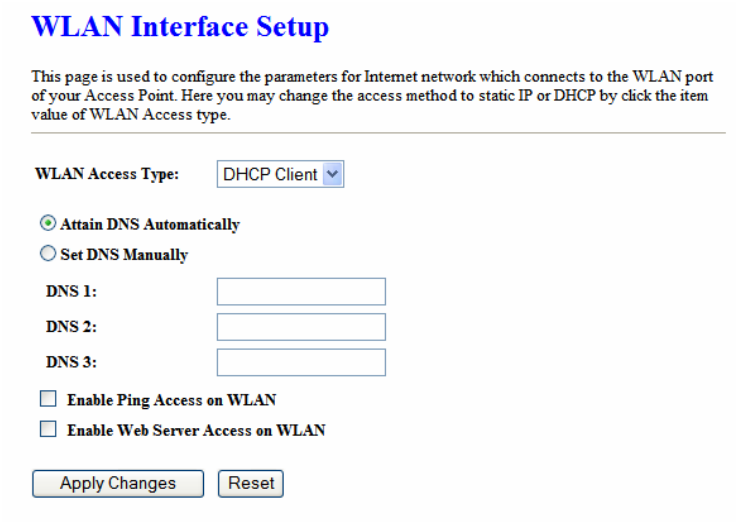
Static IP address – Choose this option if you have a dedicated IP address.

DHCP Client

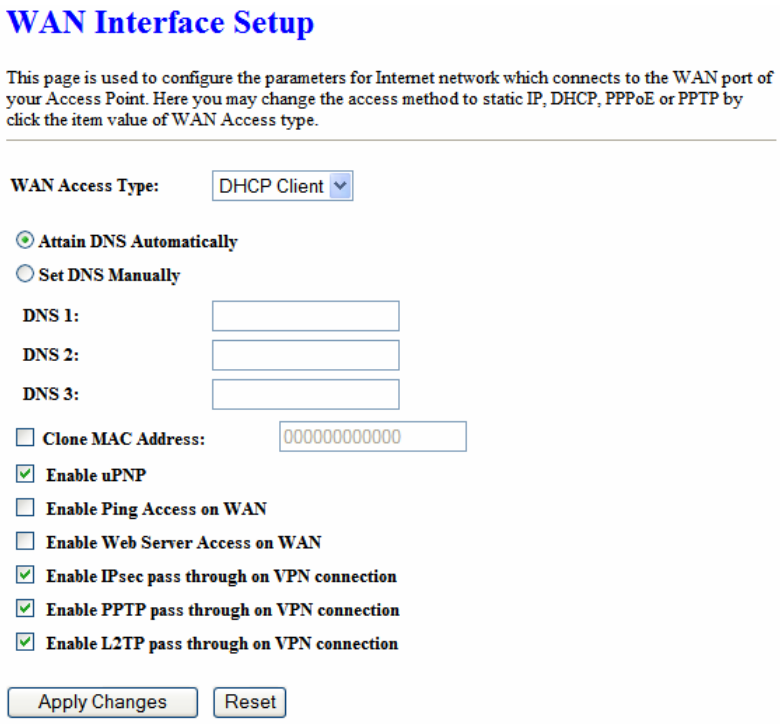
WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.

- Select the **DHCP** and click on the **Apply Changes** button.

  You have the option of cloning your PCs MAC address onto the device. Click on the **Clone Your PCs MAC Address** to automatically copy the MAC address. You may also specify a host name

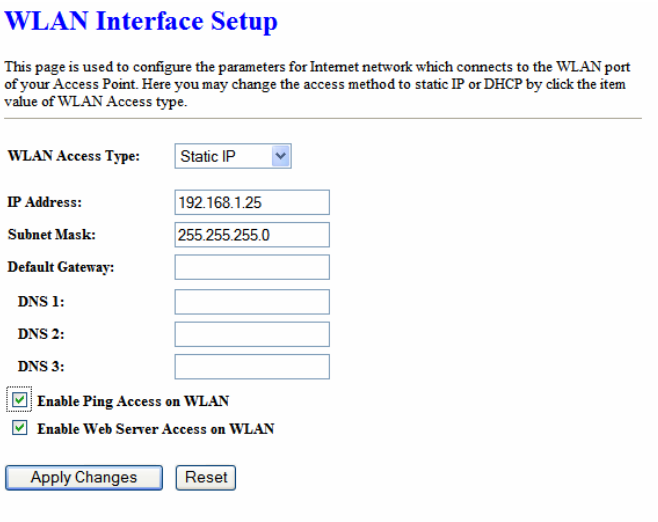


(Router mode)

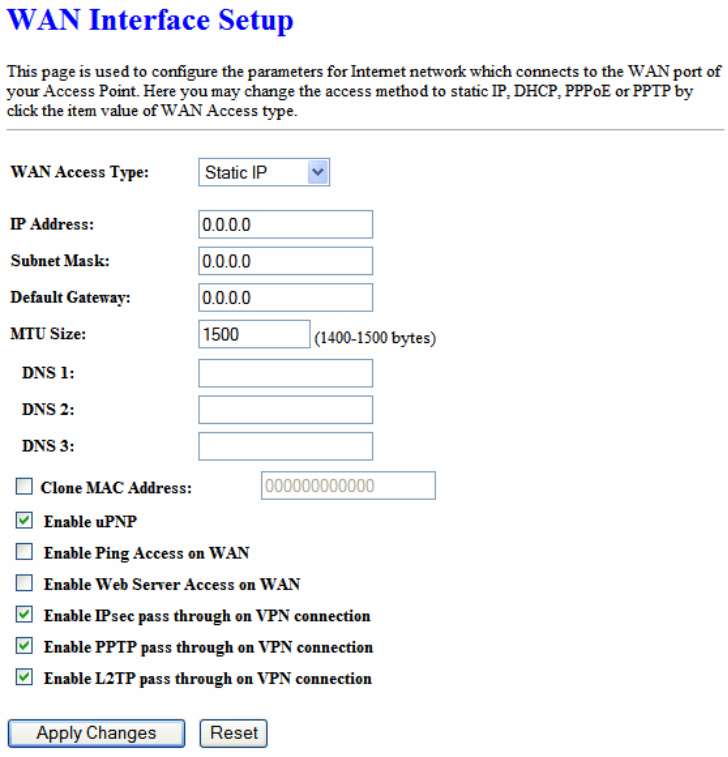


Static IP

Static IP is a fixed IP configuration whe re a ll p arameters includi ng DN S if a ny shoul d explicitly configured. VPN pass through is configured here by defining exclusivity.



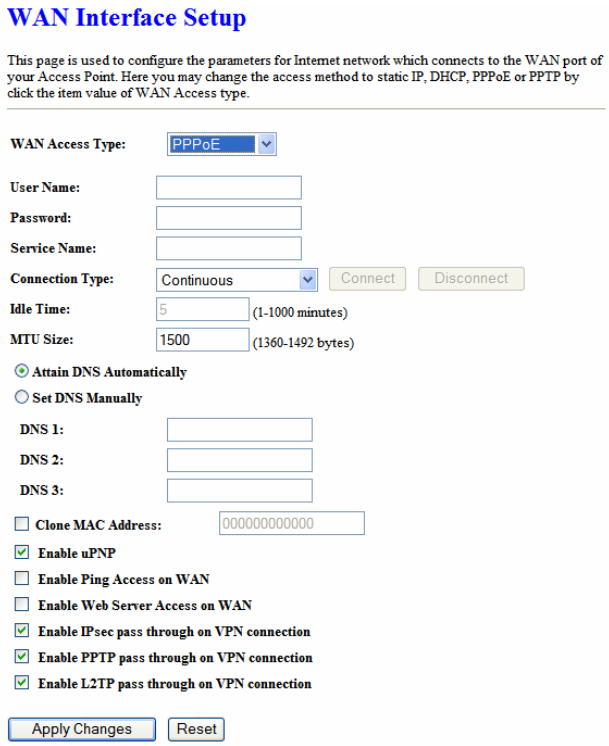
(Router *mode*)



PPPoE

This type of connection is usually used for a DSL service and requires a username and password to connect.

(Router *mode*)



Username / Password & Connection type (PPPoE) should be input then click on the **Connect** button.

