legrand®

Wireless Access Point – N

(P/N DA1101)

Owner's Manual

1308137 Rev. A

This device complies with Part 15 of the FCC Rules and RSS-210 Issue 8 of Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

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

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

Reprinted from the Code of Federal Regulations #47, part 15.193, 1993. Washington DC: Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office.

Canadian Department of Communications

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

FCC Radio Frequency Exposure Caution Statement

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations. Any changes of modifications not expressly approved by the grantee of this device could void the users authority to operate the equipment.

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Declaration of Conformity (R&TTE directive 1999/5/EC)

The following items were completed and are considered relevant and sufficient:

- Essential requirements as in [Article 3]
- Protection requirements for health and safety as in [Article 3.1a]
- Testing for electric safety according to [EN 60950]
- Protection requirements for electromagnetic compatibility in [Article 3.1b]
- Testing for electromagnetic compatibility in [EN 301 489-1] & [EN 301]
- Testing according to [489-17]
- Effective use of the radio spectrum as in [Article 3.2]
- Testing for radio test suites according to [EN 300 328-2]

WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING WATER.

CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL.

CAUTION: THIS DEVICE MUST BE INSTALLED AND USED IN STRICT ACCORDANCE WITH THE MANUFACTURER'S INSTRUCTIONS AS DESCRIBED IN THE USER DOCUMENTATION THAT COMES WITH THE PRODUCT.

WARNING: POSTPONE INSTALLATION UNTIL THERE IS NO RISK OF THUNDERSTORM OR LIGHTNING ACTIVITY IN THE AREA.

When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Read all of the instructions {listed here and/or in the user manual} before you operate this equipment.
- Give particular attention to all safety precautions.
- Retain the instructions for future reference.
- Comply with all warning and caution statements in the instructions.
- Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- Avoid using this product during an electrical storm. There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug the power supply, and disconnect the Cat 5e to the N-WAP at the POE Inserter. This will prevent damage to the product due to lightning and power surges. It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the equipment by local lightning strikes and other electrical surges. A Data Surge Conditioning Unit is also available from Legrand (P/N 364598-01) to help protect the data connection from the POE Injector to the N-WAP.
- Operate this product only from the type of power source indicated on the product's marking label.
- If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

Installation of this product must be in accordance with national wiring codes and conform to local regulations.

Place POE Inserter to allow for easy access when disconnecting the power cord/adapter of the device from the AC wall outlet.

Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

When not utilizing the recommended 3-gang or 1-gang plastic switch & outlet box, do not directly cover the device, or block the airflow to the device with insulation or any other objects.

Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.

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 our Wireless Access Point family: the DA1101 N-WAP.

The N-WAP provides 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 in an even wider 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

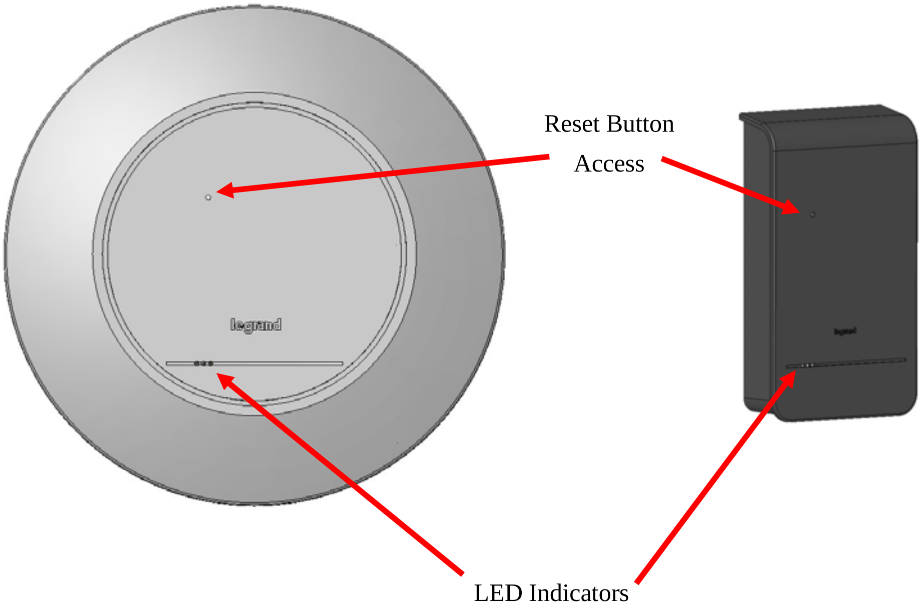
Package Content

The contents of your product should contain the following items:

- DA1101 802.11n Wireless Access Point
- POE Module w/AC adapter
- Installation Bracket
- Round and Rectangular Cover
- Installation/Instruction Sheet

Physical Details

The following figures illustrate the 3-gang (round) and 1-gang (rectangular) versions of an installed DA1101 N-WAP.

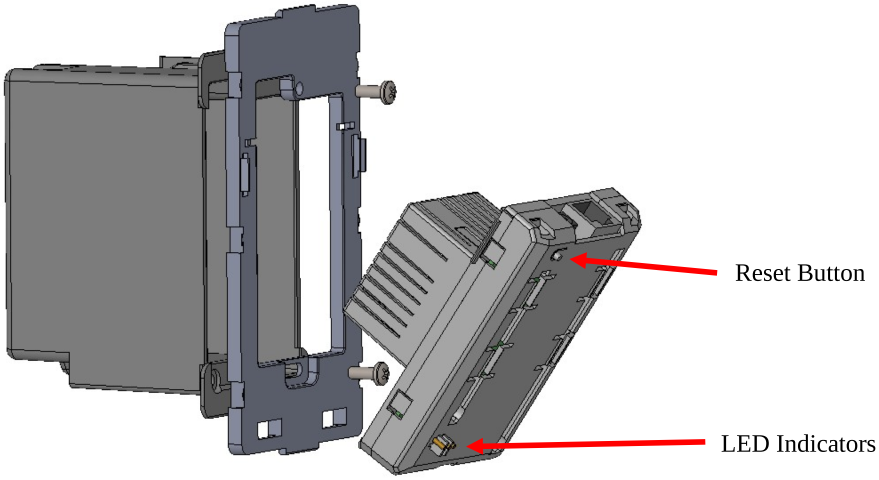


LED Indicators:

LED	Color	State	Descriptions
Ethernet	Green	Solid Green Blinking Green	Power Present Ethernet Active
Power	Blue/Orange	Blue Solid Orange Blinking Orange	Power OK Initializing Signal Survey
WiFi	Green/Red	Solid Green Blinking Green Red	Connected Streaming in Session No WiFi Signal

Reset Button:

The DA1101 has a reset button accessible through either cover or with the cover off that can be pushed and held for 10 seconds to reset the DA1101 to factory default condition (the IP address is reset to 192.168.1.254).



Chapter 2

Physical Installation

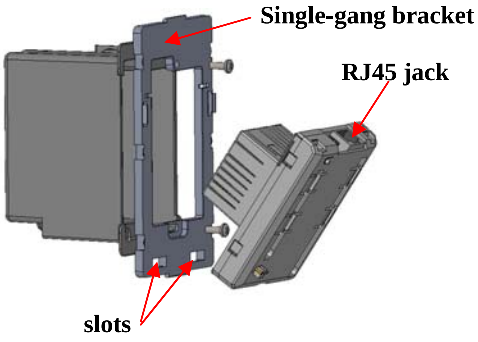
Physical Installation Steps

This chapter illustrates the physical installation of the DA1101 Wireless Access Point –N.

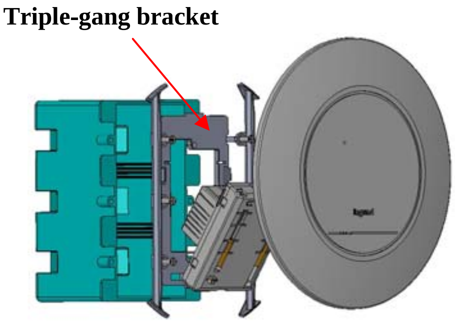
1. Run a Category 5 cable from the triple-gang or single-gang electrical box at the intended DA1101 room location to the POE module located in the structured wiring enclosure.

2. Make sure that the Power Supply is not connected to the POE module at this time.

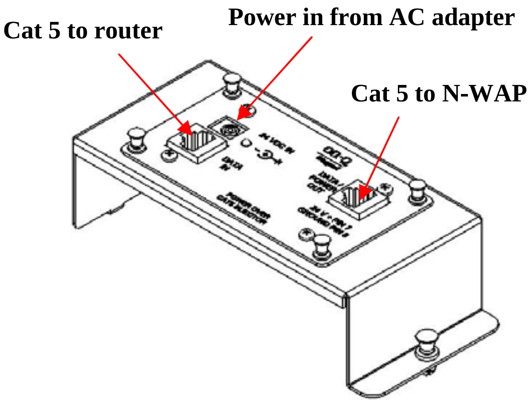
3. Pull the Category 5 cable out from the electrical box through the supplied triple-gang or modified into a single-gang bracket and attach the bracket to the associated electrical box with the supplied screws.



4. Terminate the Cat 5 cable with an RJ45 plug and connect it to the RJ45 jack on the DA1101. The DA1101 is then snapped into the mounting bracket by first inserting the two tabs on one end into the slots on the bracket and tilting it until it is flush with the bracket, where it should snap into place.



5. If this is a triple-gang installation, line the feet on the triple gang bracket up with the indentions inside the round cover, and snap that cover in place. There is a protrusion inside the round cover that allows it only to be installed in the correct orientation. If this is a single-gang installation, simply hang the top of the rectangular cover on the single-gang bracket and tilt the cover to snap it into place.



6. In the enclosure, terminate the other end of the Cat 5 cable from the DA1101 with an RJ45 plug and connect it to the POE output RJ45 jack. A Cat 5 jumper is run from the POE input jack to a local router port.

7. Plug the power supply into the POE module and into an AC outlet, and refer to the next chapter for software configuration and operation information.

Chapter 3

Network Settings

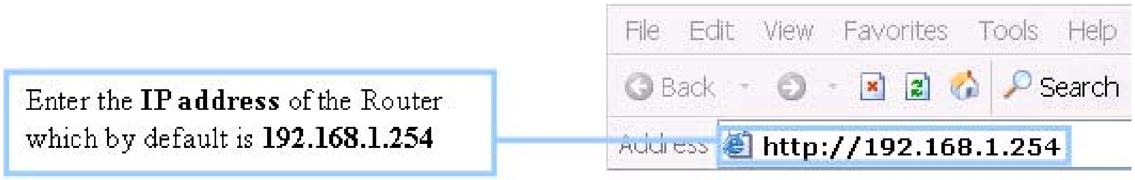
Configuring and monitoring your DA1101 from web browser

The DA1101 integrates a web-based graphical user interface that can cover most configurations and machine status monitoring. Via a standard web browser, you can configure and check machine status from anywhere around the world.

