User's Manual

N-WAP

802.11n Wireless Access Point

Copyright

The products and programs described in this User’s Manual are licensed products of Legrand, This User’s Manual contains proprietary information protected by copyright, and this User’s Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User’s Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Legrand.

Disclaimer

Legrand does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

Legrand has made every effort to ensure that this User’s Manual is accurate; Legrand disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User’s Manual is subject to change without notice and does not represent a commitment on the part of Legrand. Legrand assumes no responsibility for any inaccuracies that may be contained in this User’s Manual. Legrand makes no commitment to update or keep current the information in this User’s Manual, and reserves the right to make improvements to this User’s Manual and/or to the products described in this User’s Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to pro-vide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equip-ment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the inter-ference at his own expense.

FCC Caution

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

FCC Radiation Exposure Statement

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

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

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

CE mark Warning

The is a class B device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Trademarks

The Legrand logo is a trademark of Legrand Inc. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, their respective companies claim these designations as trademarks or registered trademarks.

Revision

User’s Manual for 802.11n Wireless Access Point:

Model: N-WAP

Rev: 1.0 (2011, July)

Part No. EM-N-WAP_v1

TABLE OF CONTENTS

Chapter 1
Introduction

Overview

Integrating the cutting edge of Internet Telephony and Access Point manufacturing experience, LEGRAND now introduces the latest member of LEGRAND Wireless Access Point family: the N-WAP.

The N-WAP provides not only high-performance Access Point (AP) function for flexible wireless communication.

With built-in IEEE 802.11b/g/n wireless network capability, the N-WAP allows any computer and wireless enabled network client connect to it without additional cabling. The 802.11n wireless capability gives users the highest speed of wireless experience ever. With an 802.11n compatible wireless adapter installed in your PC, the files can be transferred at up to 300Mbps. The radio coverage is also doubled to offer the high speed wireless connection even in a wide space of your office or house.

To secure the wireless communication, the N-WAP supports most up-to-date encryption: WEP, WPA-PSK and WPA2-PSK. In addition, the N-WAP supports WPS configuration with PBC/PIN type for users to connect to a secured wireless network easily.

Product Features

- IEEE 802.11b/g/n wireless standard compliant
- Multi-mode: AP, Client, Router Mode
- Supports 64/128-bit WEP, WPA, WPA-PSK, WPA2, WPA2-PSK and 802.1x encryption

Package Content

The contents of your product should contain the following items:

- 802.11n Wireless Access Point
- ~~Power adapter~~
- ~~Quick Installation Guide~~
- ~~User's Manual CD~~
- ~~RJ-45 cable x1~~

Physical Details

The following figure illustrates the each panel of N-WAP

Front Panel of N-WAP

Rear Panel of N-WAP

Physical Interface & Button

Front Panel LED Indicators

LED	Color	State	Descriptions
PWR	**Blue**	ON	Access Point is power ON
		Off	Access Point is power Off
LAN	**Yellow**	ON	LAN is connected successfully
		Flashing	Data is transmitting
		Off	Ethernet not connected to PC
WPS	**Red**	ON	WPS Active
		Off	WPS Not Active
Reset Button		Pressing over 5 seconds to reset to the factory default setting	

Rear Panel Indicators

LAN	**RJ-45 connector, to maintain the existing network structure, connected directly to the PC through straight CAT-5 cable**

Note

1. Machine LAN port default IP is http://192.168.1.254. Press RESET button on front panel over 5 seconds will reset the Access Point to factory default value.

2. Using the power supply that is not the one included in package will cause damage and void the warranty for this product.

Physical Installation Requirement

This chapter illustrates basic installation of Wireless Access Point ("**Access Point**" in the following term)

- Network cables. Use standard 10/100Base-TX network (UTP) cables with RJ-45 connectors.
- TCP/IP protocol must be installed on all PCs.

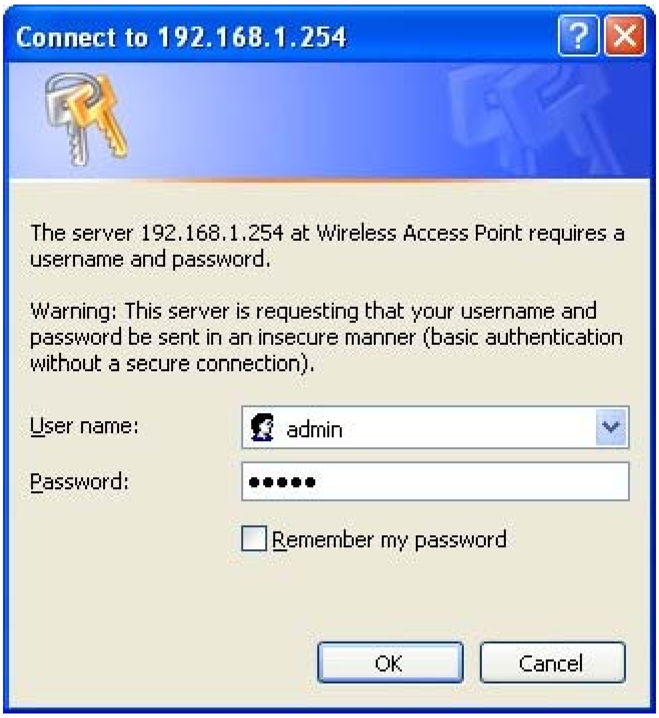
For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem

Administration Interface

LEGRAND Access Point provides GUI (Web based, Graphical User Interface) and utility for machine management and administration.

Web configuration access

You will connect to Access Point via your web browser automatically. Access Point will prompt for logon username / password, please enter: **admin / admin** to continue machine administration.



Connect to 192.168.1.254

The server 192.168.1.254 at Wireless Access Point requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: •••••

☐ Remember my password

Access Point will prompt for logon username/password, please enter: ***admin*** / **admin** to continue machine administration.

The default IP address of LAN port is **192.168.1.254**. You also could open your web browser, and insert

http://192.168.1.254 in the address bar of your web browser to logon Access Point web configuration page.

To start Access Point web configuration, you must have one of these web browsers installed on computer for management

Microsoft Internet Explorer 6.00 or higher with Java support

Note

Please locate your PC in the same network segment (**192.168.1.x**) of Router. If you're not familiar with TCP/IP, please refer to related chapter on user's manual CD or consult your network administrator for proper network configurations.

Chapter 3

Network Settings

3

Configuring and monitoring your Access Point from web browser

The Access Point integrates a web-based graphical user interface that can cover most configurations and machine status monitoring. Via standard web browser, you can configure and check machine status from anywhere around the world.

Overview on the web interface of Access Point

With web graphical user interface, you may have:

More comprehensive setting feels than traditional command line interface.

Provides user input data fields, check boxes, and for changing machine configuration settings

- Displays machine running configuration

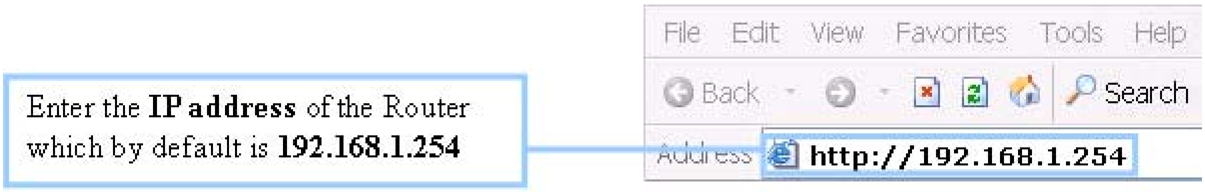
To start Access Point web configuration, you must have one of these web browsers installed on computer for management

Microsoft Internet Explorer 6.00 or higher with Java support

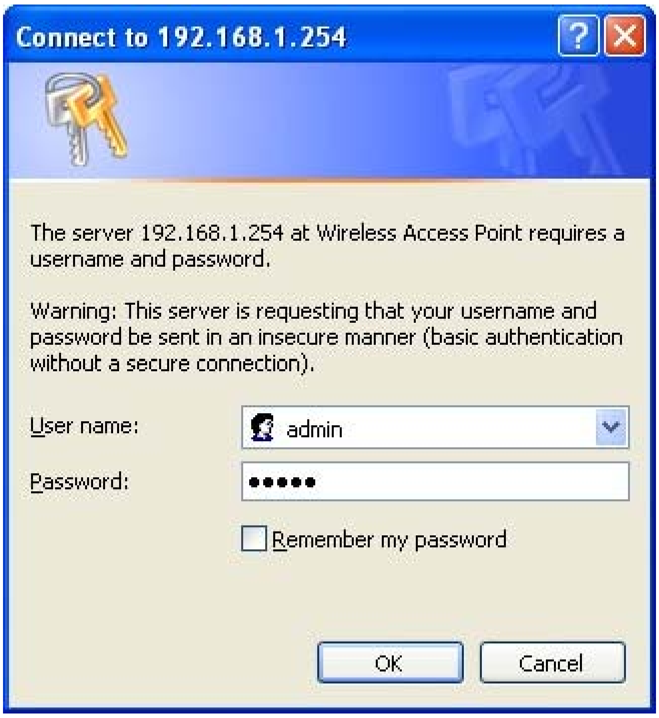
Manipulation of Access Point via web browser

Log on Access Point via web browser

After TCP/IP configurations on your PC, you may now open your web browser, and input http://192.168.1.254 (Default LAN port IP address) to logon Access Point web configuration page.


Enter the IP address of the Router
which by default is 192.168.1.254
File
Edit
View
Favorites
Tools
Help
Back
Search
Address
http://192.168.1.254

The Access Point will prompt for logon username/password: ***admin*** / ***admin***



Connect to 192.168.1.254

The server 192.168.1.254 at Wireless Access Point requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

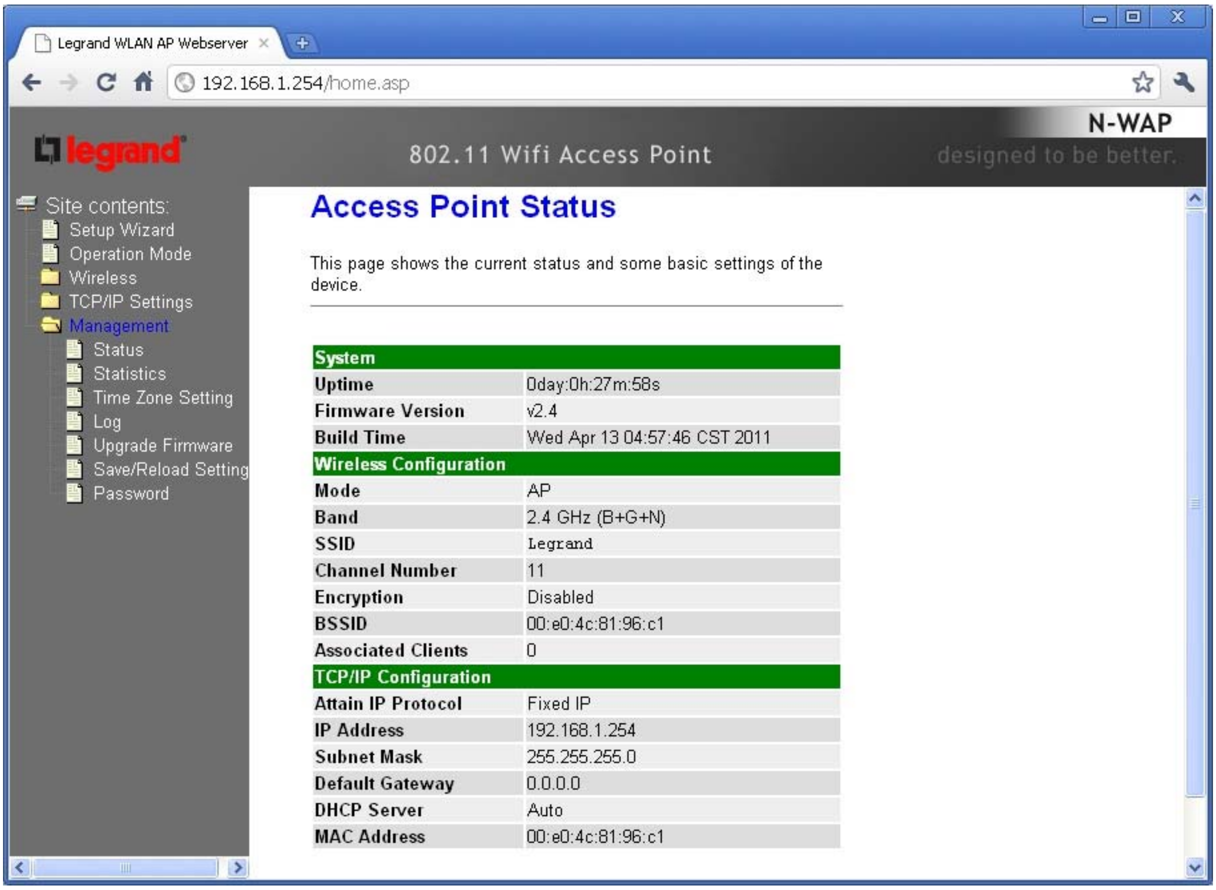
User name: admin

Password: ●●●●●

☐ Remember my password

Access Point login prompt screen

When users login the web page, users can see the general information like company…etc in this main page.



Access Point Status

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

System	
Uptime	0day:0h:27m:58s
Firmware Version	v2.4
Build Time	Wed Apr 13 04:57:46 CST 2011
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	Legrand
Channel Number	11
Encryption	Disabled
BSSID	00:e0:4c:81:96:c1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Auto
MAC Address	00:e0:4c:81:96:c1

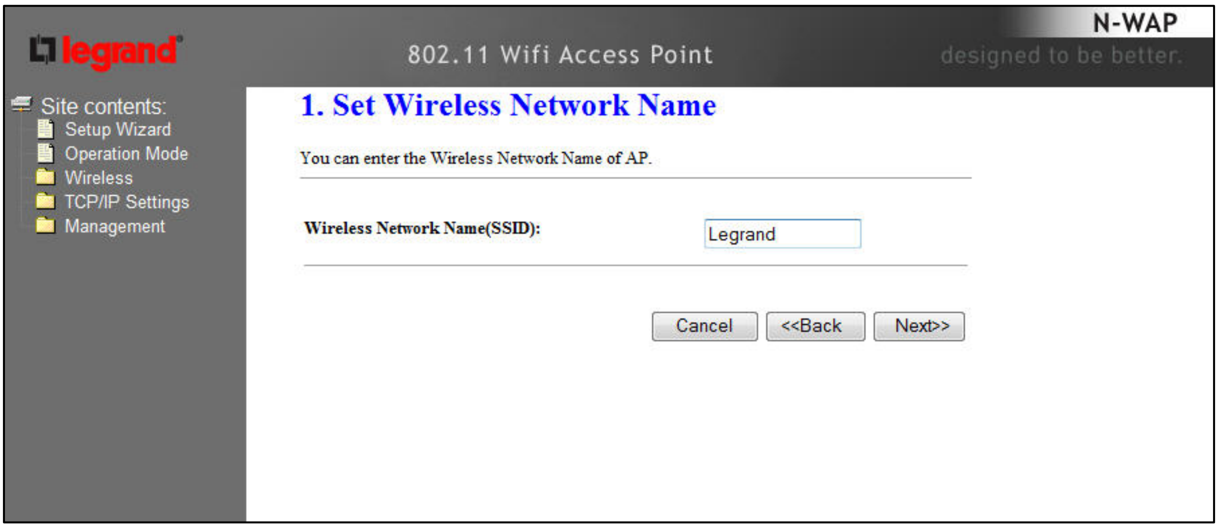
Access Point main page

Starting Setup in Web UI

It is easy to configure and manage the AP/ Router with web browser. After successfully login, you can click **Setup Wizard** to quickly configure your AP/ Router.

■ AP Mode

Step 1. Set Wireless Network Name (SSID), and then click **Next>>**.

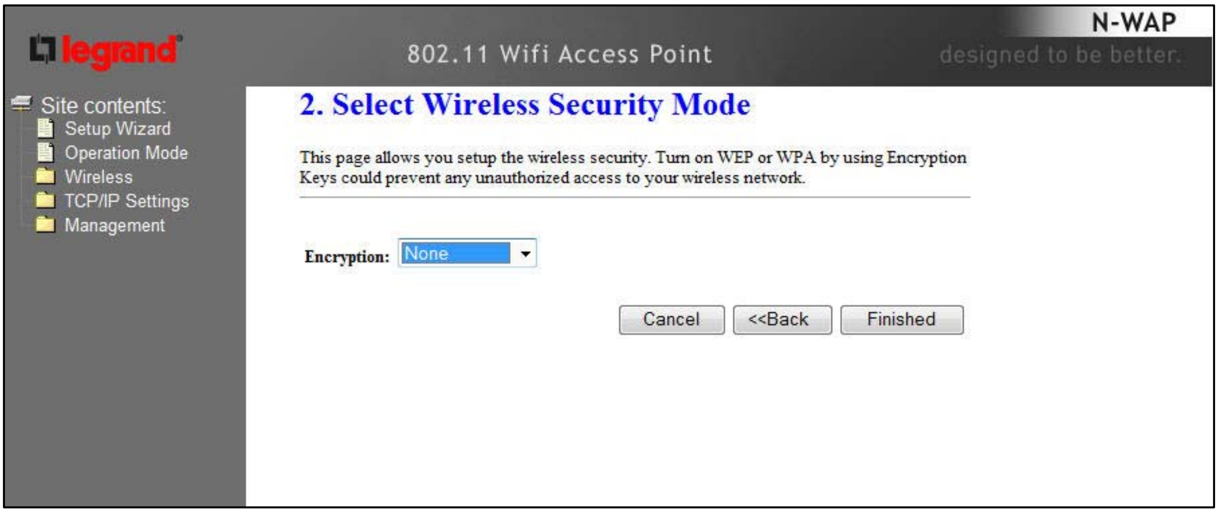


1. Set Wireless Network Name

You can enter the Wireless Network Name of AP.

Wireless Network Name(SSID): Legrand

Step 2. Select Wireless Security Mode.



2. Select Wireless Security Mode

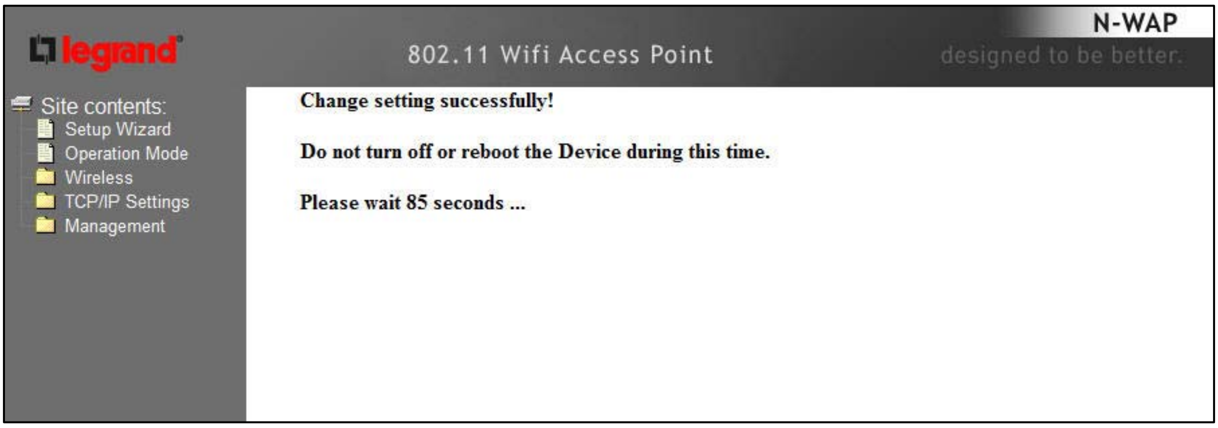
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: None

Step 3. Click the **Finished** button. You will then see the **Finish** page as shown below.

The AP will reboot automatically to make your wireless configuration to take effect and finish the **Setup**.

.



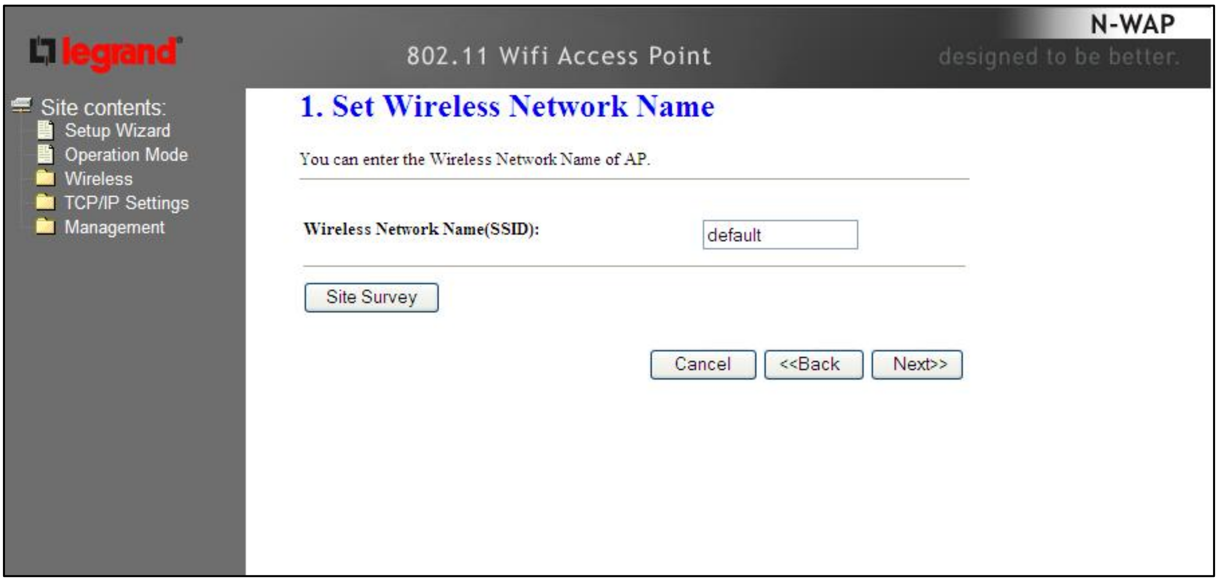
Change setting successfully!

Do not turn off or reboot the Device during this time.

Please wait 85 seconds ...

Client Mode

Step 1. Set Wireless Network Name, or click **Site Survey** to scan the nearby AP.