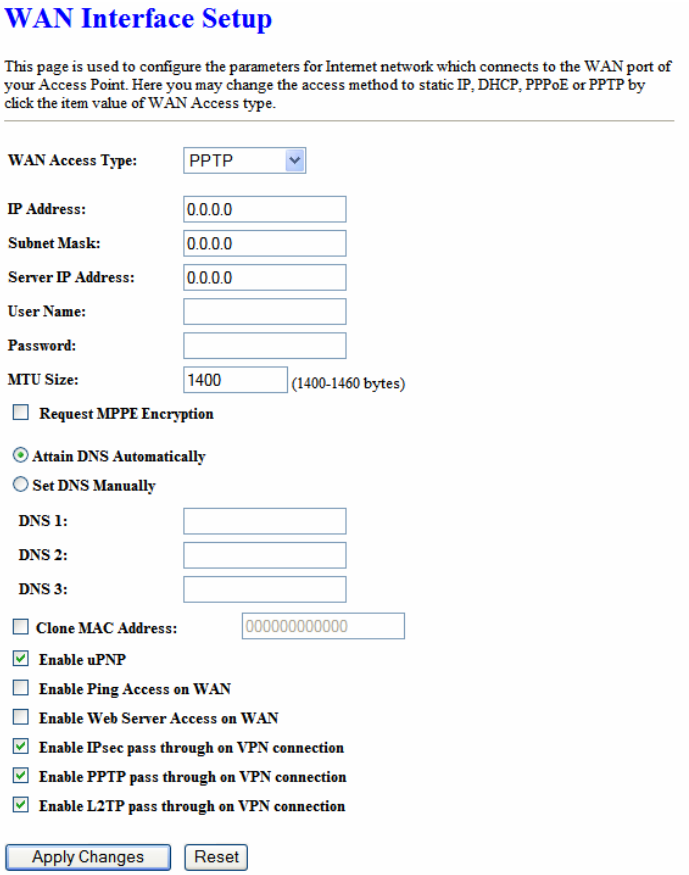
- **Address Mode**: PPPoE can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IIP address in the next field is not required.
- However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **User Name**: Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.

PPTP (Point-to-Point Tunneling Protocol) (Router *mode*)

- The WAN interface can be configured as PPTP. PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to

enter a username and password (provided by your ISP) to gain access to the Internet. The supported authentication protocols are PAP and CHAP.

- Select the **Username / Password Connection (PPTP)** radio button and then click on the **Next** button.
- **Address Mode**: PPTP can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IIP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **PPTP Address**: Specify the IP address
- **PPTP Subnet Mask**: Specify the subnet mask for the IP address.
- **PPTP Server IP Address**: If the PPTP Server's IP address is different from the default gateway, then you may specify it here.
- **User Name**: Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.

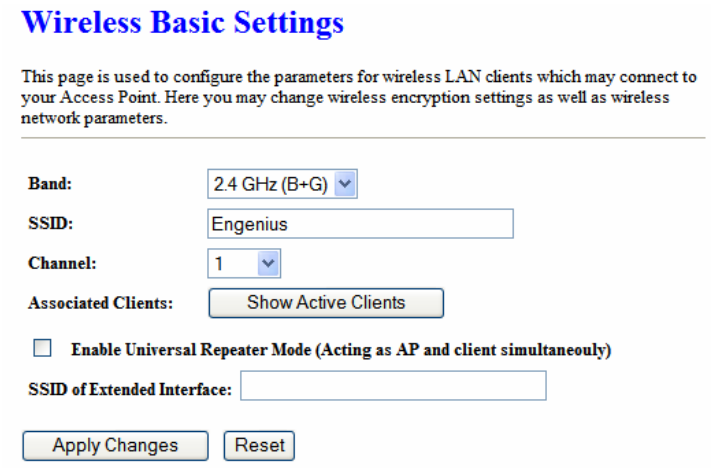


Wireless

- Click on the **Wireless** link on the navigation drop-down menu. You will then see four options: basic settings, advanced settings, security and site survey. Each option is described below.

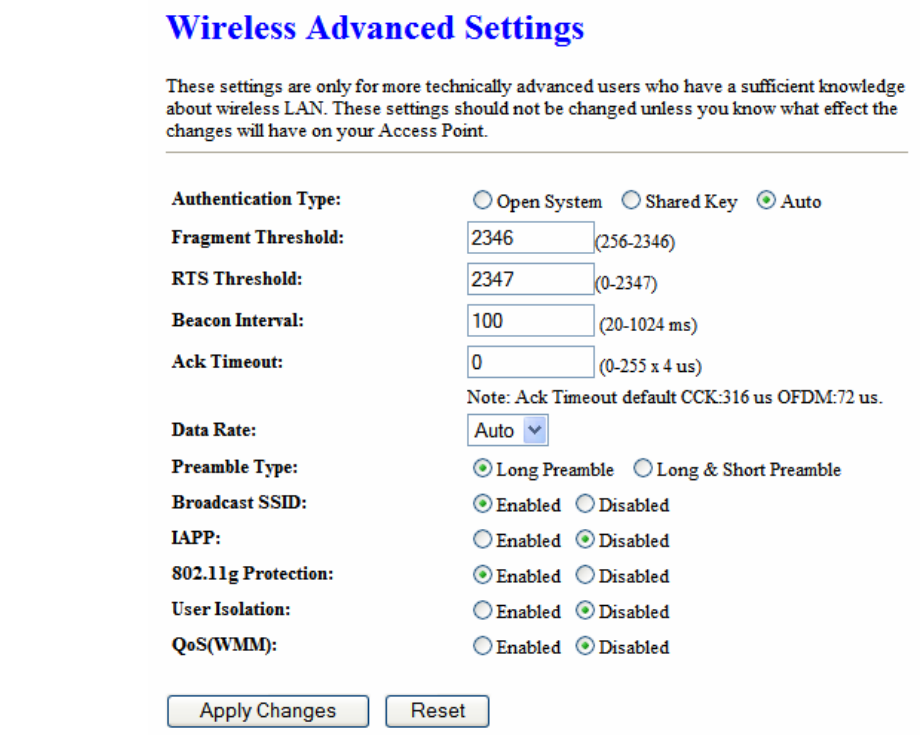
Basic Settings (Infrastructure, Adhoc)

- Click on the **Basic Settings** link under the **Wireless** menu. Using this option you may configure the 802.11b/g settings as well as the frequency, channel, and SSID.
-



- **Band**: Depending on the type of wireless clients that are connected to the network, you may select **B**, **G**, or **B+G**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B+G** for the best performance.
- **SSID**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- **Channel**: Select a channel from the drop-down list. The channels available are based on the country's regulation. When selecting Infrastructure mode, a channel is not required, however, when selecting Adhoc mode, you must select the same channel on all points.
- **Enable Universal Repeater Mode**: Select **Enable** to activate Universal Repeater Mode and type below SSID for extended wireless interface.

Advanced Settings



- Click on the **Advanced Settings** link under the **Wireless** menu. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: fragmentation threshold, RTS threshold, beacon interval, data rate, preamble type, and 802.11g protection.

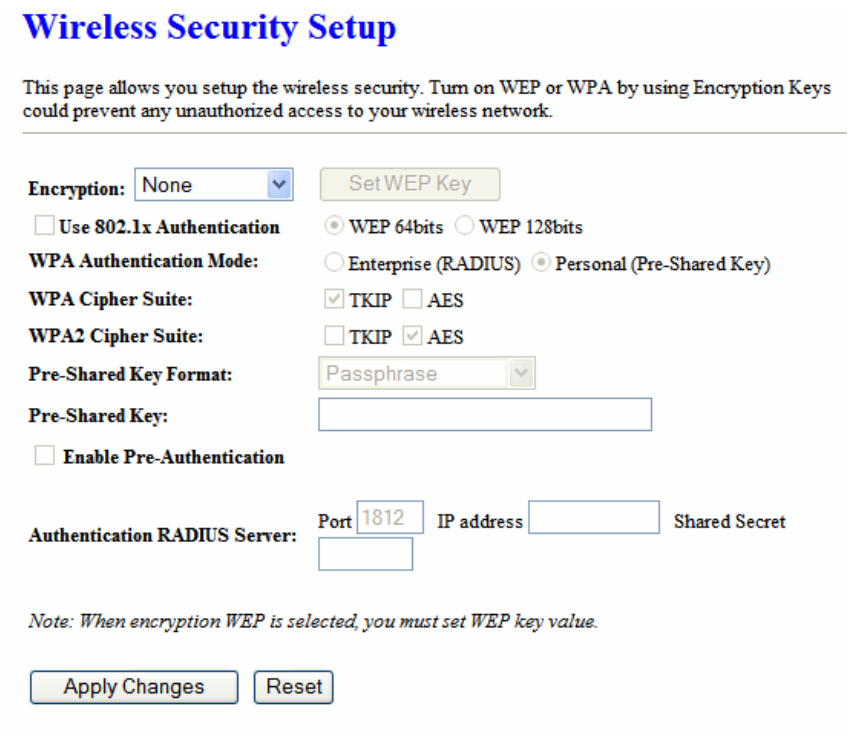
- **Authentication Type:** select an authentication method. Options available are **Open System**, **Shared Key** or **Auto**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- **Fragment Threshold**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.

- **RTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Beacon Interval**: Beacons will be sent out to devices at the specified intervals. This value is measured in milliseconds (ms).
- **ACK Timeout**: You may specify a value for the acknowledge timeout.
- **Data Rate**: Select a data rate from the drop-down list. However, it is recommended to select **auto** for the best performance.
- **Preamble Type**: For best performance, all devices on the wireless network should use the same preamble type. However, the wireless network will still function even though the wrong preamble type is used.
- **Enable/Disable**: A few options to enable some Wireless settings.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

Security

- Click on the **Security** link under the **Wireless** menu. On this page you can configure the authentication and encryption settings such as WEP, WPA, and 80.1x.