Configuration of the DA1101 via web browser

First insure that your PC is on the 192.168.1.xxx subnet (ie. 192.168.1.10) by configuring its IP address to that subnet.

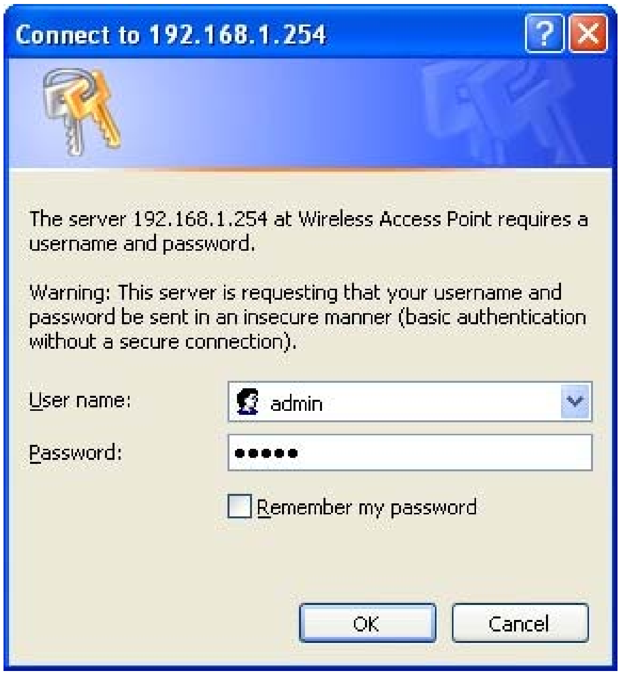
After TCP/IP configurations on your PC, you may now open your web browser, and input http://192.168.1.254 (Default LAN port IP address) to logon to the DA1101 web configuration page.



Enter the **IP address** of the Router which by default is **192.168.1.254**

Address **http://192.168.1.254**

The DA1101 will prompt for logon username/password: use admin / admin



Connect to 192.168.1.254

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

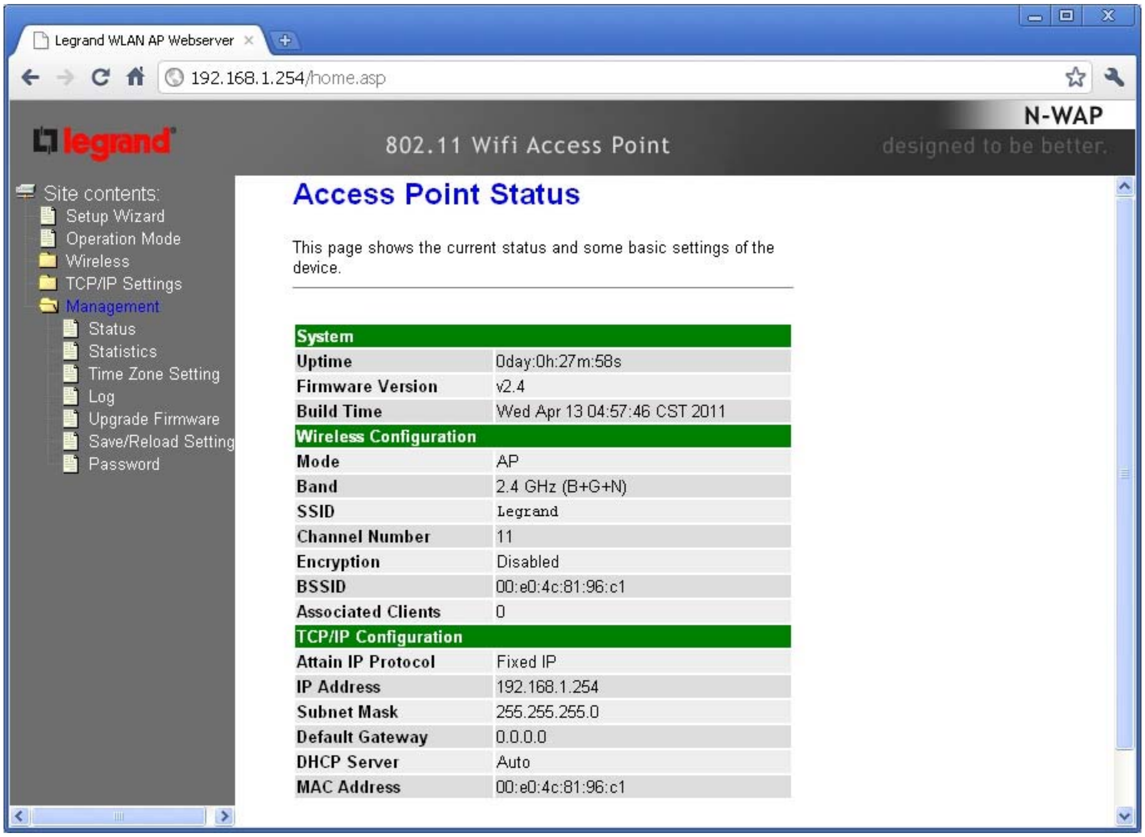
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: ●●●●●

□ Remember my password

DA1101 login prompt screen



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

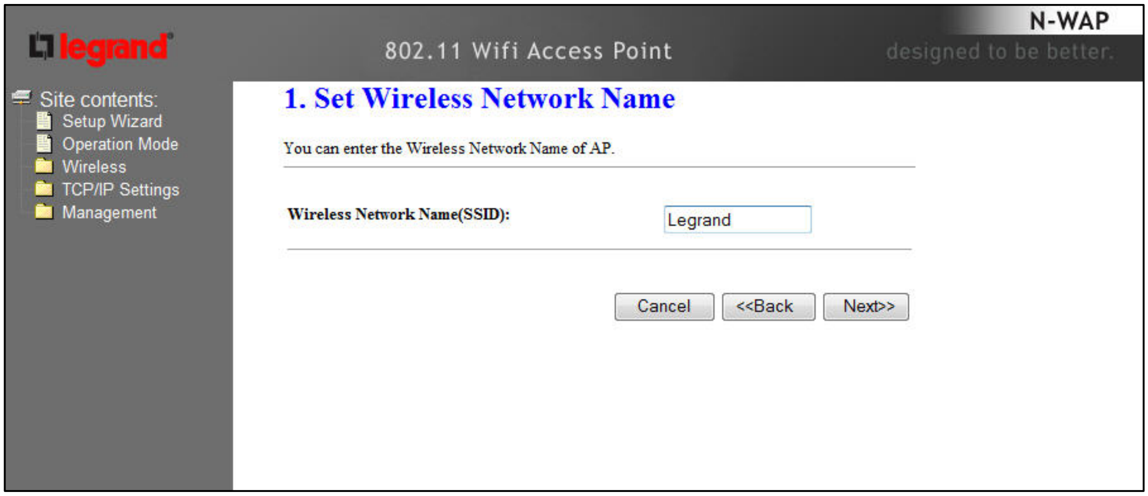
DA1101 main page

Starting Setup in Web UI

It is easy to configure and manage the DA1101 with a web browser. After successfully logging in, you can click Setup Wizard to quickly configure your DA1101.

- AP Mode is the default mode where the DA1101 works with a local router. The router provides DHCP addressing to the wirelessly connected devices (PCs). An additional DA1101 may be used as a repeater which allows for both directly connected LAN and wireless devices.

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

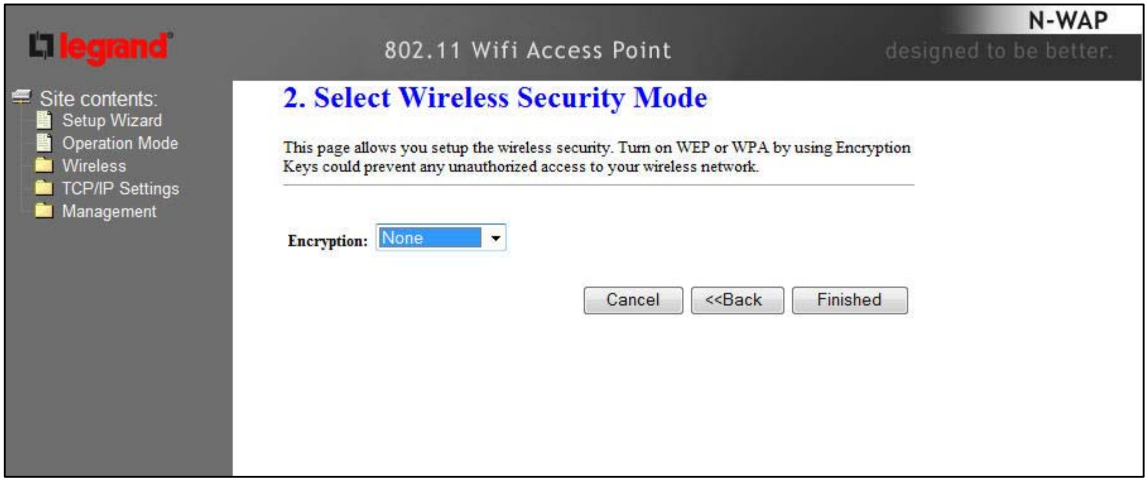


1. Set Wireless Network Name

You can enter the Wireless Network Name of AP.

Wireless Network Name(SSID): Legrand

Step 2. Select Wireless Security Mode.



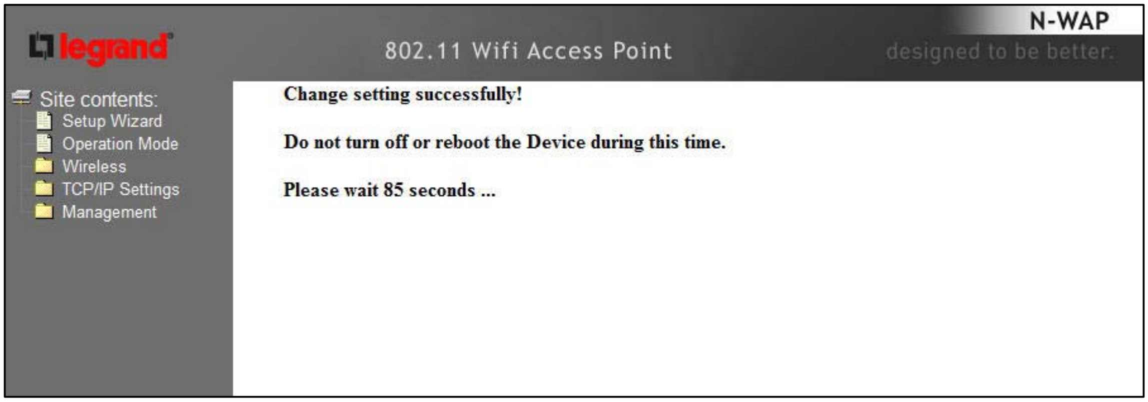
2. Select Wireless Security Mode

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 DA1101 will reboot automatically to make your wireless re-configuration take effect and finish the Setup.