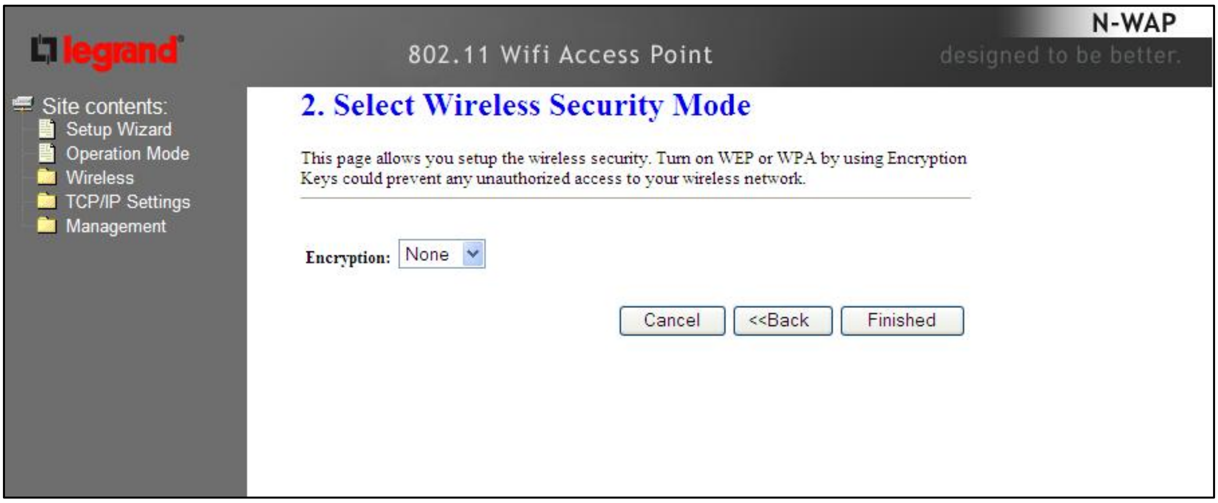


1. Set Wireless Network Name

You can enter the Wireless Network Name of AP.

Wireless Network Name(SSID): default

Step 2. Select Wireless Security Mode.



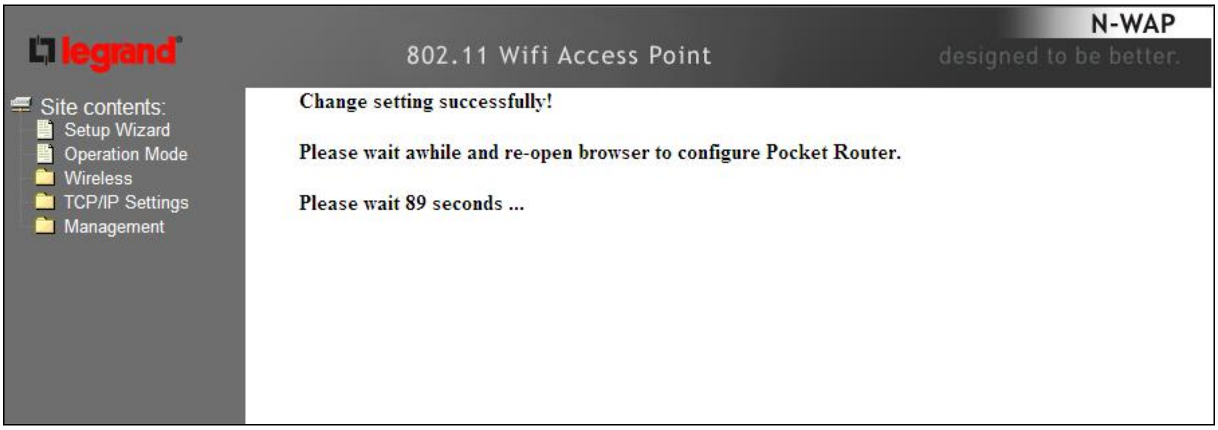
2. Select Wireless Security Mode

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

Step 3. Click the **Finished** button. You will then see the **Finish** page as shown below.

The AP will reboot automatically to make your wireless configuration to take effect and finish the **Setup**.



Change setting successfully!

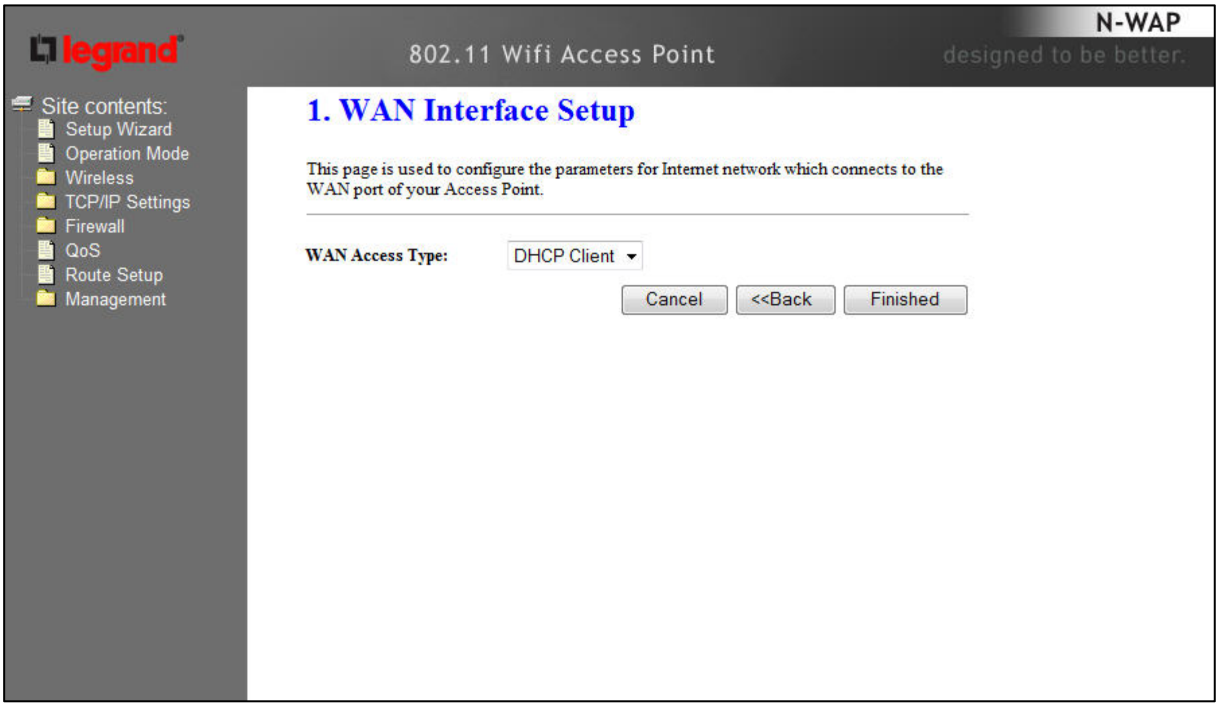
Please wait awhile and re-open browser to configure Pocket Router.

Please wait 89 seconds ...

- **Router Mode**

Step 1. Select the WAN Access Type.

Step 2. Enter the information for the selected WAN Access Type, and then click **Next**. If your access type is **DHCP Client**, then you can get the IP address from the ISP, so you do not need to enter the information like other modes. For other modes, please refer to the section WAN Interface Setup.



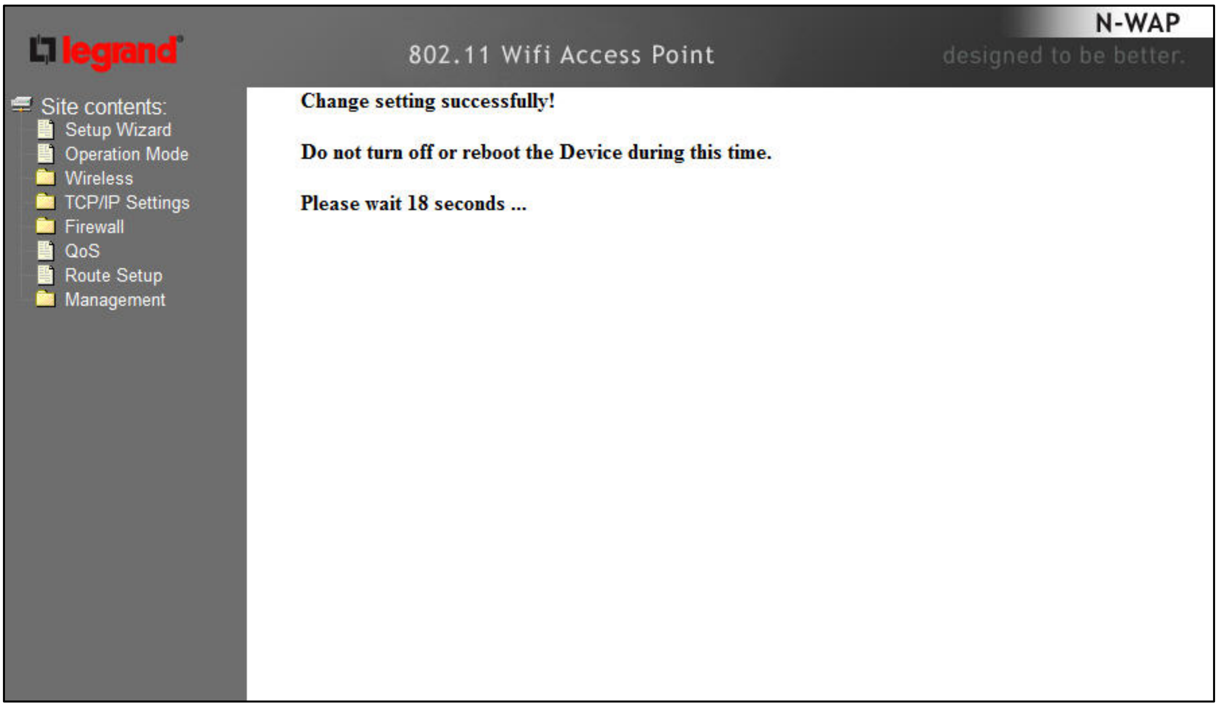
1. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.

WAN Access Type: DHCP Client

Step 3. Click the **Finished** button. You will then see the **Finish** page as shown below.

The AP will reboot automatically to make your wireless configuration to take effect and finish the **Setup**.



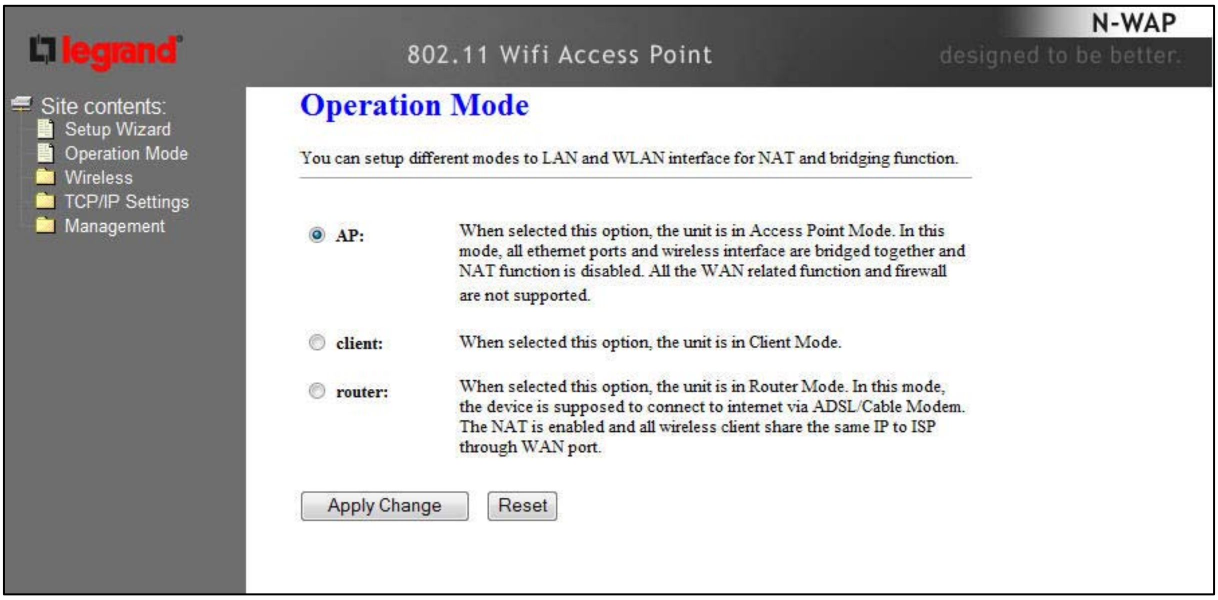
Change setting successfully!

Do not turn off or reboot the Device during this time.

Please wait 18 seconds ...

Network Operation Mode

You can setup different modes to WAN and LAN interface for NAT, Bridging and Wireless ISP function.



Operation Mode

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

● AP: When selected this option, the unit is in Access Point Mode. In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

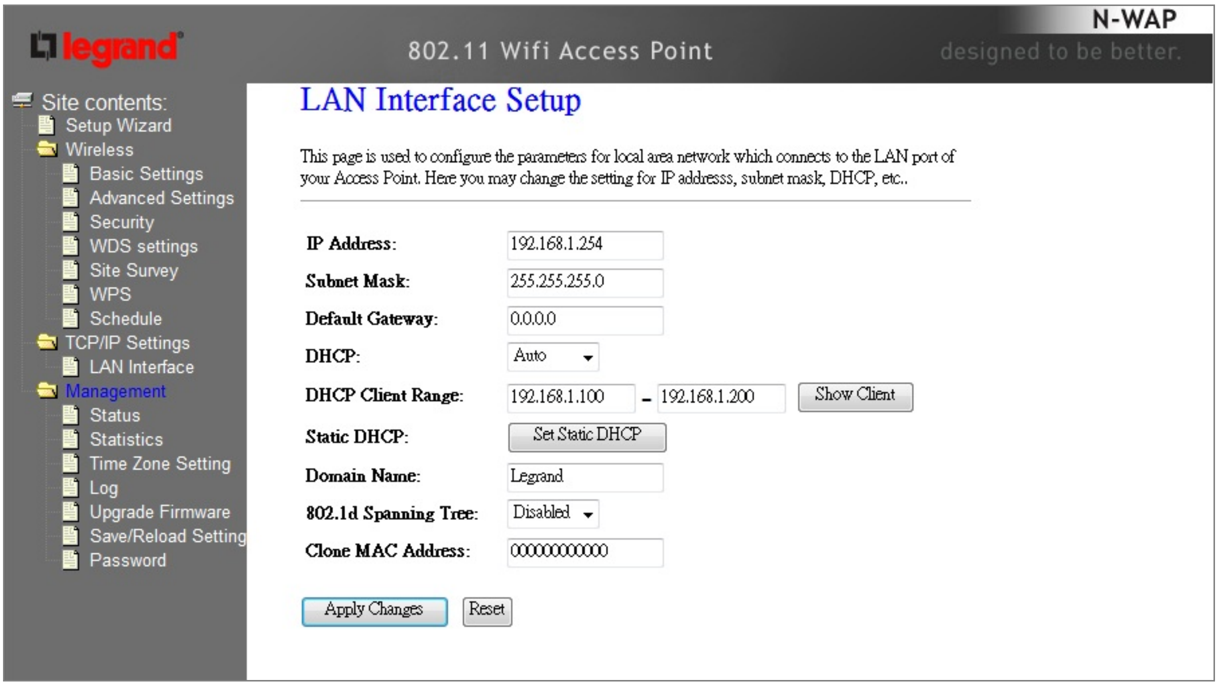
○ client: When selected this option, the unit is in Client Mode.

○ router: When selected this option, the unit is in Router Mode. In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and all wireless client share the same IP to ISP through WAN port.

AP	In this mode, all Ethernet ports are bridged together and NAT function is disabled. All the LAN port related function and firewall are not supported.
Client	In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page.
Router	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and your PC in LAN port shares the same IP to ISP through WAN port. The connection type can be setup in WAN page by using Static, DHCP Client, PPPOE, PPTP or L2TP.

LAN Interface Setup

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



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:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Auto
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
Static DHCP:	Set Static DHCP
Domain Name:	Legrand
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Apply Changes Reset

IP Address	LAN IP Address of the Access Point
	Default : 192.168.1.254
Subnet Mask	LAN mask of the Access Point
	Default : 255.255.255.0
DHCP Server	You can select **Server** or **Disable**. If you select Disable, the DHCP service of LAN port is disabled.
	Default : Server
DHCP Client Range	The first and last IP address that DHCP server assigns.
	Default : 192.168.1.100 – 192.168.1.200
Static DHCP	It allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address
	Default : Disable
Domain Name	Set three alternatives Domain Name Server for LAN interface.
	Default : Null
802.11d Spanning Tree	Spanning Tree Protocol. You can select Enable or Disable.
	Default : Disable

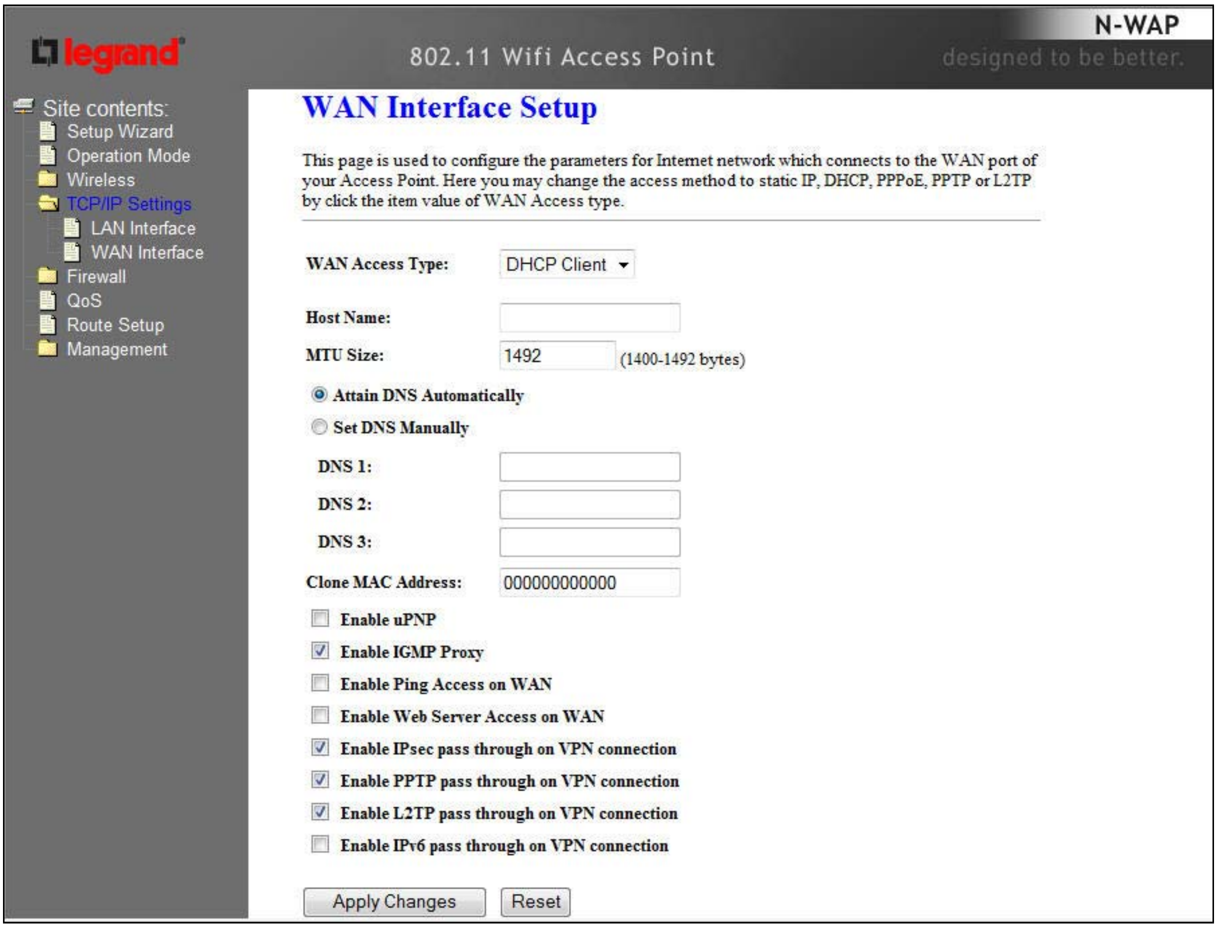
WAN Interface Setup

Choose menu “**TCP/IP Settings→WAN Interface**”, you can configure the IP parameters of the WAN on the screen below when router mode is enabled.

WAN Access Type	**DHCP Client**	Connections which use dynamic IP address assignment.
	Static IP	Connections which use static IP address assignment.
	PPPoE	Connections which use PPPoE that requires a user name and password.
	PPTP	Connections which use a Point-to-Point Tunneling Protocol (PPTP) connection.
	L2TP	Connections which use a Layer2 Tunneling Protocol (L2TP) connection.
Attain DNS Automatically	Select to attain DNS automatically from your ISP.	
Set DNS Manually	Select to specify your own preferred DNS Server IP address. The DNS 2 or DNS 3 is optional. You can enter the secondary and the third DNS Server's IP address as an alternative of DNS 1.	
Clone MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet to. Type in this section to replace the WAN MAC address with the MAC address of that PC.	
Enable uPNP	Check to enable the **uPNP** function.	
Enable IGMP Proxy	Check to enable the **IGMP Proxy** function.	
Enable Ping Access on WAN	Check to enable the **Ping Access on WAN** function.	
Enable Web Server Access on WAN	Check to enable the **Web Server Access on WAN** function.	
Enable IPsec pass through on VPN connection	Check to enable the **IPsec pass through on VPN connection** function.	
Enable PPTP pass through on VPN connection	Check to enable the **PPTP pass through on VPN connection** function.	
Enable L2TP pass through on VPN connection	Check to enable the **L2TP pass through on VPN connection** function.	
Enable IPv6 pass through on VPN connection	Check to enable the **IPv6 pass through on VPN connection** function.	
Apply Changes	After completing the settings on this page, click **Apply changes** button to save the settings.	
Reset	Click **Reset** to restore to default values.	