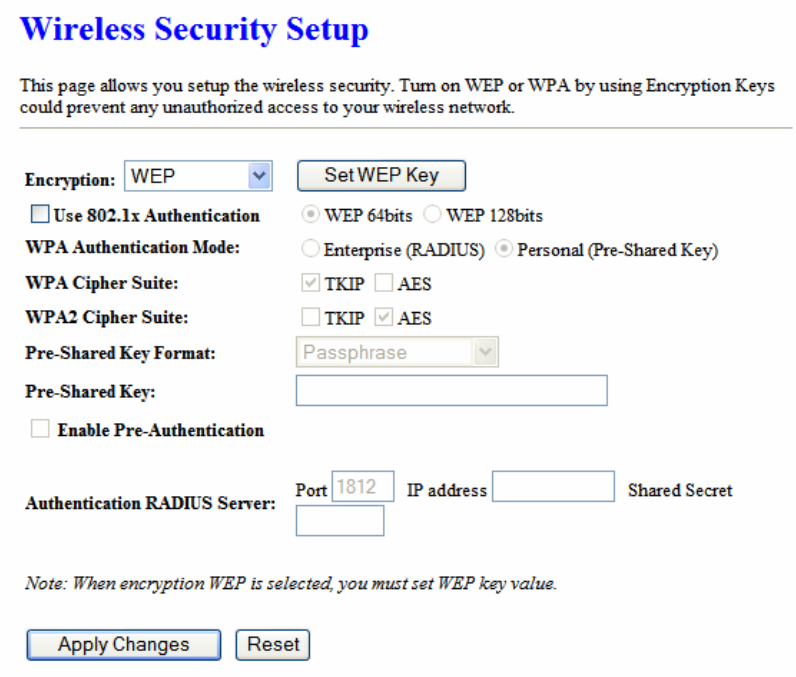
Encryption Disabled



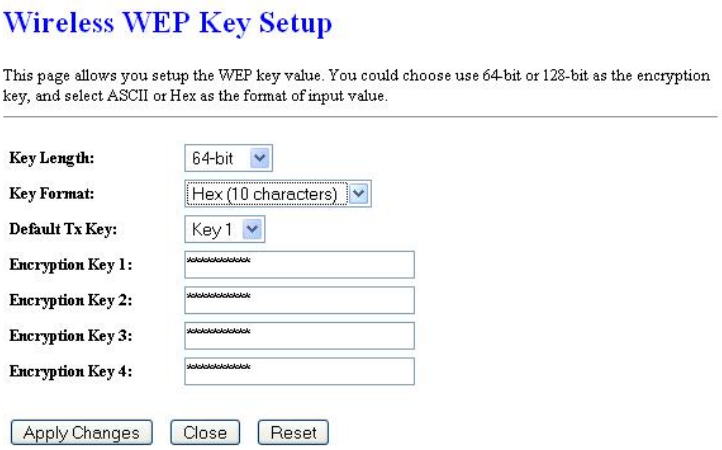
- **Encryption**: Select **None** from the drop-down list if your wireless network does not use any type of encryption.

- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

WEP 64-bit / 128-bit

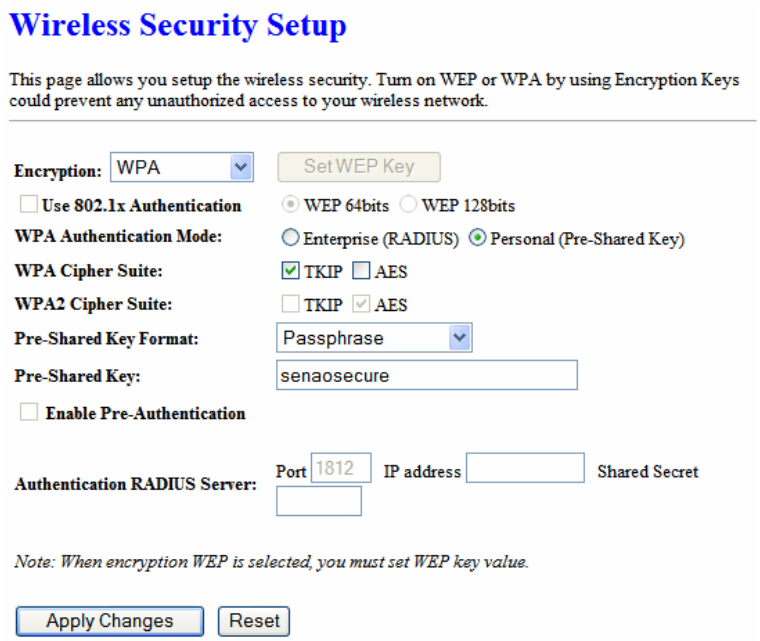


- **Encryption**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WE P is an ac ronym for Wired Equivalent P rivacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- **Set WEP Key**: Click on this button to configure the WEP Key.



- **Key Length**: Select a **64-bit** or **128-bit** from the drop-down list.
- **Key Format:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Default Tx Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Encryption Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply Changes** button to confirm the changes and then click on the **Close** button to return to the pervious window.

WPA / WPA2 Passphrase



- **Encryption**: Select **WPA** or **WPA2** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

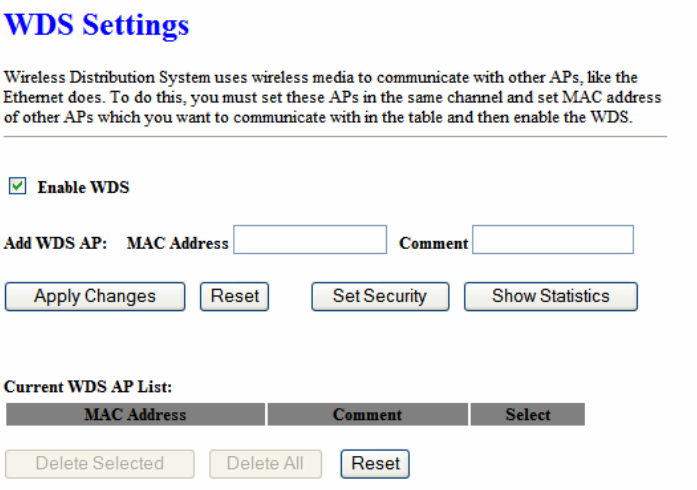
- **WPA Authentication Mode**: Select the **Personal (Pre-Shared Key)** radio button.
- **WPA/WPA2**: Select **TKIP** or **AES** as the cipher suite.
- **Pre-Shared Key Format**: Select **Passphrase** from the drop-down list.
- **Pre-Shared Key**: Enter the pass phrase here; this should be between 8 and 63 characters.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

WPA / WPA2 RADIUS Authentication

- **Encryption**: Select **WPA** or **WPA2** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **WPA Authentication Mode**: Select the **Enterprise (RADIUS)** radio button.
- **WPA/WPA2**: Select **TKIP** or **AES** as the cipher suite.
- **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.
- **RADIUS IP Address:** Enter the IP address of the RADIUS server.
- **RADIUS Password:** Enter the shared password of the RADIUS server.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

Wireless Distribution System

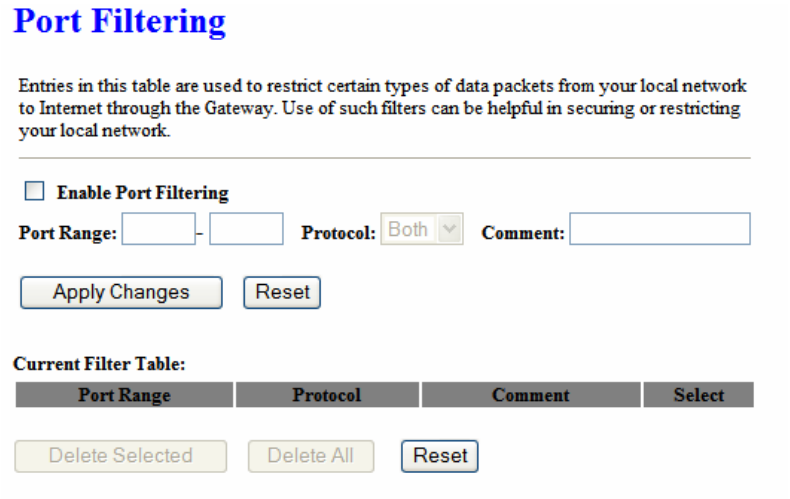
- Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.



