11b/g Wireless SOHO Router

User’s Manual

Version: 1.0

Table of Contents

Revision History

Version	**Date**	**Notes**
1.0	November 6, 2006	Initial Version

1 Introduction

The Wireless SOHO Router operates seamlessly in the 2.4 GHz frequency spectrum supporting the 802.11b (2.4GHz, 11Mbps) and the newer, faster 802.11g (2.4GHz, 54Mbpswireless standard.

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, this device can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA2/WPA/802.1x for powerful security authentication. The MAC addresses filter lets you select exactly which stations should have access to your network.

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

1.1 Features & Benefits

Features	Benefits
High Speed Data Rate Up to 54Mbps	Capable of handling heavy data payloads such as MPEG video streaming
IEEE 802.11b/g Compliant	Fully Interoperable with IEEE 802.11b/IEEE802.11g compliant devices with legacy protection
NAT Router	Multiple computer Internet Access, also act as natural firewall
WEP/WPA/WPA2/ IEEE 802.1x support	Securing network from malicious access
Hide SSID	Avoid free-rider stealing your bandwidth
DHCP	Simplify network configuration and management
MAC address filtering	Ensures secure network connection
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/LAN-to-WAN access control (allow/disallow), prevent users from access unwanted content
Firewall with SPI (Stateful Packet Inspection)	Prevent malicious access from Internet
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

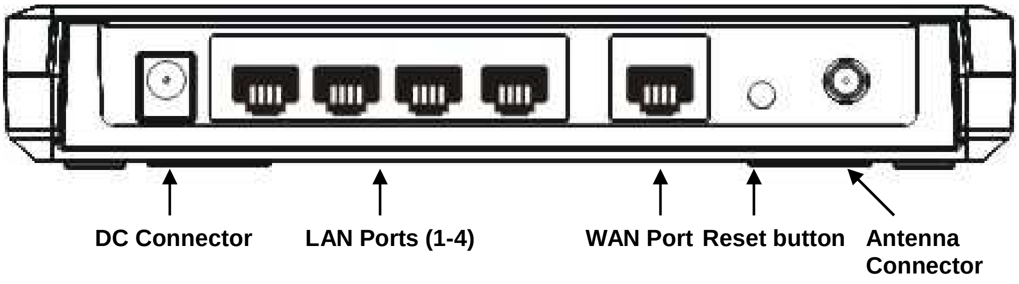
1.2 Package Contents

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.

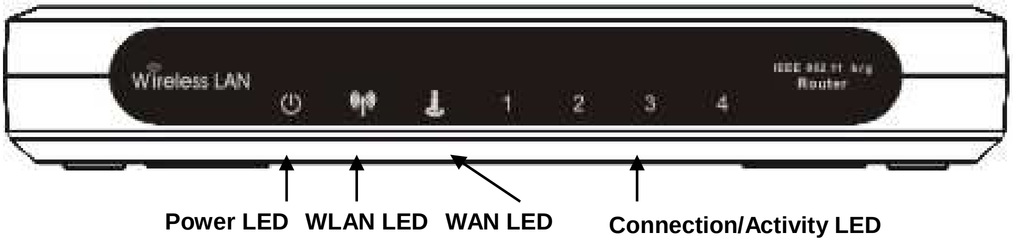
- One Wireless SOHO Router
- One Power Adapter
- One CAT5 UTP Cable
- One Omni-directional antenna
- One CD-ROM with User’s Manual

1.3 Wireless SOHO Router Description

Front Panel



Rear Panel



Step	Label	Description
1	LAN Ports (1 – 4)	Use an Ethernet cable to connect each port to a computer on your Local Area Network (LAN).
2	WAN Port	Use an Ethernet cable to connect this port to your WAN router.
3	DC Connector	Use the power cable and connect the adapter to the power socket on the wall, and the DC inlet into the DC connector.
4	Antenna Connector	Connect the omni-directional antenna to the SMA connector.
	Connection / Activity LED	This LED will light up once an Ethernet cable is connected to one of the LAN ports or the WAN port.

	WAN LED	This LED will light up once an Ethernet cable is connected to WAN (Internet) port.
	WLAN LED	This LED will light up once the RF (wireless LAN) feature is enabled
	Power LED	This LED will light up once the power cable is connected to the DC connector.

1.4 System Requirements

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

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

1.5 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.

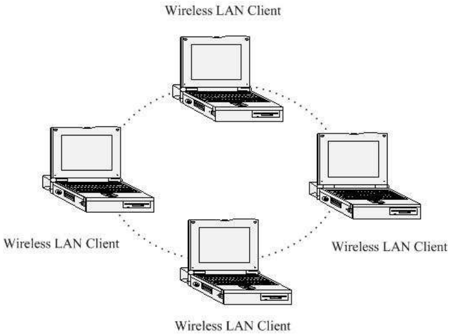
1.6 Network Configuration

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.

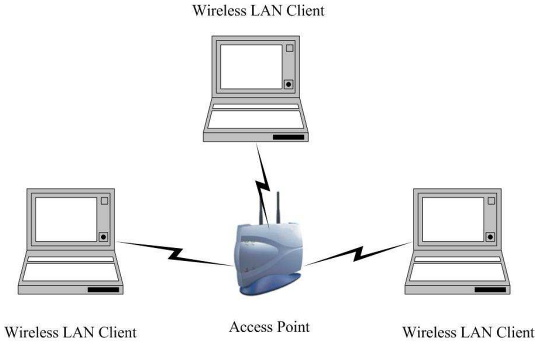
a) Ad-hoc (peer-to-peer) Mode

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.

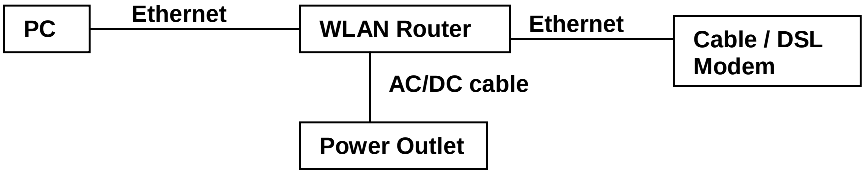


2 Understanding the Hardware

2.1 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 LAN port of the device and another end into your PC/Notebook.
3. Plug one end of another Ethernet cable to WAN port of the device and the other end into you cable/DSL modem (Internet)
4. 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.

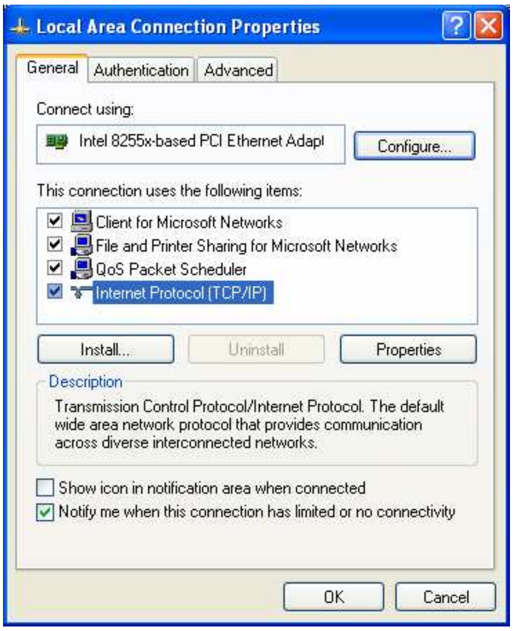
This diagram depicts the hardware configuration



2.2 IP Address Configuration

This device can be configured as a Bridge/Router or Access Point. The default IP address of the device is **192.168.1.1** 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.



Connect using:

Intel 8255x-based PCI Ethernet Adapl

This connection uses the following items:

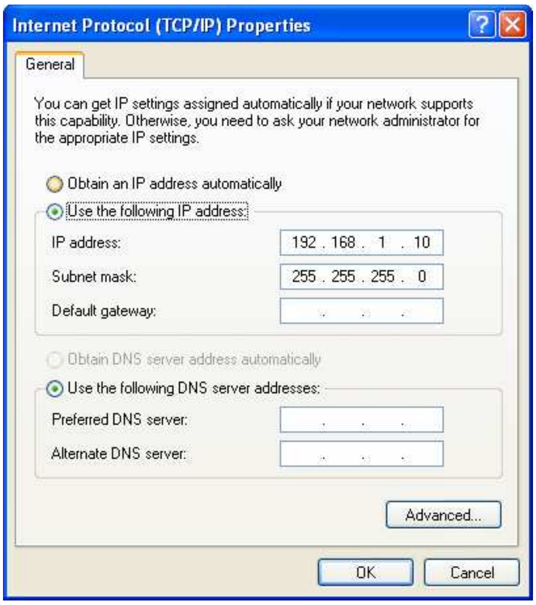
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

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.



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

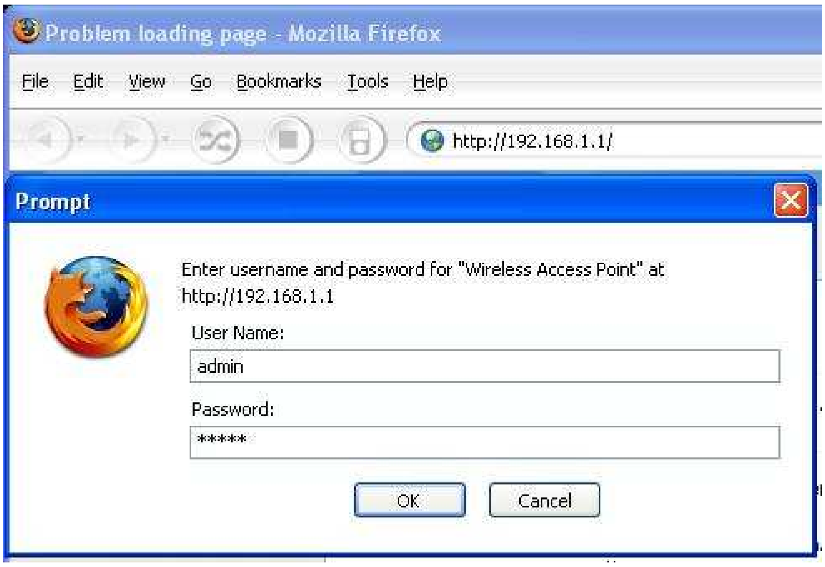
3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.
   For Example: Device IP address: 192.168.1.1
   PC IP address: 192.168.1.10
   PC subnet mask: 255.255.255.0

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

3 Web Configuration

3.1 Logging In

- To configure the device 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 device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Specify the **User Name** and **Password**. The User name and password are set to **admin** by default, click on the **Login** or **OK** button.


Problem loading page - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.1.1/
Prompt
OK
Cancel

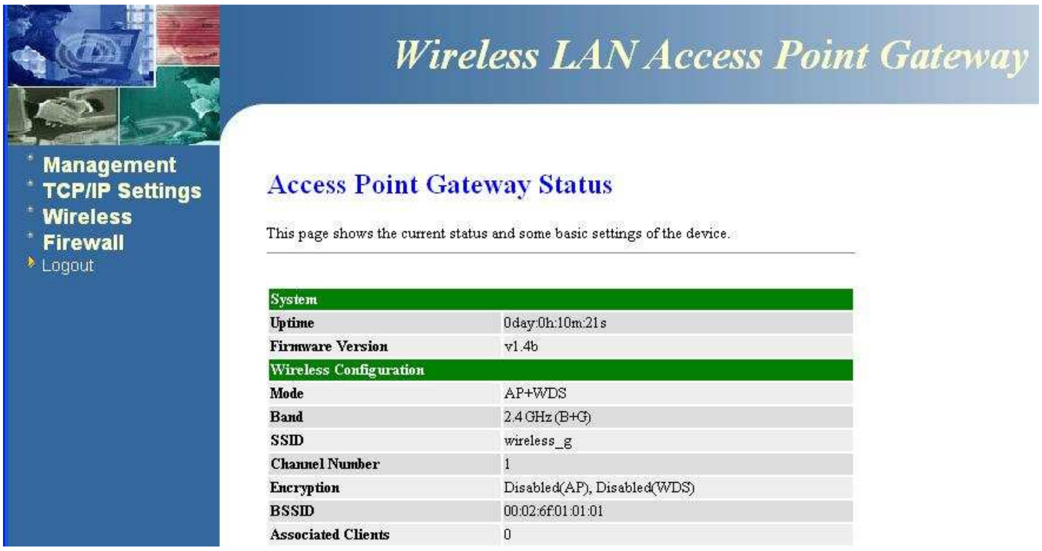
Enter username and password for "Wireless Access Point" at http://192.168.1.1

User Name: admin

Password: *****

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

1. **Management**: This menu includes the administrator settings, advanced wireless settings such as wireless MAC clone and RTS/fragmentation threshold. Also included are other system related settings such as firmware upgrade, reset to factory defaults, and system date/time configuration.
2. **TCIP/IP**: This menu includes the configuration of the LAN port and settings for the LAN IP, subnet mask, default gateway and DHCP client. Also, included are the settings for the WAN connection
3. **Wireless**: This menu includes the settings such as network type (infrastructure/ad-hoc), data rate, and security.
4. **Firewall**: This menu displays the security settings such as MAC filter, content filter, port blocking and DoS protection.