DHCP Client

If your ISP provides the DHCP service, please choose **DHCP Client** type, and the Router will automatically obtain IP parameters from your ISP. You can see the page as follows.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1492 (1400-1492 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

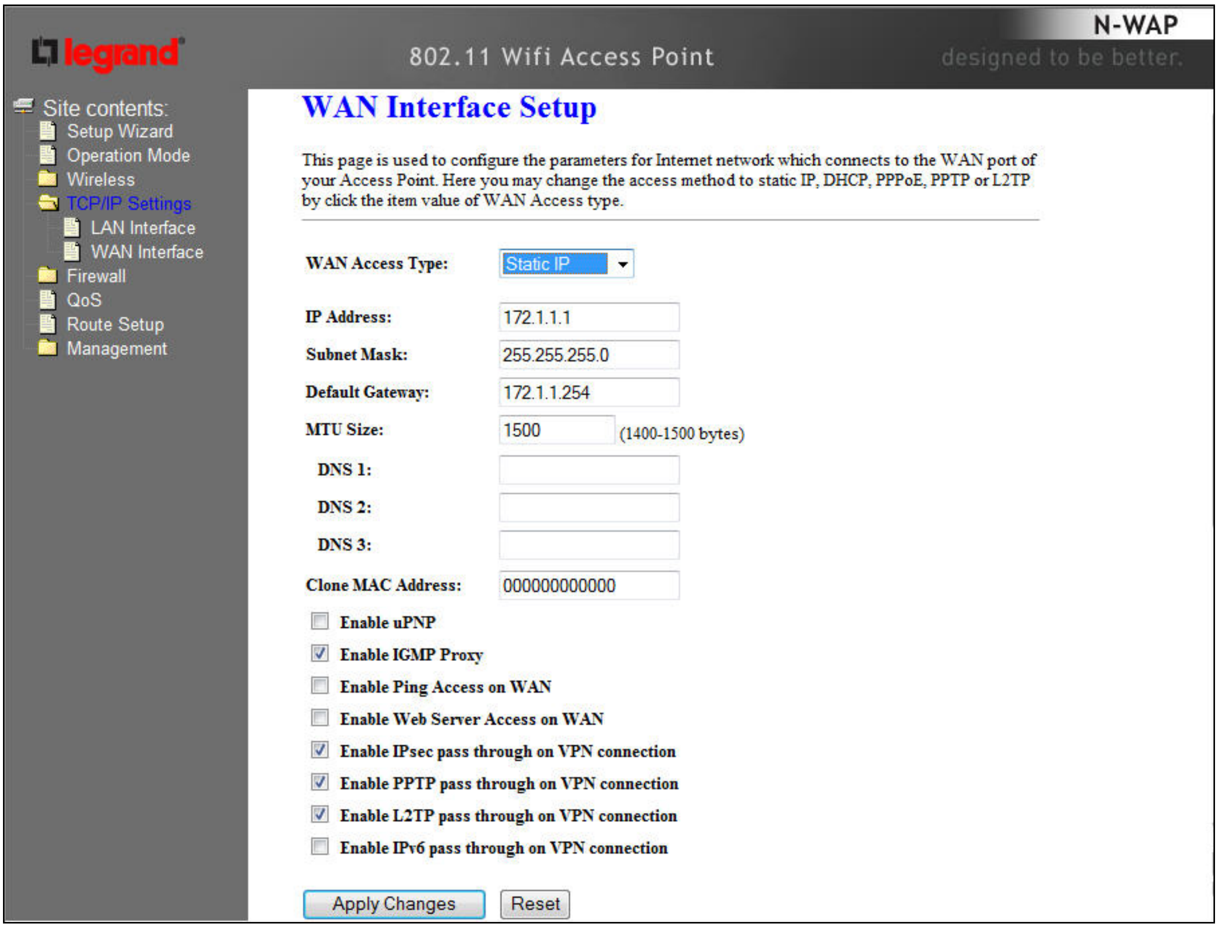
□ Enable IPv6 pass through on VPN connection

The page includes the following fields:

Object	Description
Host Name	This option specifies the Host Name of the Router.
MTU Size	**The default MTU (Maximum Transmission Unit) value is 1492 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.**

Static IP

If your ISP provides a static or fixed IP Address, then you have to setup the IP address, Subnet Mask, Gateway and DNS setting. You can see the page as follows.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

MTU Size: 1500 (1400-1500 bytes)

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

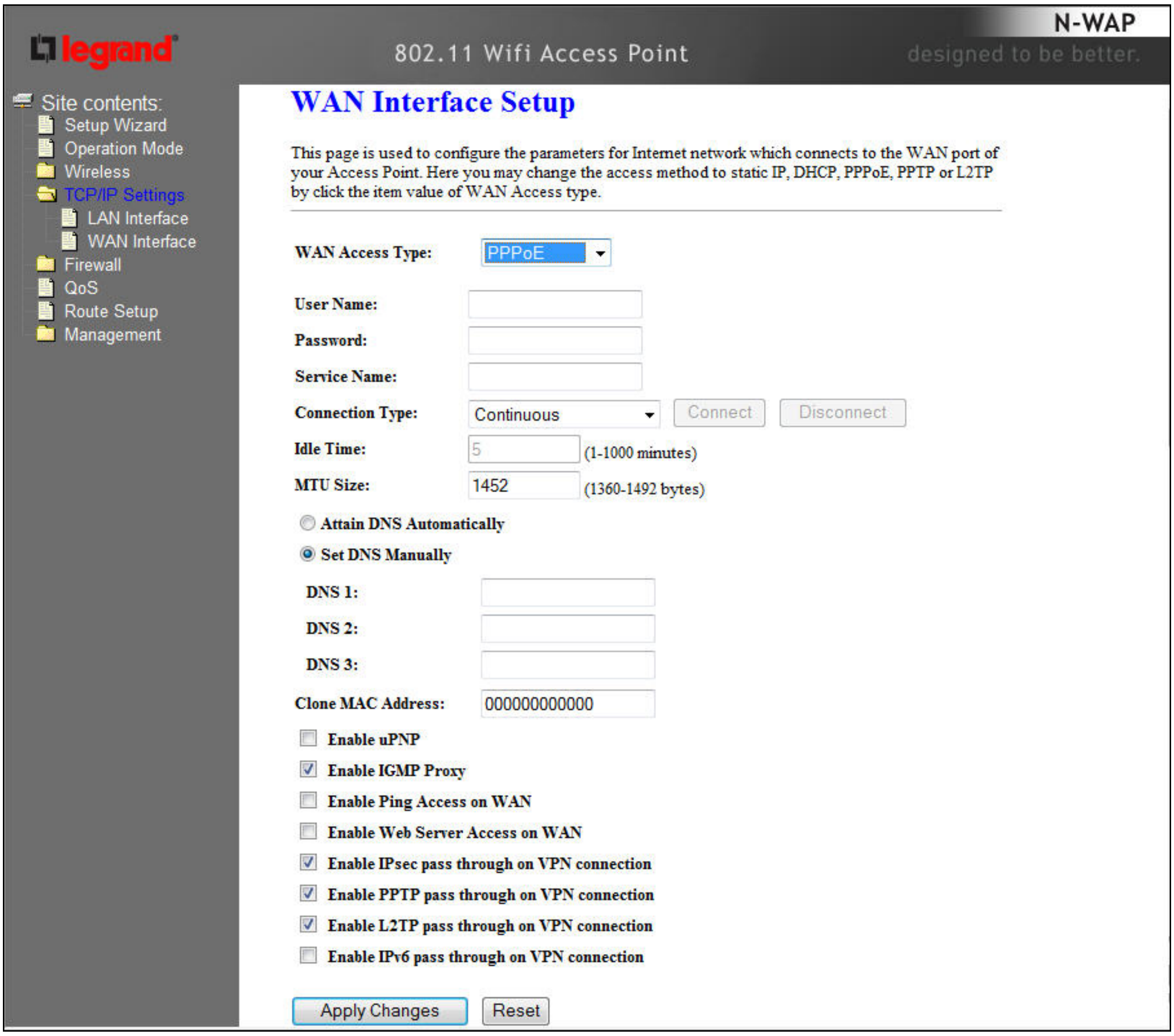
□ Enable IPv6 pass through on VPN connection

The page includes the following fields:

Object	Description
IP Address	Enter the IP address in dotted-decimal notation provided by your ISP.
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Default Gateway	(Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
MTU Size	The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
DNS 1	Enter the DNS server IP address provided by your ISP, or you can specify your own preferred DNS server IP address.
DNS 2 & DNS 3	You can enter another DNS server’s IP address as a backup. DNS 2 and 3 servers will be used when the DNS 1 server fails.

PPPoE

If your ISP provides a PPPoE connection, select **PPPoE** option. User has to setup the user name and password according to the ISP that provided the related information. You can see the page as follows.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPPoE

User Name:

Password:

Service Name:

Connection Type: Continuous [Connect] [Disconnect]

Idle Time: 5 (1-1000 minutes)

MTU Size: 1452 (1360-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

□ Enable IPv6 pass through on VPN connection

[Apply Changes] [Reset]

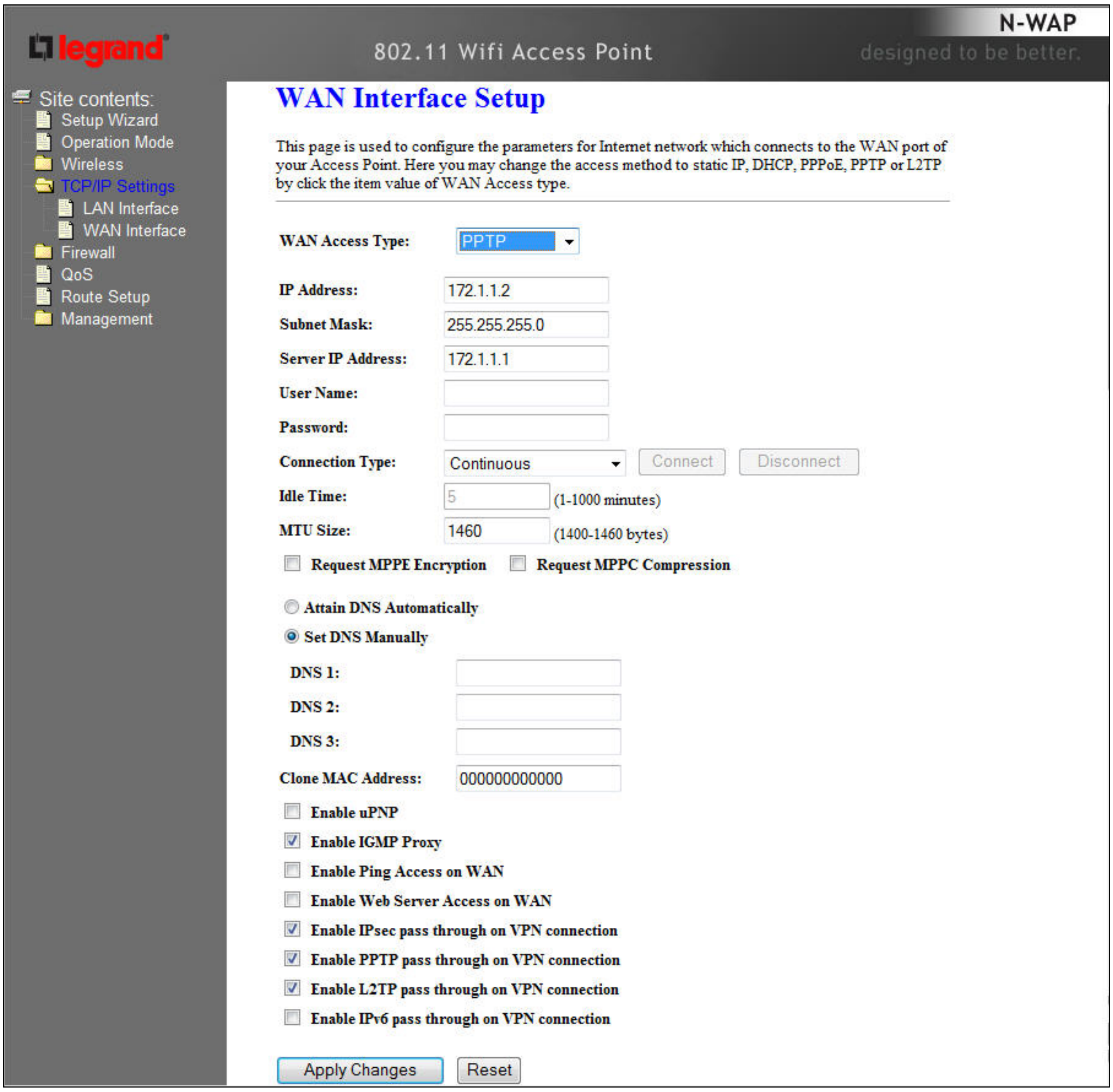
The page includes the following fields:

Object	Description
User Name	Enter the User Name provided by your ISP. This field is case-sensitive.
Password	Enter the Password provided by your ISP. This field is case-sensitive.
Service Name	Enter the Internet service provider name in this field.
Connection Type	Select the connection type **Continuous**, **Connect on Demand** or **Manual** from the drop-down menu. If selected **Manual**, user can click Connect button to make a connection.
Idle Time	It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time

	is 5 minutes. This function will be available when the Connection Type is selected to **Connect on Demand**.
MTU Size	The default **MTU** (Maximum Transmission Unit) value is 1452 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.

PPTP

If your ISP provides PPTP connection, please select **PPTP** option. And enter the following parameters. You can see the page as follows.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPTP

IP Address: 172.1.1.2

Subnet Mask: 255.255.255.0

Server IP Address: 172.1.1.1

User Name:

Password:

Connection Type: Continuous [Connect] [Disconnect]

Idle Time: 5 (1-1000 minutes)

MTU Size: 1460 (1400-1460 bytes)

□ Request MPPE Encryption □ Request MPPC Compression

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

□ Enable IPv6 pass through on VPN connection

[Apply Changes] [Reset]

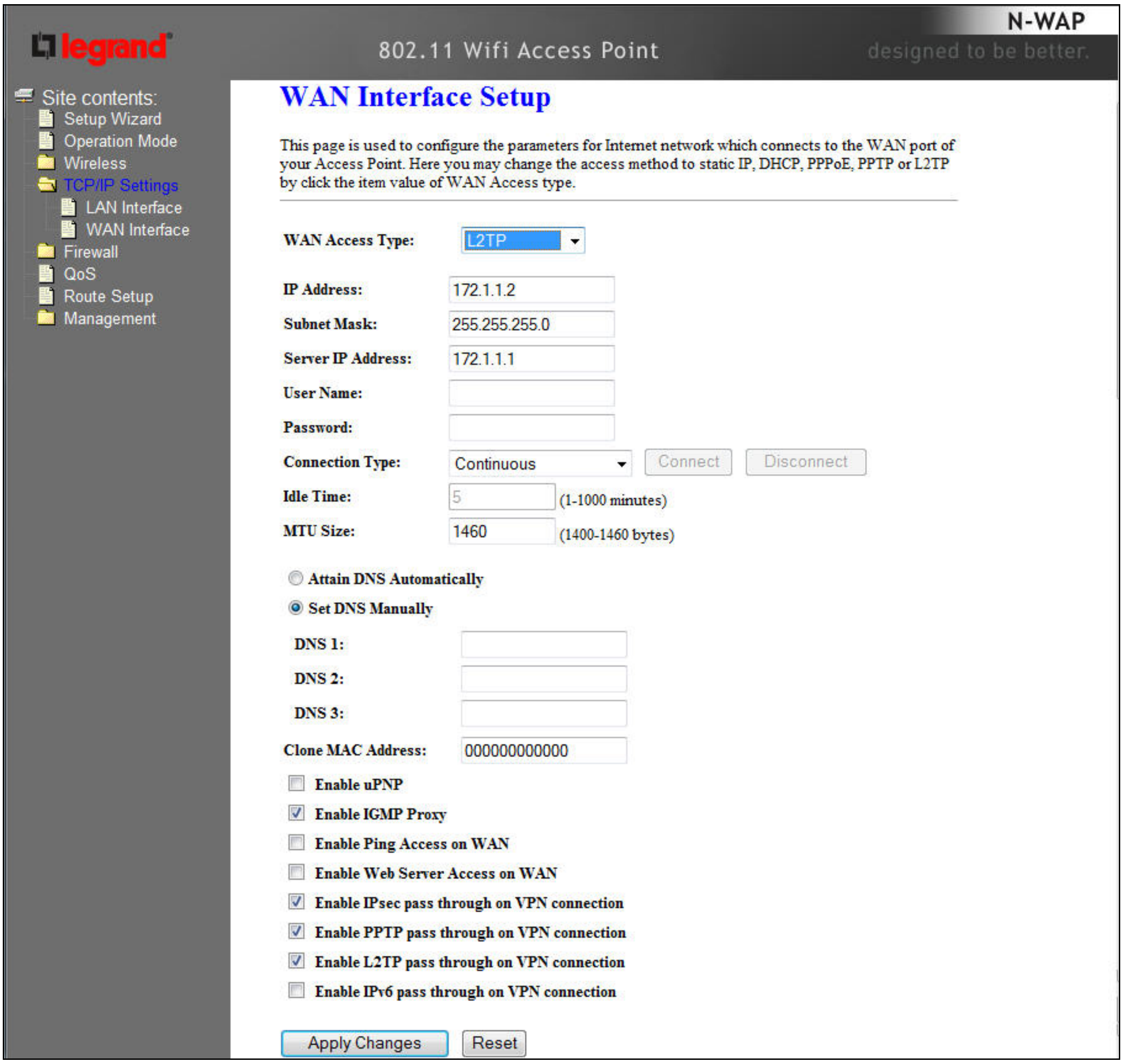
The page includes the following fields:

Object	Description
IP Address	Enter the IP address in dotted-decimal notation provided by your ISP.

Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Server IP Address	Enter the PPTP Server IP address in dotted-decimal notation provided by your ISP.
User Name	Enter the User Name provided by your ISP. The Maximum input is 20 alphanumeric characters (case-sensitive).
Password	Enter the Password provided by your ISP. The Maximum input is 32 alphanumeric characters (case-sensitive).
Connection Type	Select the connection type **Continuous**, **Connect on Demand** or **Manual** from the drop-down menu. If selected **Manual**, user can click Connect button to make a connection.
Idle Time	It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the Connection Type is selected to **Connect on Demand**.
MTU Size	The default **MTU** (Maximum Transmission Unit) value is 1460 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.

- **L2TP**

If your ISP provides L2TP connection, please select **L2TP** option. And enter the following parameters. You can see the page as follows.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	L2TP
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	
Connection Type:	Continuous
Idle Time:	5 (1-1000 minutes)
MTU Size:	1460 (1400-1460 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

- □ Enable uPNP
- ☑ Enable IGMP Proxy
- □ 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
- □ Enable IPv6 pass through on VPN connection

The page includes the following fields:

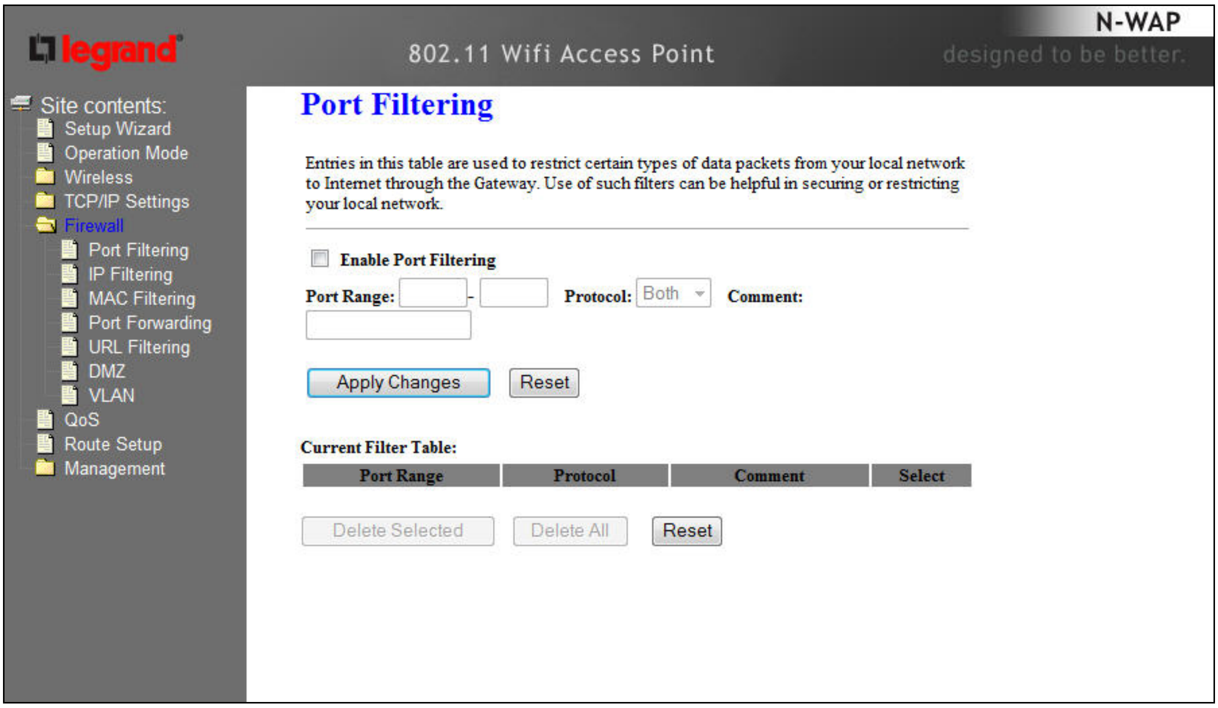
Object	Description
IP Address	Enter the IP address in dotted-decimal notation provided by your ISP.
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Server IP Address	Enter the L2TP Server IP address in dotted-decimal notation provided by your ISP.
User Name	Enter the User Name provided by your ISP. The Maximum input is 20 alphanumeric characters (case-sensitive).
Password	Enter the Password provided by your ISP. The Maximum input is 32 alphanumeric characters (case-sensitive).
Connection Type	Select the connection type **Continuous**, **Connect on Demand** or

	Manual from the drop-down menu. If selected **Manual**, user can click Connect button to make a connection.
Idle Time	It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the Connection Type is selected to **Connect on Demand**.
MTU Size	The default **MTU** (Maximum Transmission Unit) value is 1460 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.

Chapter 4
Firewall

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.



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: ____

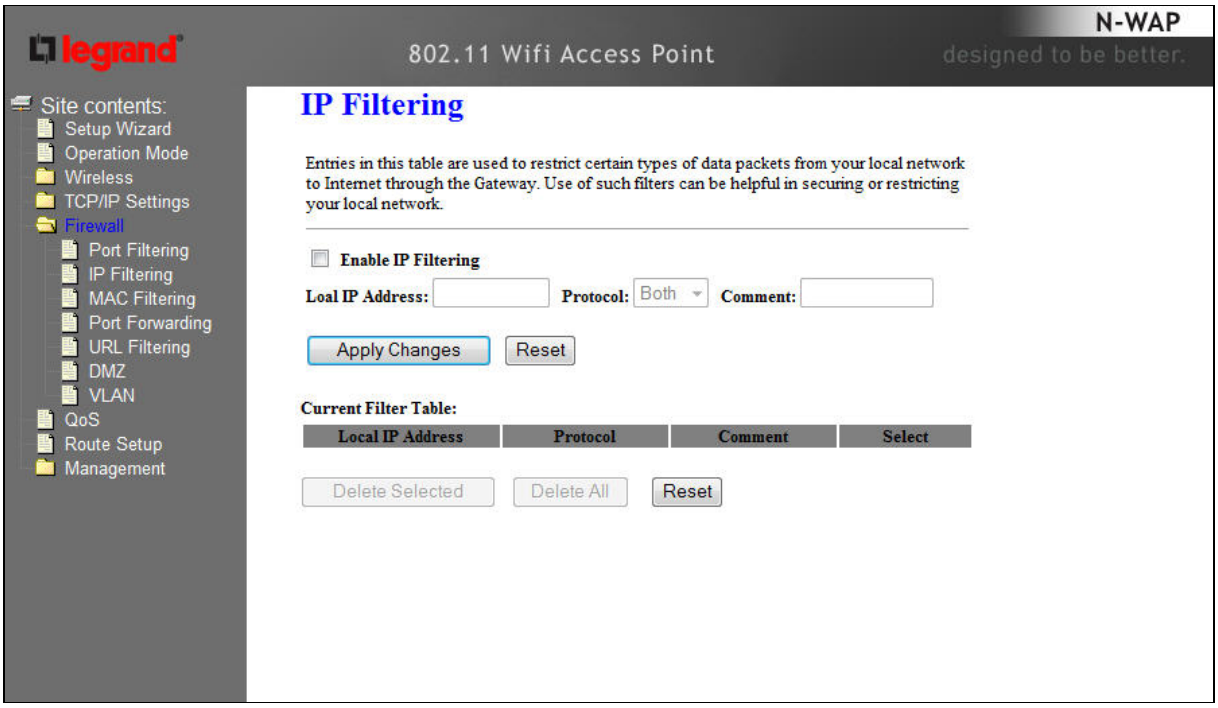
Current Filter Table:

Port Range	Protocol	Comment	Select

Enable Port Filtering	Check to enable Port Filtering function.
Port Range	Enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Comment	You may key in a description MAC address.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current Port Forwarding information.
Delete Selected	Click Delete Selected button to delete items which are selected.
Delete All	Click Delete All button to delete all the items.
Reset	Click Reset button to reset.