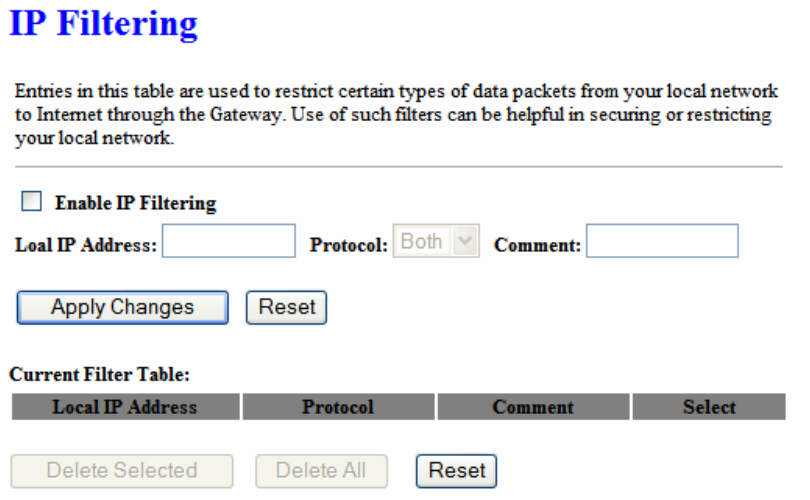
- **Enable WDS** - choose to enable/disable
- **Adding WDS AP:** Enter MAC address.
- **Set Security** – WEP/WPA/WPA2-mixed
- **Show Statistics** – shows details of WDS AP
- **Apply settings** – click to save settings.

Firewall

- The device provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attacks. However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control several ways of opening the firewall to address the needs of specific types of applications.

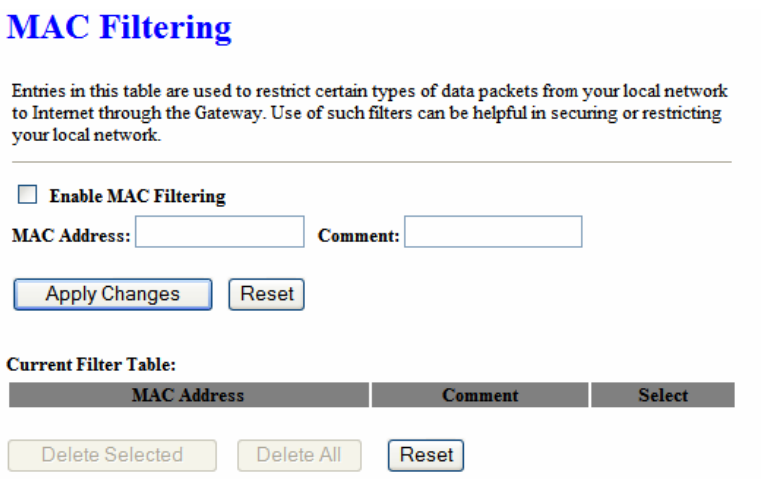


- The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.
- When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.



MAC Address Filter

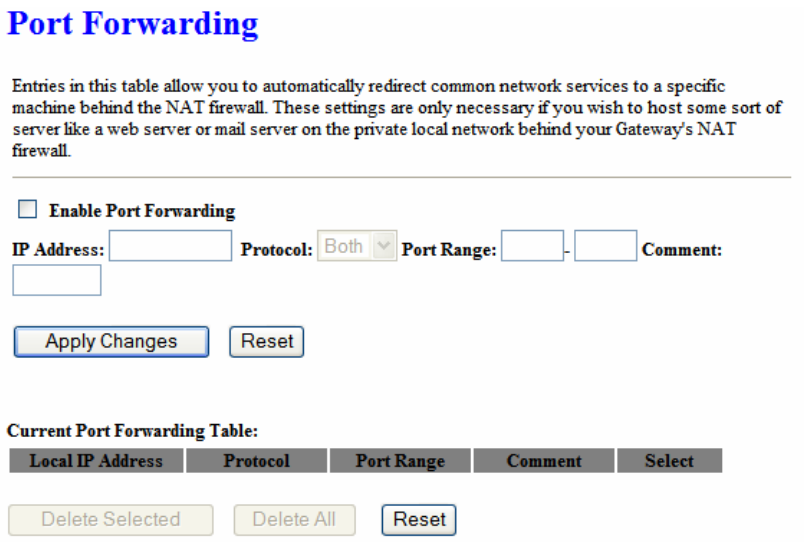
- This feature is used to restrict certain MAC address from accessing the Internet. These filters can be used for securing and restricting your network.
- **Configure MAC Filtering**: Select one of the options from the drop-down list.
  - **Turn MAC Filtering OFF:** When "OFF" is selected, MAC addresses are not used to control network access.
  - **Turn MAC Filtering ON and ALLOW computers listed to access the network:** When "ALLOW" is selected, only computers with MAC addresses listed in the MAC Filtering Rules list are granted network access.
  - **Turn MAC Filtering ON and DENY computers listed to access the network:** When "DENY" is selected, any computer with a MAC address listed in the MAC Filtering Rules list is refused access to the network.
- **MAC Address**: Specify that MAC address that you would like to filter.
- Click **Apply Changes** button to store the changes.



Port Forwarding

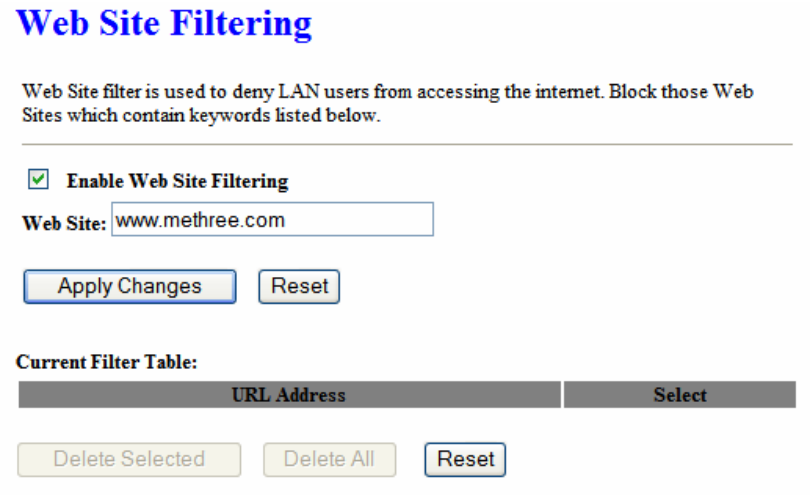
- Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network.

- **Enable**: Place a check in this box to enable the port forwarding rule.
- **Name**: Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the Application Name drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **IP Address**: Specify the IP address for the virtual server entry.
- **TCP/UDP Ports**: Specify the TCP or UDP port numbers.



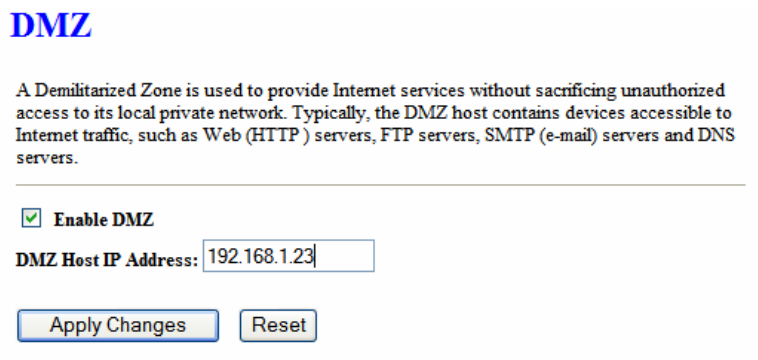
Web site Filter

- This is a type of parental control feature used to restrict certain websites form being accessed through your network. These filters can be used for securing and restricting your network.
- **Website/URL/Domain**: Specify the web address that you would like to filter. Do not use “http://”
- Click on the **Apply changes** button to store the changes.



DMZ

- Place check in this box to enable DMZ host. DMZ host is a demilitarized zone 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, FTP, email and DNS servers.
- **DMZ IP Address**: Specify the IP address of the DMZ host.
- Click on the **Apply changes** button to store the changes.



4 Client Bridge/Router Mode – Config

Logging In

- To configure the Access Point through the web-browser, enter the IP address of the Bridge (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.

- Make sure that the Access Point and your computers are on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- Log in User name：**admin**; Password：**admin**
- After logging in you will graphical user interface (GUI) of the Access Point. The navigation drop-down menu on left is divided into three main sections:

4. **Management**: This includes operation mode, status, statistics, logs, upgrade firmware, save/reload settings, and password.
5. **TCP/IP Settings**: This includes the configuration of the LAN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
6. **Wireless**: This includes the basic, advanced, security and site-survey settings for the wireless interface.

- The Access Point status page is also displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.