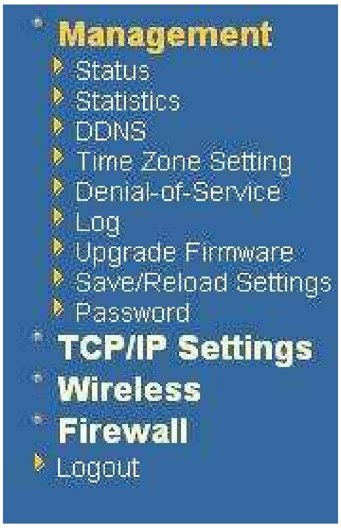


Access Point Gateway Status

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

System	
Uptime	0day:0h:10m:21s
Firmware Version	v1.4b
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	wireless_g
Channel Number	1
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:02:6f:01:01:01
Associated Clients	0

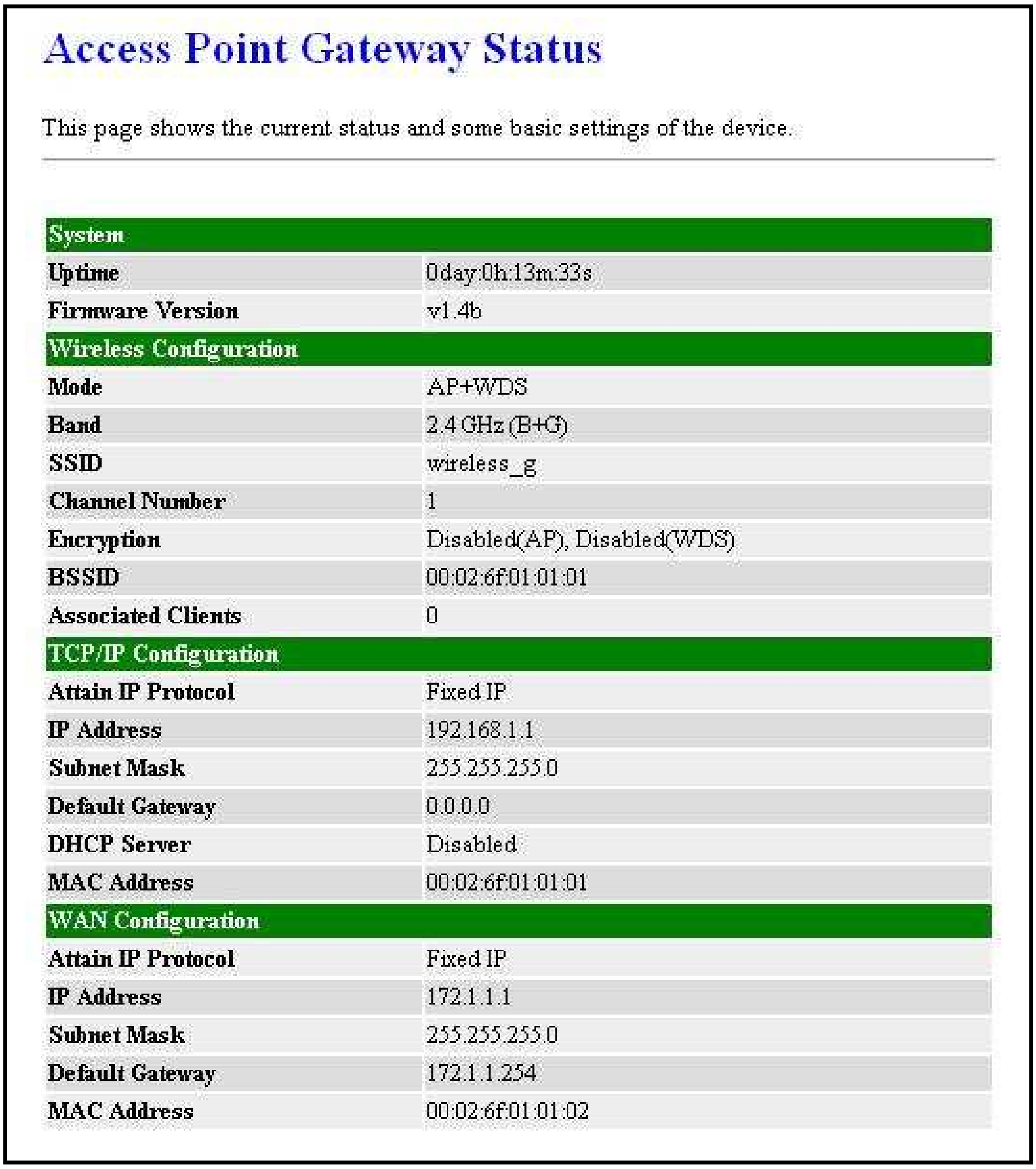
3.2 Management



- Click on the **Management** link on the navigation drop-down menu. You will then see nine options: Status, Statistics, DDNS, Time Zone Setting, Denial-of-Service, Log, Upgrade Firmware, Save/Reload Settings and Password. Each option is described below.

3.2.1 Status

- Click on the **Status** link under the **Management** menu. The device status page is also displayed once you have logged in. This includes details about the system uptime and firmware, LAN IP address and MAC address and the wireless settings such as the radio status, MAC address, SSID, RF channel, as well as WAN settings.



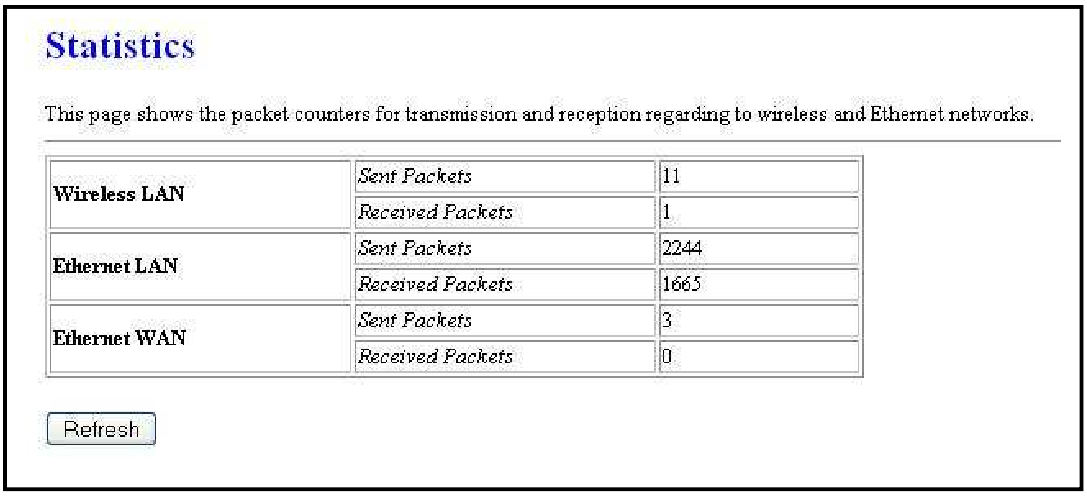
Access Point Gateway Status

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

System	
Uptime	0day:0h:13m:33s
Firmware Version	v1.4b
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	wireless_g
Channel Number	1
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:02:6f:01:01:01
Associated Clients	0
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 Server	Disabled
MAC Address	00:02:6f:01:01:01
WAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	172.1.1.1
Subnet Mask	255.255.255.0
Default Gateway	172.1.1.254
MAC Address	00:02:6f:01:01:02

3.2.2 Statistics

- Click on the **Statistics** link on the navigation drop-down menu. This page displays the transmitted and received packet statistics of the wired and wireless interface. Click on the Refresh button to refresh the statistics.



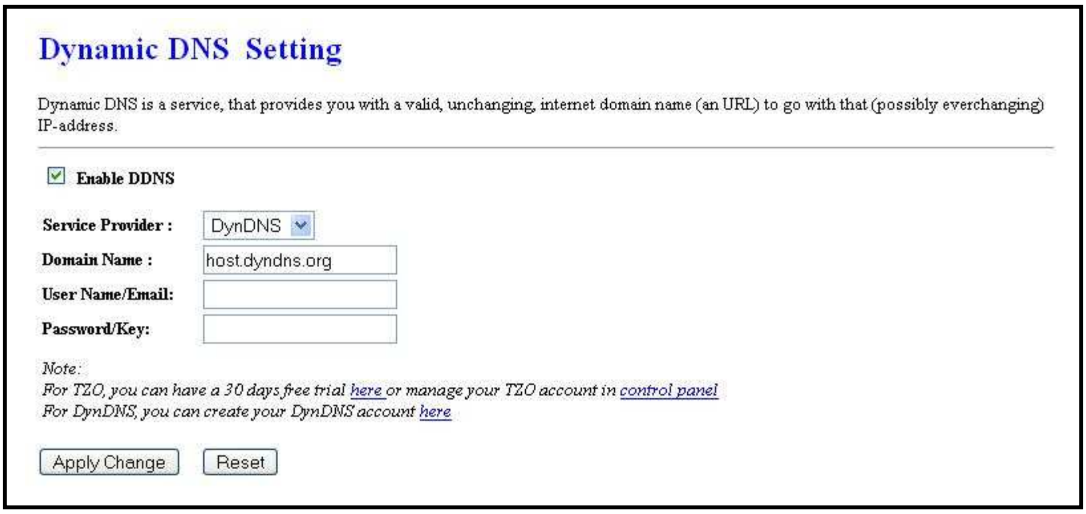
Statistics

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

Wireless LAN	*Sent Packets*	11
	Received Packets	1
Ethernet LAN	*Sent Packets*	2244
	Received Packets	1665
Ethernet WAN	*Sent Packets*	3
	Received Packets	0

3.2.3 Dynamic DNS

- Click on the **DDNS** link on the navigation drop-down menu. This feature allows you to maintain your Internet domain name even if you IP address supplied by your ISP is a dynamic one.



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 : host.dyndns.org

User Name/Email:

Password/Key:

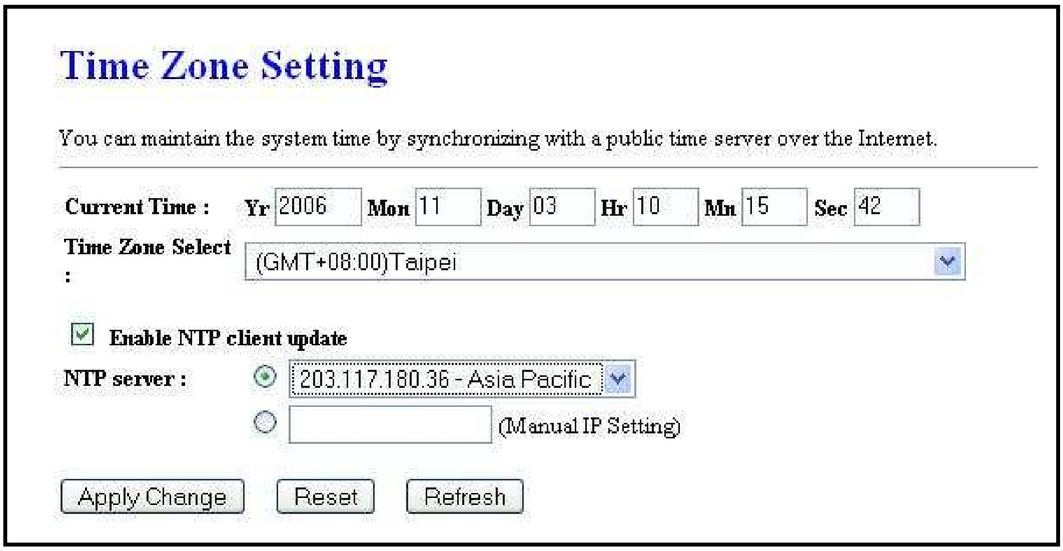
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

- **Enable DDNS**: Place a check in this box to enable the DDNS feature.
- **Service Provider**: Select a DDNS service provider from the drop-down list. DynDNS is a free service while TZO offers a 30 day free trial.
- **Domain Name**: Specify the website URL.
- **User Name**: Specify the user name for the DDNS service.
- **Password**: Specify the password for the DDNS service.

- Click on the **Apply Change** to save the changes or the **Reset** button to clear the fields.

3.2.4 Time Zone Setting

- Click on the **Time Zone Setting** link in the navigation 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 will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.



Time Zone Setting

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

Current Time : Yr 2006 Mon 11 Day 03 Hr 10 Mn 15 Sec 42

Time Zone Select : (GMT+08:00)Taipei

☑ Enable NTP client update

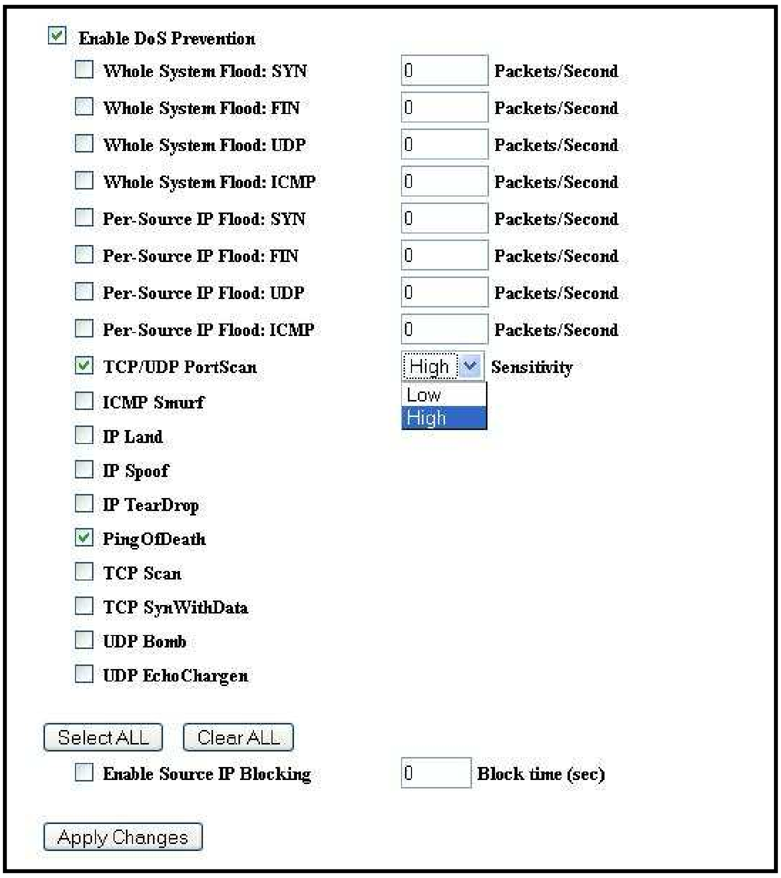
NTP server : ● 203.117.180.36 - Asia Pacific

○ (Manual IP Setting)

- **Current Time**: You may specify the date and time manually, if you choose not to use the Network Timing Protocol (NTP)
- **Time Zone**: Select a time zone from the drop-down list
- **Enable NTP client update**: Place a check in this box if you choose to enable the NTP client service.
- **NTP Server**: Select a service IP address from the drop-down list or manually assign the IP address of the NTP server.
- Click on the **Apply Change** to save the changes or the **Reset** button to clear the fields.