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 IP filters can be helpful in securing or restricting your local 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

Loal IP Address: ______ Protocol: Both Comment: ______

Apply Changes | Reset

Current Filter Table:

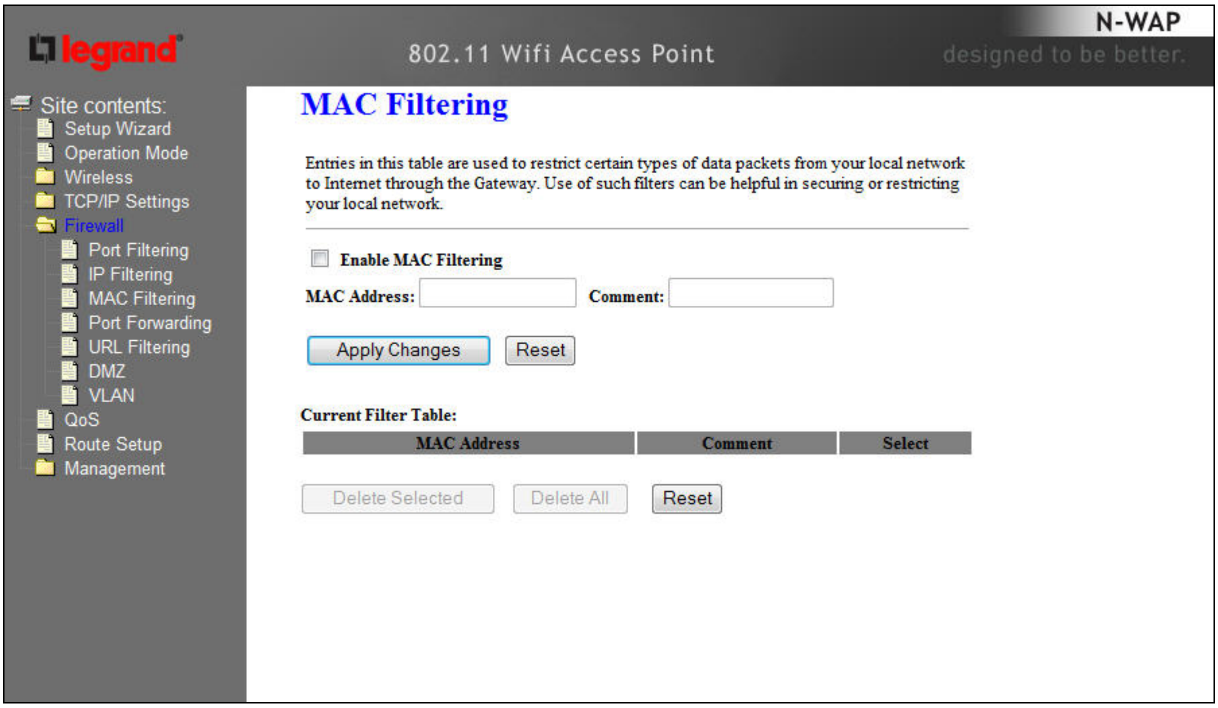
Local IP Address	Protocol	Comment	Select

Delete Selected | Delete All | Reset

Enable IP Filtering	Check to enable IP filtering function.
Local IP Address	Enter the local computer’s IP address.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Comment	You may key in a description for the port range.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current IP filter information.
Delete Selected	Click Delete Selected button to delete items which are selected.
Delete All	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

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.



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: Comment:

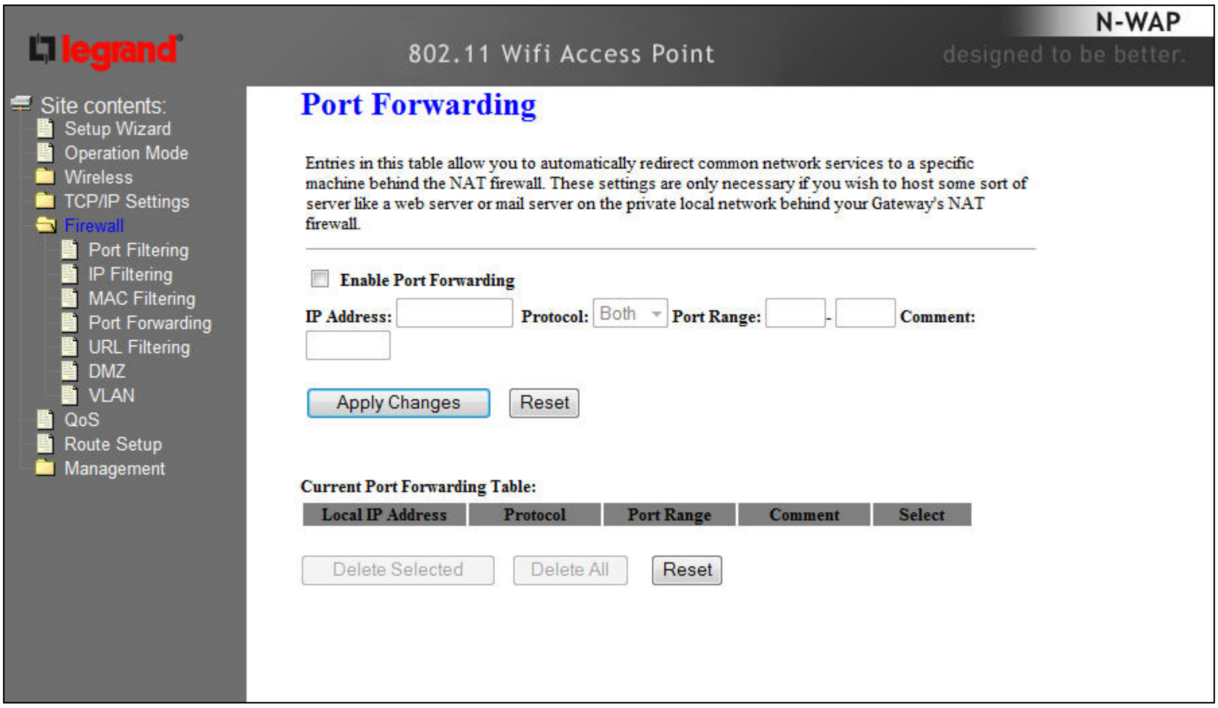
Current Filter Table:

MAC Address	Comment	Select

Enable MAC Filtering	Check to enable MAC filtering function.
MAC Address	Enter the client MAC address in the field.
Comment	You may key in a description MAC address.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current MAC filter information.
Deleted Selected	Click Delete Selected button to delete items which are selected.
Deleted All	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

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.



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:

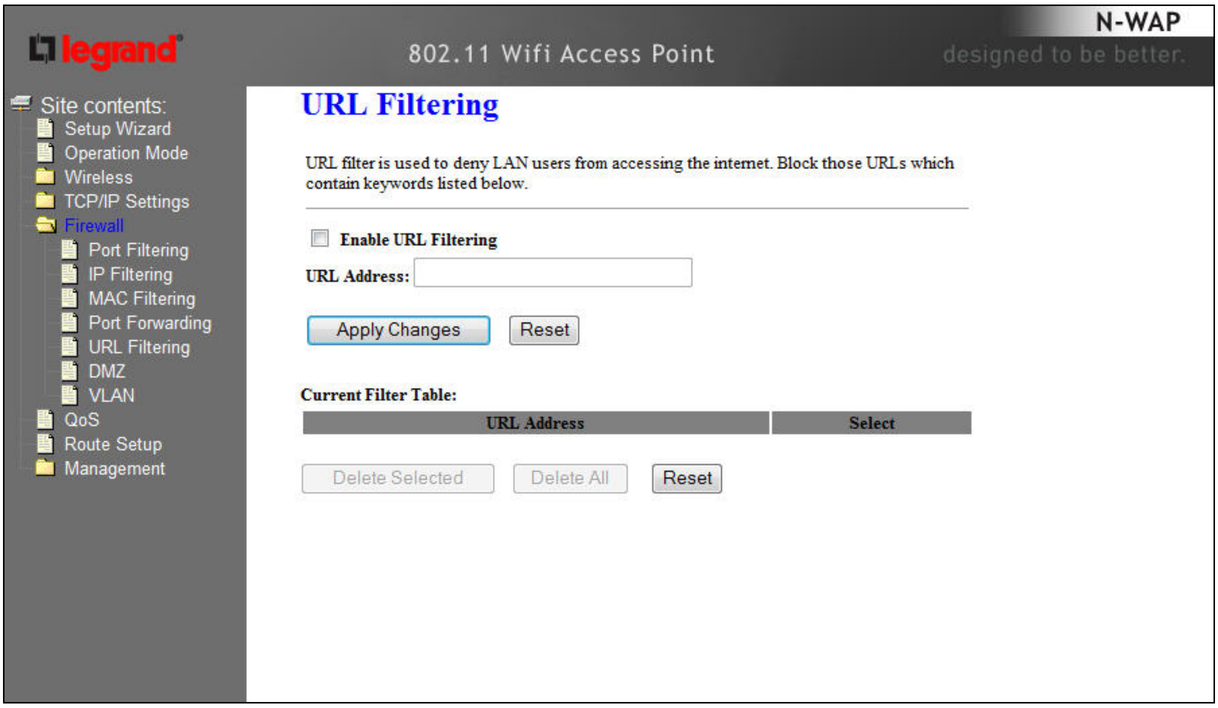
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Enable Port Forwarding	Check to enable Port Forwarding function.
IP Address	Enter the IP address in the field.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Port Range	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Comment	You may key in a description MAC address.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Port Forwading Table	Shows the current Port Forwarding information.
Delete Selected	Click Delete Selected button to delete items which are selected.
Delete All	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

URL Filtering

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



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:

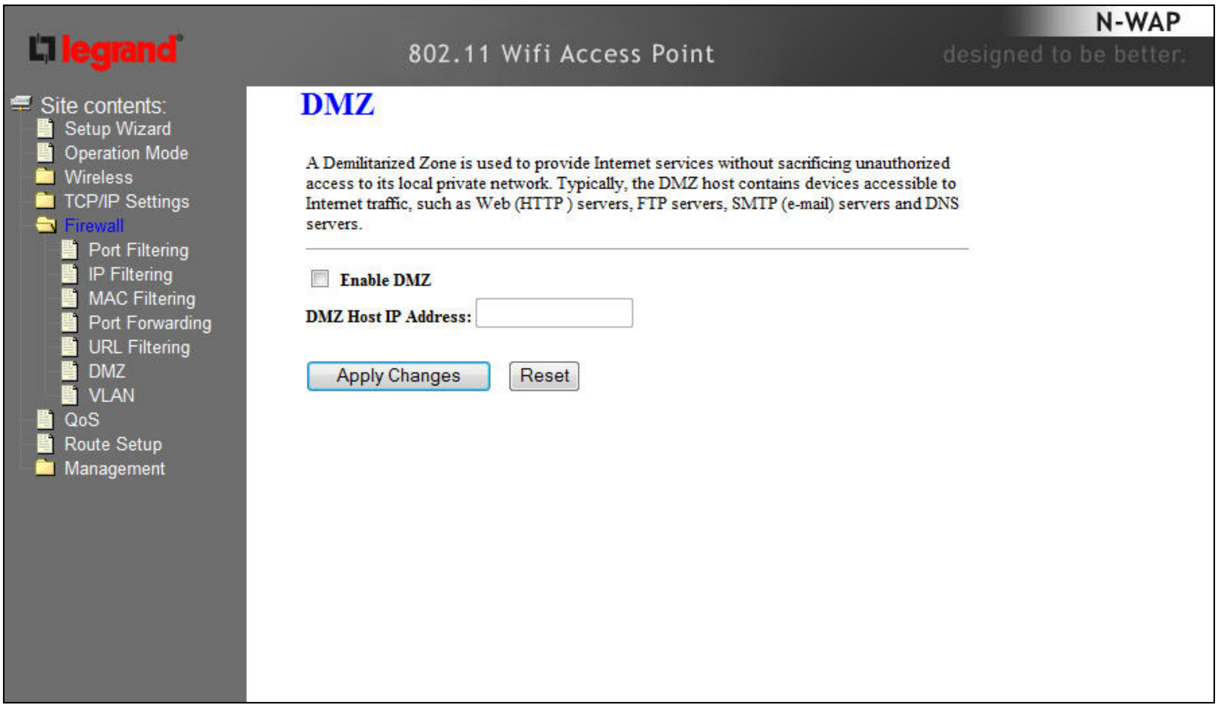
Current Filter Table:

URL Address	Select

Enable URL Filtering	Check to enable URL filtering function.
URL Address	Enter the URL address in the field.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current URL address filter information.
Delete Selected	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

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.



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:

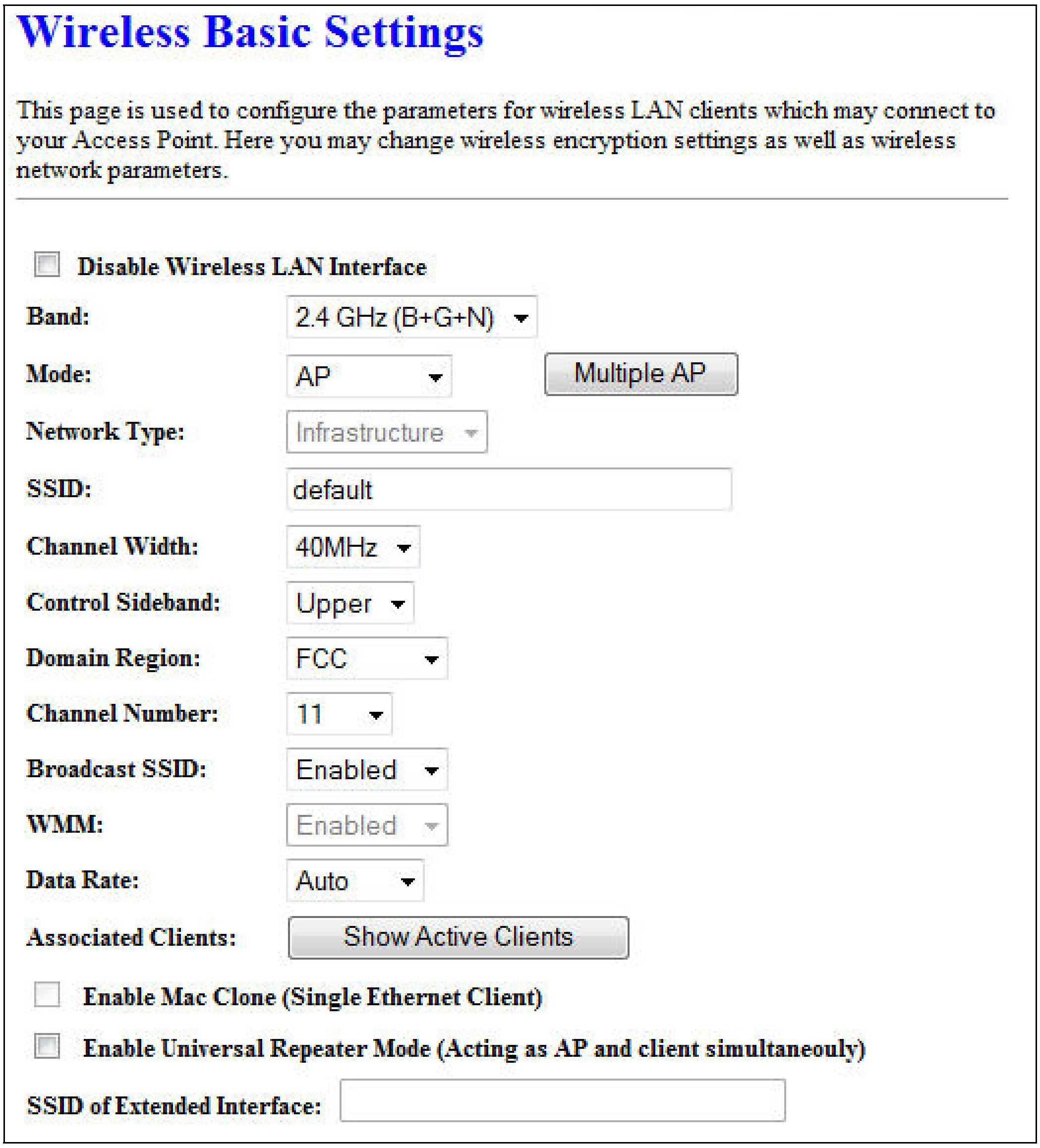
Enable DMZ	Check the box to enable DMZ function. If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two way connections.
DMZ Host IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values

Chapter 5

Wireless Settings

Basic Settings

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



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+N)

Mode: AP

Network Type: Infrastructure

SSID: default

Channel Width: 40MHz

Control Sideband: Upper

Domain Region: FCC

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients:

□ **Enable Mac Clone (Single Ethernet Client)**

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

SSID of Extended Interface:

Disable Wireless LAN Interface	Enable or disable the wireless LAN.
Band	There are 6 modes: 2.4GHz (B), 2.4GHz (G), 2.4GHz (N), 2.4GHz (B+G), 2.4GHz (G+N), and 2.4GHz (B+G+N) mode.
	Default : 2.4GHz (B+G+N)

Mode	- **AP**: The AP functions as a wireless hub to which wireless clients can connect. The clients must make sure that they are configured to match the AP's wireless settings. The AP must be connected to switch or other LAN segment patch cable. - **WDS**: WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement. - **AP+WDS**: It means the device can support WDS and AP Mode simultaneously.
	Default : AP mode
Network Type -	- **Infrastructure**: The wireless LAN serves as a wireless station (infrastructure). Connected to a PC or a small LAN (no more than 5 PCs), it allows the PC or small LAN able to access the wireless network via Access Point.
	- **Ad hoc:** The wireless LAN will use the Ad hoc mode to operate.
SSID	Wireless stations associating to the access point must have the same SSID. Enter a descriptive name for the wireless LAN.
	Default : 802.11bgn-SSID
Channel Width	There are 20MHz and 40MHz bandwidths for cohesion
	Default : 20MHz
Control Sideband	Specify if the extension channel should be in the Upper or Lower sideband
	Default : Upper (Unavailable)

Domain Region

The Domain Region decides what channels are available for your country. Please note that using the incorrect Domain Region is strictly prohibited. If you live in United States, you must use the FCC Domain Region. If you live inside EU, you must use ETSI domain.

Domain Region	Available Channels
FCC (U.S.)	20MHz: 1~11 40MHz: 5~11
IC (Canada)	20MHz: 1~11 40MHz: 5~11
ETSI (EMEA)	20MHz: 1~13 40MHz: 5~13
SPAIN	20MHz: 10, 11 40MHz: 11
FRANCE	20MHz: 10~13 40MHz: 13
MKK (Japan)	20MHz: 1~14 40MHz: 5~14

Default : FCC

Channel Number

Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country.

Default : Auto

Broadcast SSID

If you enable "Broadcast ESSID", every wireless station located within the coverage of this access point can discover this Access Point easily. If you are building a public wireless network, enabling this feature is recommended. In private network, disabling "Broadcast ESSID" can provide better security.

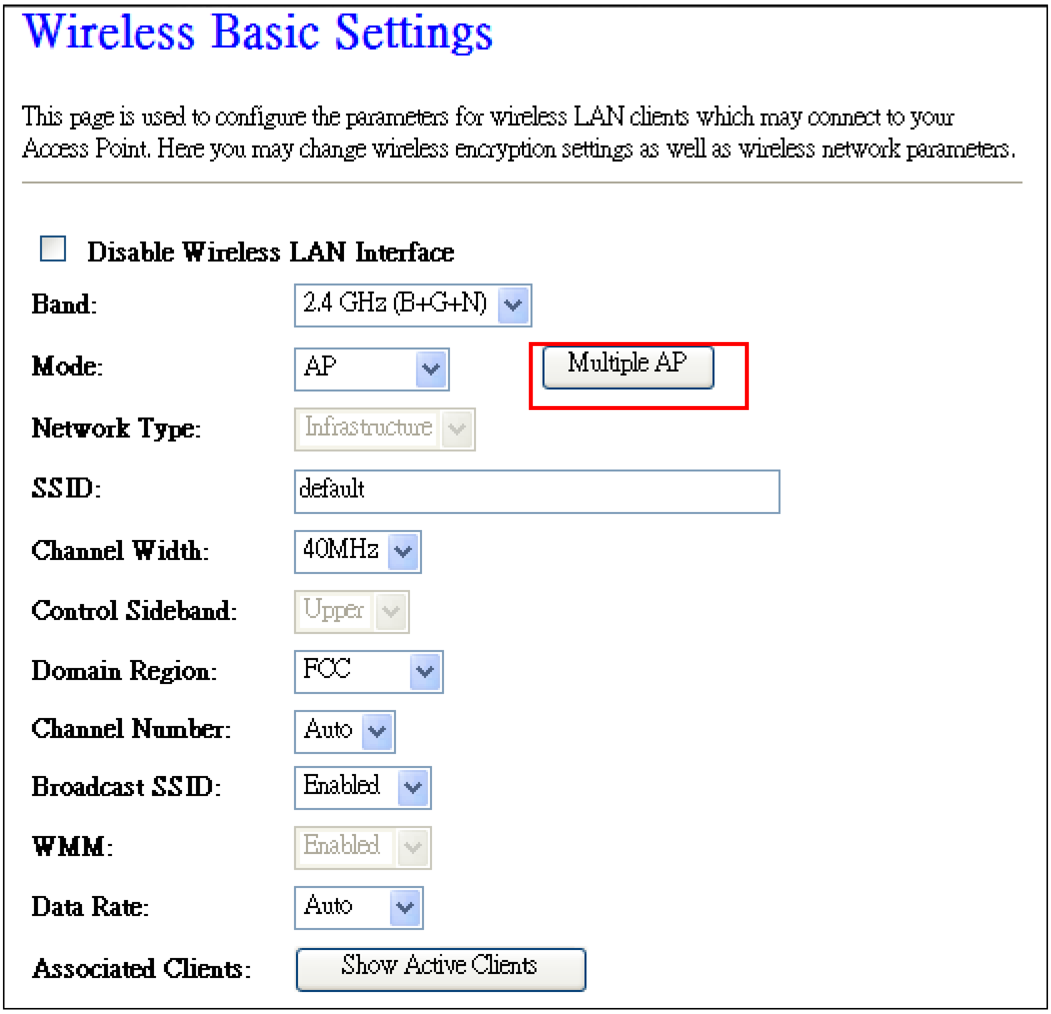
Default : Enable

WMM	The short of Wi-Fi Multi-Media, it will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. **Default :** Enable (Unavailable)
Data Rate	The Data Rate is the rate of data transmission for 802.11b/g/n clients. The Access Point will use the highest possible selected transmission rate to transmit the data packets. **Default :** Auto **Default :** Auto
Associated Clients	To show the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.
Enable Mac Clone	When set at Client mode, it provides wireless LAN to connect to a MAC address. **Default :** Disable
Enable Universal Repeater Mode	Universal Repeater is a technology used to extend wireless coverage. **Default :** Disable
SSID of Extended Interface	Universal Repeater is a technology used to extend wireless coverage. To enable Universal Repeater Mode, check the box and enter the SSID you want to broadcast in the field below. Then please click "Security" submenu for the related settings of the AP you want to connect with. It is only available in Client Mode. **Default :** Null

Multiple APs

Multiple APs/SSIDs allow the ability for separate security mode and key settings to be set by users for both convenience and increased protection. Users are able to configure their network devices to access the first SSID with the WPA2 PSK (Pre-Shared Key) and secret key, whilst share the second SSID with WEP and the periodically changed key for visitors. In addition, users are able to isolate these SSIDs to avoid malicious attacks and prevent certain access for visitors using the second SSID. This then provides users an extremely convenient approach to share the wireless access, provide access internet access for visitors, while possessing a strong security protection system at all times.