Client Bridge Status

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

System	
Uptime	0day:13h:31m:47s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	4
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
Signal Strength	0.00
Noise Level	0.00
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP	Disabled
MAC Address	00:e0:4c:81:88:90

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

Bridge Router Status

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

System	
Uptime	0day:14h:45m:2s
Firmware Version	v1.01.02
Wireless Configuration	
Mode	Infrastructure Bridge Router
Band	2.4 GHz (B+G)
SSID	Engenius
Channel Number	11
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
Signal Strength	0.00
Noise Level	0.00
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP	Server
MAC Address	00:e0:4c:81:88:90
WLAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:88:90

The Configuration Web Pages are optimized with 1024x768 resolution & Microsoft Internet Explorer 6.0 above

- **System**
- **Uptime:** Duration of time since the device was last reset.
- **Firmware version**: Version of the firmware that is currently loaded on the device.

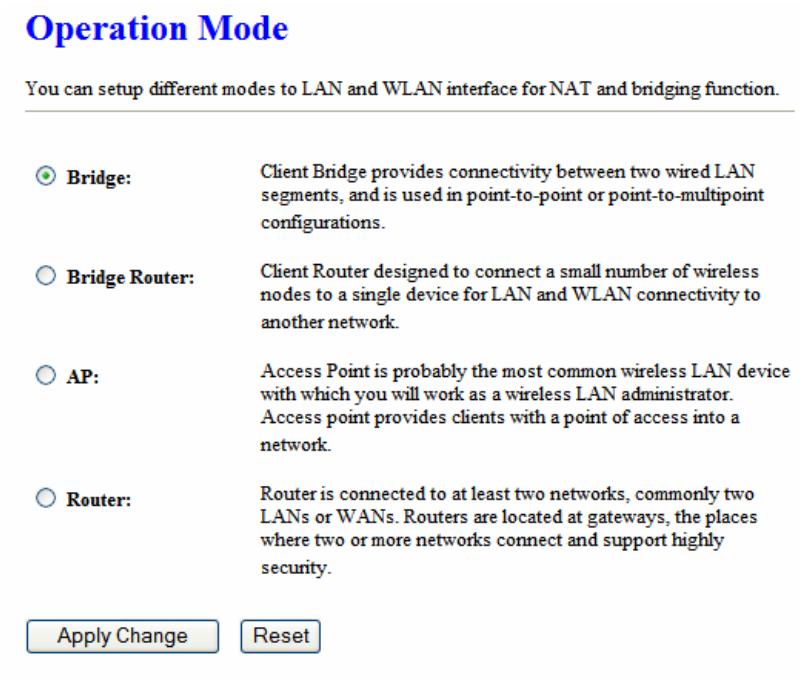
- **Wireless Configuration**:
  - **Mode**: Wireless configuration mode such as client bridge, AP, or WDS.
  - **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
  - **SSID**: The name used to identify the wireless network.
  - **Channel Number**: The channel used to communicate on the wireless network.
  - **Encryption**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
  - **BSSID**: The MAC address of the SSID.
  - **Associated Clients**: Displays the number of clients currently associated to the Access Point.
- **TCP/IP Configuration:**
  - **Attain IP Protocol**: The IP address setting may be fixed or static.
  - **IP Address**: Displays the current IP address of the LAN port.
  - **Subnet Mask**: Displays the current subnet mask for the IP address.
  - **Default Gateway**: Displays the default gateway for the device.
  - **DHCP**: Displays the DHCP setting.
  - **MAC Address**: Displays the MAC address of the device.

Management

- Click on the **Management** link on the navigation drop-down menu. You will then see five options: operation mode, status, statistics, log, upgrade firmware, save/reload settings, and password. Each option is described below.

Operation Mode

- Click on the **Operation Mode** link under the **Management** menu. The **Operation Mode** allows you to switch from Access Point to Client Bridge mode.



- Select the **AP**, **Bridge** or **Bridge Router** and then click on the **Apply Change** button.

- Wait for about a minute until you see the Pop-Up message.

- Click on the **OK** button and then enter the specified IP address into the web-browser.
- Please wait and then enter the specified IP address into the web-browser. The previous settings will be retained in AP mode. .

- Refer to **Chapter 4** to learn how to configure this device in Bridge/Bridge Router mode.

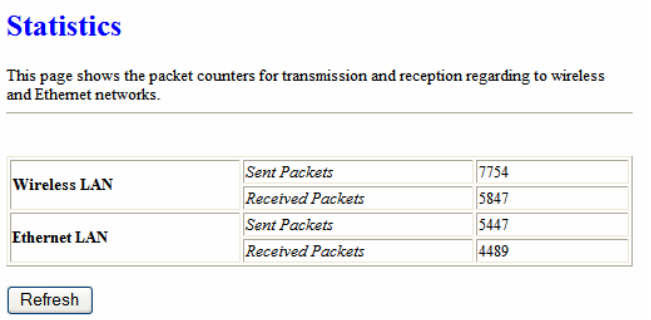
Status

- Click on the **Status** link under the **Management** menu. The **Status** page is the first page that is displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.

- **System**
  - **Uptime:** Duration of time since the device was last reset.
  - **Firmware version**: Version of the firmware that is currently loaded on the device.
- **Wireless Configuration**:
  - **Mode**: Wireless configuration mode such as client bridge, AP, or WDS.
  - **Band**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
  - **SSID**: The name used to identify the wireless network.
  - **Channel Number**: The channel used to communicate on the wireless network.
  - **Encryption**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
  - **BSSID**: The MAC address of the SSID.
  - **Associated Clients**: Displays the number of clients currently associated to the Access Point.
- **TCP/IP Configuration:**
  - **Attain IP Protocol**: The IP address setting may be fixed or static.
  - **IP Address**: Displays the current IP address of the LAN port.
  - **Subnet Mask**: Displays the current subnet mask for the IP address.
  - **Default Gateway**: Displays the default gateway for the device.
  - **DHCP**: Displays the DHCP setting.
  - **MAC Address**: Displays the MAC address of the device.

Statistics

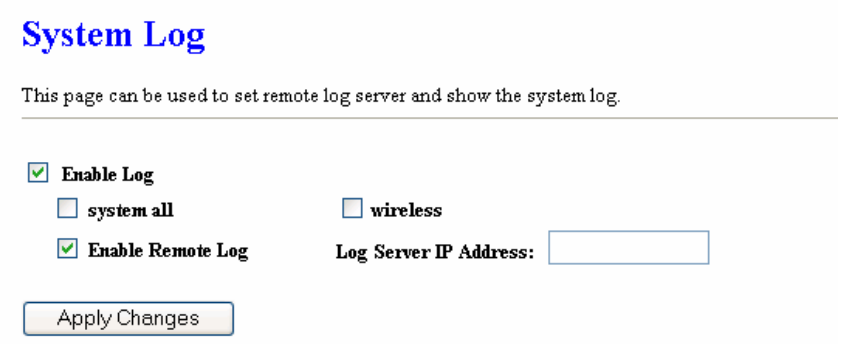
- Click on the **Statistics** link under the **Management** menu. This page displays the number of sent and received packets on the Ethernet and Wireless interface.



- Since the packet counter is not dynamic, you must click on the **Refresh** button for the most recent statistics.

Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

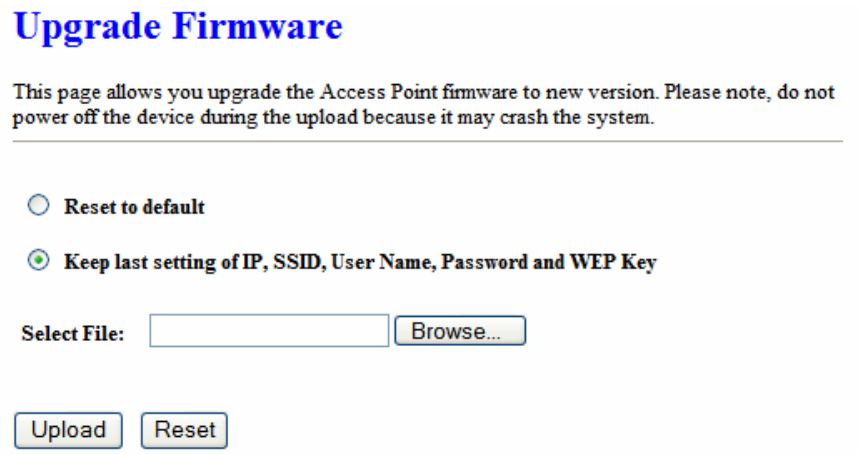


- In order for the log to record all the events, you must first place a check in the **Enable Log** or **Enable Remote Log (Log Server required)** check box.
- Select **system all** or **wireless** depending on the type of events you want recorded.

- Since the log is not dynamic, you must click on the **Refresh** button for the most recent events, or click on the **Clear** button to clear the log.