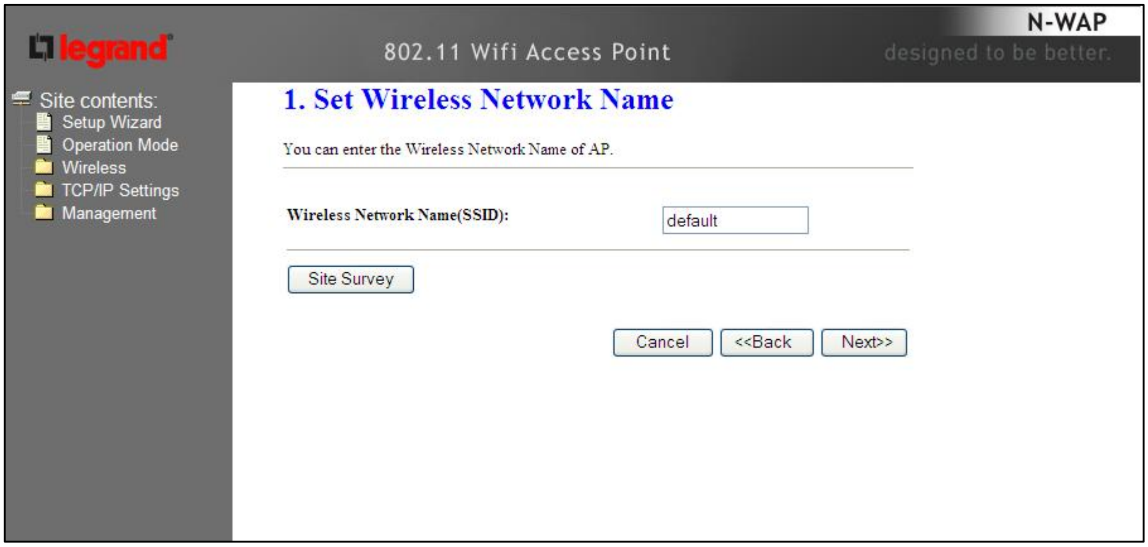
Change setting successfully!

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

Please wait 85 seconds ...

- Client Mode is used where an additional DA1101 is configured as the client and connects directly to a LAN or PC (no wireless devices), while the original DA1101 connects to a router.

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

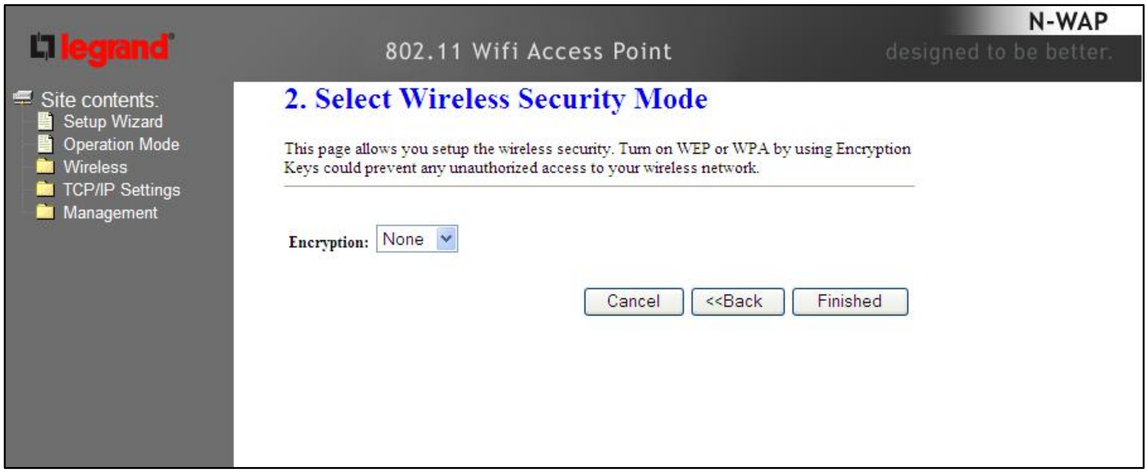


1. Set Wireless Network Name

You can enter the Wireless Network Name of AP.

Wireless Network Name(SSID): default

Step 2. Select Wireless Security Mode.



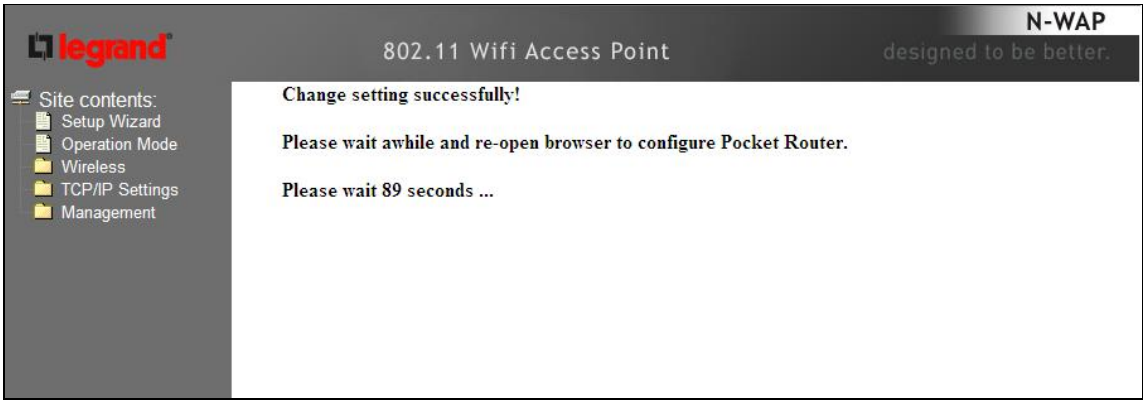
2. Select Wireless Security Mode

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 DA1101 will reboot automatically to make your wireless configuration to take effect and finish the Setup.



Change setting successfully!

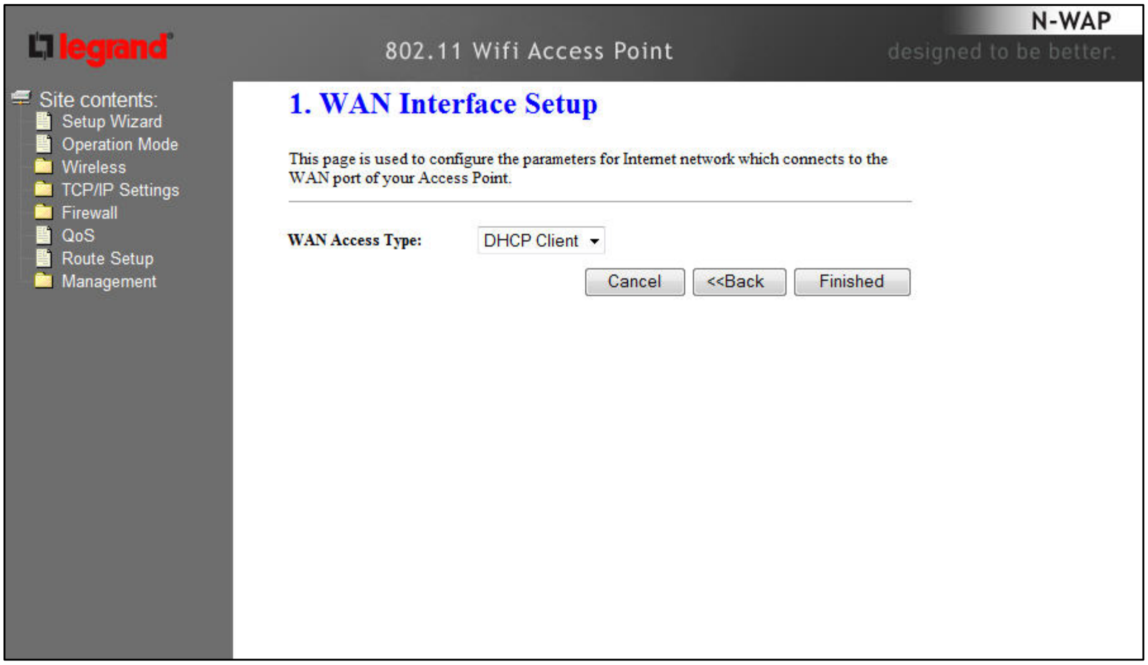
Please wait awhile and re-open browser to configure Pocket Router.

Please wait 89 seconds ...

- Router Mode is used when the DA1101 is connected to a cable modem and the DA1101 is performing the routing functions, including providing DHCP addresses for devices (PCs).

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 (see WAN Interface Setup section).



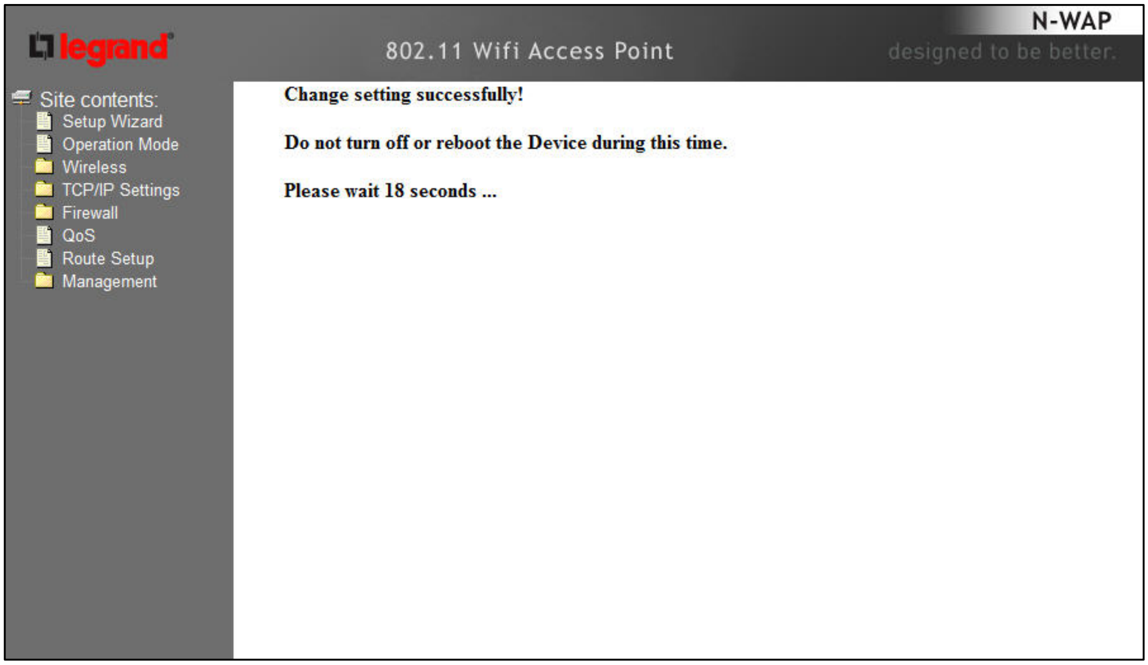
1. WAN Interface Setup

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 DA1101 will reboot automatically to make your wireless configuration to take effect and finish the Setup.