In Wireless Basic Settings page, click the **Multiple AP** button. You will then see the **Multiple APs Settings** page as shown below.

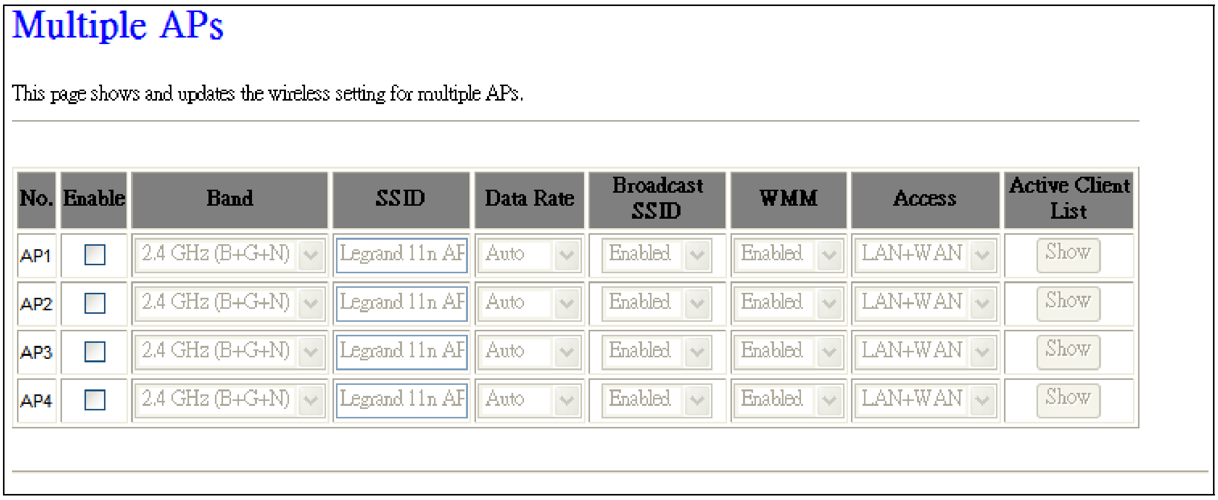


Wireless Basic Settings

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+N)
Mode:	AP Multiple AP
Network Type:	Infrastructure
SSID:	default
Channel Width:	40MHz
Control Sideband:	Upper
Domain Region:	FCC
Channel Number:	Auto
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients



Multiple APs

This page shows and updates the wireless setting for multiple APs.

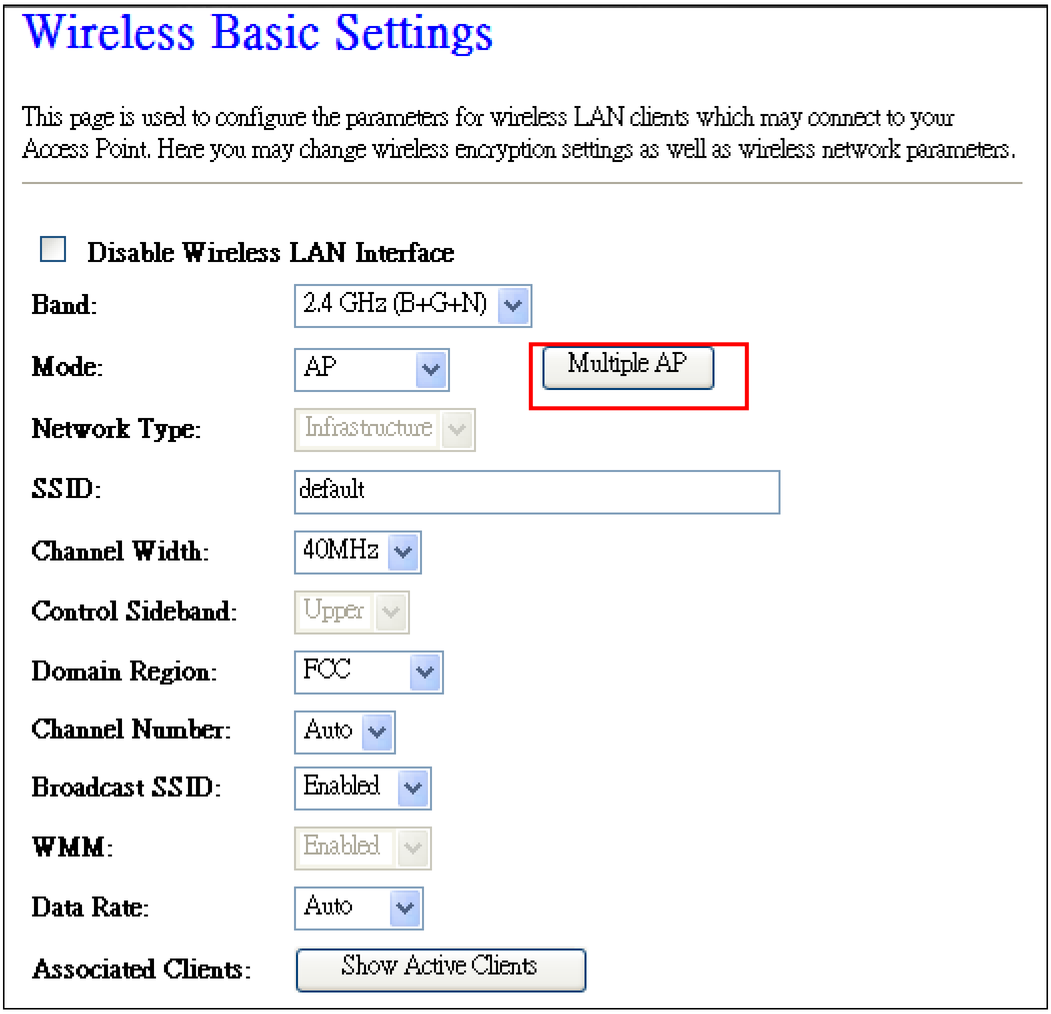
No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List
AP1	□	2.4 GHz (B+G+N)	Legrand 11n AP	Auto	Enabled	Enabled	LAN+WAN	Show
AP2	□	2.4 GHz (B+G+N)	Legrand 11n AP	Auto	Enabled	Enabled	LAN+WAN	Show
AP3	□	2.4 GHz (B+G+N)	Legrand 11n AP	Auto	Enabled	Enabled	LAN+WAN	Show
AP4	□	2.4 GHz (B+G+N)	Legrand 11n AP	Auto	Enabled	Enabled	LAN+WAN	Show

Enable Multiple APs	Check the checkbox to enable the Multiple AP/SSID. Up to 4 SSIDs for each BSS can be entered in the filed SSID. The name can be up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. If **Enable VLAN** is checked, the wireless stations connecting to SSID of different VID can not communicate with each other.

VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

In Wireless Basic Settings page, click the **Multiple AP** button. You will then see the **VLAN Settings** page as shown below.

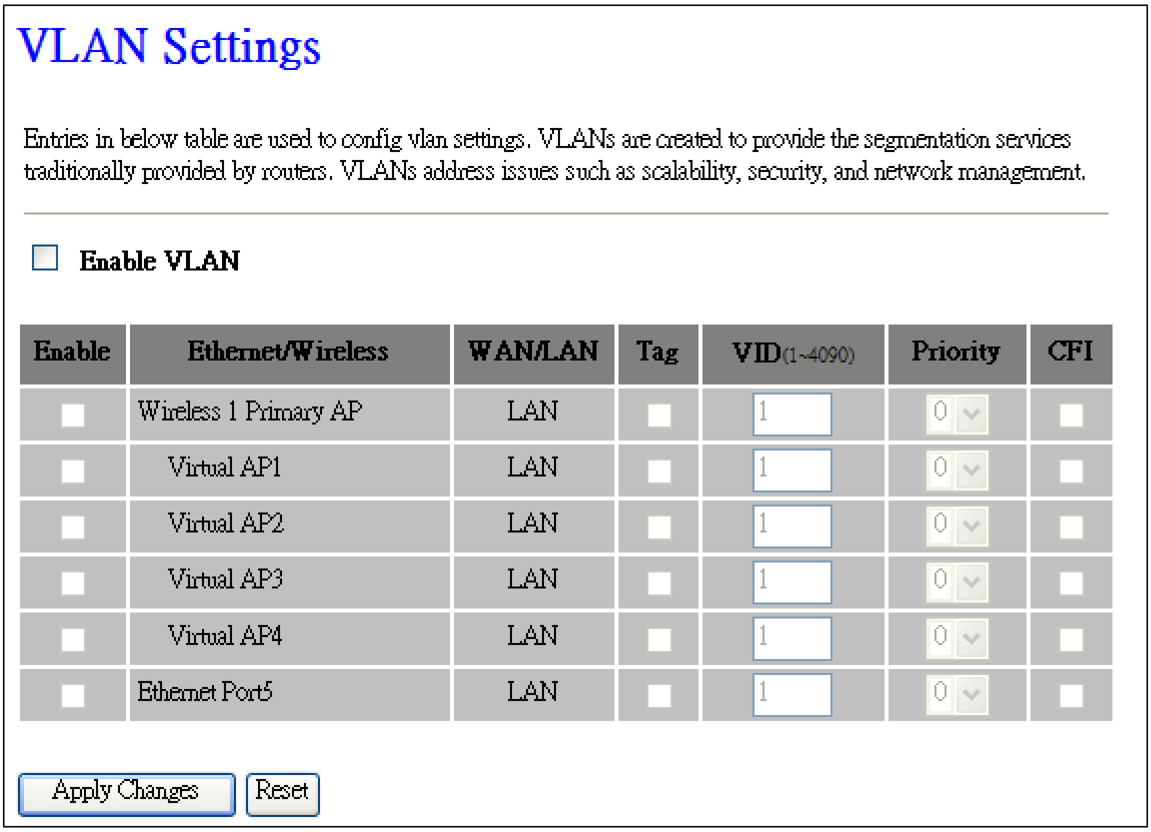


Wireless Basic Settings

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+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	default
Channel Width:	40MHz
Control Sideband:	Upper
Domain Region:	FCC
Channel Number:	Auto
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients



VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

□ Enable VLAN

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1~4090)	Priority	CFI
□	Wireless 1 Primary AP	LAN	□	1	0	□
□	Virtual AP1	LAN	□	1	0	□
□	Virtual AP2	LAN	□	1	0	□
□	Virtual AP3	LAN	□	1	0	□
□	Virtual AP4	LAN	□	1	0	□
□	Ethernet Port5	LAN	□	1	0	□

Enable VLAN

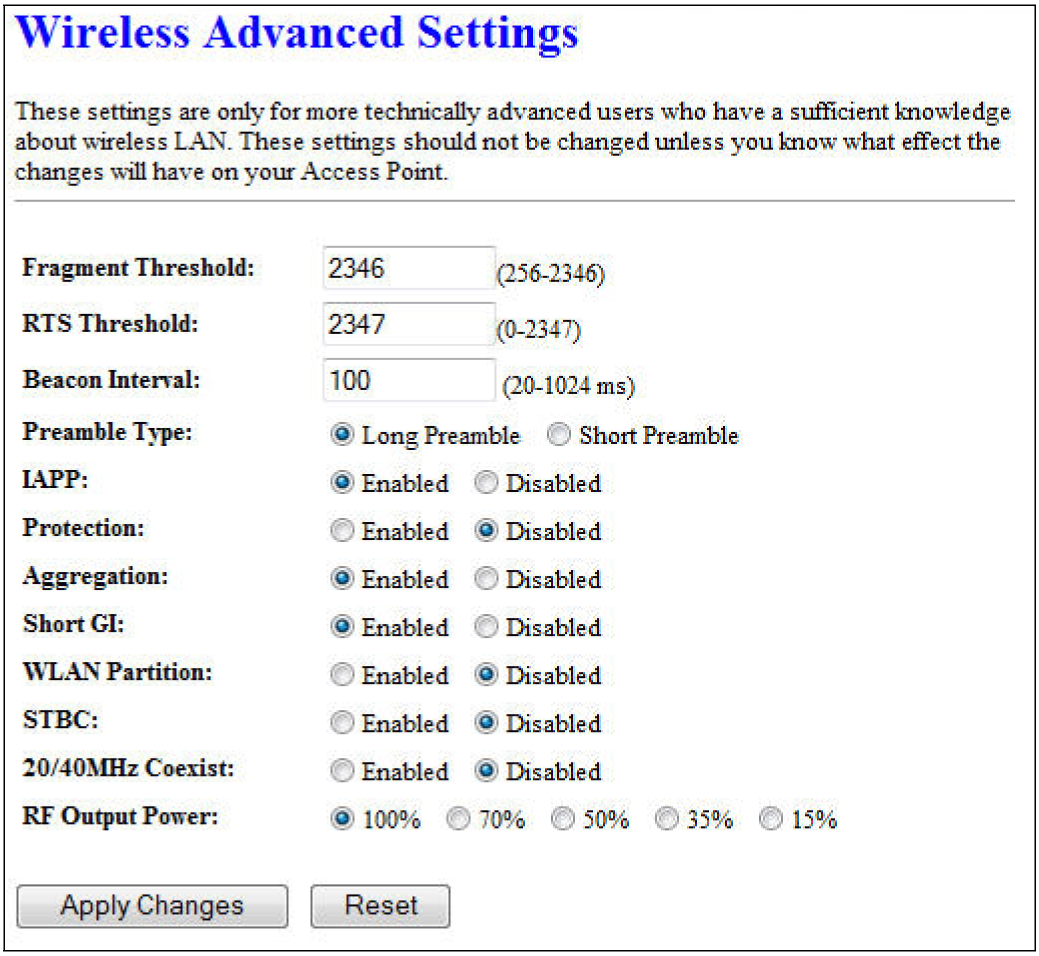
VLAN (Virtual Local Area Network) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management.

VID

Provide a number between 1 and 4090 for VLAN. This will cause the AP to send packets with VLAN tags. The switch connecting with the AP must support VLAN IEEE802.1Q frames. The wireless stations connecting to the SSID of a specified VLANID can communicate with the PC connecting to the port with the same VLANID on the Switch.

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.



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.

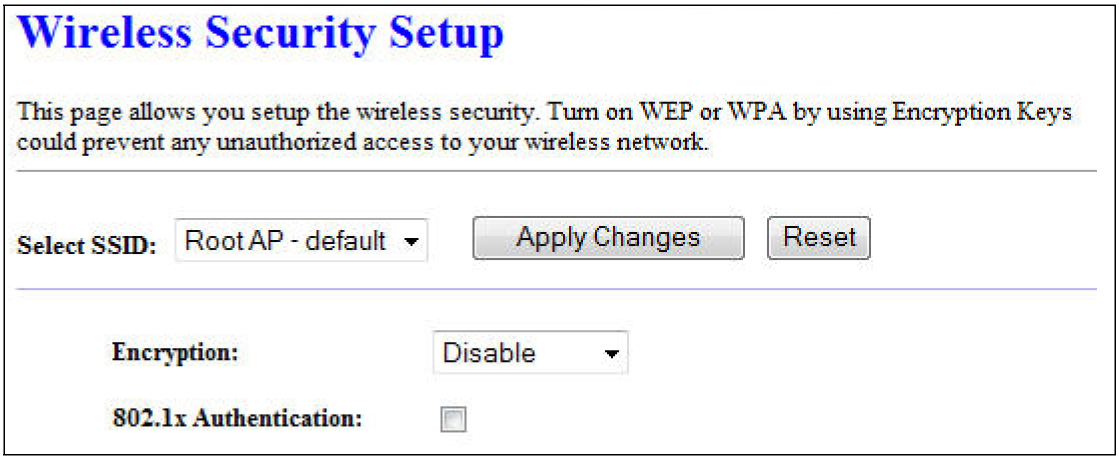
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Preamble Type:	● Long Preamble ○ Short Preamble
IAPP:	● Enabled ○ Disabled
Protection:	○ Enabled ● Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled
WLAN Partition:	○ Enabled ● Disabled
STBC:	○ Enabled ● Disabled
20/40MHz Coexist:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 70% ○ 50% ○ 35% ○ 15%

Fragment Threshold	"Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance. **Default :** 2346
RTS Threshold	When the packet size is smaller the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet. **Default :** 2347
Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network. **Default :** 100
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. "**Short Preamble**" is suitable for high traffic wireless network. "**Long Preamble**" can provide more reliable communication. **Default :** Long Preamble

IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
	Default : Enable
Protection	It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.
	Default : Enable
Aggregation	It is a function where the values of multiple rows are grouped together.
	Default : Enable
Short GI	It is used to set the time that the receiver waits for RF reflections to settle out before sampling data.
	Default : Enable
WLAN Partition	This feature also called WLAN isolation or Block Relay. If this feature is disabled, then there is no barrier between communications among wireless stations connecting to the Access Point, i.e the Access Point. If this is enabled, wireless stations of the selected band are not allowed to exchange data through the Access Point. The default value is set to 'Disabled'.
	Default : Disable
RF Output Power	Users can adjust the output power to 100%, 75% 50% 35% and 15%.
	Default : 100%

Security Setup

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



Wireless Security Setup

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

Select SSID: Root AP - default

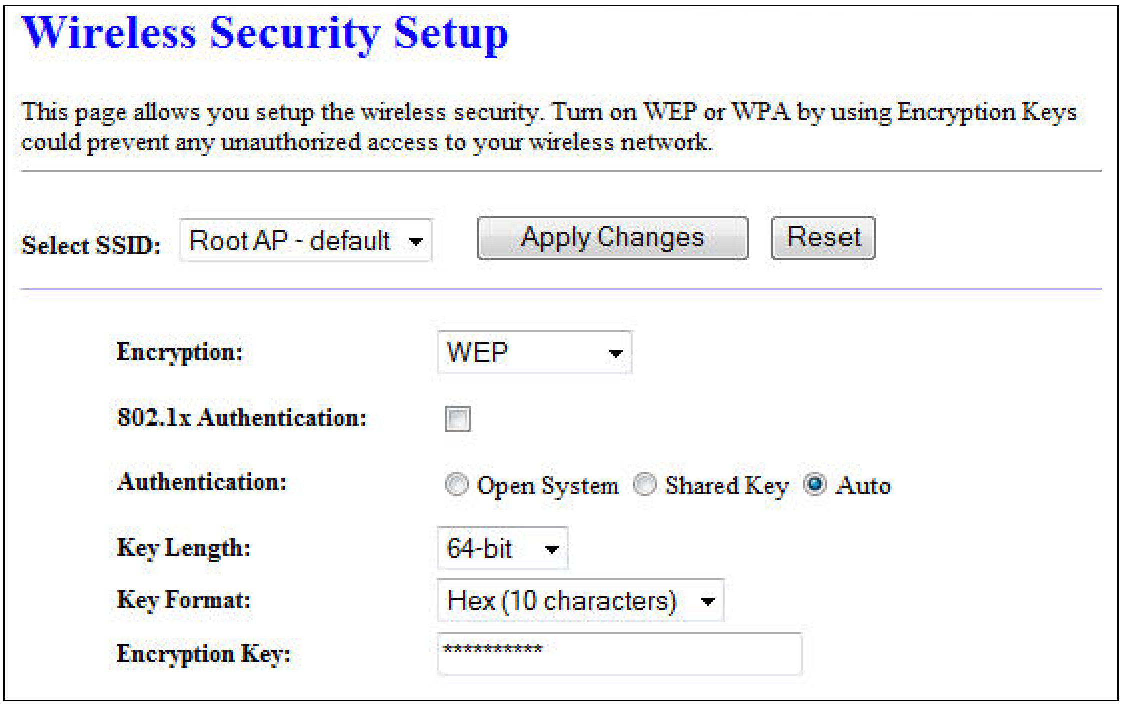
Encryption: Disable

802.1x Authentication: □

Select SSID	If assigned multiple AP feature, you could choose the SSID that want to setup encryption function.
Encryption	Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another. **Default :** Disable
802.1x Authentication	Check Box was used to switch the function of the 802.1X. When the 802.1X function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. **Default :** Uncheck

- WEP

When you select the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.



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.

Select SSID: Root AP - default

Encryption: WEP

802.1x Authentication: □

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

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

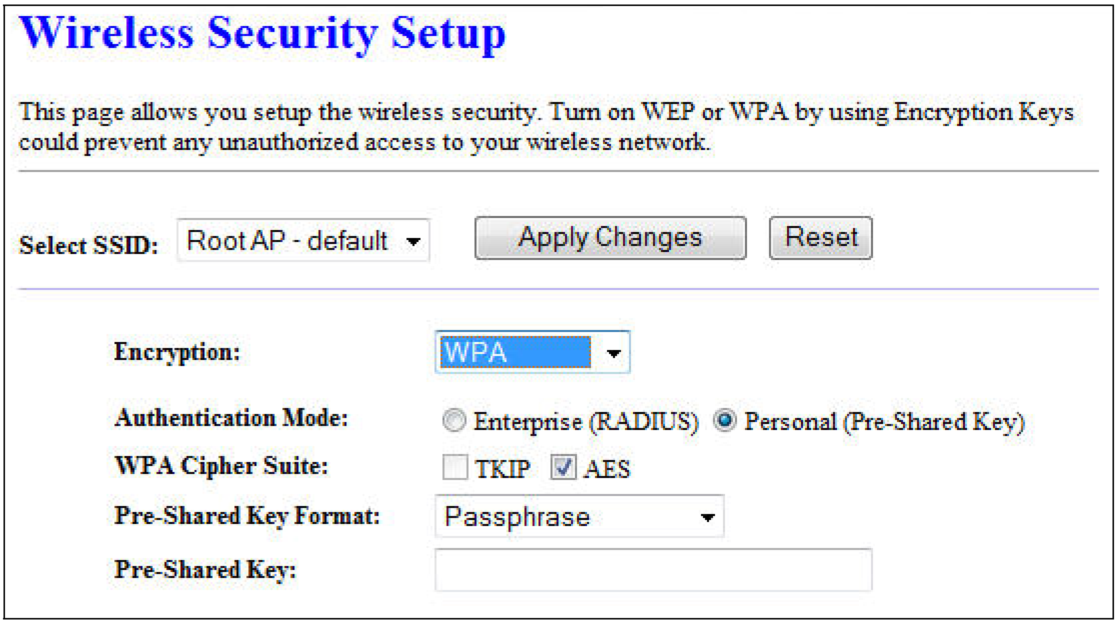
- WPA

When select the WPA function, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



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.