Upgrade Firmware

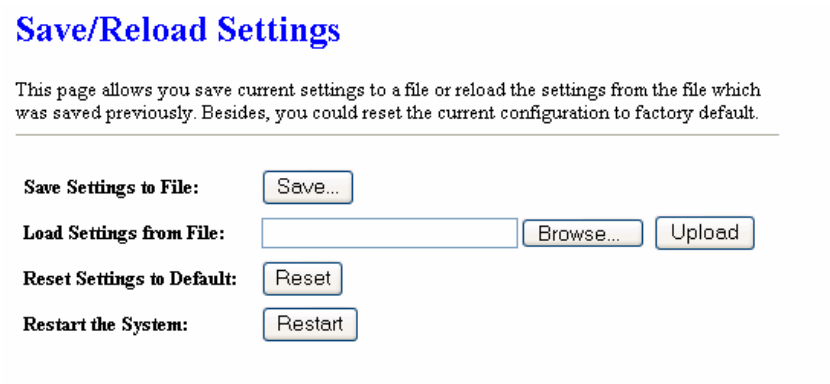
- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



- Click on the Browse button and then select the appropriate firmware and then click on the **Upload** button.
  Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

Save / Reload Settings, Reset to Default

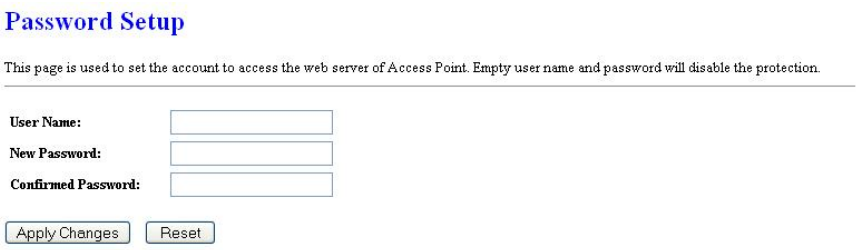
- Click on the **Save / Reload Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.
- This page also allows you to reset the device to its factory default settings.



- Click on the **Save** button to save the current settings to a file on the local disk.
- Click on the **Browse** button to select the settings file and then click on the Upload button to load the previously saved settings.
- Click on the **Reset** button to reset the device to its factory default settings. Click **Restart** to reboot the device.

Password

- Click on the **Password** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password. For security reasons it is highly recommended that you create a user name and password.



- Enter a **user name** into the first field.
- Enter a password into the **New Password** field and then re-type the password into the **Confirmed Password** field. Then click on the **Apply Changes** button.
- By clicking on the **Reset** button, the user name and password fields will become blank indicating that the username and password has been disabled.

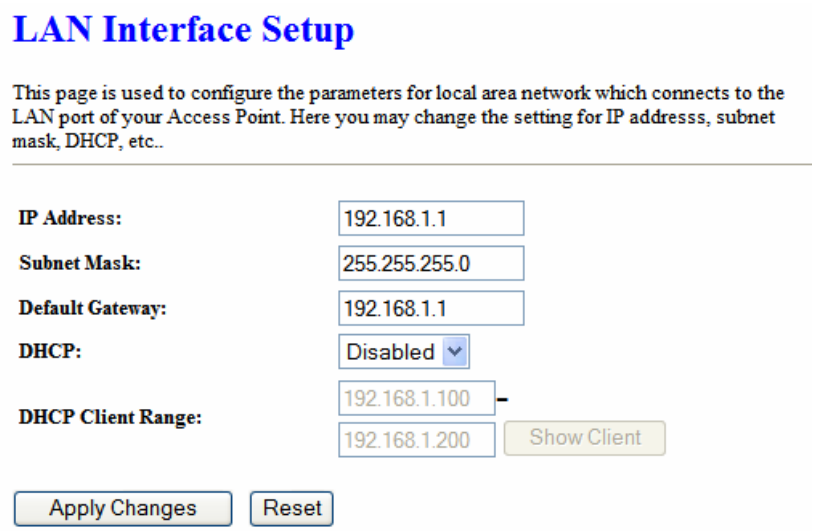
TCP/IP Settings

- Click on the **TCP/IP Settings** link on the navigation drop-down menu. You will then see the LAN Interface and SNMP option. The options are described in detail below.

LAN Interface

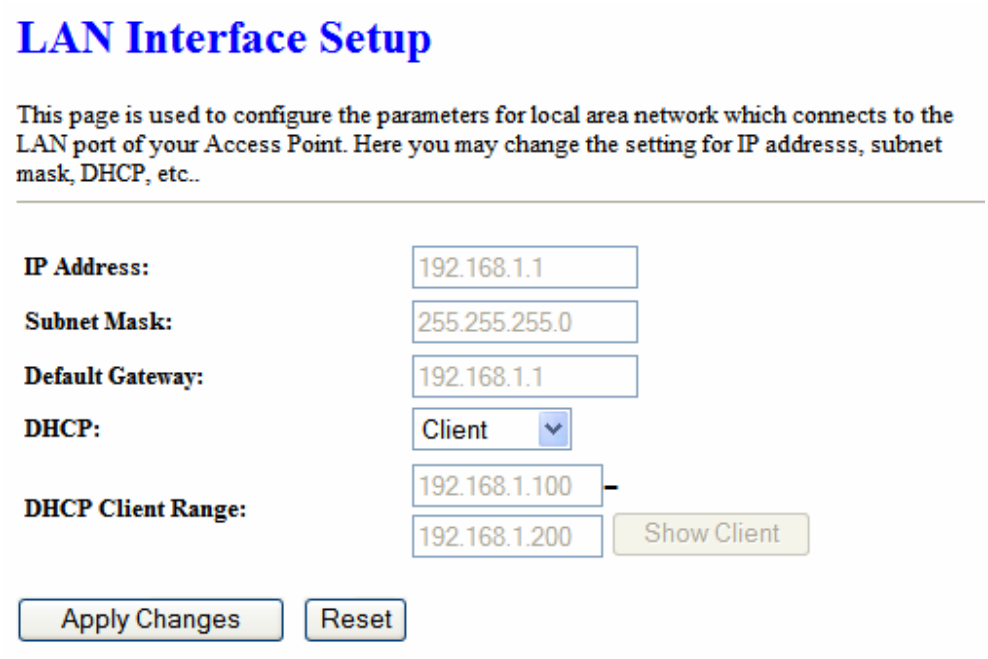
- Click on the **LAN Interface** link under the **TCP/IP Settings** menu. Using this option you may change the IP address of the device as well as toggle the DHCP server/client and 802.1d spanning tree feature.

Static IP Address



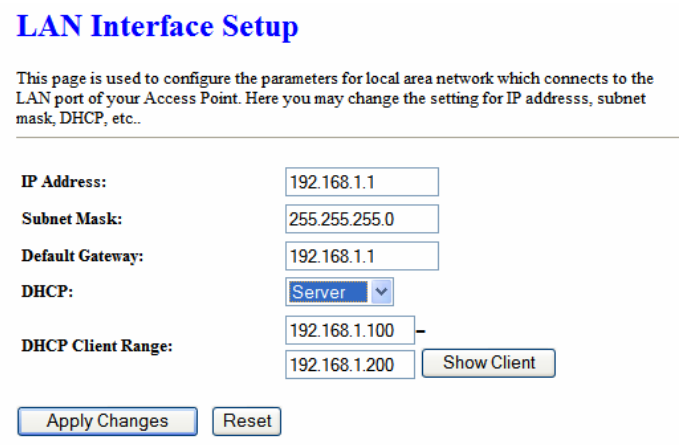
- **IP Address**: Enter the IP address.
- **Subnet Mask**: Enter the subnet mask for the IP address.
- **Default Gateway**: Enter the IP address for the default gateway.
- **DHCP**: Since a static IP address is used, this option must be set to **Disabled**. If this device is a DHCP client and will receive its IP settings from a DHCP server, then select **Enabled** from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is **Disabled**, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

DHCP Client



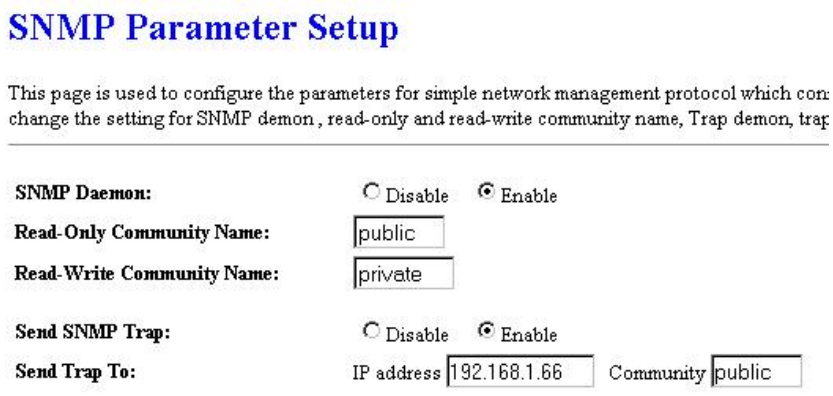
- **DHCP**: If this device is a DHCP client and will receive its IP settings from a DHCP server, then select **Client** from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is **disabled**, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

DHCP Server



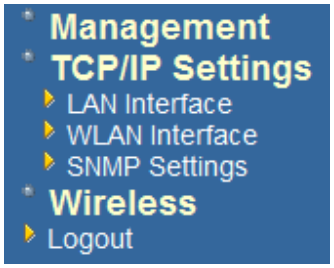
- **IP Address**: Enter the IP address.
- **Subnet Mask**: Enter the subnet mask for the IP address.
- **Default Gateway**: Enter the IP address for the default gateway.
- **DHCP**: Select Server from the drop-down list since this device is the DHCP server. This device will distribute the IP addresses to the clients associated.
- **DHCP Client Range**: Enter the first and last IP address of the range. Make sure that the range is on the same subnet as the device. You may click on the Show Client button to view a list of IP addresses that were distributed.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

SNMP Settings



- **SNMI**
- **Read** S NMP comm
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap**: Select **Enable** if you would like to receive SNMP traps.
- **Send Trap To**: Specify the IP address that would receive the SNMP traps.
- Click on the **Save Settings** button once you have modified the settings.