3.2.5 Denial of Service (DoS)

- Click on the **Denial of Service** link in the navigation menu. This is a security feature that blocks intrusions from the Internet that may disrupt the network service.

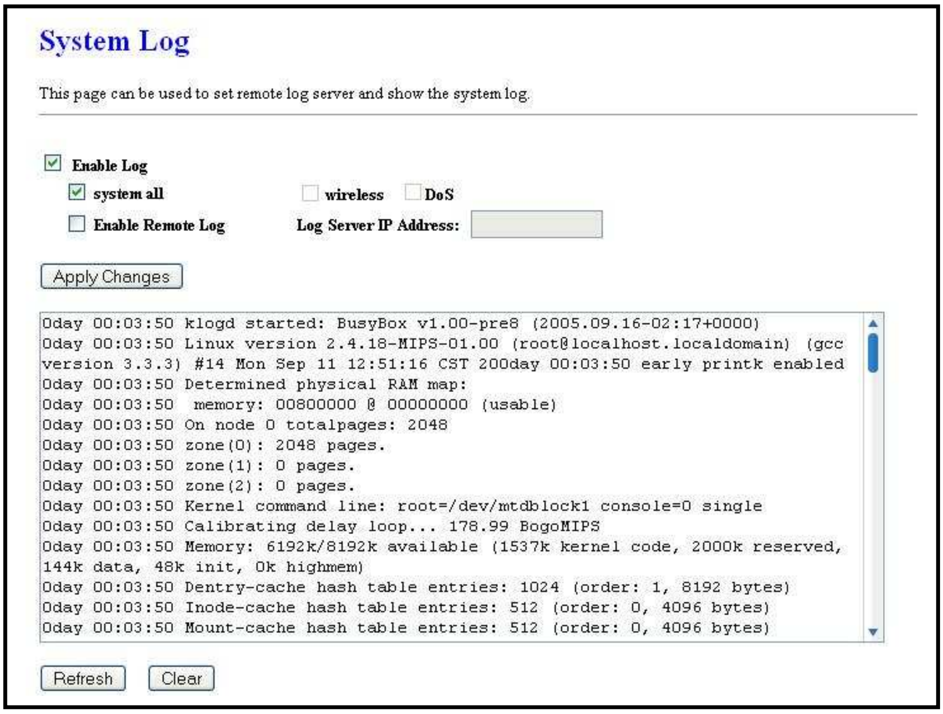


☑ Enable DoS Prevention		
☐ Whole System Flood: SYN	0	Packets/Second
☐ Whole System Flood: FIN	0	Packets/Second
☐ Whole System Flood: UDP	0	Packets/Second
☐ Whole System Flood: ICMP	0	Packets/Second
☐ Per-Source IP Flood: SYN	0	Packets/Second
☐ Per-Source IP Flood: FIN	0	Packets/Second
☐ Per-Source IP Flood: UDP	0	Packets/Second
☐ Per-Source IP Flood: ICMP	0	Packets/Second
☑ TCP/UDP PortScan	High	Sensitivity
☐ ICMP Smurf		
☐ IP Land		
☐ IP Spoof		
☐ IP TearDrop		
☑ PingOfDeath		
☐ TCP Scan		
☐ TCP SynWithData		
☐ UDP Bomb		
☐ UDP EchoChargen		
☐ Enable Source IP Blocking	0	Block time (sec)

- **Enable DoS protection**: Place a check in this box to enable the DoS features. You may also enable the other DoS protection features listed below. If you are not sure what the DoS protection feature is used for, it is recommend keeping the feature disabled.
- Click on the **Apply Change** to save the changes or the **Reset** button to clear the fields.

3.2.6 Log

- Click on the **Log** link on the navigation drop-down menu. Logs display 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.



System Log

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

☑ Enable Log

☑ system all □ wireless □ DoS

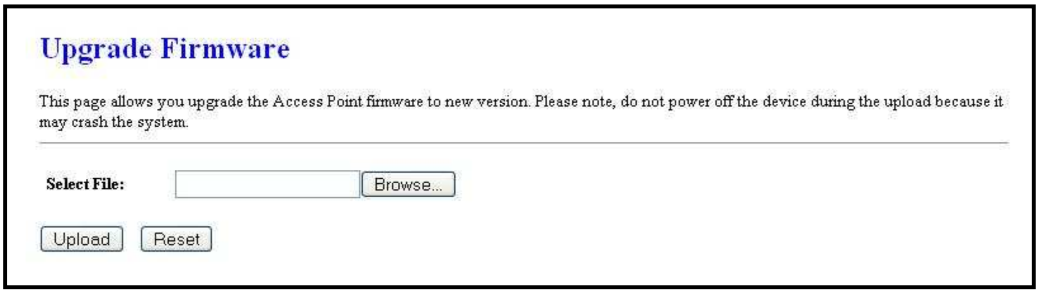
□ Enable Remote Log Log Server IP Address:

```
0day 00:03:50 klogd started: BusyBox v1.00-pre8 (2005.09.16-02:17+0000)
0day 00:03:50 Linux version 2.4.18-MIPS-01.00 (root@localhost.localdomain) (gcc
version 3.3.3) #14 Mon Sep 11 12:51:16 CST 200day 00:03:50 early printk enabled
0day 00:03:50 Determined physical RAM map:
0day 00:03:50  memory: 00800000 @ 00000000 (usable)
0day 00:03:50 On node 0 totalpages: 2048
0day 00:03:50 zone(0): 2048 pages.
0day 00:03:50 zone(1): 0 pages.
0day 00:03:50 zone(2): 0 pages.
0day 00:03:50 Kernel command line: root=/dev/mtdblock1 console=0 single
0day 00:03:50 Calibrating delay loop... 178.99 BogoMIPS
0day 00:03:50 Memory: 6192k/8192k available (1537k kernel code, 2000k reserved,
144k data, 48k init, 0k highmem)
0day 00:03:50 Dentry-cache hash table entries: 1024 (order: 1, 8192 bytes)
0day 00:03:50 Inode-cache hash table entries: 512 (order: 0, 4096 bytes)
0day 00:03:50 Mount-cache hash table entries: 512 (order: 0, 4096 bytes)
```

- **Enable Log**: Place a check in this box to enable the system logging feature. You may also click on **system all**, which will log wireless and DoS events.
- **Enable Remote Log**: You may also enable remote logging by placing a check in this box and then specifying the IP address of the log server.
- Click on the **Apply Change** to save the changes. You may also use the **Refresh** and **Clear** button.

3.2.7 Upgrade Firmware

- Click on the **Upgrade Firmware** link on the navigation drop-down menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance.



Upgrade Firmware

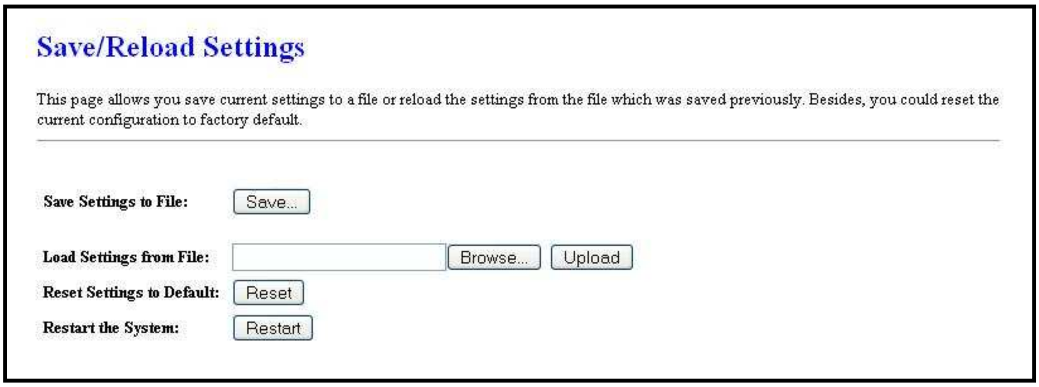
This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

- Ensure that you have downloaded the appropriate firmware from the vendor’s website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded using the wireless interface.
- Click on the **Browse** button to select the firmware and then click on the **Upload** button.

Note: Do not un-plug the device during this process. Some firmware upgrades may restore the configuration back to the factory default settings. Therefore you may need to restore a configuration from a file. Refer to the next two sections for details on saving and restoring configurations.

3.2.8 Save Configuration to a File

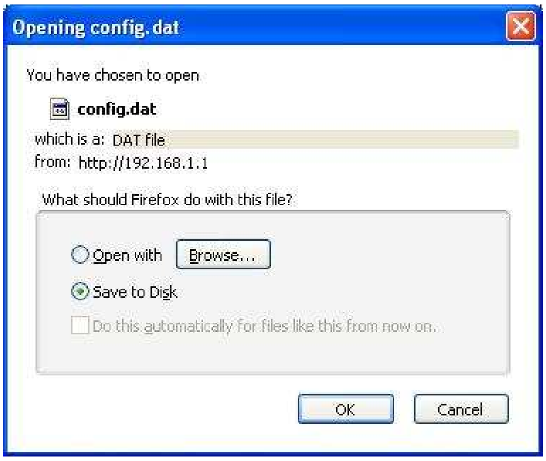
- Click on the **Save / Reload Settings** link on the navigation drop-down menu. This option allows you to save the current configuration of the device into a file. Click on the **Save** button to begin.



Save/Reload Settings

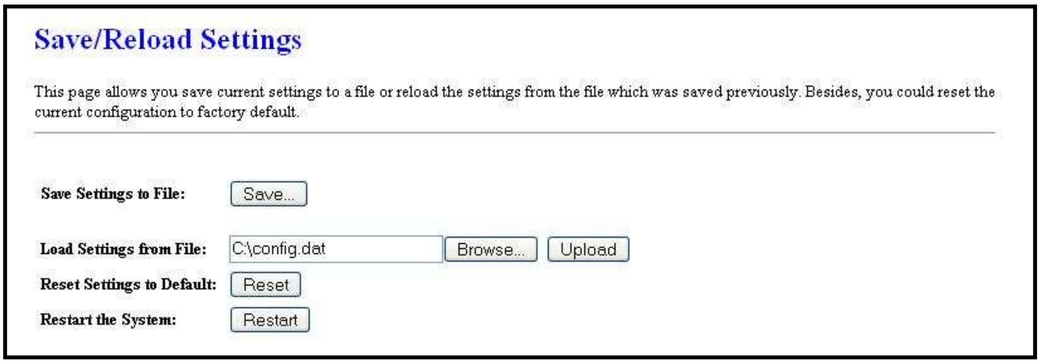
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

- Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.



3.2.9 Restore the Configuration from a File

- Click on the **Save / Reload Settings** link on the navigation drop-down menu. This option allows you to restore a backup configuration from a file to the device. Click on the **Browse** button to select the file and then click on **Upload** button.



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.

Load Settings from File: C:\config.dat

- A page indicating the reloading process will be displayed. Please wait while the system restarts and load the configuration page based on the pervious IP address.

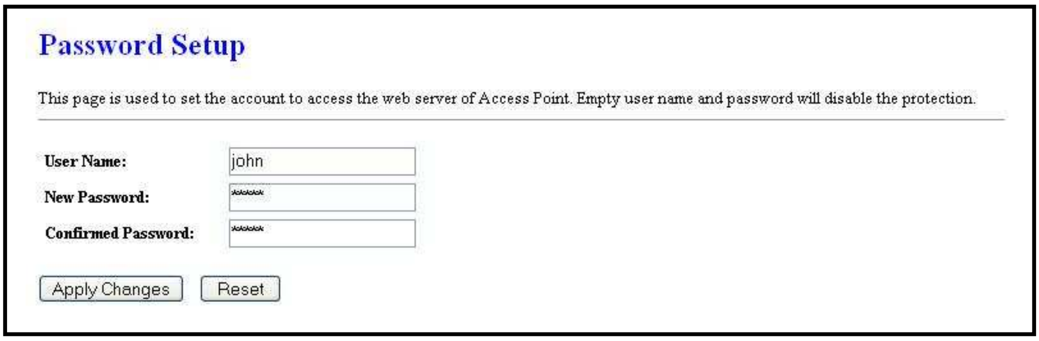
3.2.10 Restore Settings to Factory Defaults

- Click on the **Save / Reload Settings** link on the navigation drop-down menu. This option allows you to restore the configuration back to the factory default settings.
- Click on the **Reset** button to restore the configuration.
- Click on the **Restart** button to reboot the device using the current settings.

3.2.11 Administrator Settings

- Click on the **Password** link on the navigation drop-down menu. This page allows you to configure the password to access this device from the web-browser.

Note: The default user name and password of the device is **admin**



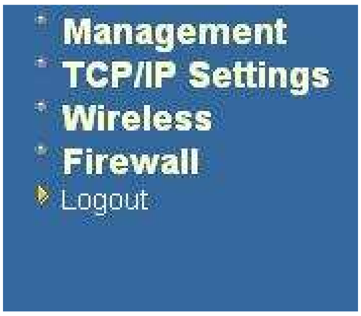
Password Setup

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

User Name:	john
New Password:	******
Confirmed Password:	******

- **User Name**: Specify a user name that will be used to connect to the device.
- **New Password**: Specify a password.
- **Confirmed Password**: Re-type the password.
- Click on the **Apply Change** to save the changes.