Select SSID: Root AP - default

Encryption: WPA

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

WPA Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

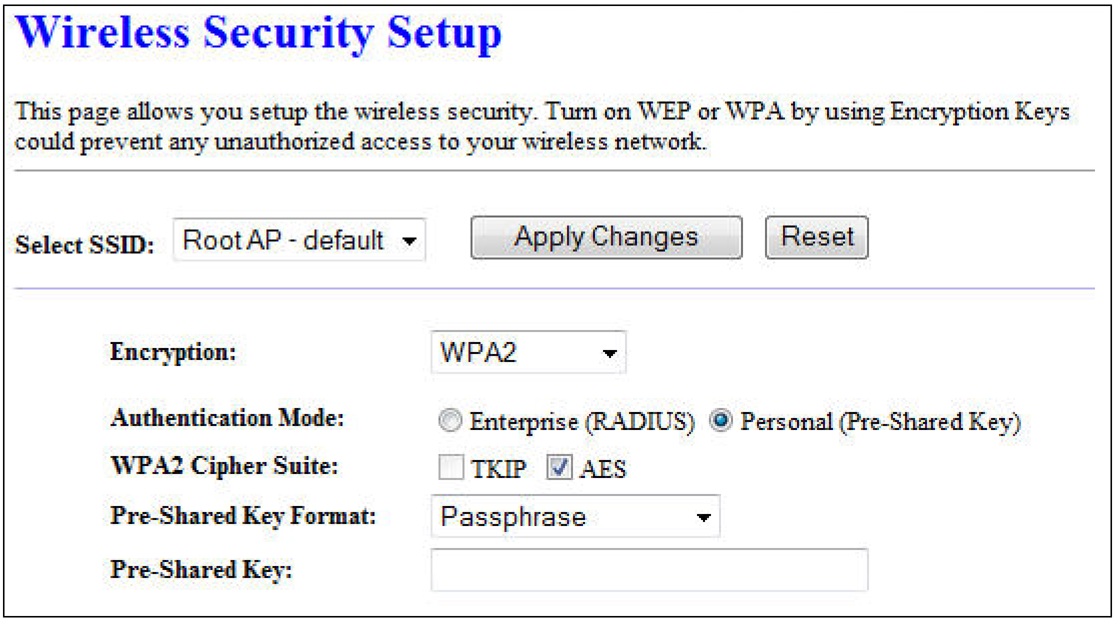
- WPA2

When select the WPA function, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



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.

Select SSID: Root AP - default

Encryption: WPA2

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

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

- WPA-Mixed

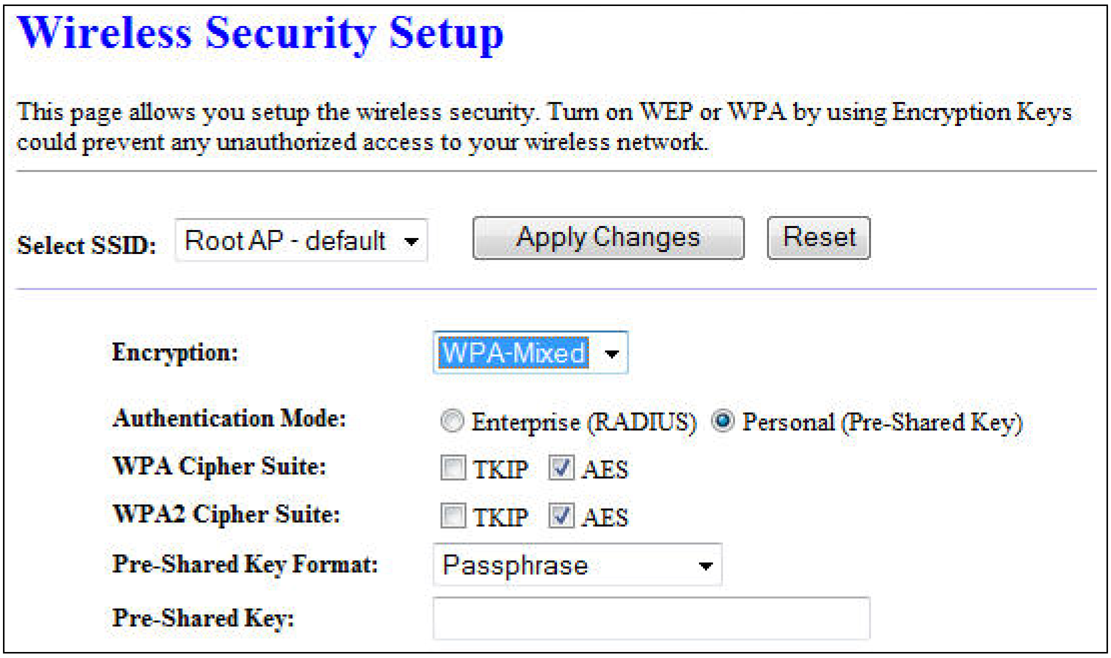
When select the WPA-Mixed function, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server

The router will detect automatically which Security type (WPA-PSK version 1 or 2) the client uses to encrypt. IP address or the 802.1X server's domain-name.

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



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.

Select SSID: Root AP - default

Encryption: WPA-Mixed

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

WPA Cipher Suite: □ TKIP ☑ AES

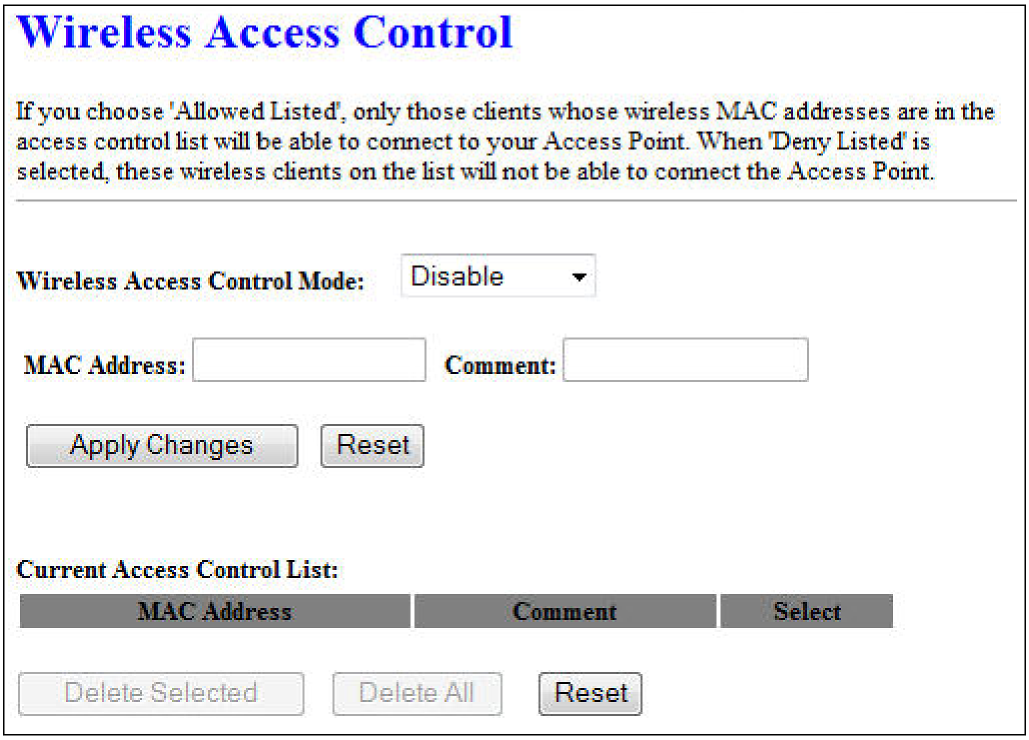
WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

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

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

Wireless Access Control Mode: Disable

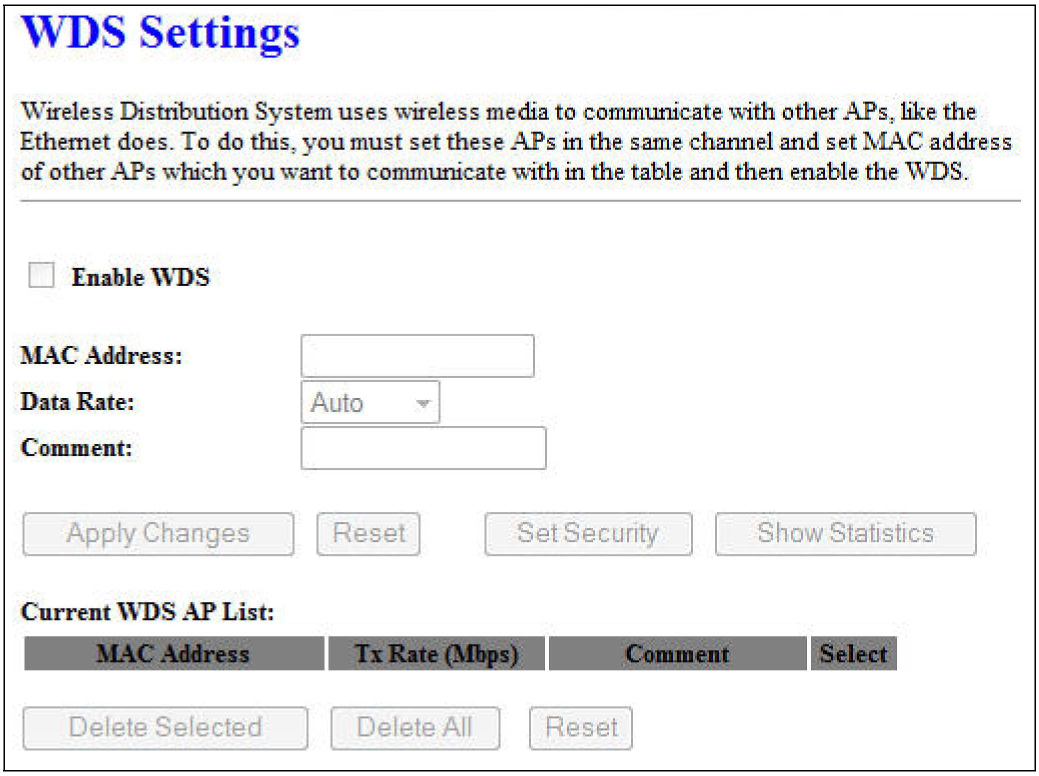
MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select

WDS Settings

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



WDS Settings

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

□ Enable WDS

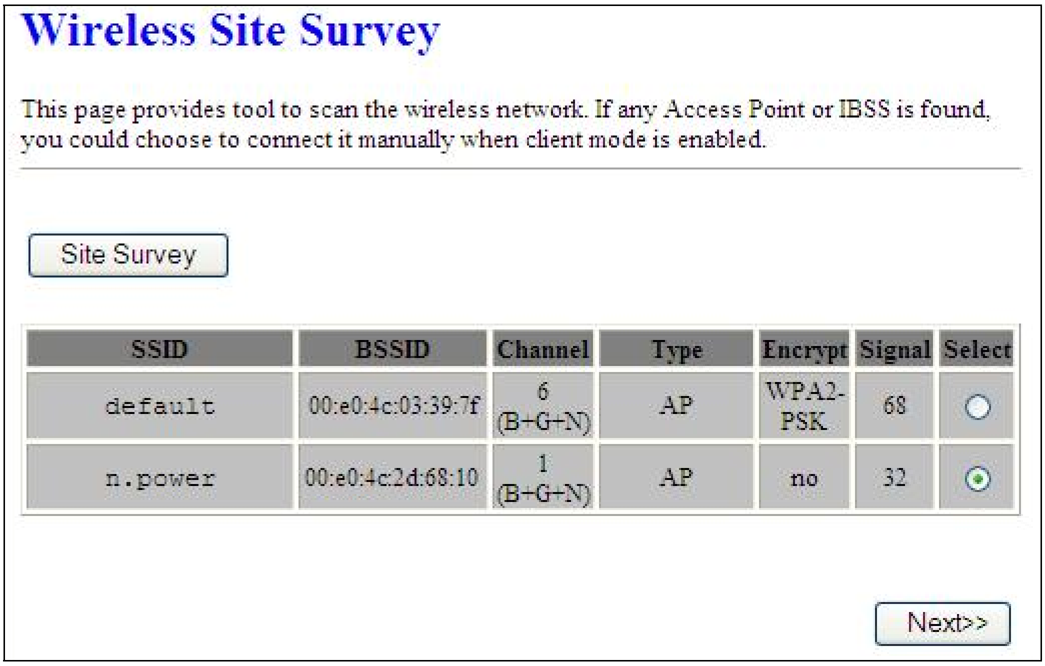
MAC Address:	
Data Rate:	Auto
Comment:	

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

Site Survey

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



Wireless Site Survey

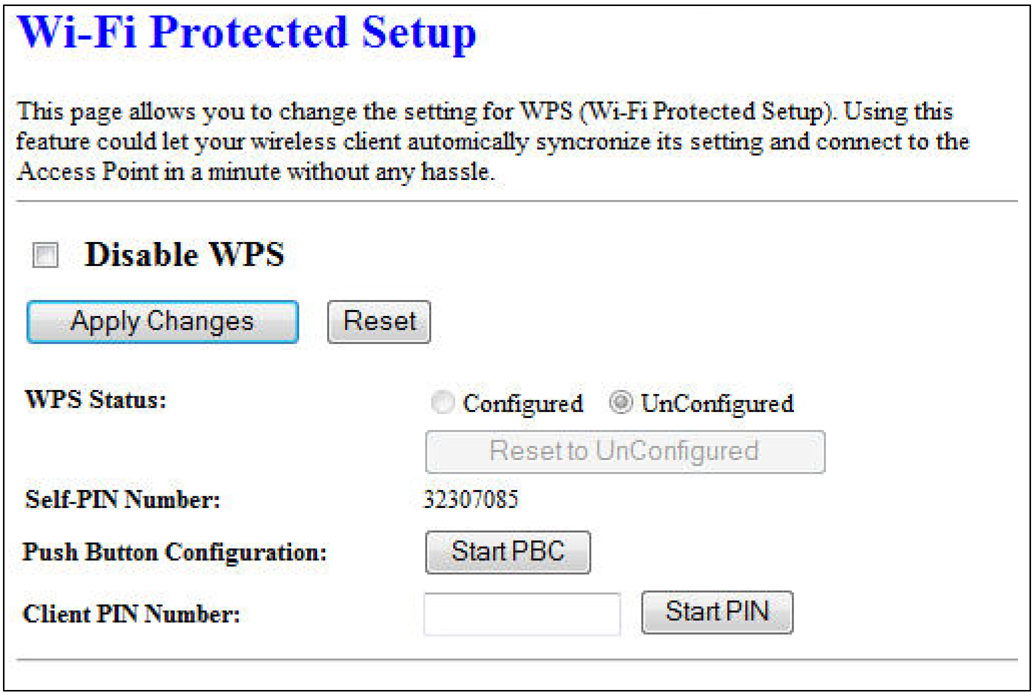
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
default	00:e0:4c:03:39:7f	6 (B+G+N)	AP	WPA2-PSK	68	○
n.power	00:e0:4c:2d:68:10	1 (B+G+N)	AP	no	32	●

WPS Settings

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this wireless router. You don’t have to select encryption mode and input a long encryption pass phrase every time when you need to setup a wireless client, you only have to press a button on wireless client and router, and the WPS will do the rest for you.

This wireless router supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless router to WPS mode too. You can push RET/WPS button of this wireless router, or click 'Start PBC' button in the web configuration interface to do this. If you want to use PIN code, you can see the setup as below.



Wi-Fi Protected Setup

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

□ Disable WPS

WPS Status: ○ Configured ● UnConfigured

Self-PIN Number: 32307085

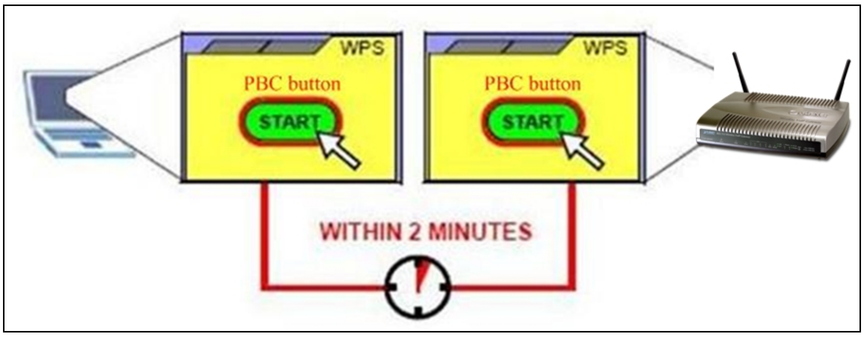
Push Button Configuration:

Client PIN Number:

Disable WPS	Check this box to disable WPS function, uncheck it to enable WPS.
WPS Status	If the wireless security (encryption) function of this wireless router is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'unConfigured'.
Self-PIN Number	This is the WPS PIN code of this wireless router. This code is useful when router sets as Enrollee, you need to fill this number into the web page of the other device.
Push Button Configuration	Click 'Start PBC' to start Push-Button style WPS setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The 'WLAN' LED on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.
Client PIN Number	Please input the PIN code of the other device you wish to connect, and click 'Start PIN' button. The 'WLAN' led on the wireless router will be steady on when this wireless router is waiting for incoming WPS request. (Please see the detail as below.)

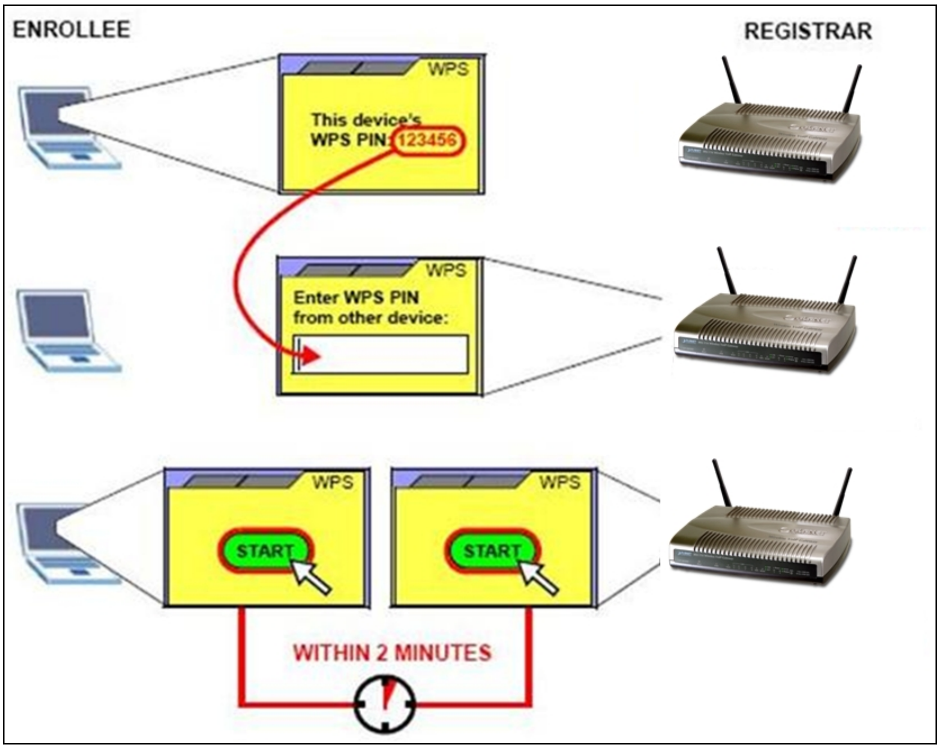
- PBC setup step:

1. Ensure you have set the security setting on Access Point (as Registrar).
2. Click the WPS button on Access Point (or the “Start PBC” button on the web interface of Access Point) and the other device (supports PBC function) in 2 minutes.
3. Access Point (Registrar) would send SSID and security key to the other device (Enrollee) through tunnel to connect.
4. If you see the wireless client in the list, WPS-PBC setting is successful.



- PIN (as register) setup step:

1. Fill the PIN code of the other device (as Enrollee that support WPS-PIN setting) into the “Client PIN Number” of Access Point.
2. Click the “Start PIN” buttons on Access Point and the other device in 2 minutes.
3. If you see the wireless client in the list, WPS-PIN setting is successful.



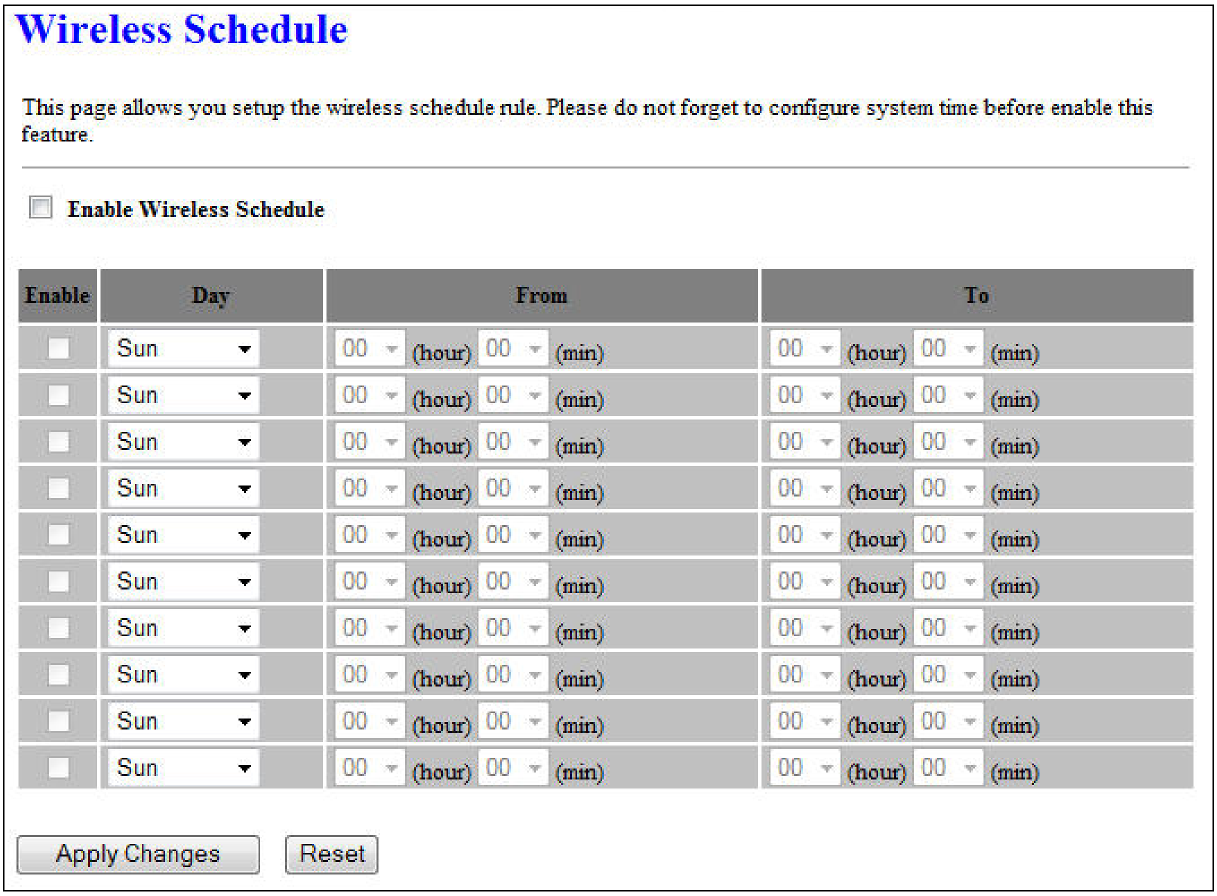
- PIN (as Enrollee) setup step:

1. Fill the PIN code of Access Point into the other device (as Registrar).
2. Click the “Start PIN” buttons on Access Point and the other device in 2 minutes.
3. If you see the wireless client in the list, WPS-PIN setting is successful.