Client Bridge Router



WLAN Interface

DHCP Connection (Dynamic IP address) – Choose this connection type if your ISP provides you the IP address. Most cable modems use this type of connection.

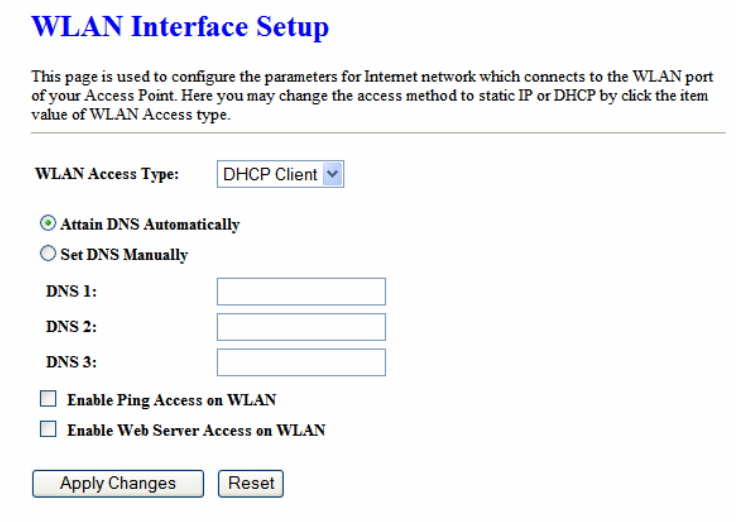
PPPoE (Point-to-Point Protocol over Ethernet) – Choose this option if your internet connection requires a user name and password. Most DSL modems use this type of connection.

Static IP address – Choose this option if you have a dedicated IP address.

DHCP Client

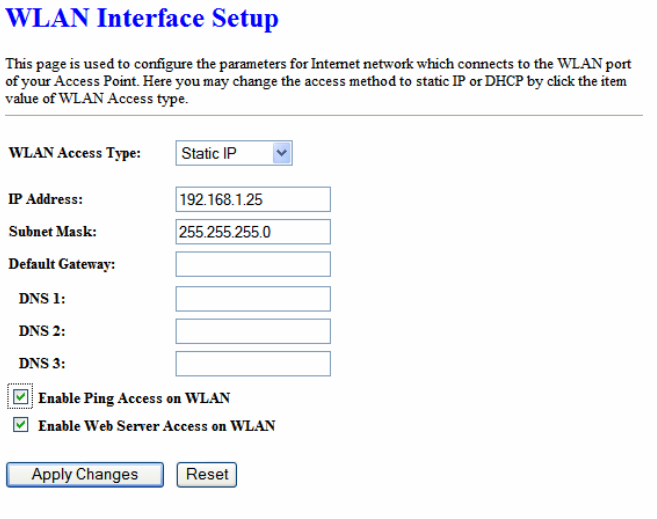
WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.

- Select the **DHCP** and click on the **Apply Changes** button.
  You have the option of cloning your PCs MAC address onto the device. Click on the **Clone Your PCs MAC Address** to automatically copy the MAC address. You may also specify a host name



Static IP

Static IP is a fixed IP configuration where all parameters including DNS if any should explicitly configured. VPN pass through is configured here by defining exclusivity.

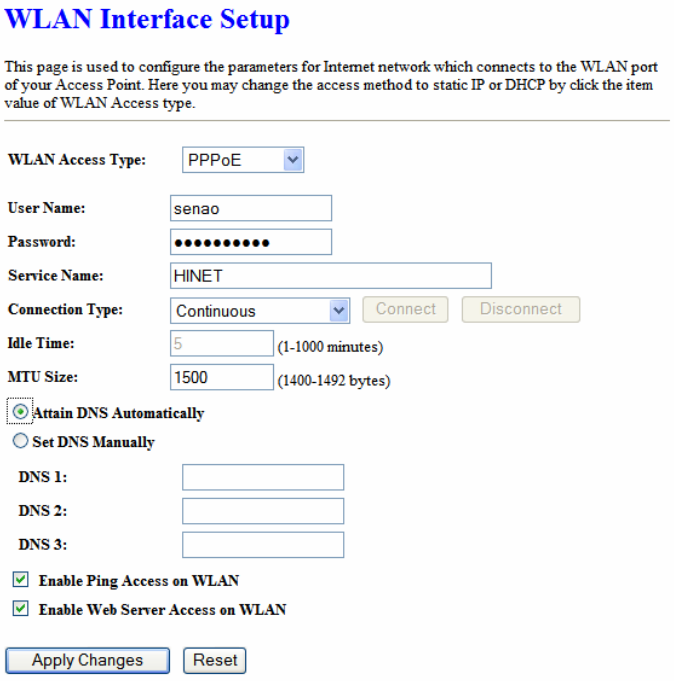


PPPoE

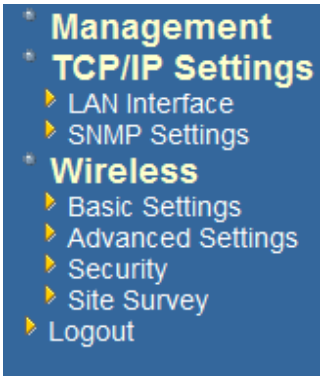
This type of connection is usually used for a DSL service and requires a username and password to connect.

Username / Password & Connection type (PPPoE) should be input then click on the **Connect** button.

- **Address Mode**: PPPoE can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IIP address in the next field is not required.
- However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **User Name**: Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.



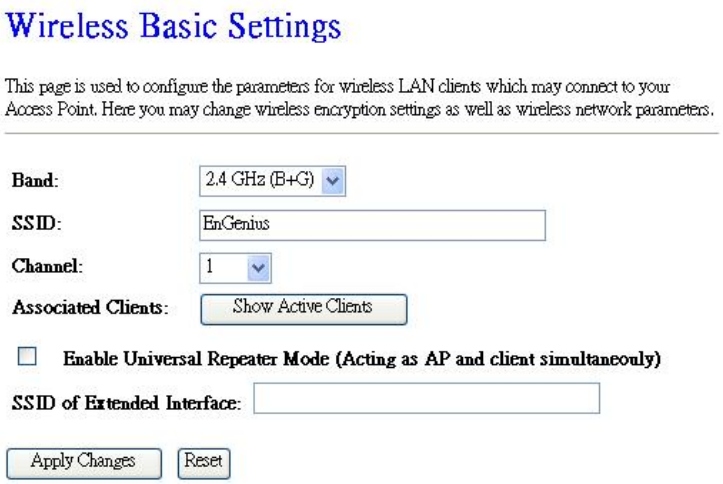
Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see five options: basic settings, advanced settings security, access control and WDS. Each option is described below.

Basic Settings

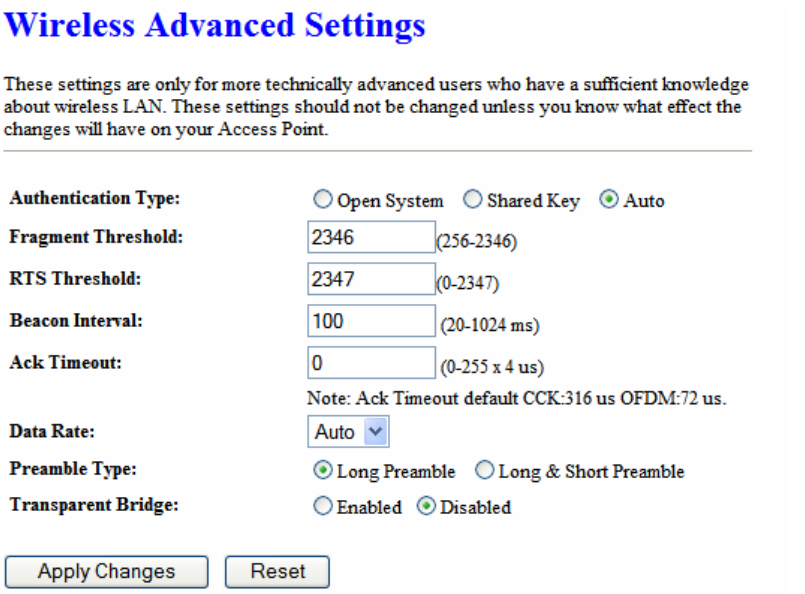
- Click on the **Basic Settings** link under the **Wireless** menu. Using this option you may configure the 802.11b/g settings as well as the frequency, channel, and SSID.