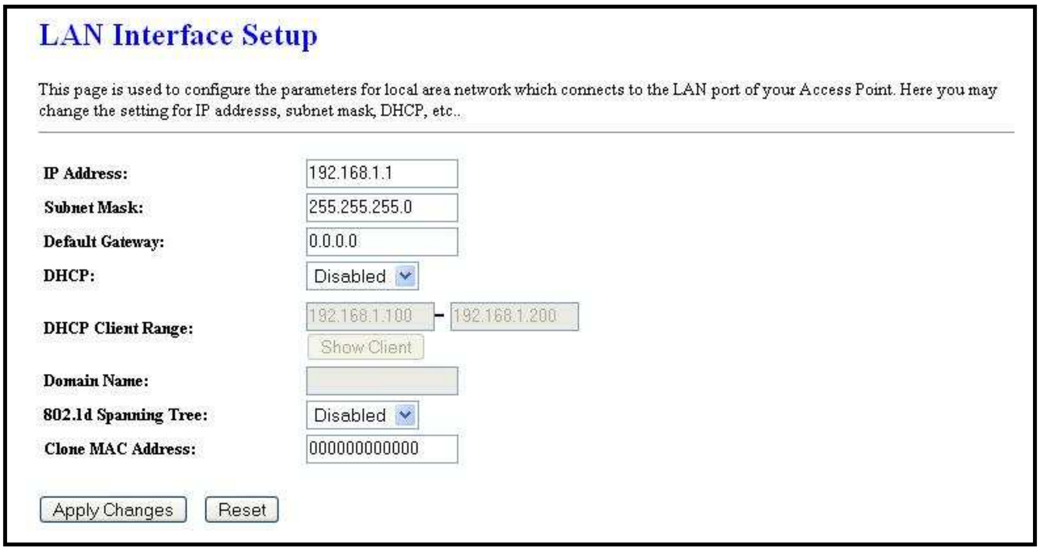
3.3 TCP/ IP Settings



- Click on the **TCP/IP Settings** link on the navigation drop-down menu. You will then see two options. You this menu you may configure the LAN IP address, DHCP, Static or Dynamic WAN IP and PPPoE. Each option is described below.

3.3.1 LAN Settings – Static IP

- Click on the **LAN** link on the navigation drop-down menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP server/client. This IP address is also used to access the web-based interface.



LAN Interface Setup

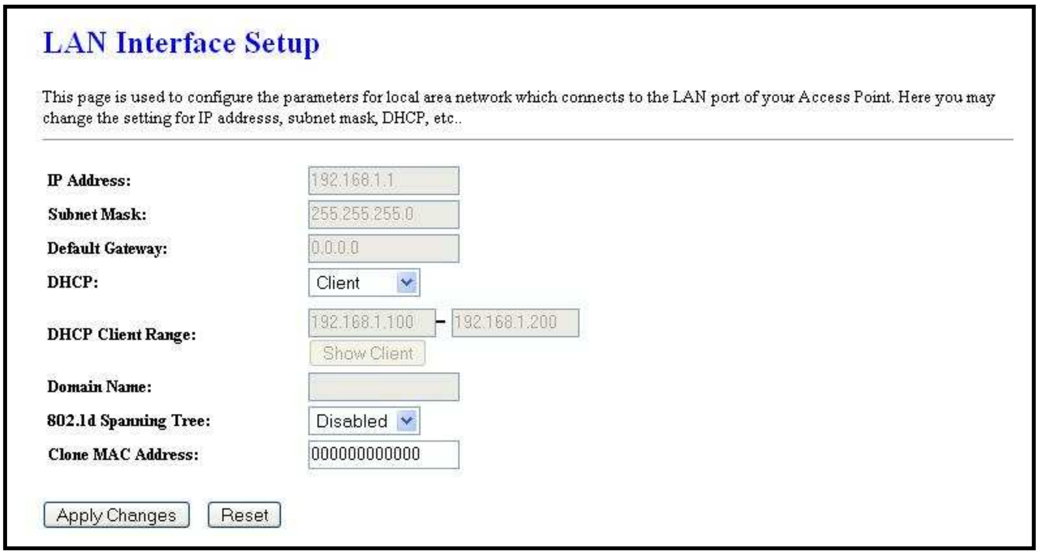
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Disabled
DHCP Client Range:	192.168.1.100 - 192.168.1.200
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

- **IP Address:** Enter an IP address for this device.
- **Subnet Mask:** Enter the subnet mask for this IP address.
- **Default Gateway:** Enter the IP address of the default gateway.
- **DHCP:** Since you have specified a static IP address, select Disabled from the drop-down list.
- **802.1d**: You may enable this option if you would like to use the spanning tree feature for bridging. (optional)
- **Clone MAC Address**: Specify a MAC address if you would like to use a different MAC address on this device. (optional)
- Click on the **Apply Change** to save the changes.
  Note: If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

3.3.2 LAN Settings – DHCP Client

- Click on the **LAN** link on the navigation drop-down menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP server/client. This IP address is also used to access the web-based interface.



LAN Interface Setup

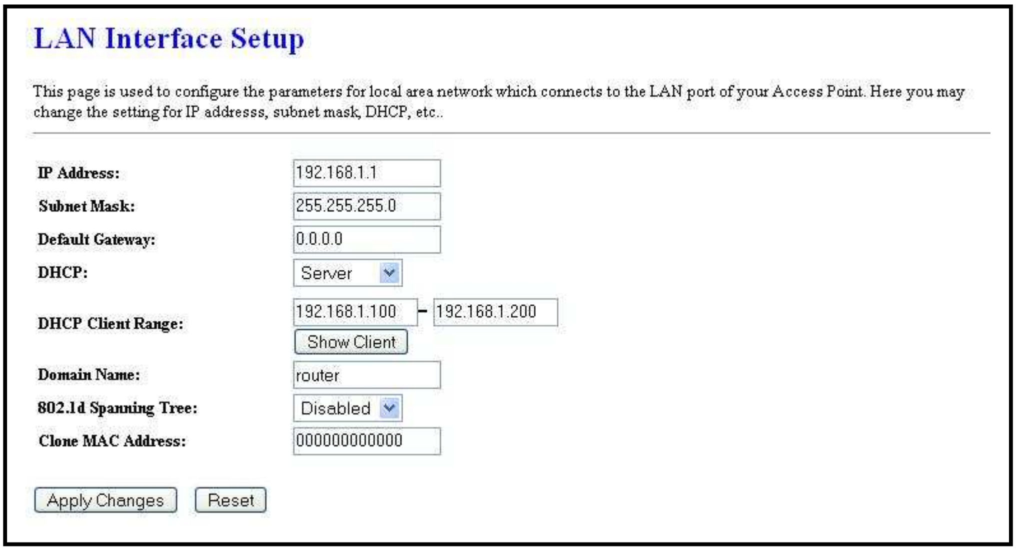
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Client
DHCP Client Range:	192.168.1.100 – 192.168.1.200 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

- **DHCP:** If you select **DHCP** radio button, you are not required to enter the rest of the fields, as the IP address will be provided to the device by the AP or DHCP server
- **802.1d**: You may enable this option if you would like to use the spanning tree feature for bridging. (optional)
- **Clone MAC Address**: Specify a MAC address if you would like to use a different MAC address on this device. (optional)
- Click on the **Apply Change** to save the changes.
- **Note**: If you change the IP address here, you may need to adjust your PC's network settings to access the network again. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to **DHCP** or **Obtain an IP address automatically**.

3.3.3 LAN Settings – DHCP Server

- Click on the **LAN** link on the navigation drop-down menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP server/client. DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN). In most situations, the router provides DHCP services, and you can leave this option disabled. However, if for any reason the router does not provide DHCP services, enable this option. The device's DHCP Server will then manage the IP addresses and other network configuration information for wireless clients associated with the AP. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to **DHCP** or **Obtain an IP address automatically**.



LAN Interface Setup

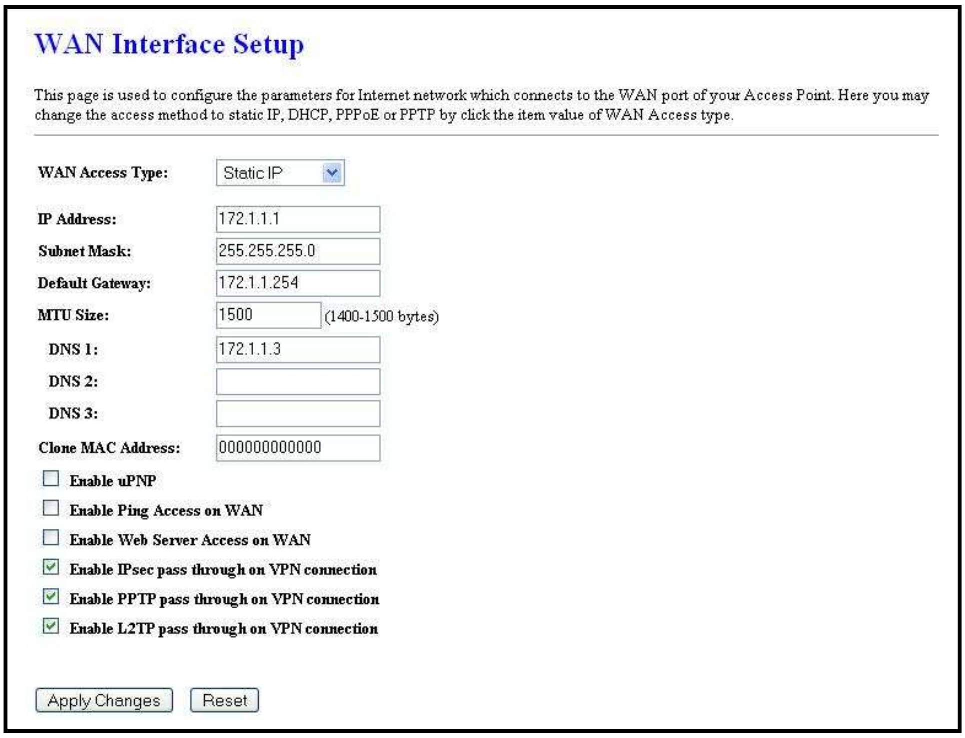
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address: 192.168.1.1
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: router
802.1d Spanning Tree: Disabled
Clone MAC Address: 000000000000

- **IP Address:** Enter an IP address for this device.
- **Subnet Mask:** Enter the subnet mask for this IP address.
- **Default Gateway:** Enter the IP address of the default gateway.
- **DHCP:** Select Server from the drop-down list. This device will act as a DHCP server and assign IP address to it clients.
- **DHCP Client Range:** You may limit the number of IP addresses that are distributed on the network. Specify a starting and ending range that is part of the same subnet.
- **Domain Name:** Specify a domain name for this device/network.
- **802.1d**: You may enable this option if you would like to use the spanning tree feature for bridging. (optional)
- **Clone MAC Address**: Specify a MAC address if you would like to use a different MAC address on this device. (optional)
- Click on the **Apply Change** to save the changes.
- **Note**: If you change the IP address here, you may need to adjust your PC's network settings to access the network again. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to **DHCP** or **Obtain an IP address automatically**.

3.3.4 WAN Settings – Static IP

- Click on the **WAN** link on the navigation drop-down menu. This feature allows you to configure the WAN interface using a static IP address, DHCP Client, PPoE, or PPTP.



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 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:	172.1.1.3
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

□ Enable uPNP

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

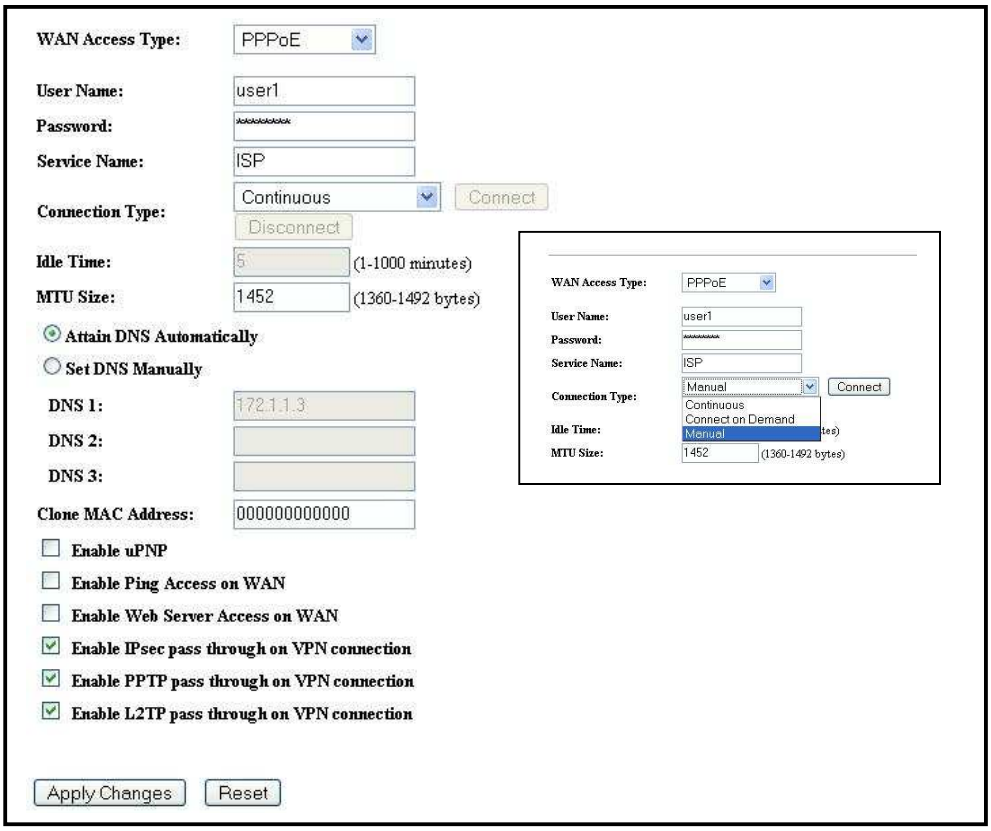
☑ Enable L2TP pass through on VPN connection

- **WAN Access Type:** Select **Static IP** from the drop-down list. This type of connection is used when your ISP has provided you a dedicated IP address.
- **IP Address:** Enter an IP address for this device, which is assigned by your ISP.
- **Subnet Mask:** Enter the subnet mask for this IP address, which is assigned by your ISP.
- **Default Gateway:** Enter the IP address of the default gateway, which is assigned by your ISP.
- **MTU:** You may adjust the Maximum Transmit Unit (MTU), however it is recommend that this value is set to the default: 1500 bytes
- **DNS 1-3:** Specify the IP address of the DNS server
- **Clone MAC Address**: Specify a MAC address if you would like to use a different MAC address on this device. (optional)
- **Enable uPNP**: Place a check in this box to enable UPnP. It is recommended to enable this feature as it's used by several applications.
- **Enable PING Access on WAN**: Place a check in this box if you would like the device to be pinged from the WAN side (ISP).
- **Enable Web Sever Access on WAN**: Place a check in this box if the static IP address if used for a web-server.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of IPsec packets on a VPN connection.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of PPTP packets on a VPN connection.

- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of L2TP packets on a VPN connection.
- Click on the **Apply Change** to save the changes.

3.3.5 WAN Settings – PPPoE

- Click on the **WAN** link on the navigation drop-down menu. This feature allows you to configure the WAN interface using a static IP address, DHCP Client, PPoE, or PPTP. A PPPoE service requires a user name and password to log into the Internet and is usually a DSL service.



WAN Access Type: PPPoE

User Name: user1

Password: *********

Service Name: ISP

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1452 (1360-1492 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 172.1.1.3

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

WAN Access Type: PPPoE

User Name: user1

Password: *******

Service Name: ISP

Connection Type: Manual

Idle Time: tes)

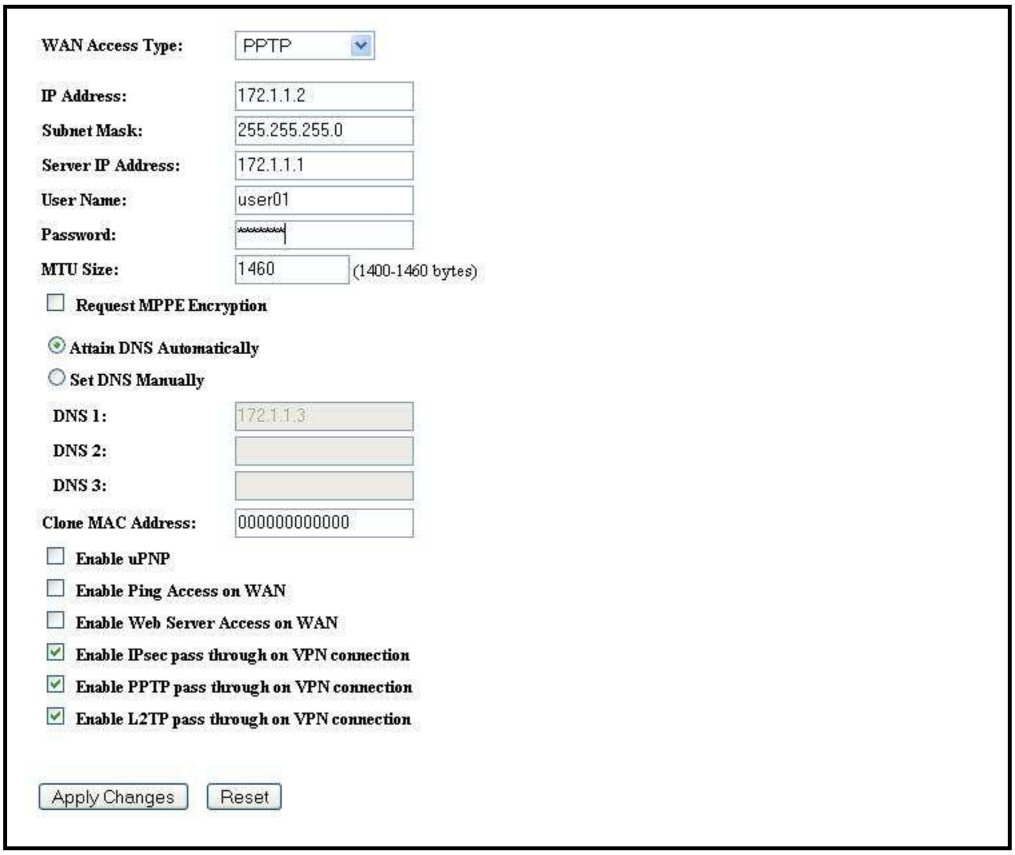
MTU Size: 1452 (1360-1492 bytes)

- **WAN Access Type:** Select PPPoE from the drop-down list. This type of connection is usually used for a DSL service and requires a username and password to connect.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP.
- **Service Name:** Specify the name of the ISP.
- **Connection Type:** Select **Continuous** (always online), **Connect on Demand** (connect to the ISP only when you click on a website), or **Manual** (connect to the ISP only when you click on a '**Connect**' button) from the drop-down list.
- **Idle Time:** The PPPoE service can automatically disconnect if the connection is idle. Specify the number of minutes after between 1 and 100.
- **DNS:** A PPoE service usually automatically assigns the DNS IP address, in case you need to assign it manually then click on the **Set DNS Manually** and fill in the fields.
- **MTU:** You may adjust the Maximum Transmit Unit (MTU), however it is recommend that this value is set to the default: 1500 bytes
- **DNS 1-3:** Specify the IP address of the DNS server

- **Clone MAC Address**: Specify a MAC address if you would like to use a different MAC address on this device. (optional)
- **Enable uPNP**: Place a check in this box to enable UPnP. It is recommended to enable this feature as it's used by several applications.
- **Enable PING Access on WAN**: Place a check in this box if you would like the device to be pinged from the WAN side (ISP).
- **Enable Web Sever Access on WAN**: Place a check in this box if the static IP address if used for a web-server.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of IPsec packets on a VPN connection.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of PPTP packets on a VPN connection.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of L2TP packets on a VPN connection.
- Click on the **Apply Change** to save the changes.

3.3.6 WAN Settings – PPTP

- Click on the **WAN** link on the navigation drop-down menu. This feature allows you to configure the WAN interface using a static IP address, DHCP Client, PPoE, or PPTP.



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: user01

Password: *******

MTU Size: 1460 (1400-1460 bytes)

□ Request MPPE Encryption

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 172.1.1.3

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

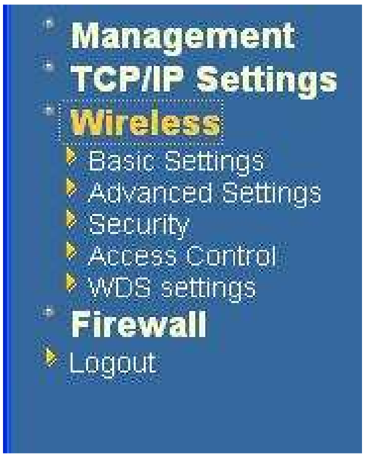
☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

- **WAN Access Type:** Select **PPTP** from the drop-down list. This type of connection is used when your ISP has provided you a dedicated IP address.
- **IP Address:** Enter an IP address for this device, which is assigned by your ISP.

- **Subnet Mask:** Enter the subnet mask for this IP address, which is assigned by your ISP.
- **Default Gateway:** Enter the IP address of the default gateway, which is assigned by your ISP.
- **MTU:** You may adjust the Maximum Transmit Unit (MTU), however it is recommend that this value is set to the default: 1500 bytes
- **DNS 1-3:** Specify the IP address of the DNS server
- **Clone MAC Address**: Specify a MAC address if you would like to use a different MAC address on this device. (optional)
- **Enable uPNP**: Place a check in this box to enable UPnP. It is recommended to enable this feature as it's used by several applications.
- **Enable PING Access on WAN**: Place a check in this box if you would like the device to be pinged from the WAN side (ISP).
- **Enable Web Sever Access on WAN**: Place a check in this box if the static IP address if used for a web-server.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of IPsec packets on a VPN connection.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of PPTP packets on a VPN connection.
- **Enable IPsec pass through on VPN connection**: Place a check in this box to enable the pass through of L2TP packets on a VPN connection.
- Click on the **Apply Change** to save the changes.

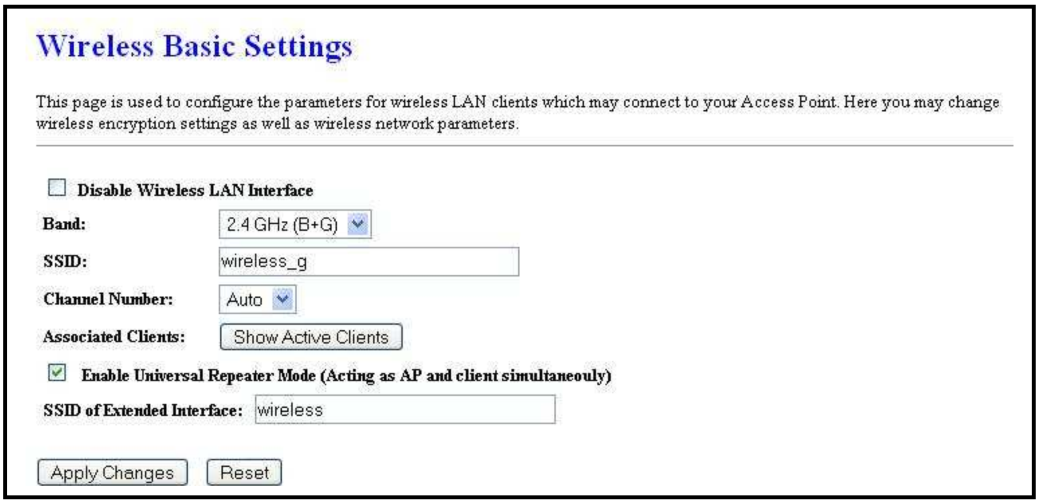
3.4 Wireless



- Click on the **TCP/IP Settings** link on the navigation drop-down menu. You will then see five options. Basic Settings, Advanced Settings, Security, Access Control, and WDS Settings. Each option is described below.

3.4.1 Wireless Basic Settings

- Click on the **Basic Settings** link on the navigation drop-down menu. These options allow you to enable/disable the wireless interface, switch between the 11b/g and 11b radio band and channel frequency



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)

SSID: wireless_g

Channel Number: Auto

Associated Clients: Show Active Clients

☑ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

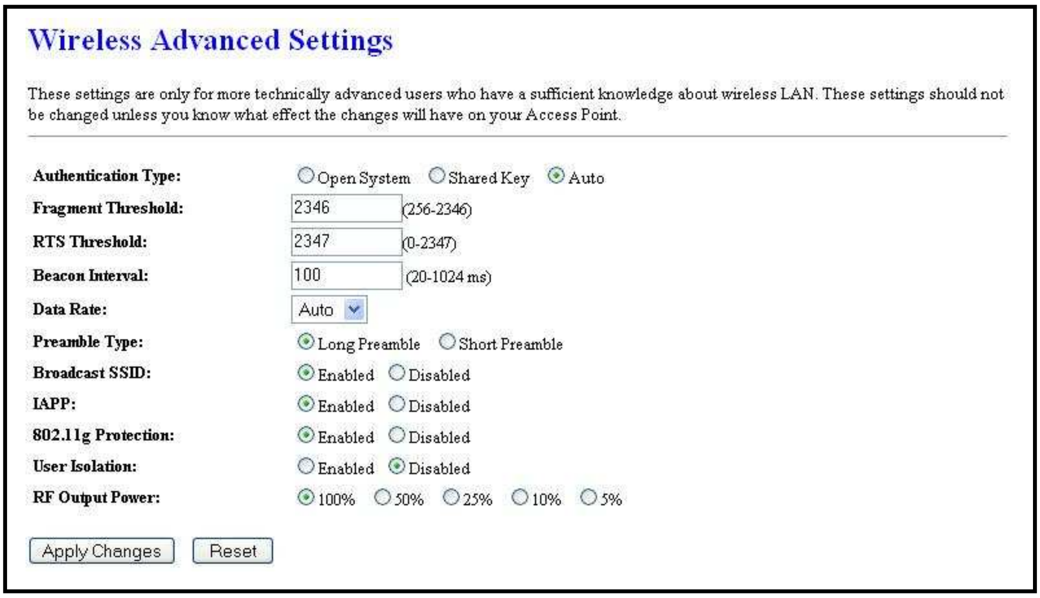
SSID of Extended Interface: wireless

- **Wireless Interface:** Place a check in this box to disable the wireless interface, it is enabled by default.
- **Band**: Select the IEEE 802.11 mode from the drop-down list. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select **802.11g** only instead of **2.4 GHz B+G** which will reduce the performance of the wireless network. You may also select **2.4GHz B or 2.4GHz G**
- **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.

- **Show Active Clients**: Click on this button to view a list of clients that are associated with this device.
- **Universal Repeater Mode**: This device can also perform as a repeater. To enable this, place a check in the box and then enter SSID.
- Click on the **Apply Change** to save the changes.

3.4.2 Wireless Advanced Settings

- Click on the **Advanced Settings** link on the navigation drop-down menu. These options allow you to configure the authentication type, fragment threshold, RTS threshold, beacon interval, and RF output power.