**** As the figure as above, just change two roles.**

Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.



Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

□ **Enable Wireless Schedule**

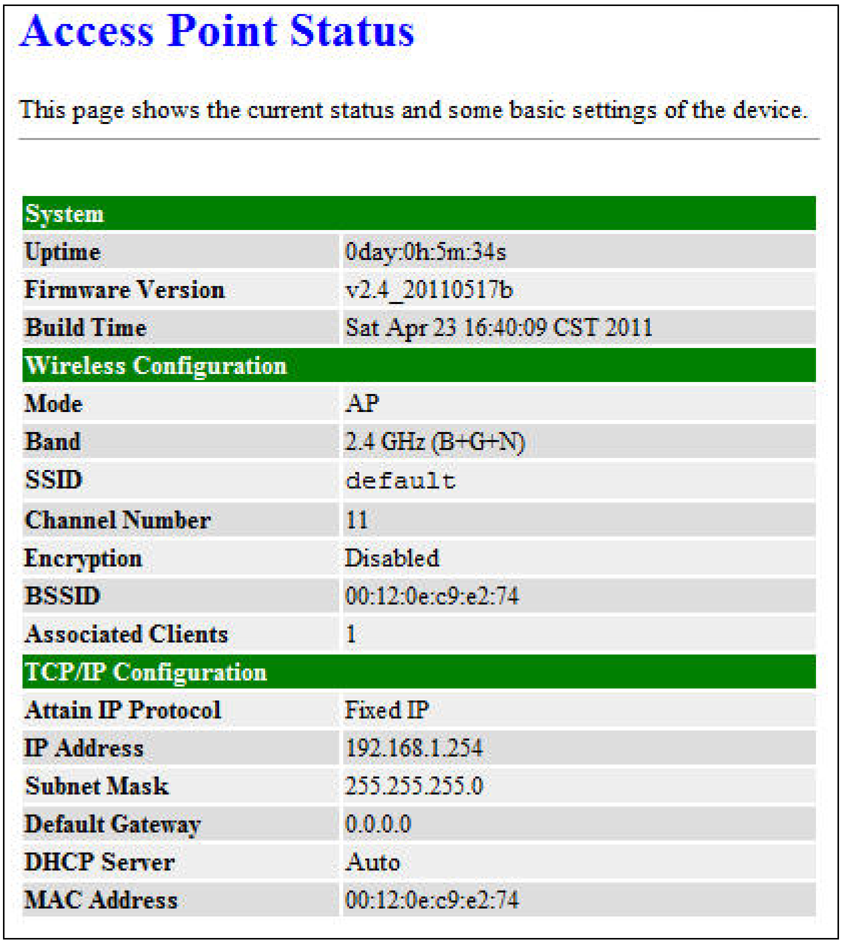
Enable	Day	From	To
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)

Chapter 6

Management

Status

In this page can show the current status and some basic settings of the Access Point.



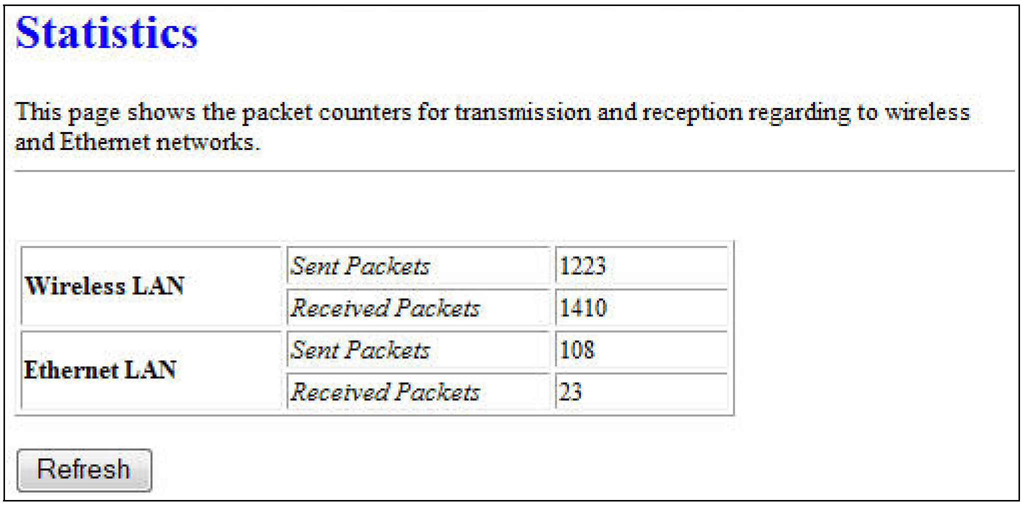
Access Point Status

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

System	
Uptime	0day:0h:5m:34s
Firmware Version	v2.4_20110517b
Build Time	Sat Apr 23 16:40:09 CST 2011
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	default
Channel Number	11
Encryption	Disabled
BSSID	00:12:0e:c9:e2:74
Associated Clients	1
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Auto
MAC Address	00:12:0e:c9:e2:74

Statistics

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



Statistics

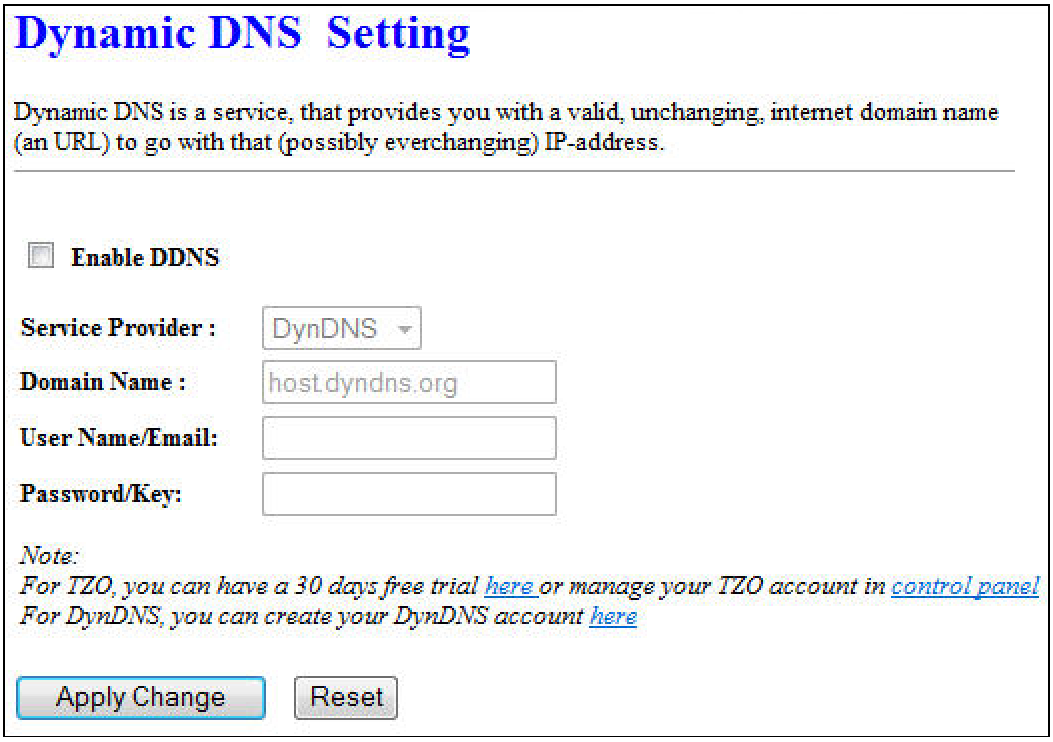
This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	1223
	Received Packets	1410
Ethernet LAN	*Sent Packets*	108
	Received Packets	23

DDNS

Choose menu “**Dynamic DNS**”, and you can configure the Dynamic DNS function when enabled router mode.

The Router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.



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

To set up for DDNS, follow these instructions:

Step 1. Check **Enable DDNS**.

Step 2. Select the **Service Provider** from the drop-down menu.

Step 3. Type the **Domain Name** received from your dynamic DNS service provider.

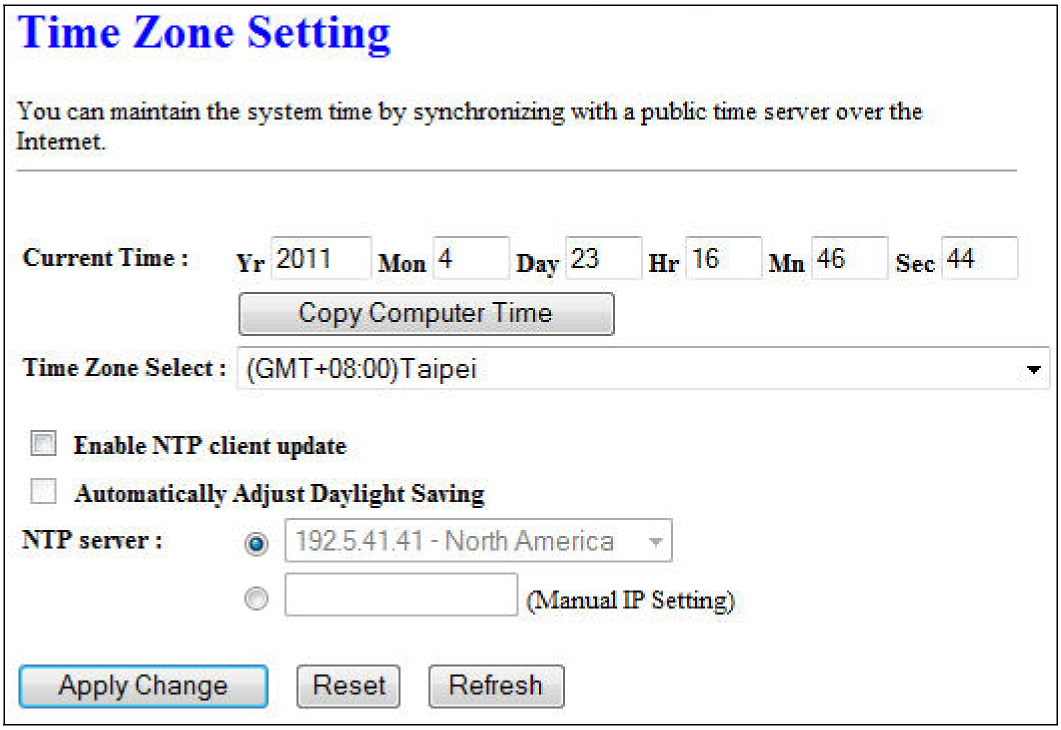
Step 4. Type the **User Name/Email** for your DDNS account.

Step 5. Type the **Password/Key** for your DDNS account.

Step 6. Click the **Apply Change** button to apply the settings.

Time Zone Setting

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



Time Zone Setting

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

Current Time : Yr 2011 Mon 4 Day 23 Hr 16 Mn 46 Sec 44

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

☐ Enable NTP client update

☐ Automatically Adjust Daylight Saving

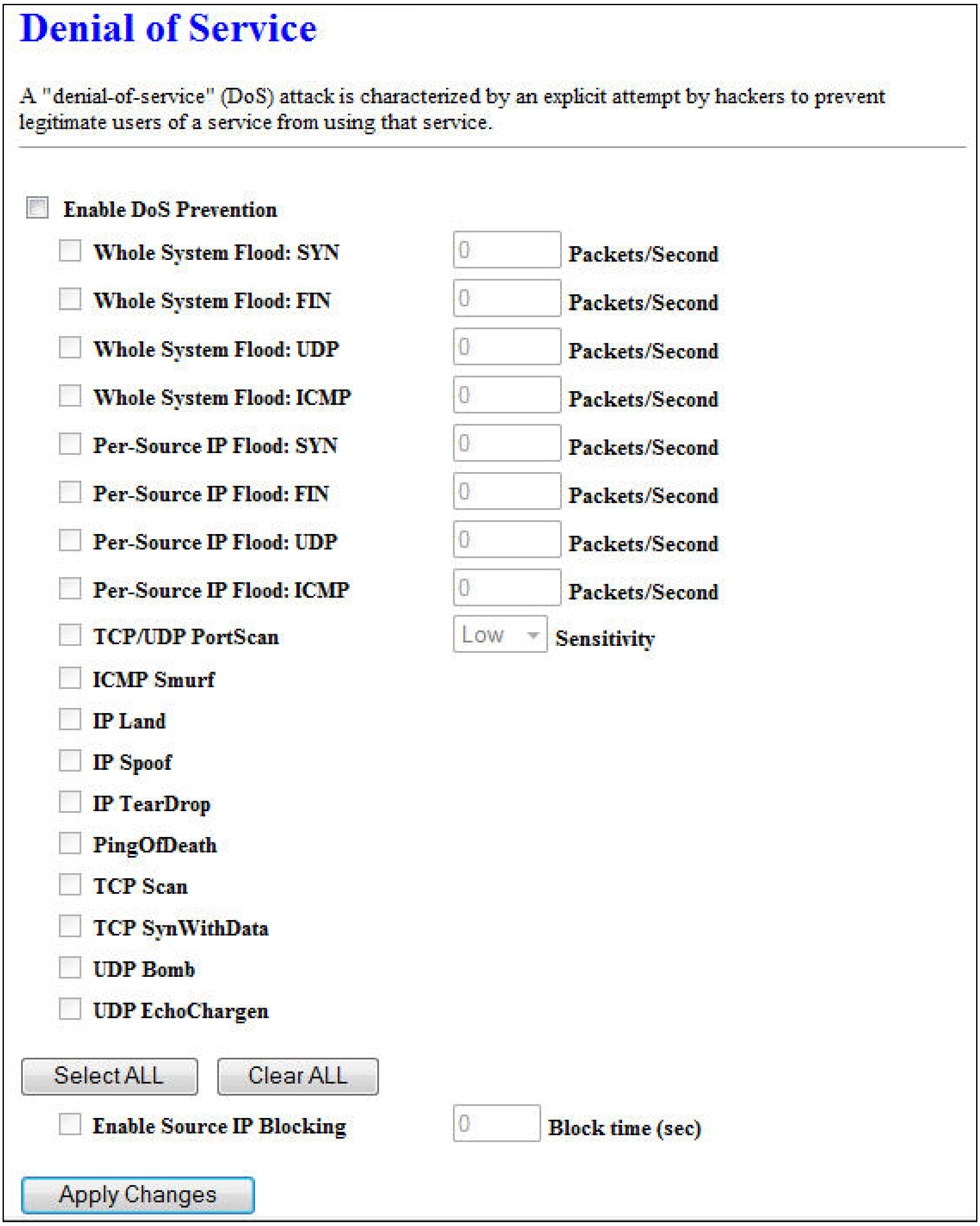
NTP server : ● 192.5.41.41 - North America

○ (Manual IP Setting)

Current Time	Input current time manually.
Time Zone Select	Select local time zone according to location.
Enable NTP client update	Check to enable NTP update. Once this function is enabled, Access Point will automatically update current time from NTP server.
NTP server	User may select prefer NTP sever or input address of NTP server manually.

Denial-of-Service

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks. This screen allows you to configure DoS protection.



Denial of Service

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

☐ Enable DoS Prevention

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

☐ ICMP Smurf

☐ IP Land

☐ IP Spoof

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

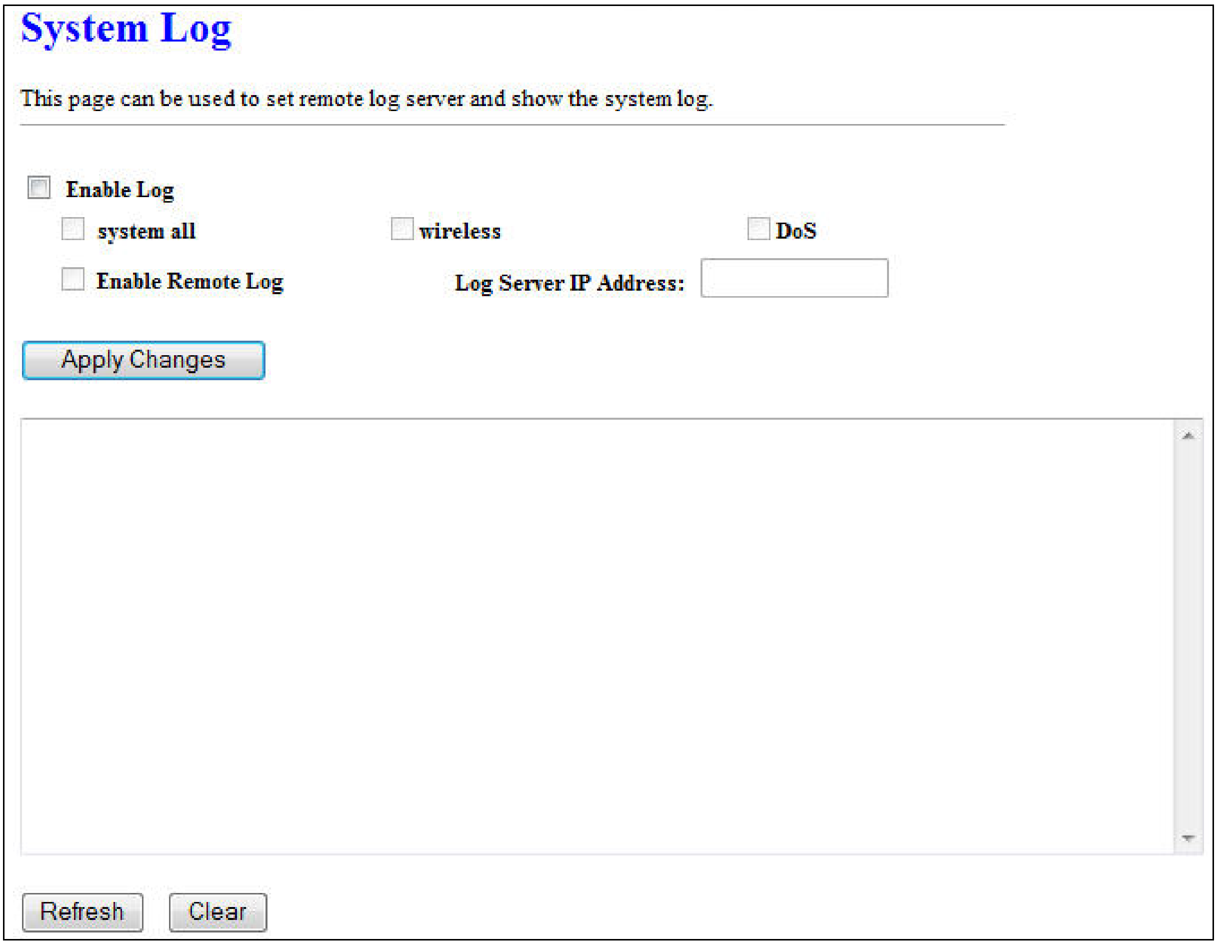
☐ UDP Bomb

☐ UDP EchoChargen

☐ Enable Source IP Blocking 0 Block time (sec)

Log

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



System Log

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

□ Enable Log

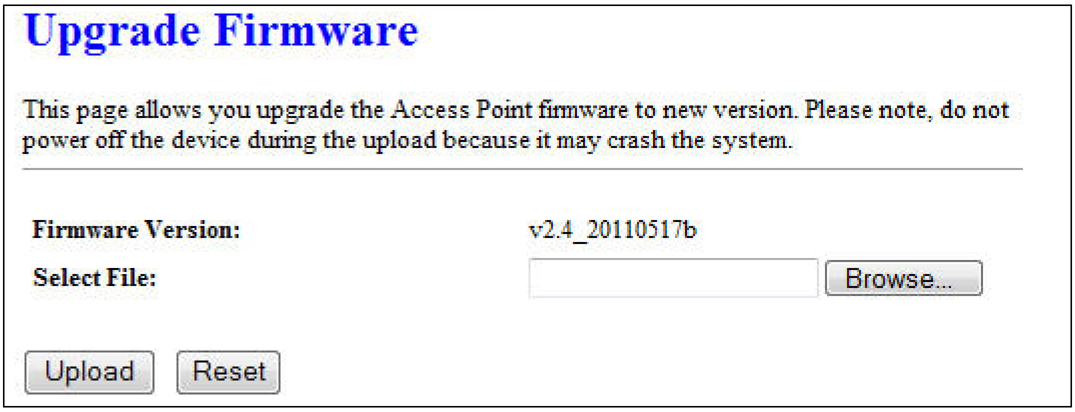
□ system all □ wireless □ DoS

□ Enable Remote Log Log Server IP Address:

Enable Log	Check to enable log function.
System all	Activates all logging functions.
Wireless	Only logs related to the wireless LAN will be recorded.
DoS	Only logs related to the DoS protection will be recorded.
Enable Remote Log	Only logs related to the Remote control will be recorded.
Log Server IP Address	Only logs related to the server will be recorded.

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.



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.