- **Band**: Select the IEEE 802.11 mode from the drop-down list. Options available are **2.4GHz (B), 2.4GHz (G), or 2.4GHz (B+G)**. Select the appropriate mode based on the type of wireless network. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select 2.4GHz (G) instead of 2.4GHz (B+G) which will reduce the performance of the wireless network.
- **SSID**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- **Channel**: Select a channel from the drop-down list. The channels available are based on the country's regulation. When selecting Infrastructure mode, a channel is not required, however, when selecting Adhoc mode, you must select the same channel on all points.
- **Show Active Clients**: Click on this button to view a list of associated clients.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.
- **Enable Universal Repeater Mode**: Select **Enable** to activate Universal Repeater Mode and type below SSID for extended wireless interface.

Advanced Settings

- Click on the **Advanced Settings** link under the **Wireless** menu. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: fragmentation threshold, RTS threshold, beacon interval, output power, preamble type, broadcast SSID, IAPP, and 802.11g protection.



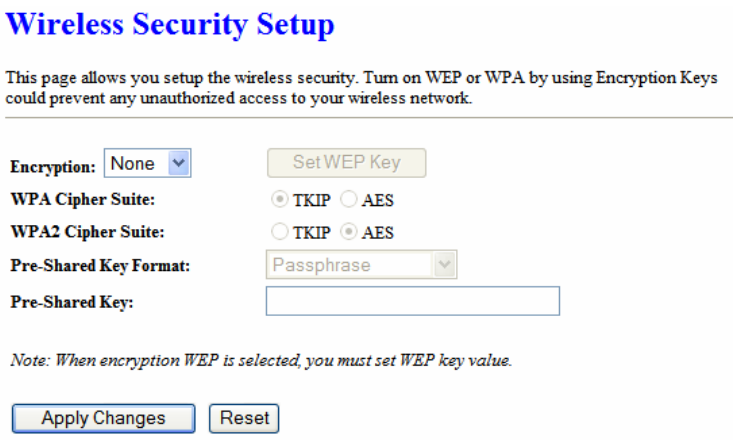
- **Authentication Type:** select an authentication method. Options available are **Open System**, **Shared Key** or **Auto**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- **Fragment Threshold**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Beacon Interval**: Beacons will be sent out to devices at the specified intervals. This value is measured in milliseconds (ms).
- **ACK Timeout**: You may specify a value for the acknowledge timeout.

- Data Rate: Select a data rate from the drop-down list. However, it is recommended to select **auto** for the best performance.
- **Data Rate**: If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Preamble Type**: For best performance, all devices on the wireless network should use the same preamble type. However, the wireless network will still function even though the wrong preamble type is used.
- **Transparent Bridge**: Can be Enabled/Disabled
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

Security

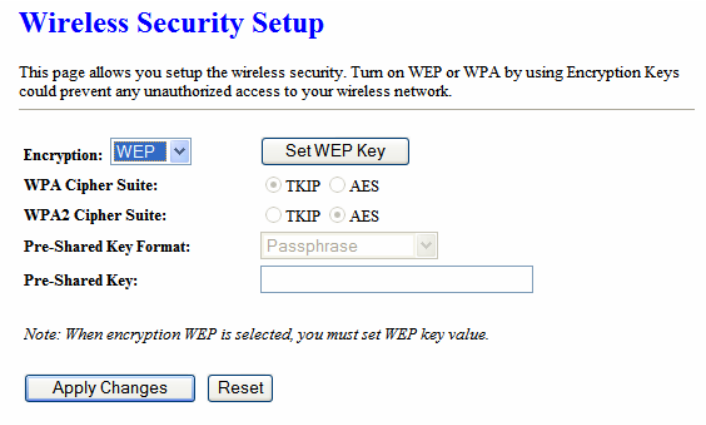
- Click on the **Security** link under the **Wireless** menu. On this page you can configure the authentication and encryption settings such as WEP, WPA, and 802.1x.

Encryption Disabled

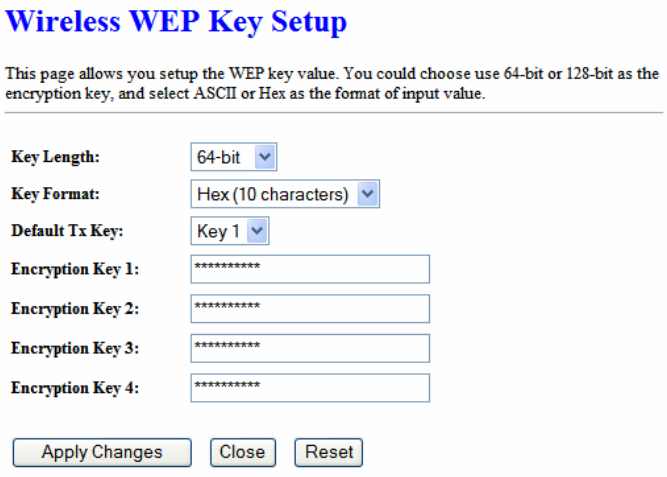


- **Encryption**: Select **None** from the drop-down list if your wireless network does not use any type of encryption.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

WEP 64-bit / 128-bit



- **Encryption**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WE P is an ac ronym for Wired Equivalent P rivacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- **Set WEP Key**: Click on this button to configure the WEP Key.

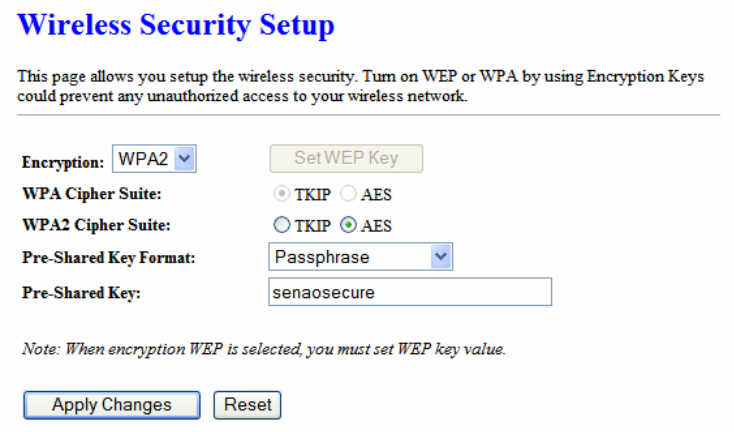


- **Key Length**: Select a **64-bit** or **128-bit** from the drop-down list.
- **Key Format:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128- bit keys require 26 characters. A hex key is def ined as a number between 0 through 9 and letter between A through F.
- **Default Tx Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Encryption Key 1-4:** You may enter four different WEP keys.

- Click on the **Apply Changes** button to confirm the changes and then click on the **Close** button to return to the pervious window.

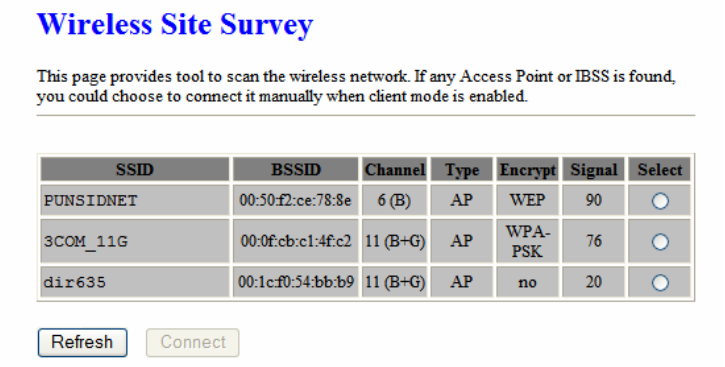
WPA / WPA2 / WPA2 Mixed Passphrase

- **Encryption**: Select **WPA**, **WPA2 or WPA2_Mixed** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve up on the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **WPA Authentication Mode**: Select the **Personal (Pre-Shared Key)** radio button.
- **WPA/WPA2**: Select **TKIP**, **AES** or both as the cipher suite.
- **Pre-Shared Key Format**: Select **Passphrase** from the drop-down list.
- **Pre-Shared Key**: Enter the pass phrase; this should be between 8 and 63 characters.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.



Wireless Site Survey

- Clic k **Refresh** to see the WLAN AP's that was detected with modest details of each of them listed.



Appendix A – FCC Interference Statement

Federal Communication Commission Interference Statement

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

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix B – IC Statement

IC statement

Operation is subject to the following two conditions:
This device may not cause interference and
This device must accept any interference, including interference that may cause undesired operation of the device.
This device has been designed to operate with an antenna having a maximum gain of 9 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

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

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:
Ce périphérique ne doit pas causer d'interférence et.
Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.