Wireless Advanced Settings

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

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
IAPP:	● Enabled ○ Disabled
802.11g Protection:	● Enabled ○ Disabled
User Isolation:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 50% ○ 25% ○ 10% ○ 5%

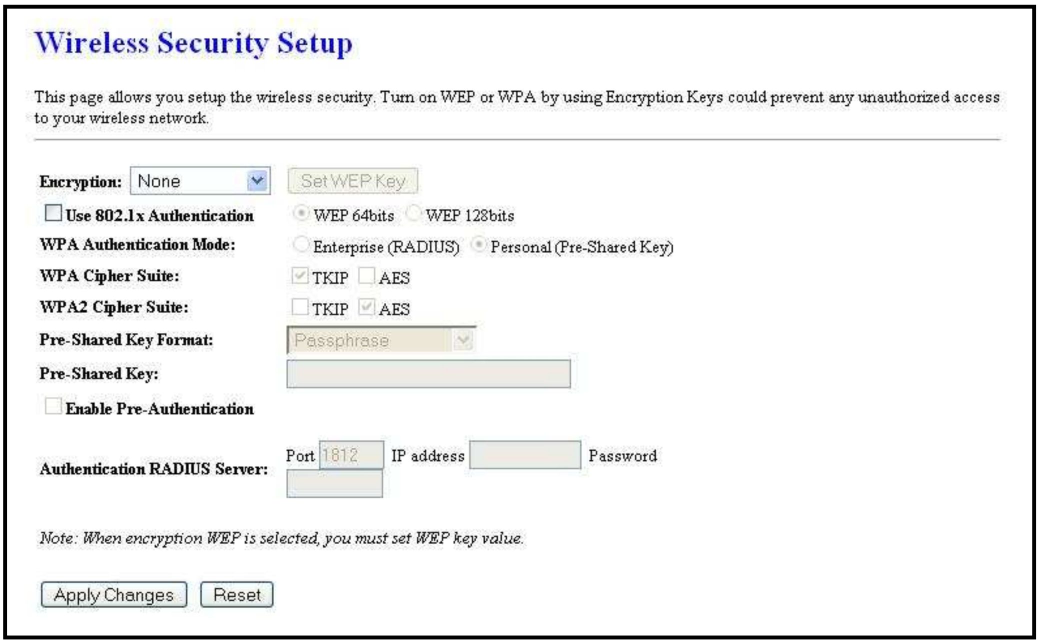
- **Authentication Type**: Select **Open System**, **Shared Key** or **Auto** as an authentication type. An **open system** allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. **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. Specify a value between 256 and 65535. The default value is 2346.
- **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. Specify a value between 1 and 2347. The default value is 2347.
- **Beacon Interval**: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1024. The default value is set to 100 milliseconds.
- **Data Rate**: Select a transmission rate from the drop-down list. It is recommended to use the **auto** option.

- Preamble Type: Select a **long** or **short** preamble type. For best performance, it is recommended that the preamble type of the AP matches that of the client.
- **Broadcast SSID**: Select **Enable** or **Disable**. This is the SSID broadcast feature. If you set this value to Visible, then the clients will be able to find this SSID on a site survey.
- **IAPP**: This is the Inter Access Point Protocol which simplifies roaming between Access Points. If you have setup several Access Point or a WDS system, it is recommended to **Enable** this feature.
- **802.11g protection**: If your network includes 11g and 11b clients, it's recommended to enable the feature as this will enhance the throughput rate in a mixed mode.
- **User Isolation**: Select **Enable** or **Disable**. This is a security feature that will isolate every client device that is associated with the device. One client device will not be able to view the other client device in a network neighborhood. If used in a public area such as a coffee shop, it is recommended to enable this feature in order to protect the privacy of the client devices.
- **RF Output Power**: You may control the output power of the device by selecting a value. This feature can be helpful in restricting the coverage area of the wireless network.
- Click on the **Apply Change** to save the changes.

3.4.3 Wireless Security

- To protect your privacy this mode supports several types of wireless security: WEP WPA, WPA2, and WPA-Mixed. WEP is the original wireless encryption standard. WPA provides a higher level of security. The following section describes the security configuration in detail.

3.4.3.1 Wireless Security - Disabled



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 802.1x 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

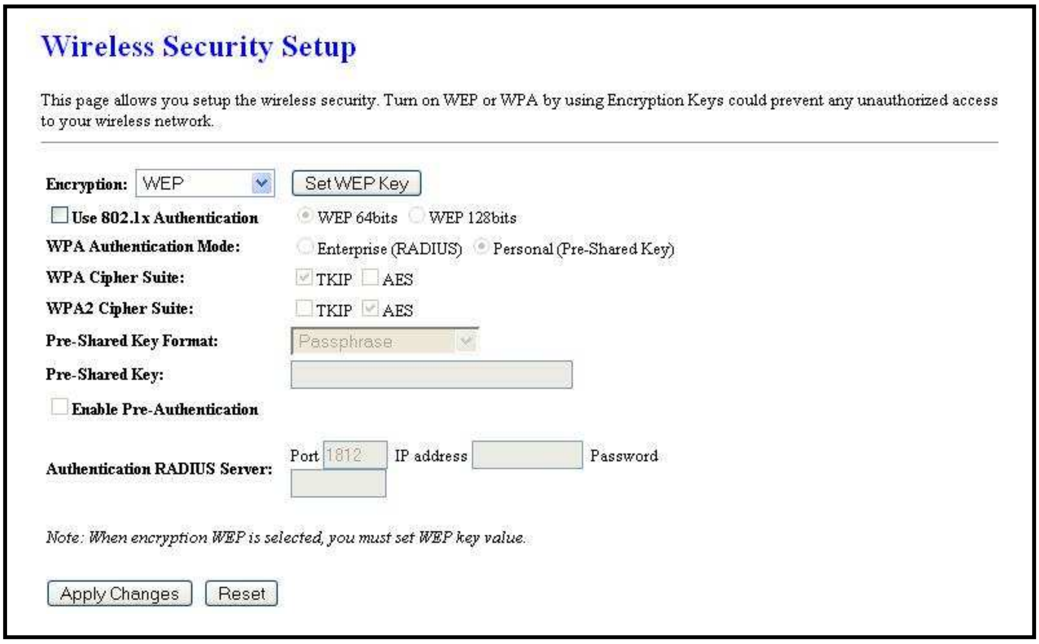
Note: When encryption WEP is selected, you must set WEP key value.

- **Encryption**: Select **None** from the drop-down list in order to disable wireless security.

- Click on the **Apply Change** to save the changes.

3.4.4 Wireless Security - WEP

- Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the 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: WEP

□ 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

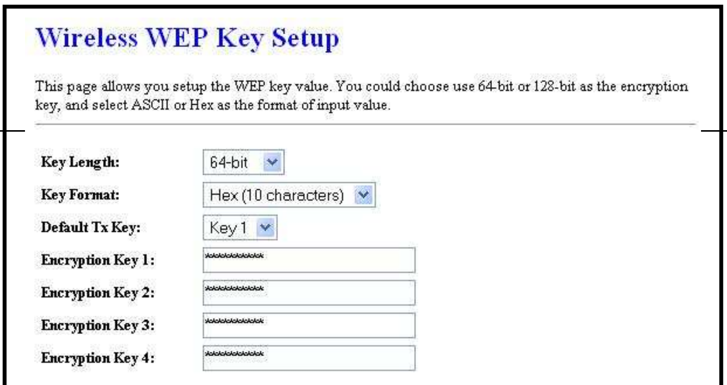
Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

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

- **Encryption**: Select **WEP** from the drop-down list in order to enable WEP security and then click on the **Set WEP key** button.



Wireless WEP Key Setup

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

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: **********

Encryption Key 2: **********

Encryption Key 3: **********

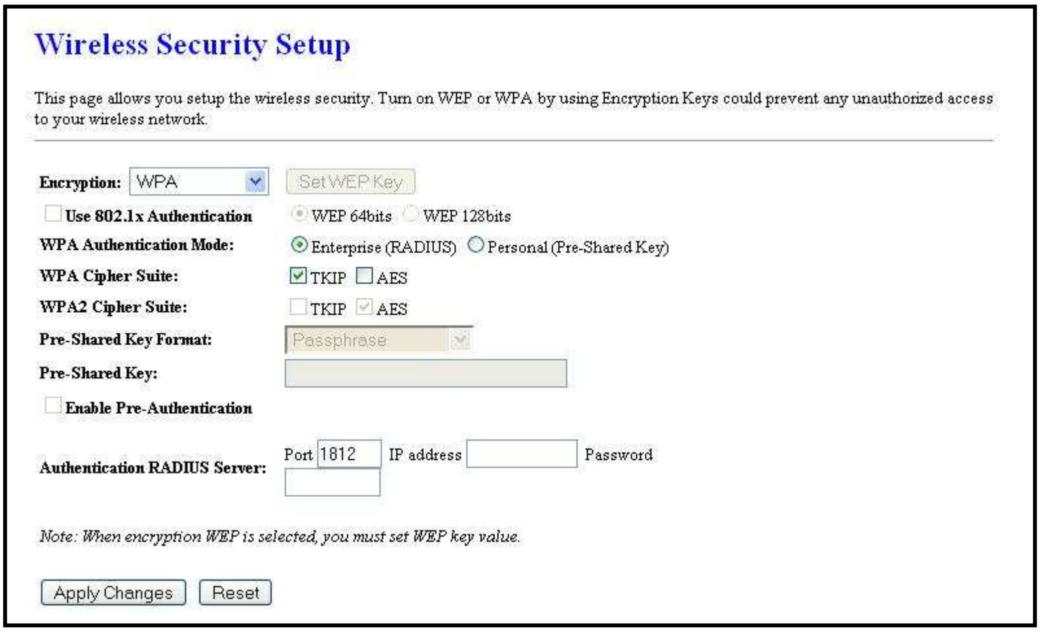
Encryption Key 4: **********

.

- **Key Length**: Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **Key Format:** Select a key format such as HEX or ASCII from the drop-down list.
- **Encryption Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- Click on the **Apply Change** to save the changes.

3.4.5 Wireless Security – WPA / WPA2-Mixed

- Select **WPA** or **WPA2-Mixed** from the drop-down list if your wireless network uses WPA 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.



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: WPA | Set WEP Key

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

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

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

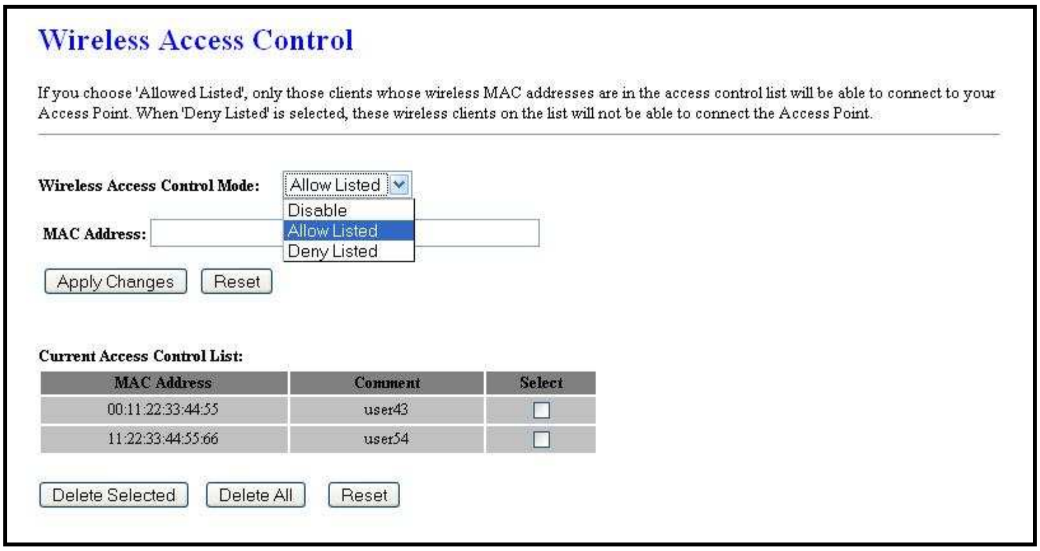
Note: When encryption WEP is selected, you must set WEP key value.

- **Encryption**: Select **WPA** or **WPA2-Mixed** from the drop-down list in order to enable WPA security.

- **WPA Authentication Mode**: Select **Enterprise (Radius)** or **Personal (Pre-Shared Key)**. If you select **Enterprise (radius)** then the pass key is located on the RADIUS server, however, if you select **Personal (Pre-Shared Key)** then you may assign a key on this configuration page.
- **WPA / WPA2 Cipher Suite**: Select **TKIP** or **AES** as the cipher suite. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. The device negotiates the cipher type with the access point, and uses AES when available.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.
- **Authentication Radius Sever:** If you have selected Enterprise (Radius) as the authentication type then you must specify the RADIUS port number, IP address, and password.
- Click on the **Apply Change** to save the changes.

3.4.6 Wireless Access Control

- Click on the **Access Control** link on the navigation drop-down menu. The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.



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: Allow Listed

MAC Address:

Current Access Control List:

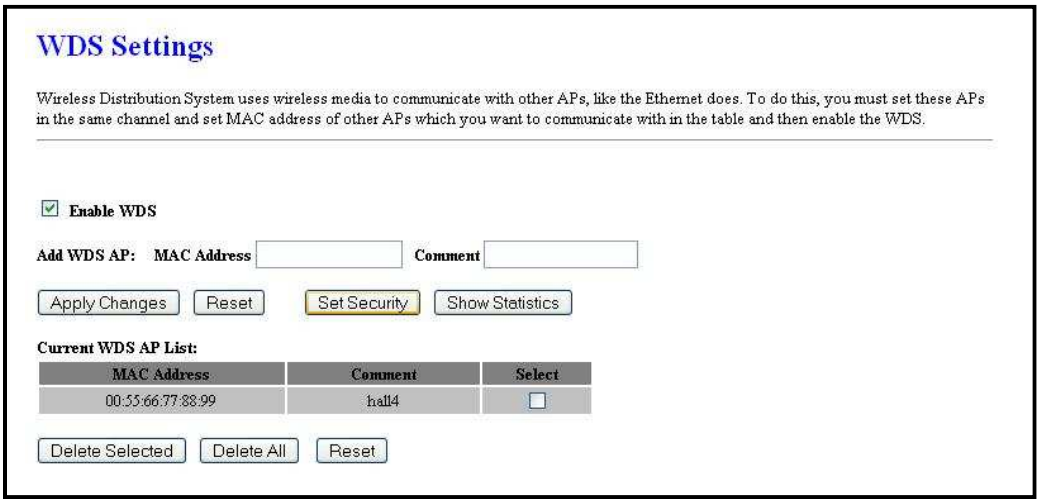
MAC Address	Comment	Select
00:11:22:33:44:55	user43	□
11:22:33:44:55:66	user54	□

- **Wireless Access Control Mode**: You may use this feature to filter the wireless clients. Select a filter setting from the drop-down list. When **allow listed** is selected; only computers with MAC addresses listed in the MAC Address List are granted network access. When **deny listed** is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.