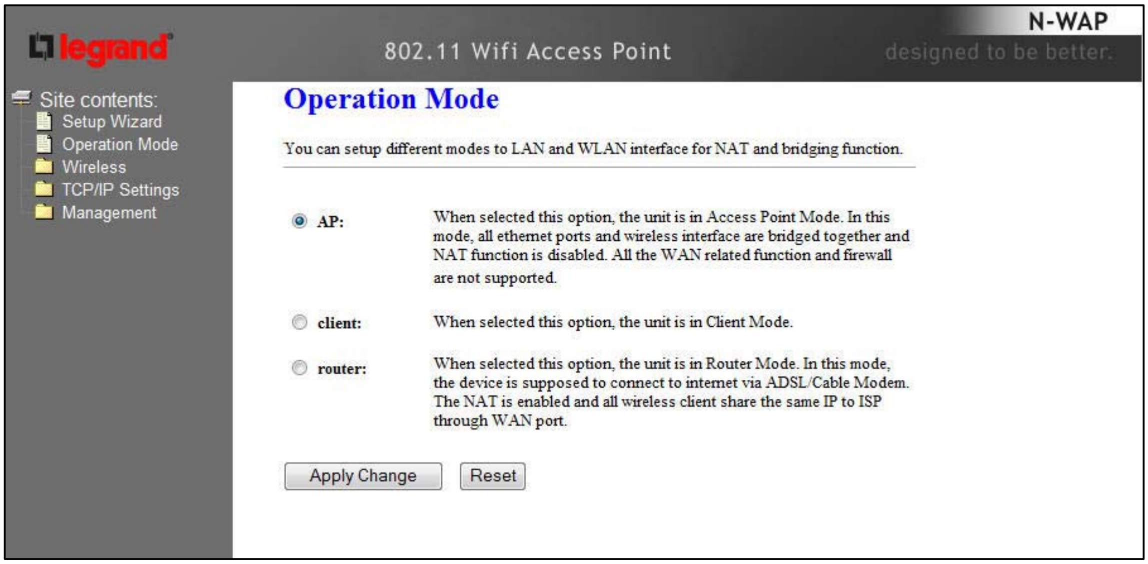
Change setting successfully!

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.

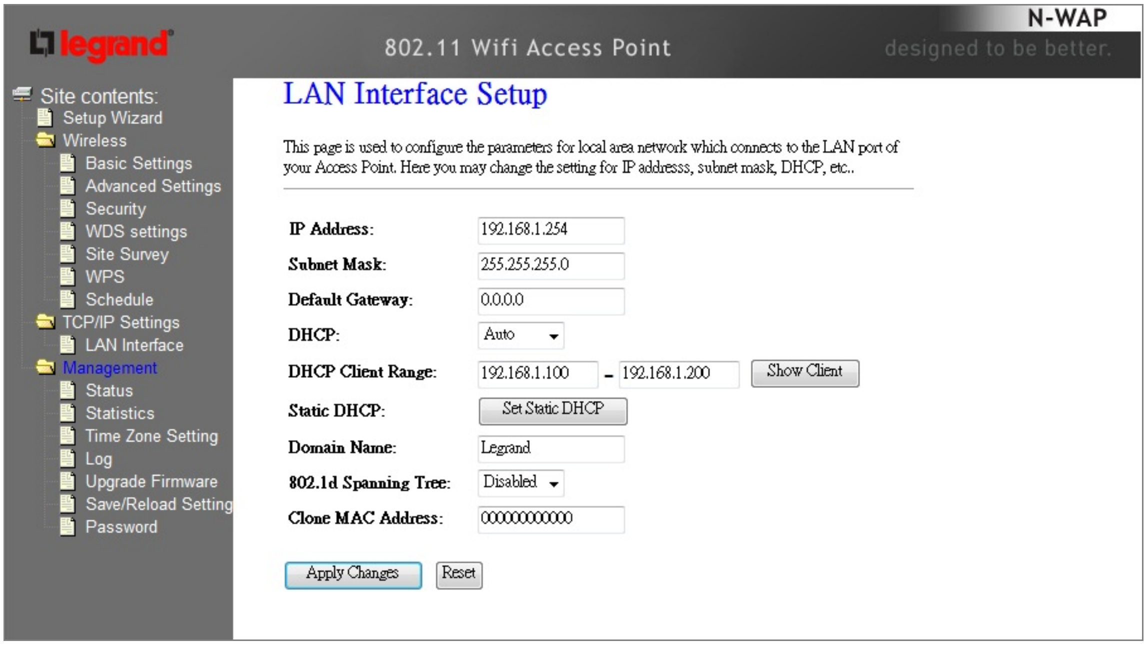
○ client: When selected this option, the unit is in Client Mode.

○ 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 DA1101. 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
Static DHCP:	Set Static DHCP
Domain Name:	Legrand
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

IP Address	LAN IP Address of the DA1101 Default : 192.168.1.254
Subnet Mask	LAN mask of the DA1101 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

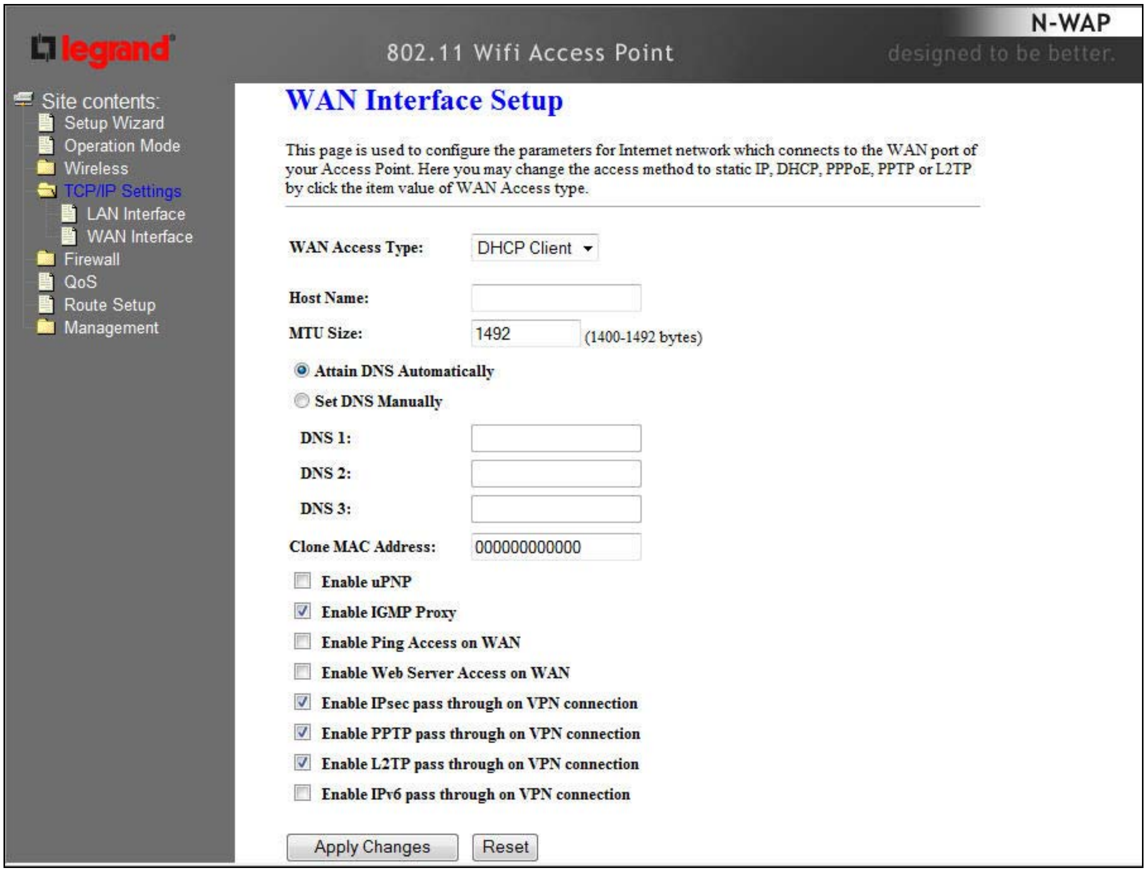
WAN Interface Setup

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

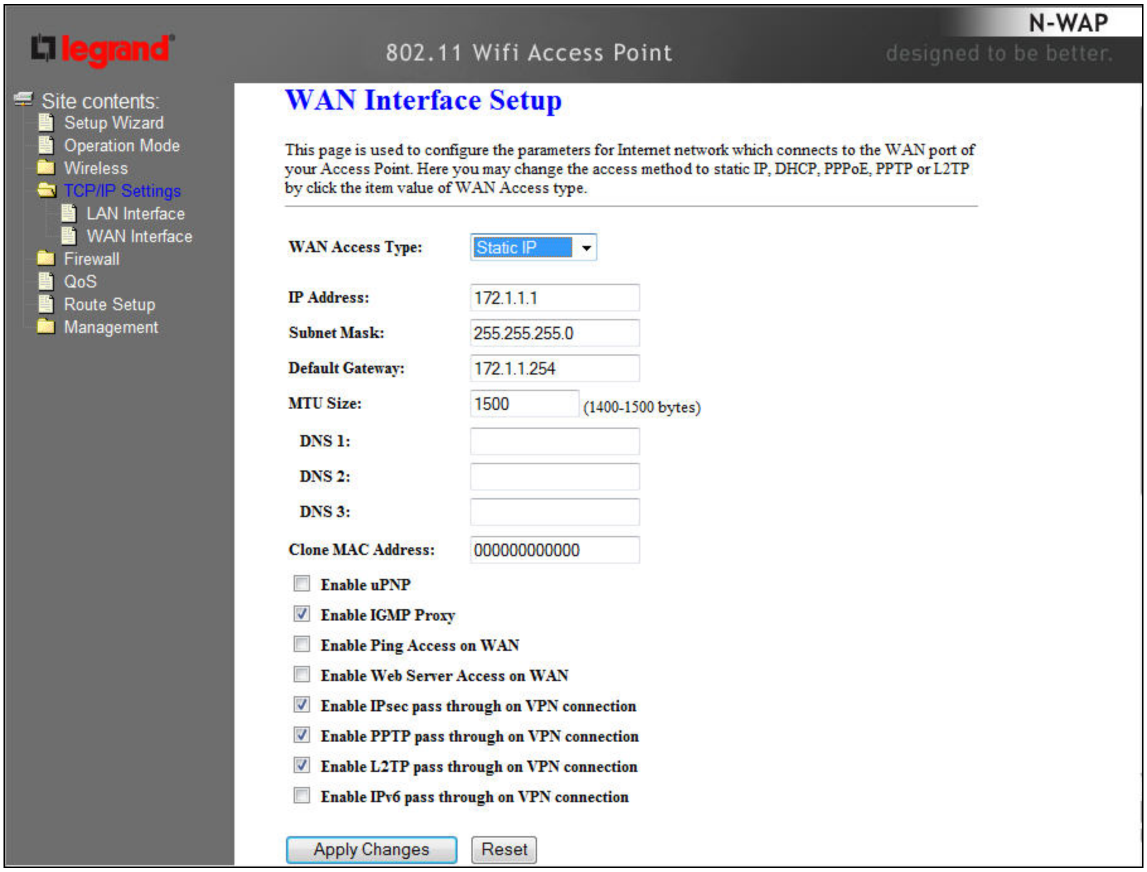
□ Enable IPv6 pass through on VPN connection