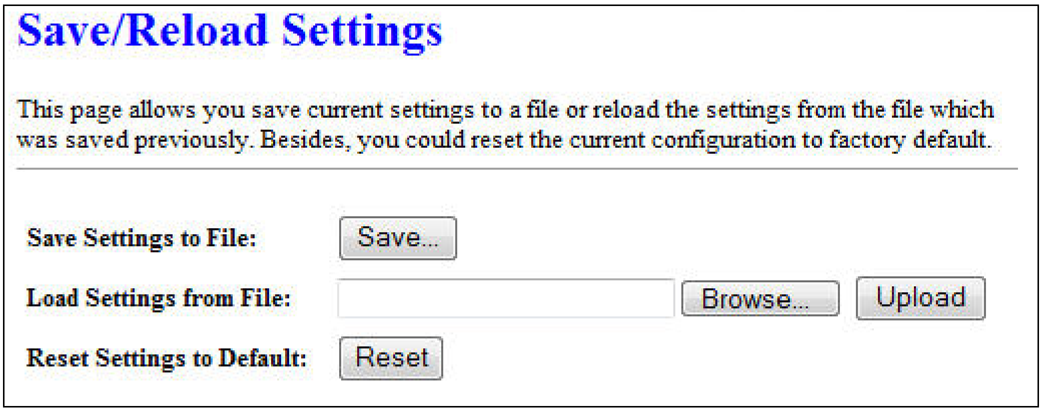
Firmware Version: v2.4_20110517b

Select File:

Firmware Version	The current version is shown in this field.
Select File	Browse and select file you want to upgrade and press Upload to perform upgrade. **Please wait till on screen shows related information after upgrade finished.**
Upload	Click the **Upload** button to perform the upgrade process.
Reset	Click **Reset** will clean all current configurations and return to default values.

Save / Reload Settings

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



Save/Reload Settings

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

Save Settings to File:

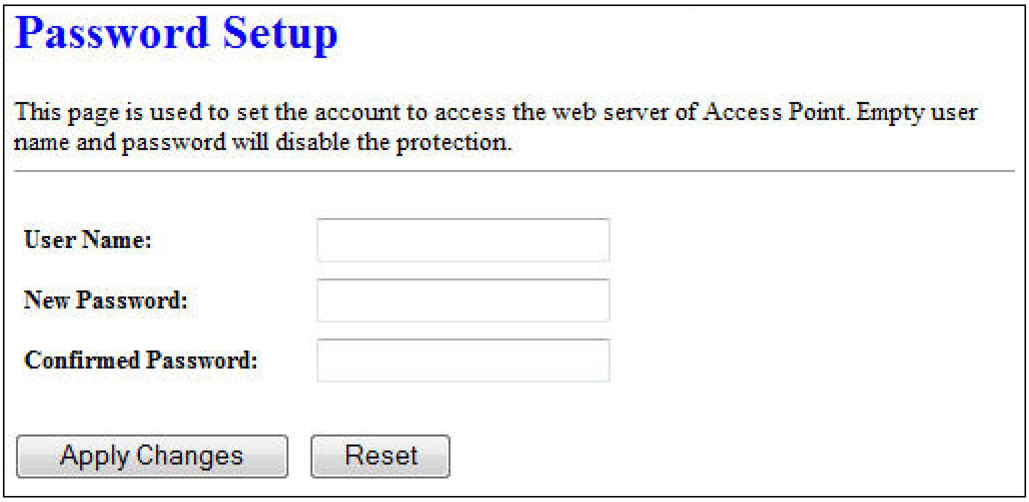
Load Settings from File:

Reset Settings to Default:

Save Settings to File	Save current settings to a file.
Load Settings from File	Browse a file and upload to reload settings.
Reset Settings to Default	Click **Reset** button to restore to factory default values.

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.



Password Setup

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

User Name:

New Password:

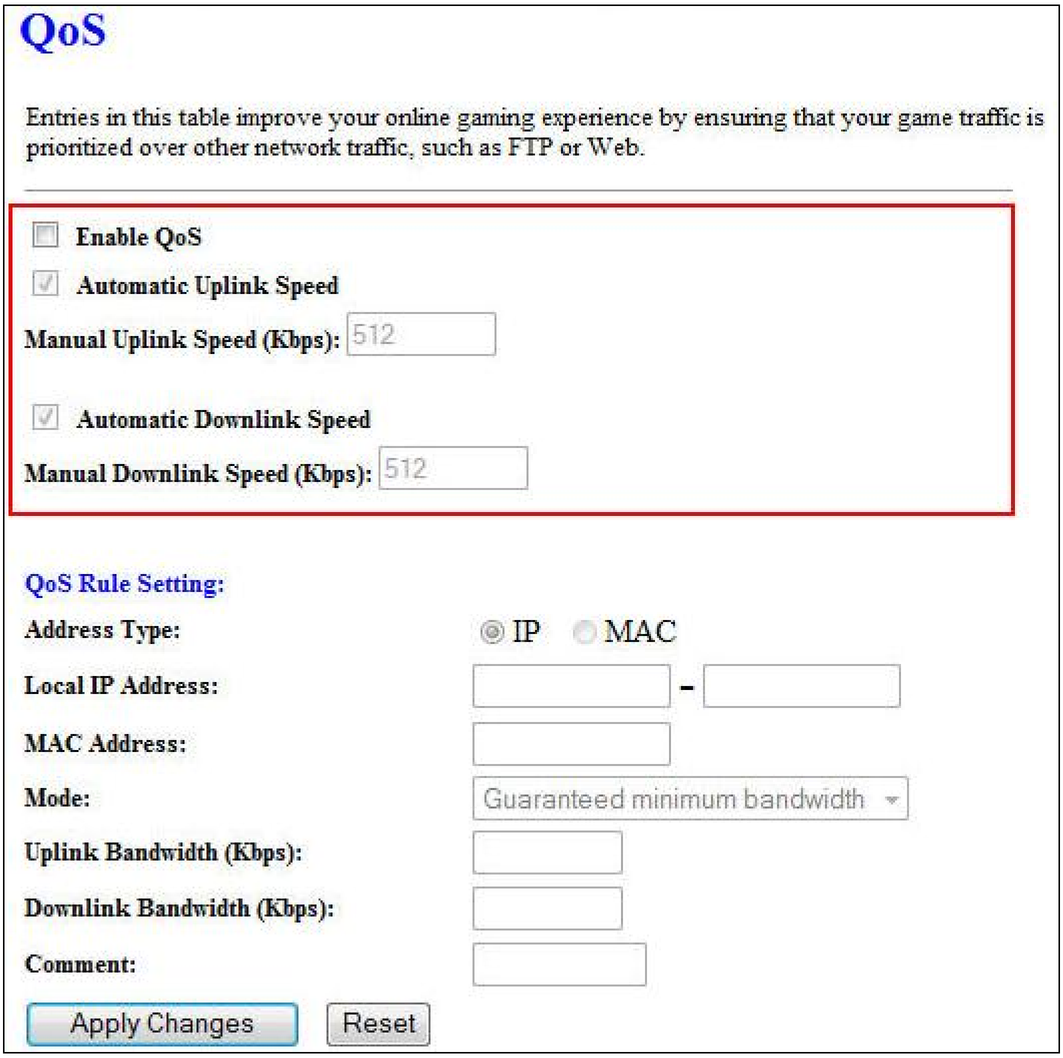
Confirmed Password:

User Name	Enter user name.
New Password	Input password for this user.
Confirmed Password	Confirm password again.

Chapter 7
QoS

Enable QoS

Use this section to configure QoS. The QoS settings improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.



QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

□ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps): 512

☑ Automatic Downlink Speed

Manual Downlink Speed (Kbps): 512

QoS Rule Setting:

Address Type: ● IP ○ MAC

Local IP Address: -

MAC Address:

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps):

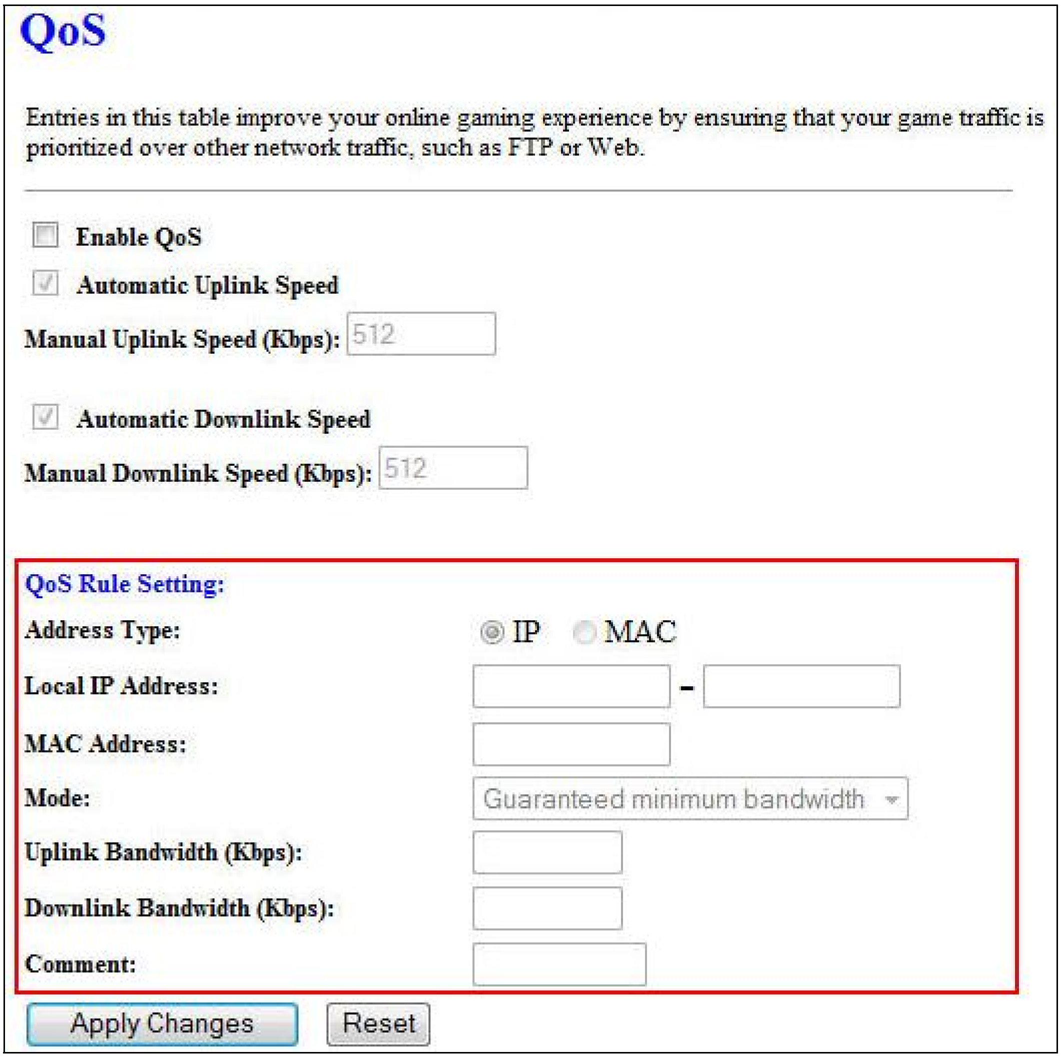
Downlink Bandwidth (Kbps):

Comment:

Enable QoS	Check the box to enable the QoS function.
Automatic Uplink/Download Speed	Check the box to enable the automatic uplink/ download speed function.
Manual Uplink/Download Speed	User can manually enter the uplink/ download speed in the blank field.

QoS Rule Setting

Administrator can setup a QoS rule for specific user depends on IP or MAC address.



QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

☐ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps): 512

☑ Automatic Downlink Speed

Manual Downlink Speed (Kbps): 512

QoS Rule Setting:

Address Type: ● IP ○ MAC

Local IP Address: ______ - ______

MAC Address: ______

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps): ______

Downlink Bandwidth (Kbps): ______

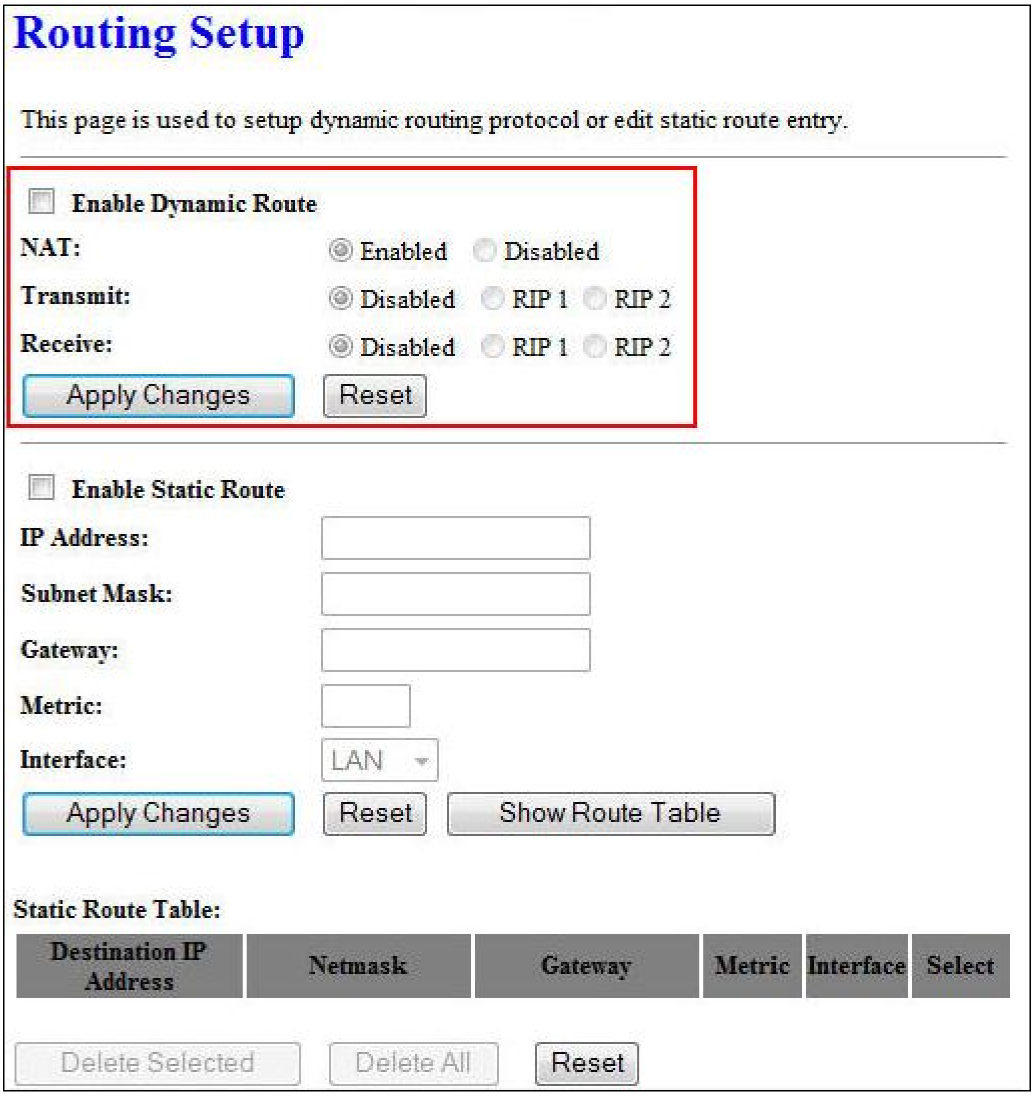
Comment: ______

Address Type	Select IP or MAC address type.
Local IP Address	Depend on the address type that selected, user can enter the IP address or MAC address of client to set up the bandwidth of the transmission.
MAC Address	
Mode	Select Guaranteed minimum bandwidth or Restricted maximum bandwidth modes.
Uplink Bandwidth (Kbps)	Enter the Uplink Bandwidth (Kbps) in the column.
Downlink Bandwidth (Kbps)	Enter the Downlink Bandwidth (Kbps) in the column.
Comment	Enter the note for the setting.

Chapter 8
Route Setup

Dynamic Route

Dynamic routing performs the same function as static routing except it is steadier. Dynamic routing allows routing tables in routers to change as the possible routes change. There are several protocols used to support dynamic routing including RIP and OSPF.



Routing Setup

This page is used to setup dynamic routing protocol or edit static route entry.

□ **Enable Dynamic Route**

NAT: ● Enabled ○ Disabled

Transmit: ● Disabled ○ RIP 1 ○ RIP 2

Receive: ● Disabled ○ RIP 1 ○ RIP 2

□ **Enable Static Route**

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface: LAN

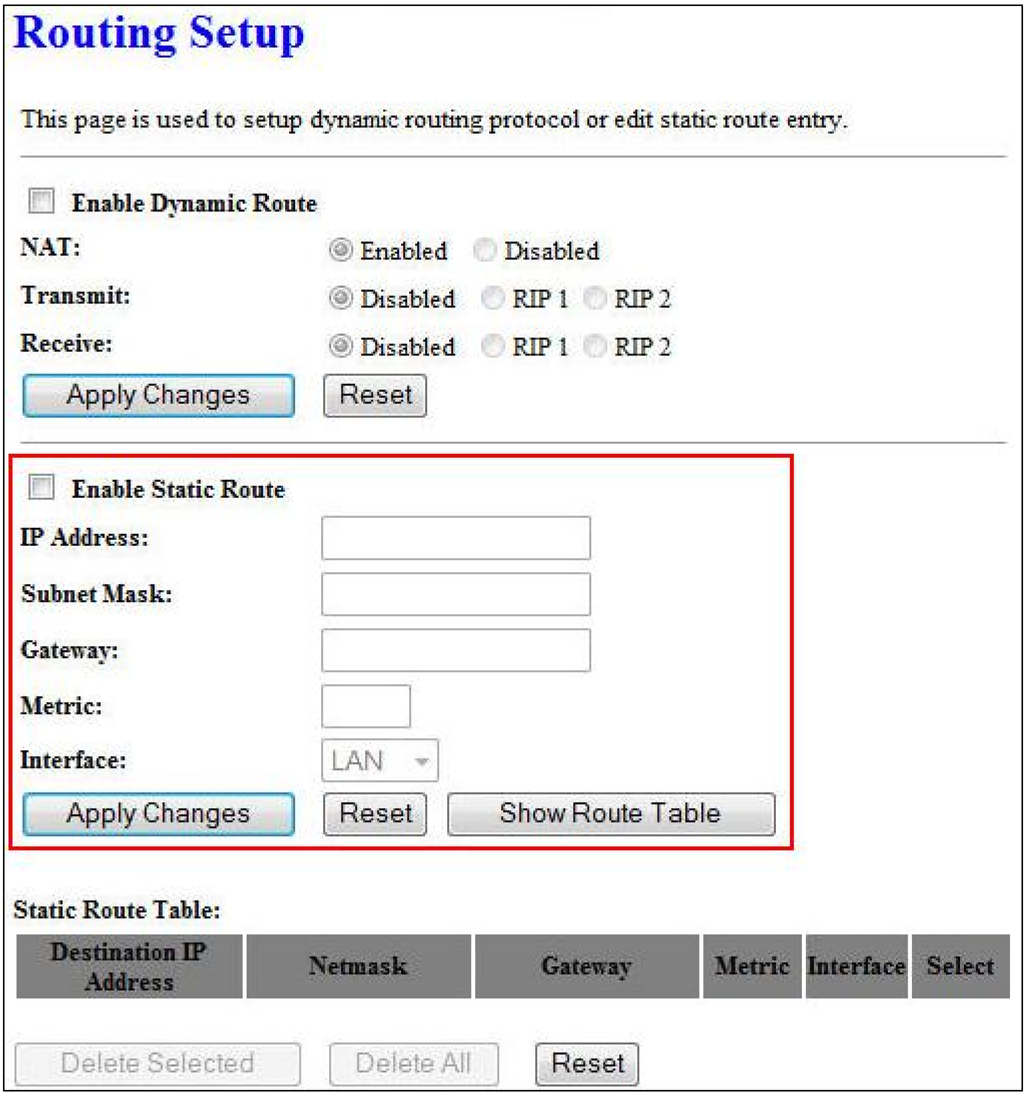
Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select

Enable Dynamic Route	Check the box to enable the Dynamic Route function.
NAT	Network Address Translation (NAT) selects to enable or disable this function.
Transmit	Select to enable or disable RIP protocol for transmit.
Receive	Select to enable or disable RIP protocol for receive.

Static Route

To set static routers, enter the settings including route IP address, route mask, route gateway and the route Interface from LAN or WAN.



Routing Setup

This page is used to setup dynamic routing protocol or edit static route entry.

☐ **Enable Dynamic Route**

NAT: ● Enabled ○ Disabled

Transmit: ● Disabled ○ RIP 1 ○ RIP 2

Receive: ● Disabled ○ RIP 1 ○ RIP 2

☐ **Enable Static Route**

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface: LAN

Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select

Enable Static Route	Check the box to enable the Static Route function.
IP Address	Set up the IP address that would like to send the packets pass through.
Subnet Mask	Set up the Subnet Mask that would like to send the packets pass through.
Gateway	Set up the gateway that would like to send the packets pass through.

Metric	It is used by a router to make routing decisions. The metrics used by a router to make routing decisions. It is typically one of many fields in a routing table. Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination. A router metric typically based on information like path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.
Interface	Select the interface of the setting path.

Appendix A Frequently Asked Questions List

If your Access Point is not functioning properly, you can refer to this chapter first for sample troubleshooting before contacting your dealer. This can save your time and effort but if the symptoms persist, please consult your dealer.

Q1: I forget my Access Point login username and / or password

A1:

1.) Restore Access Point to its factory default settings by pressing the “Reset” button which is at the side panel of the device for 5 seconds or more.

Appendix B Access Point Specifications (TBD)

Product	802.11n Wireless Access Point
Model	N-WAP
Hardware	
WLAN Standards	IEEE 802.11 b/g/n
Wireless Frequency Range	2.4GHz ~ 2.4835 GHz
Operation Mode	AP, Client, Router
Wireless Mode	AP, WDS and AP+WDS mode
Security	64/128 bit WEP data encryption, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 mix mode, 802.1x encryption and WPS PBC
Operating Frequencies / Channel	USA/Canada: 2.412 GHz – 2.426 GHz (11 channels) Europe: 2.412 GHz – 2.472 GHz (13 channels) Japan: 2.412 GHz – 2.477 GHz (14 channels)
Wireless Data Rate	IEEE 802.11b: CCK (11Mbps,5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps) IEEE 802.11g: OFDM (54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps) IEEE 802.11n: 14/29/43/58/87/116/130/144Mps in 20MHz, 30/60/90/120/180/240/270/300Mbps in 40MHz
Transmit Power	802.11b: 17dBm 802.11g: 15dBm 802.11n: 13dBm
Receiver Sensitivity	802.11b: -86dBm @11M 802.11g: -72dBm @54M 802.11n (20MHz): -68dBm 802.11n (40MHz): -66dBm
Antenna	2 x Antenna
WDS	WDS repeater support
LAN	1 x 10/100 Base-TX RJ-45 port
Protocols and Standard	
Protocols	TCP/IP, UDP/RTP/RTCP, HTTP, ICMP, ARP, DNS, DHCP, NTP/SNTP
Security	Password protection for system management
Network and Configuration	
Access Mode	Static IP, DHCP Client, PPPoE, PPTP, L2TP
Configuration & Management	Web-Based Graphical User Interface Remote management over the IP Network Web-Based firmware upgrade Backup and Restore Configuration file
Dimension (W x D x H)	
Operating Environment	0~50 Degree C 5~90% humidity
Power Requirement	
EMC/EMI	