- MAC Address: Specify the MAC address of the node which you would like to filter.
- Click on the **Apply Changes** to save the changes.

3.4.7 WDS (Wireless Distribution System)

Click on the **WDS** link on the navigation drop-down menu. The Wireless Distribution System feature configures this device as a repeater and therefore extends the range/coverage area of the wireless network.



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

Current WDS AP List:

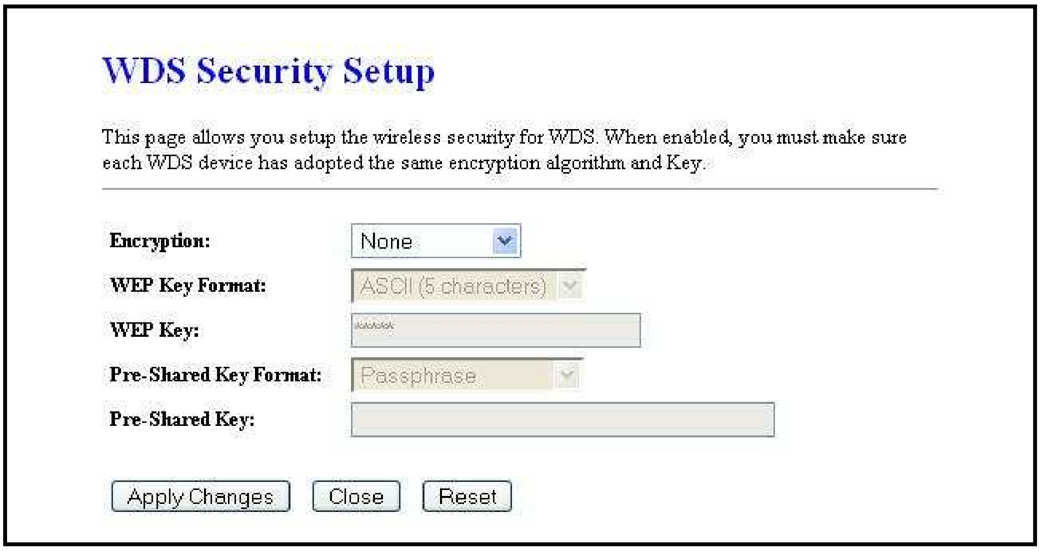
MAC Address	Comment	Select
00:55:66:77:88:99	hall4	□

- **Enable WDS**: When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links.
  A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel number.
- **Add WDS AP**: Specify one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.
- Click on the **Apply Changes** to save the changes.

3.4.7.1 WDS Security

- Click on the **Set Security** button to configure one of the security options for the WDS. Options available are WEP, WPA and WPA2, and you must configure the same security setting on each Access Point linked with this one.

3.4.7.1.1 WDS Security - None



WDS Security Setup

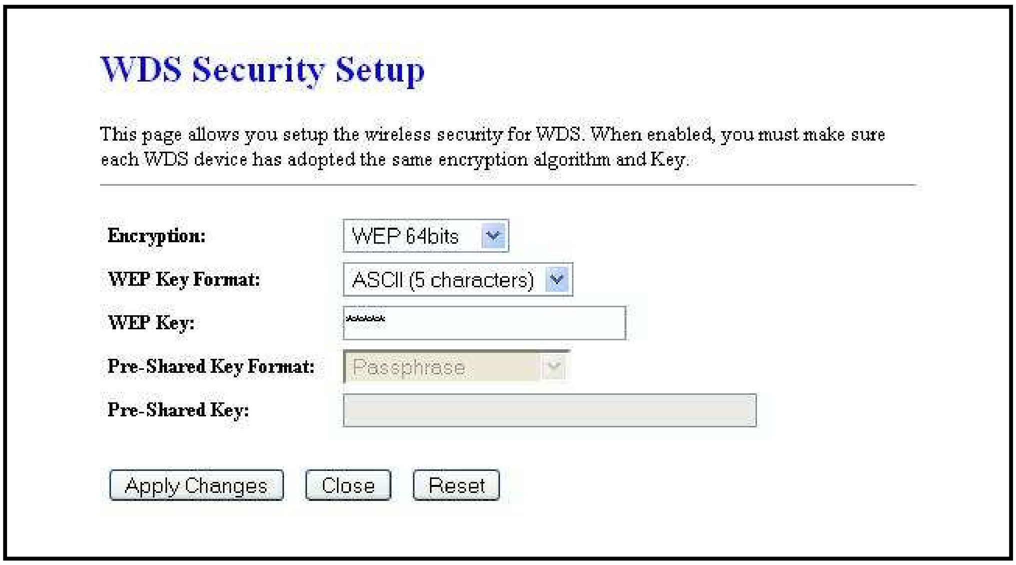
This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:	None
WEP Key Format:	ASCII (5 characters)
WEP Key:	*****
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

- **Encryption**: Select **None** from the drop-down list in order to disable wireless security.
- Click on the **Apply Changes** to save the changes.

3.4.7.1.2 WDS Security – WEP 64/128

- Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.



WDS Security Setup

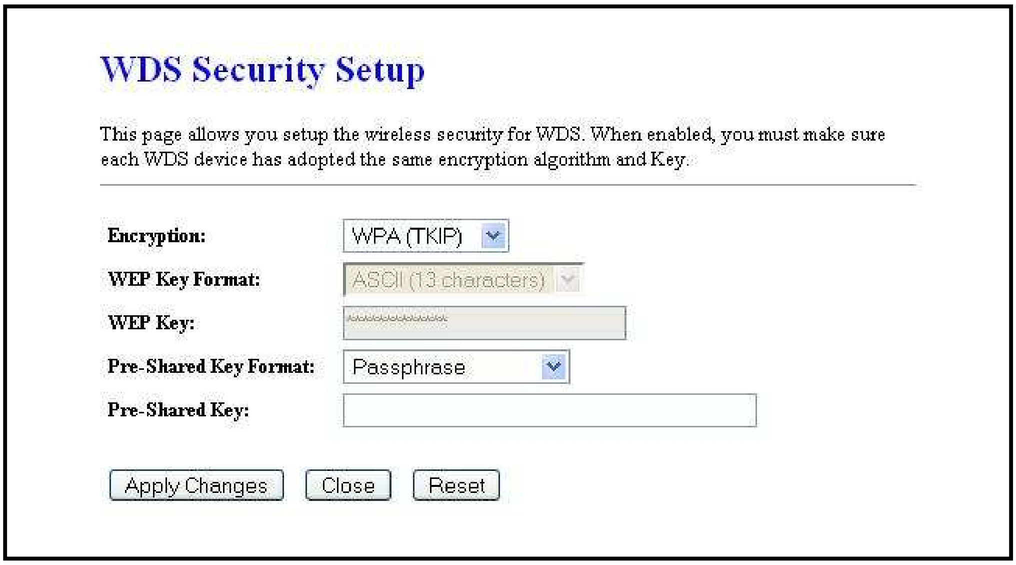
This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:	WEP 64bits
WEP Key Format:	ASCII (5 characters)
WEP Key:	*****
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

- **Encryption**: Select a **64-bit** or **128-bit** WEP encryption from the drop-down list.
- **Key Format:** Select a key format such as HEX or ASCII from the drop-down list.
- **WEP Key:** Specify the WEP key
- Click on the **Apply Changes** to save the changes and then click on the **Close** button.

3.4.7.1.3 WDS Security – WPA (TKIP), WPA2 (AES)

- Select **WPA** or **WPA2-Mixed** from the drop-down list if your wireless network uses WPA 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.



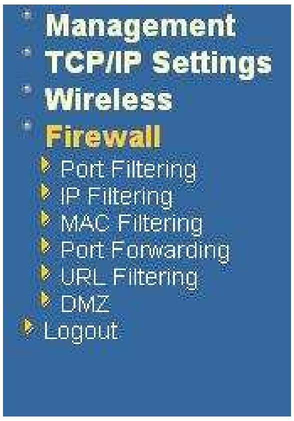
WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:	WPA (TKIP)
WEP Key Format:	ASCII (13 characters)
WEP Key:	*************
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

- **Encryption**: Select a **WPA** or **WPA2** encryption from the drop-down list. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. The device negotiates the cipher type with the access point, and uses AES when available.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

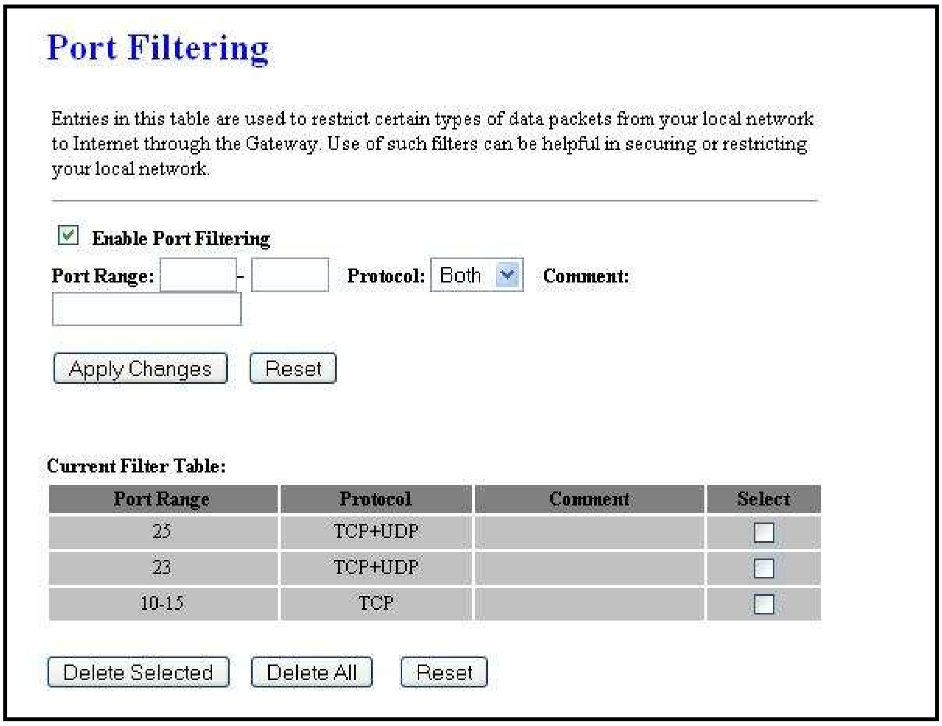
3.5 Firewall



- Click on the **Firewall** link on the navigation drop-down menu. You will then see six options. Port filtering, IP filtering, MAC filtering, Port filtering, URL filtering, DMZ. Each option is described below.

3.5.1 Port Filtering

- Select **Port Filtering** from the drop-down list This feature is used to restrict certain types of data packets on certain port numbers from your local network and the Internet. These filters can be used for securing and restricting your network.



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: ___ - ___ Protocol: Both Comment: ___

Apply Changes | Reset

Current Filter Table:

Port Range	Protocol	Comment	Select
25	TCP+UDP		□
23	TCP+UDP		□
10-15	TCP		□

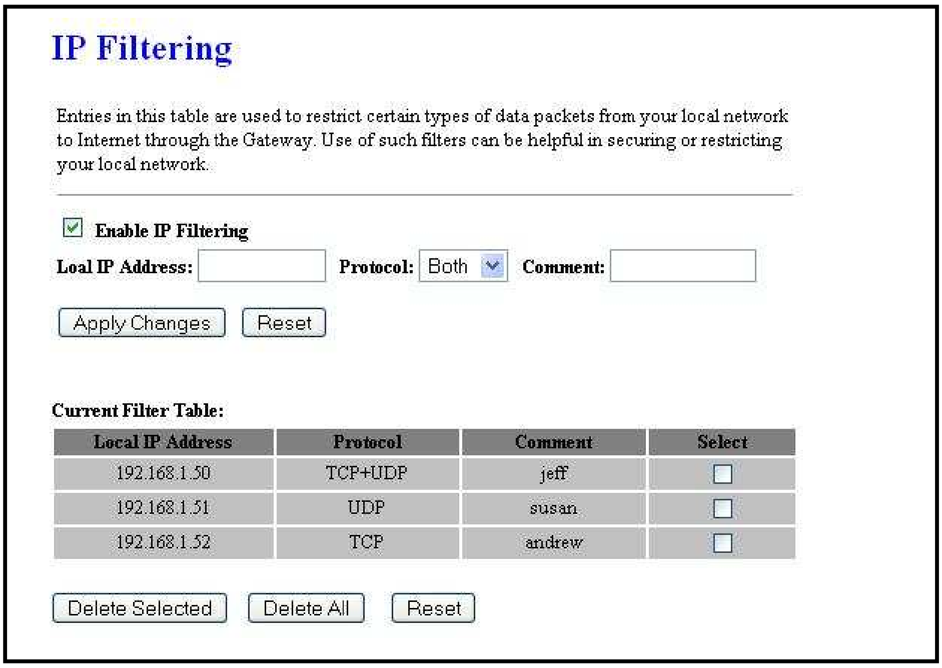
Delete Selected | Delete All | Reset

- **Enable Port Filtering:** Place a check in this box to enable this feature.
- **Port Range:** Enter the starting and ending port number. You may also enter a single port number if necessary.
- **Protocol:** Select a protocol from the drop-down list: **TCP**, **UDP**, or **Both**.
- **Comment:** You may add a comment to define the filter. (optional)
- Click on the **Apply Changes** button to add the filter to the table.

- You may place a check in the box on under the **Select** column and then click on **Delete Selected** to remove the selected entry. You may also click on **Delete All** to delete all the filtering entries.

3.5.2 IP Filtering

- Select **IP Filtering** from the drop-down list. This feature is used to restrict certain IP address from using certain protocols over the Internet. These filters can be used for securing and restricting your network.



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: ____ Protocol: Both Comment: ____

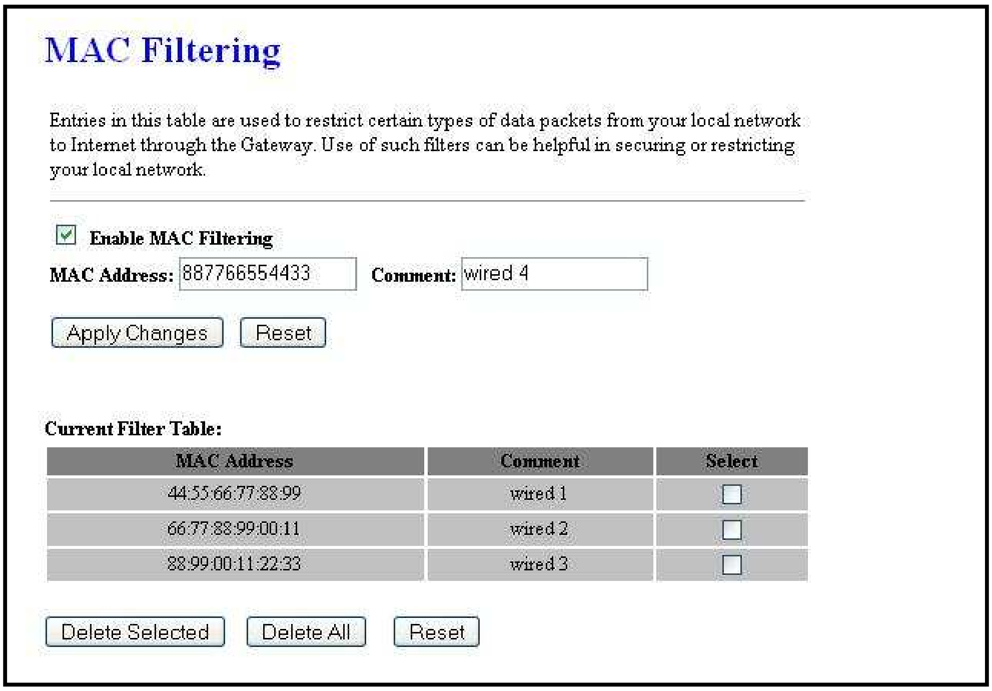
Current Filter Table:

Local IP Address	Protocol	Comment	Select
192.168.1.50	TCP+UDP	jeff	□
192.168.1.51	UDP	susan	□
192.168.1.52	TCP	andrew	□

- **Enable IP Filtering:** Place a check in this box to enable this feature.
- **Local IP Address:** Enter the IP address of the device on the local network.
- **Protocol:** Select a protocol from the drop-down list: **TCP**, **UDP**, or **Both**.
- **Comment:** You may add a comment to define the filter. (optional)
- Click on the **Apply Changes** button to add the filter to the table.
- You may place a check in the box on under the **Select** column and then click on **Delete Selected** to remove the selected entry. You may also click on **Delete All** to delete all the filtering entries.

3.5.3 MAC Filtering

- Select **MAC Filtering** from the drop-down list. This feature is used to restrict certain MAC address from accessing the Internet. These filters can be used for securing and restricting your network.



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: 887766554433 **Comment:** wired 4

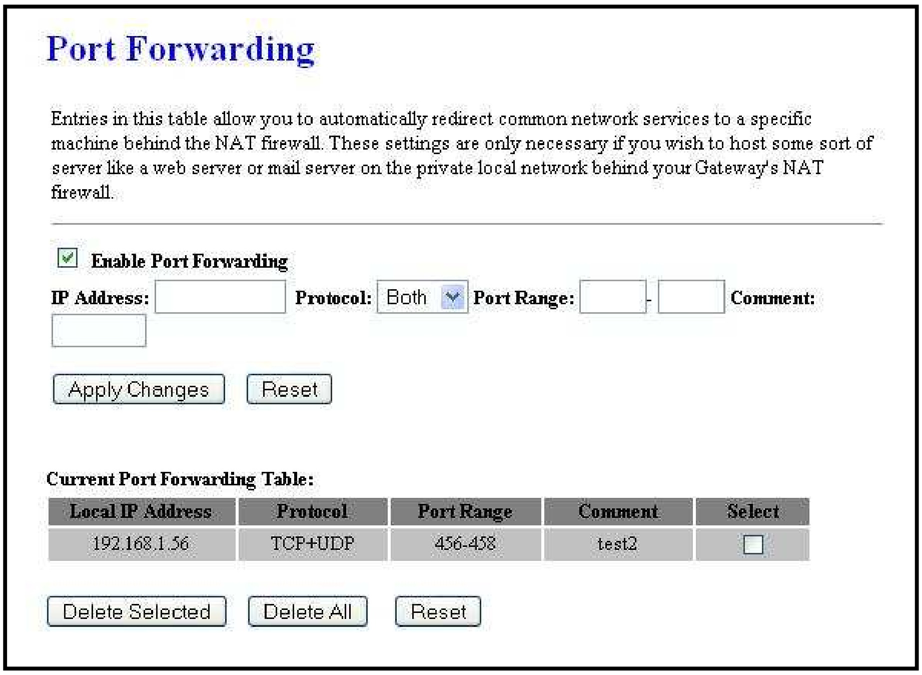
Current Filter Table:

MAC Address	Comment	Select
44:55:66:77:88:99	wired 1	□
66:77:88:99:00:11	wired 2	□
88:99:00:11:22:33	wired 3	□

- **Enable MAC Filtering:** Place a check in this box to enable this feature.
- **MAC Address:** Enter the MAC address of the device on the local network.
- **Comment:** You may add a comment to define the filter. (optional)
- Click on the **Apply Changes** button to add the filter to the table.
- You may place a check in the box on under the **Select** column and then click on **Delete Selected** to remove the selected entry. You may also click on **Delete All** to delete all the filtering entries.

3.5.4 Port Forwarding

- Select **Port Forwarding** from the drop-down list. This feature is used 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 email server on the private local network behind the NAT firewall.



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: Both Port Range: - Comment:

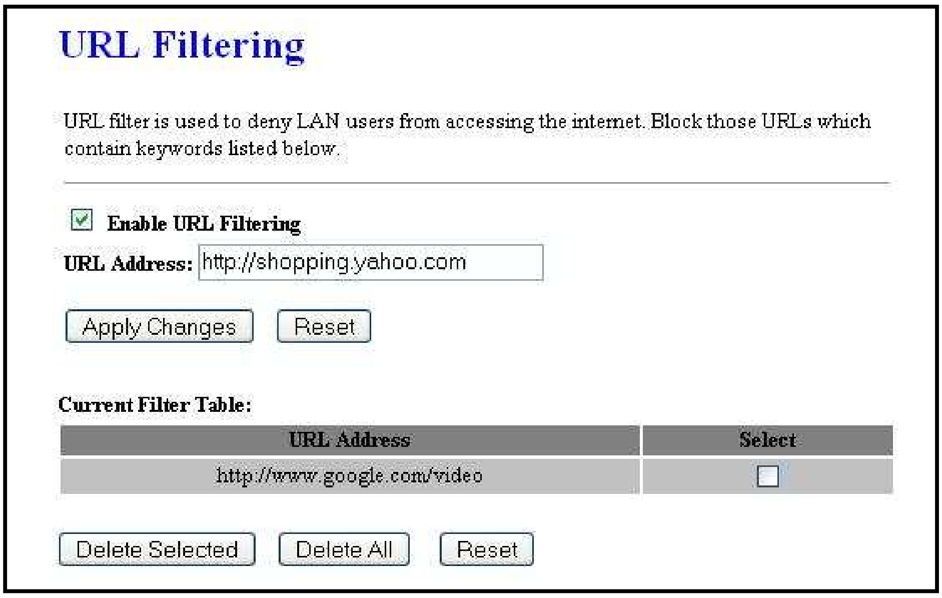
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.1.56	TCP+UDP	456-458	test2	□

- **Enable MAC Filtering:** Place a check in this box to enable this feature.
- **Local IP Address:** Enter the IP address of the device on the local network.
- **Protocol:** Select a protocol from the drop-down list: **TCP**, **UDP**, or **Both**.
- **Port Range:** Enter the starting and ending port number. You may also enter a single port number if necessary.
- **Comment:** You may add a comment to define the filter. (optional)
- Click on the **Apply Changes** button to add the filter to the table.
- You may place a check in the box on under the **Select** column and then click on **Delete Selected** to remove the selected entry. You may also click on **Delete All** to delete all the filtering entries.

3.5.5 URL Filtering

- Select **URL Filtering** from the drop-down list. 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.



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: http://shopping.yahoo.com

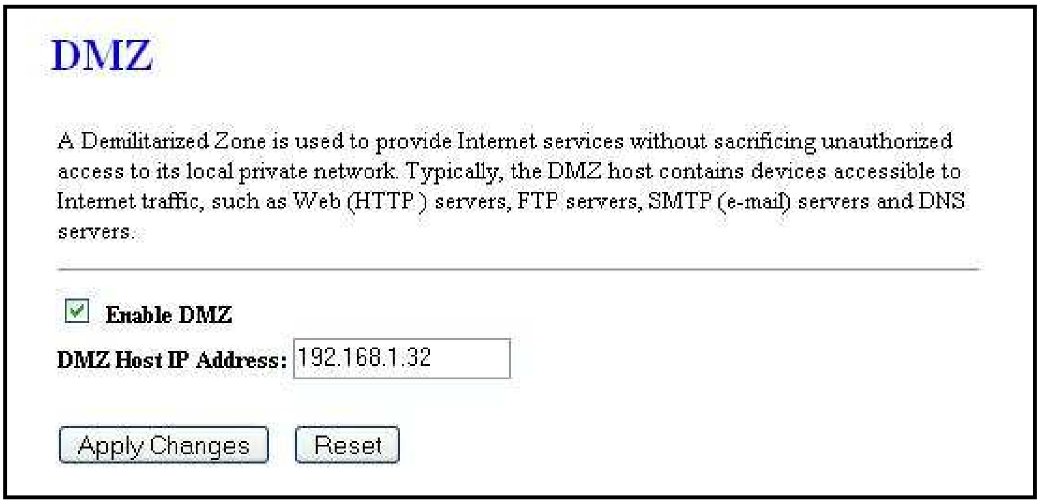
Current Filter Table:

URL Address	Select
http://www.google.com/video	□

- **Enable URL Filtering:** Place a check in this box to enable this feature.
- **URL Address:** Enter the URL of the website.
- Click on the **Apply Changes** button to add the filter to the table.
- You may place a check in the box on under the **Select** column and then click on **Delete Selected** to remove the selected entry. You may also click on **Delete All** to delete all the filtering entries.

3.5.6 DMZ

- Select **DMZ** from the drop-down list. 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, FTP, email and DNS servers.



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: 192.168.1.32

- **Enable DMZ:** Place a check in this box to enable this feature.
- **DMZ Host IP Address:** Enter the IP address of the DMZ host.
- Click on the **Apply Changes** button to add the filter to the table.

Appendix A – Specifications

Standards

IEEE802.11b/g, IEEE802.1x, IEEE802.3, IEEE802.3u

Wi-Fi data speed

IEEE 802.11b: 11/5.5/2/1Mbps
IEEE 802.11g: 54/48/36/24/18/12/9/6Mbps

Compatibility

IEEE 802.11g/ IEEE 802.11b

Power Requirements

Power Supply: 90 to 240 VDC ±10
(depends on different countries)
Device: 12 V/ 1.3A

Status LEDs

4*LAN : Link/Activity
WLAN : Link/Activity
Power : On/Off
Internet : On/Off/Activity

Regulation Certifications

FCC Part 15/UL, ETSI 300/328/CE

RF Information

Frequency Band

2.400-2.497GHz (Japan Band)
2.400-2.483GHz (North America, Europe Band)
2.455-2.475GHz (Spand Band)
2.446-2.483GHz (France Band

Media Access Protocol

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Modulation Technology

Orthogonal Frequency Division Multiplexing (OFDM)
DBPSK @ 1Mbps
DQPSK @2Mbps
CCK @ 5.5 & 11Mbps
BPSK @ 6 and 9 Mbps
QPSK @ 12 and 18 Mbps
16-QAM @ 24 and 36 Mbps
64-QAM @ 48 and 54 Mbps

Operating Channels

11 for North America, 14 for Japan, 13 for Europe,

Receive Sensitivity (Typical)

-88dBm @ 1Mbps
-70dBm @ 54Mbps

Available transmit power (Typical)

2.412~2.472G(IEEE802.11g)

18+-2 dBm min. @6 ~ 54Mbps

2.412~2.472G(IEEE802.11b)

18+-2 dBm. @1~11Mbps

Antenna Connector

Dipole antenna with reverse SMA connector

Networking

Topology

Ad-Hoc, Infrastructure

Operation Mode

AP/Router

Interface

LAN: Four 10/100Mbps Ethernet (RJ-45);
WAN: One 10/100Mbps Ethernet (RJ-45);
WLAN: 802.11b/g air interface

Security

IEEE802.1x Authenticator /RADIUS Client (EAPMD5/TLS/TTLS) Support in AP Mode
MAC address filtering
Hide SSID in beacons

Network Protocol

NAT/PAT
Internet connection management: FixedIP/DHCP/PPPoE/PPTP
DHCP (server/client)
Static route, RIP1/2
HTTP
UPnP
DDNS (Dynamic DNS)
PPTP/L2TP/IPsec (pass-thru)

Management

Web-based configuration (HTTP)

Firmware Upgrade

Upgrade firmware via web-browser

Physical

Dimensions (HxWxD)

16x10x4cm

Environmental

Temperature Range

Operating: -10℃ to 50℃ (14F to 122F)
Storage: -40℃to 70℃ (-40F to 158F)

Humidity (non-condensing)

5%~95% Typical

Appendix B – 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 instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1: 2001+A11: 2004
  Safety of Information Technology Equipment

- EN50385 : (2002)
- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
-
- EN 300 328 V1.6.1 (2004-11)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

- EN 301 489-17 V1.2.1 (2002-08) and EN 301 489-1 V1.6.1 (2005-09)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

cs Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele

	teistele asjakohastele sätetele.
en English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

CE 0560 (!)