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

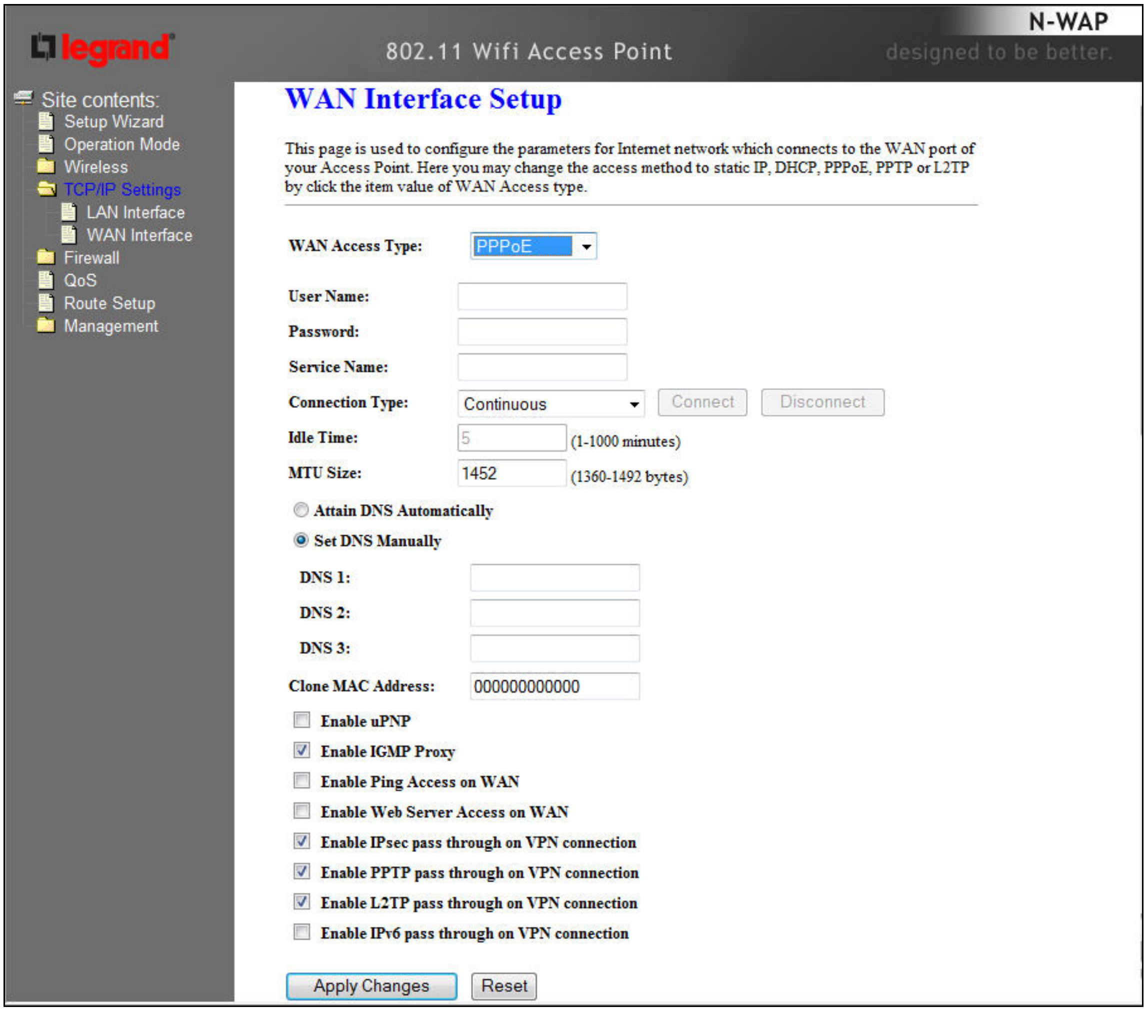
□ Enable IPv6 pass through on VPN connection

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

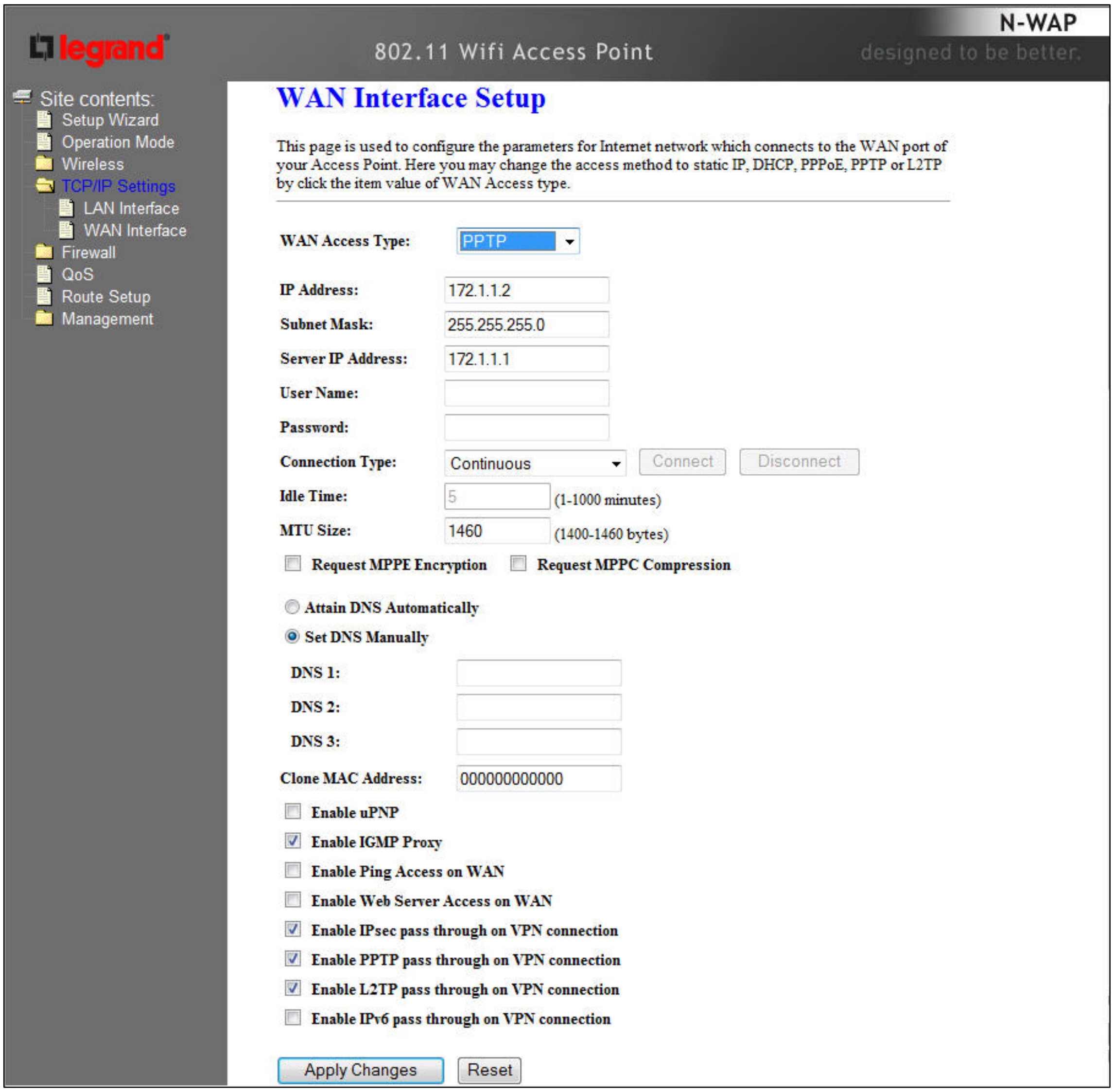
[Apply Changes] [Reset]

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:

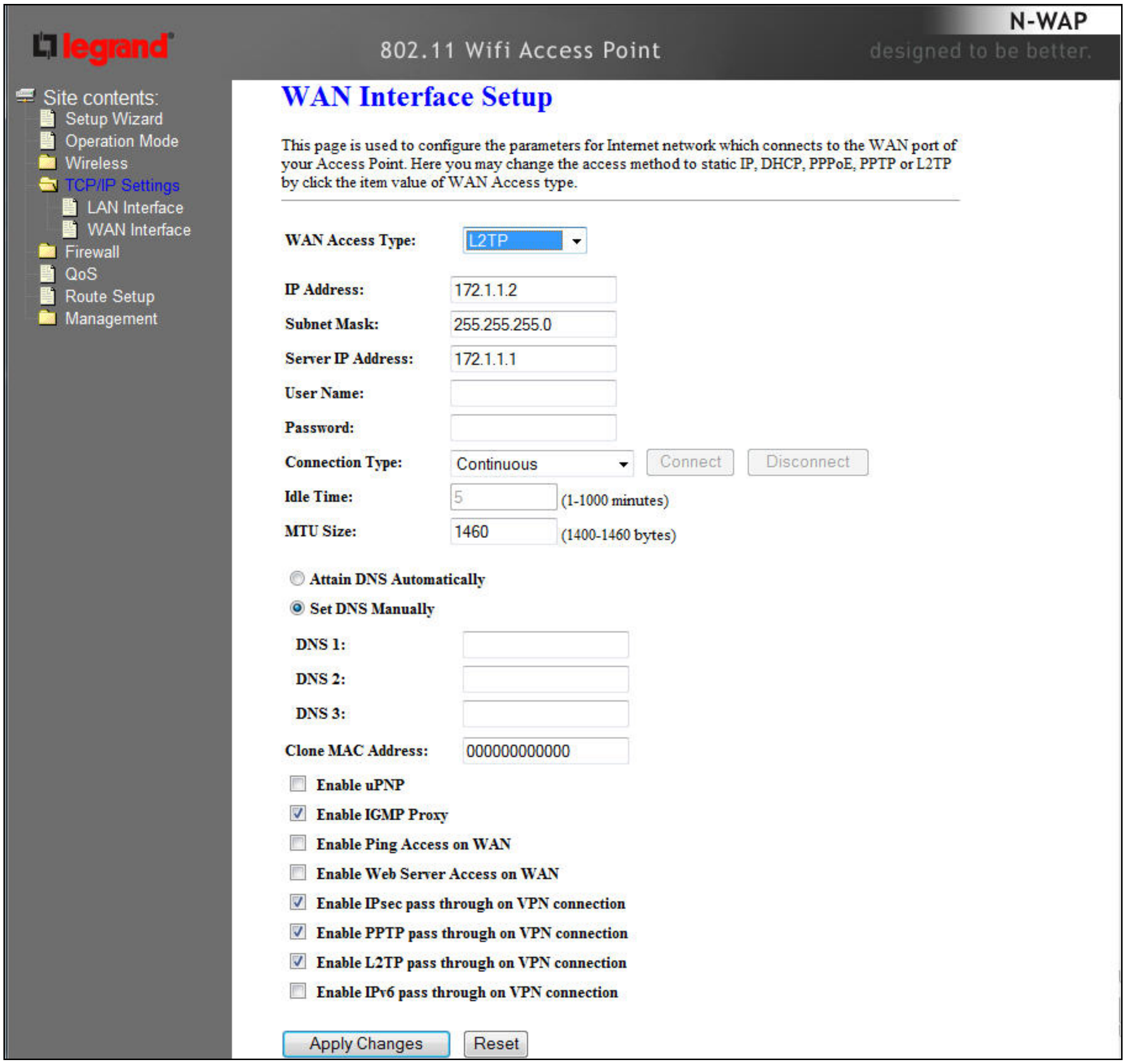
Object	Description
IP Address	Enter the IP address in dotted-decimal notation provided by your ISP.
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Server IP Address	Enter the PPTP Server IP address in dotted-decimal notation provided by your 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 [Connect] [Disconnect]

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

[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 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).

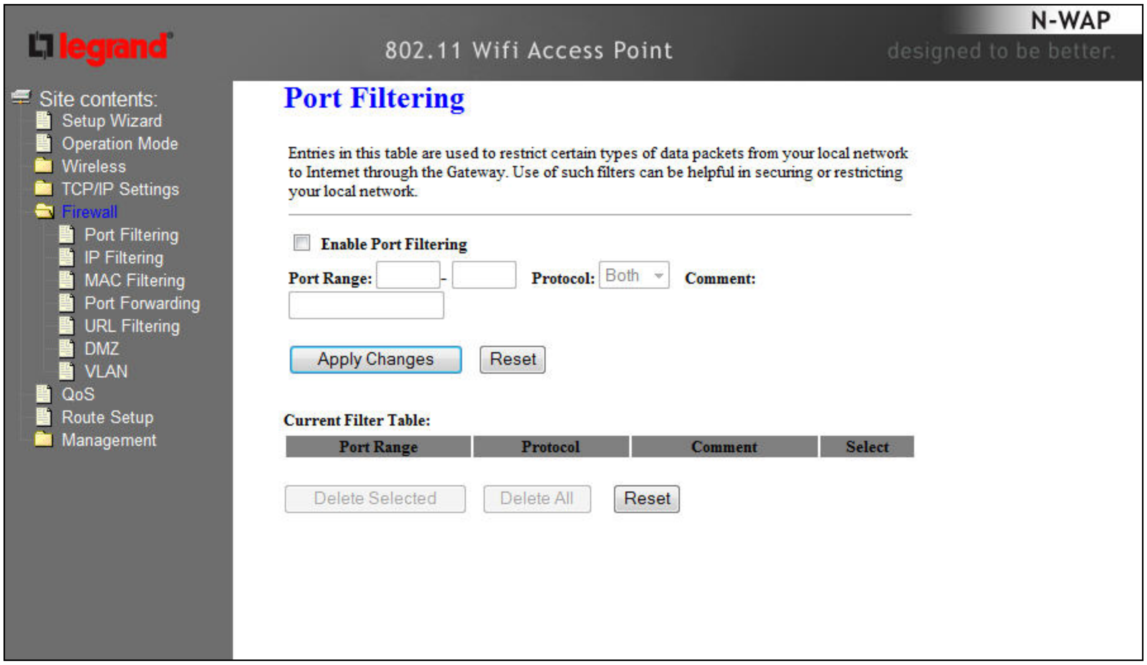
Connection Type	Select the connection type Continuous, Connect on Demand or Manual from the drop-down menu. If selected Manual, user can click Connect button to make a connection.
Idle Time	It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. 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 DA1101. 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: ______

Apply Changes Reset

Current Filter Table:

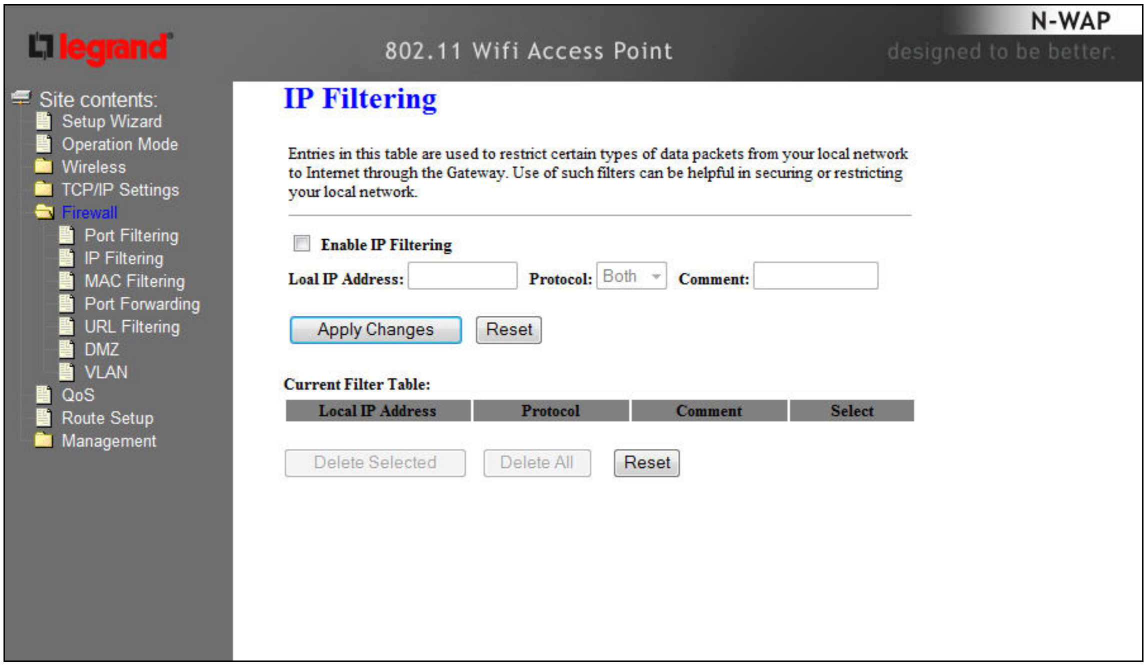
Port Range	Protocol	Comment	Select

Delete Selected Delete All Reset

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 DA1101. 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: ______

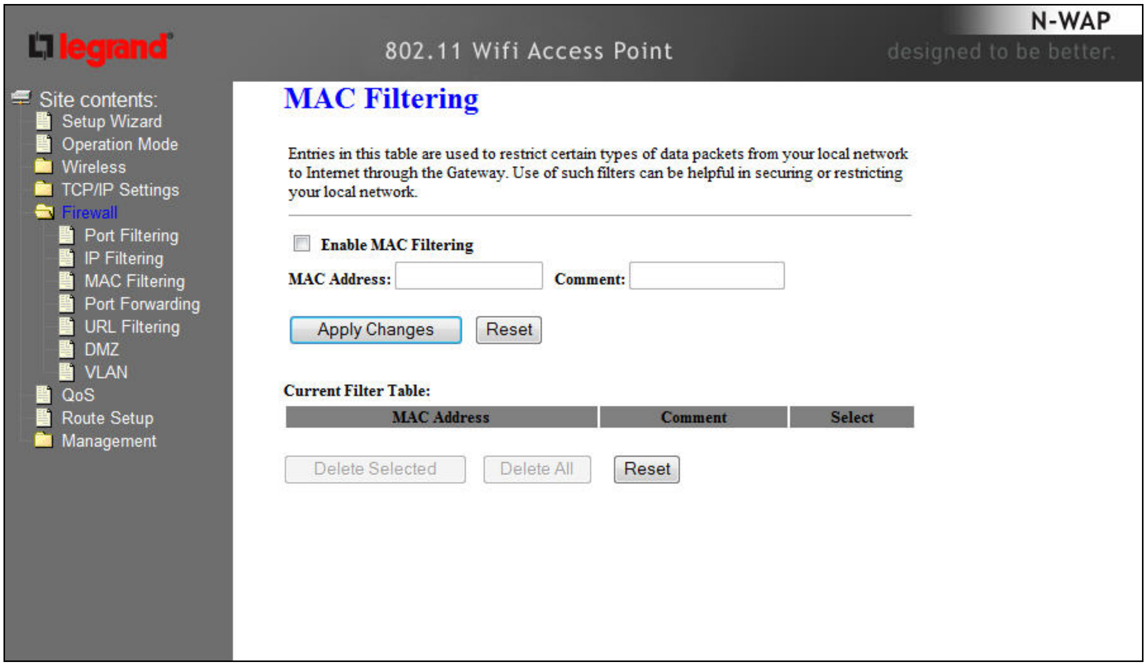
Current Filter Table:

Local IP Address	Protocol	Comment	Select

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 DA1101. 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: ________

Apply Changes | Reset

Current Filter Table:

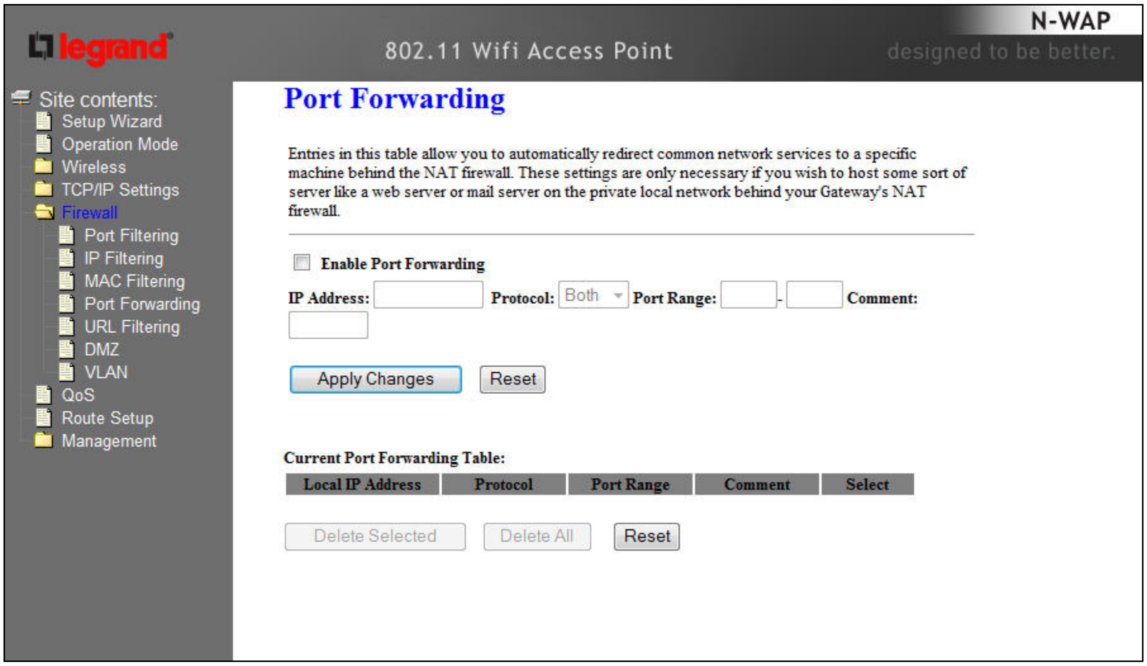
MAC Address	Comment	Select

Delete Selected | Delete All | Reset

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 DA1101'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:** ____

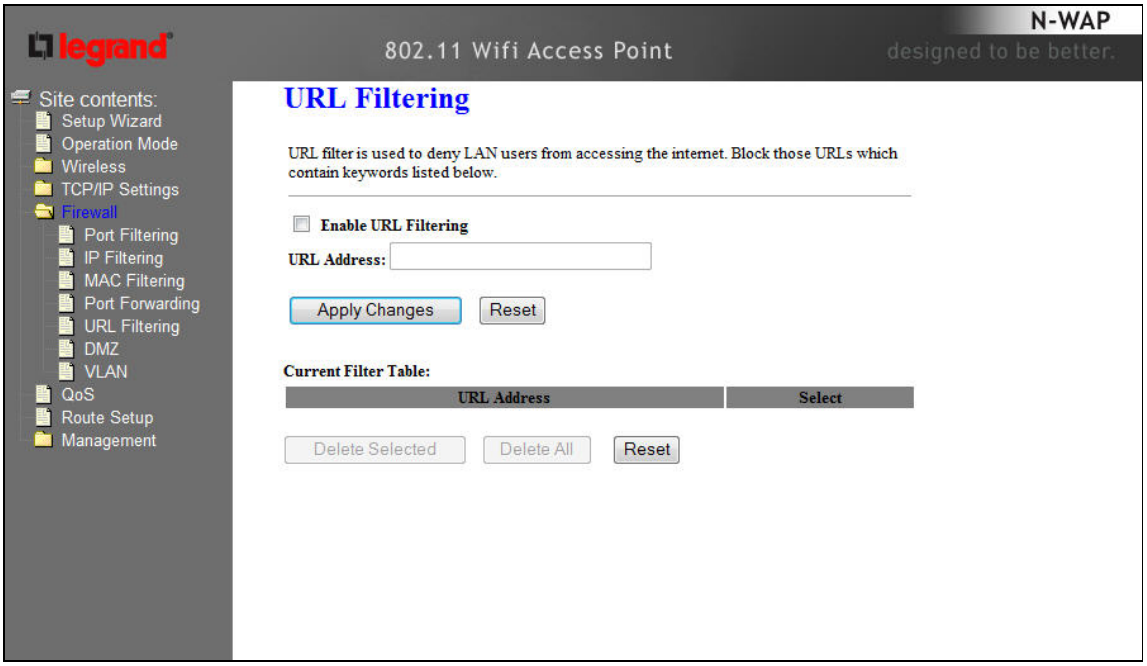
Current Port Forwarding Table:

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 Forwarding 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:

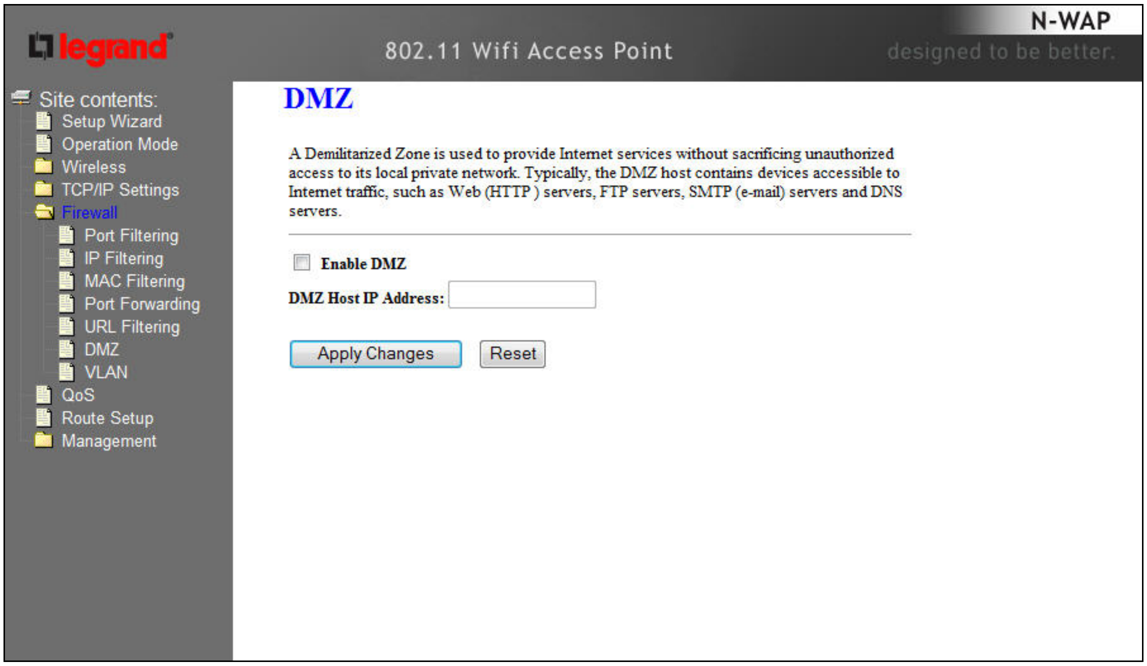
Current Filter Table:

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

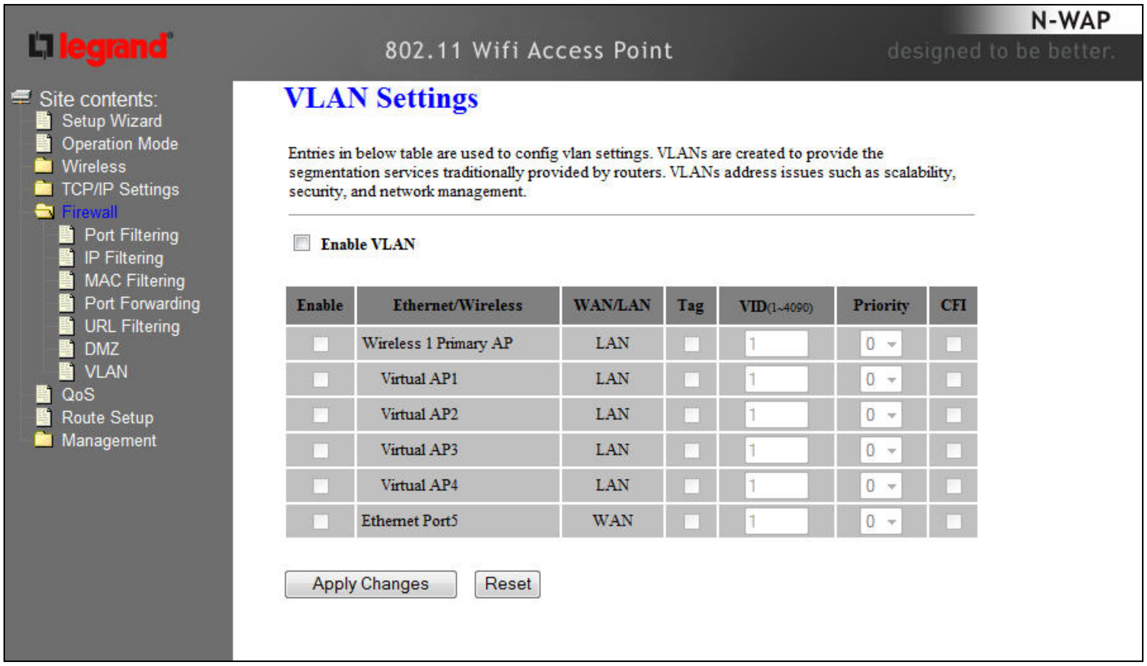
DMZ Host IP Address:

Apply Changes | Reset

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

VLAN

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



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	WAN	☐	1	0	☐

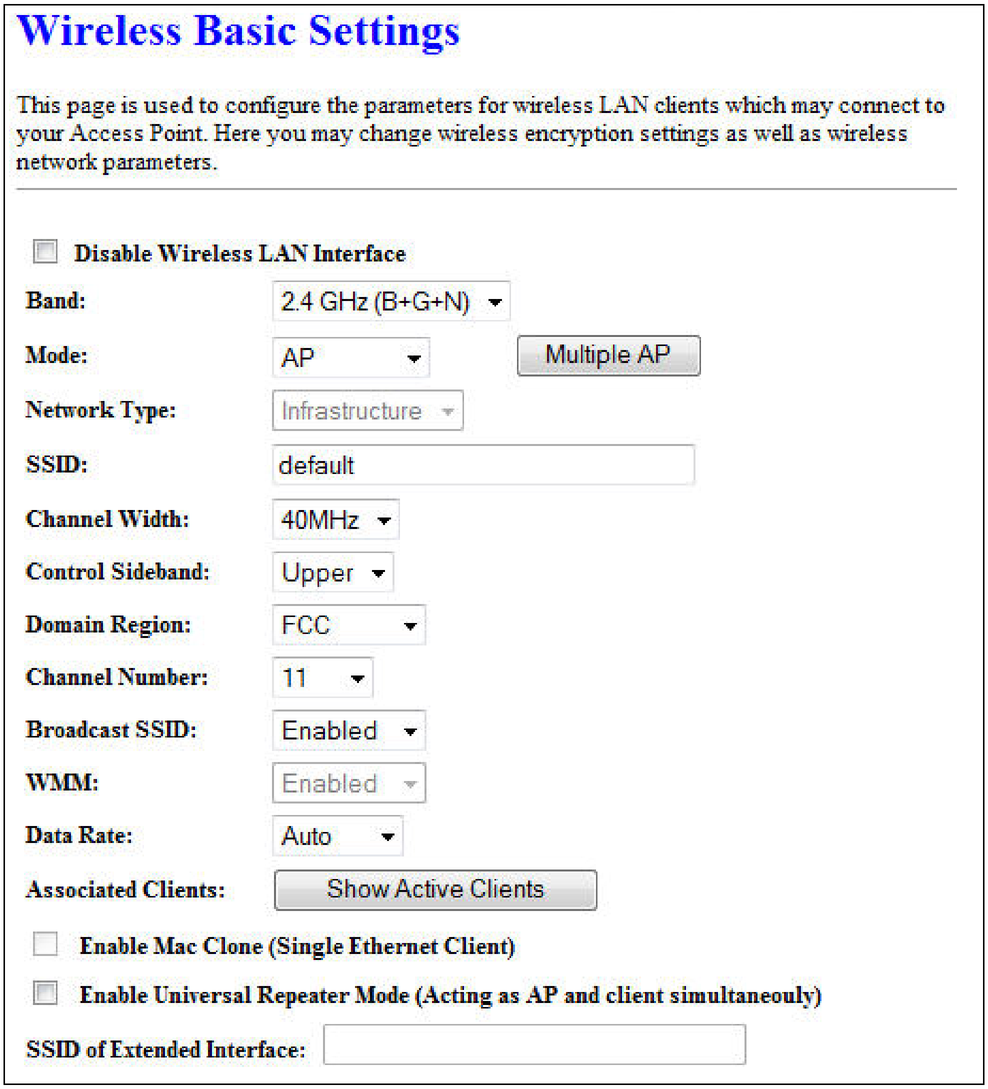
Enable VLAN	VLAN (Virtual Local Area Network) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on different LAN segments. Because VLANs are based on logical instead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

Chapter 5

Wireless Settings

Basic Settings

This page is used to configure the parameters for wireless LAN clients who may connect to your DA1101. 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:

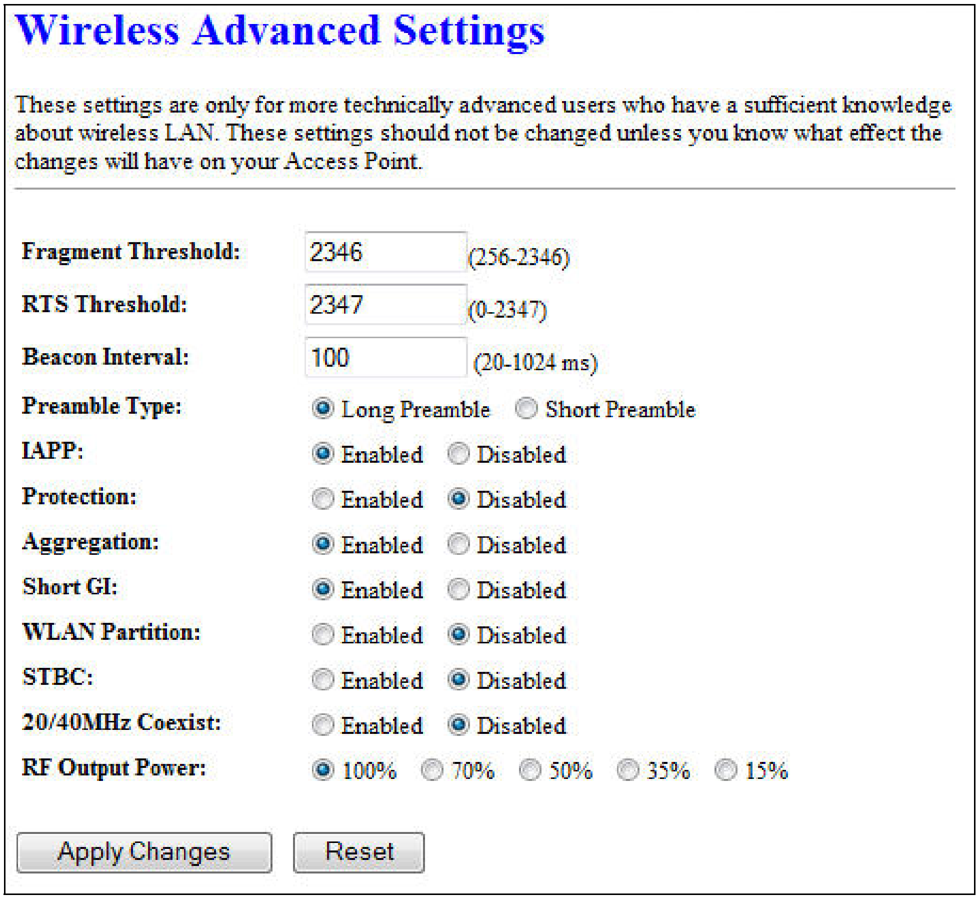
Disable Wireless LAN Interface	Enable or disable the wireless LAN.
Band	There are 6 modes: 2.4GHz (B), 2.4GHz (G), 2.4GHz (N), 2.4GHz (B+G), 2.4GHz (G+N), and 2.4GHz (B+G+N) mode. Default : 2.4GHz (B+G+N)

Mode	- AP: The DA1101 functions as a wireless hub to which wireless clients can connect. The clients must make sure that they are configured to match the DA1101's wireless settings. The DA1101 must be connected to a router for wireless devices to receive DHCP addressing. - WDS: WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect DA1101s, 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 to be able to access the wireless network via the DA1101.
	- Ad hoc: The wireless LAN will use the Ad hoc mode to operate.
SSID	Wireless stations associating to the DA1101 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)
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country.
	Default : 6
Broadcast SSID	If you enable "Broadcast ESSID", every wireless station located within the coverage of this DA1101 can discover this DA1101 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 DA1101 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. If this is enabled, a second DA1101 can be used for directly connected LAN devices and wireless devices.
	Default : Disable
SSID of Extended Interface	Click on “Enable Universal Repeater Mode”; In the “SSID of Extended Interface”, enter the SSID of the wireless router that you want to extend.
	Default : Null

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 DA1101.



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.

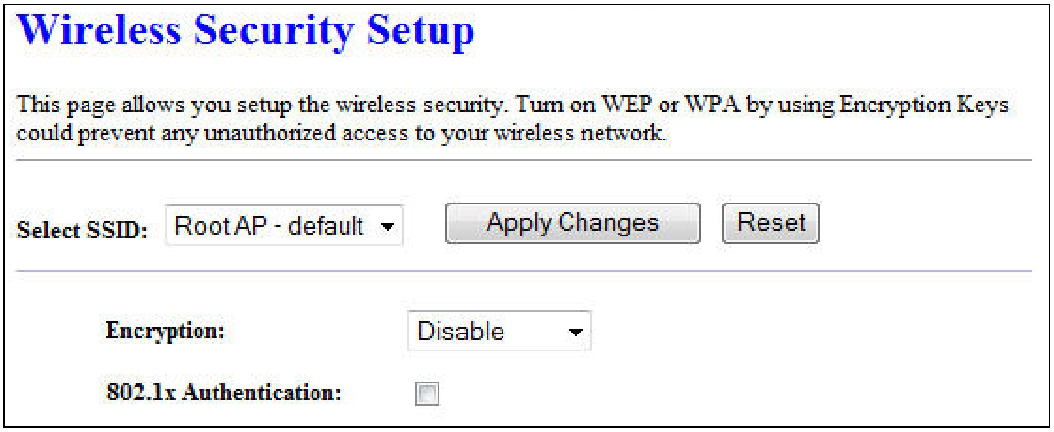
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Preamble Type:	● Long Preamble ○ Short Preamble
IAPP:	● Enabled ○ Disabled
Protection:	○ Enabled ● Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled
WLAN Partition:	○ Enabled ● Disabled
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 DA1101 will not use the RTS/CTS mechanism to send this packet. Default : 2347
Beacon Interval	The interval of time that this DA1101 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 DA1101. If this is enabled, wireless stations of the selected band are not allowed to exchange data through the DA1101. 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

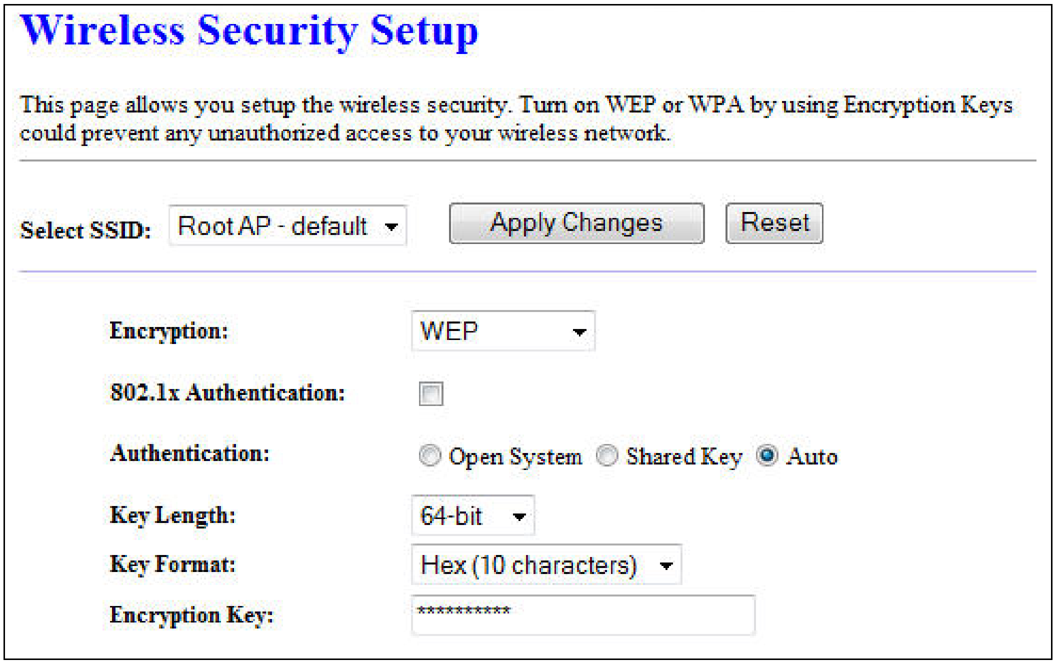
Encryption: Disable

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 ▾ [Apply Changes] [Reset]

Encryption: WEP ▾

802.1x Authentication: □

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bit ▾

Key Format: Hex (10 characters) ▾

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

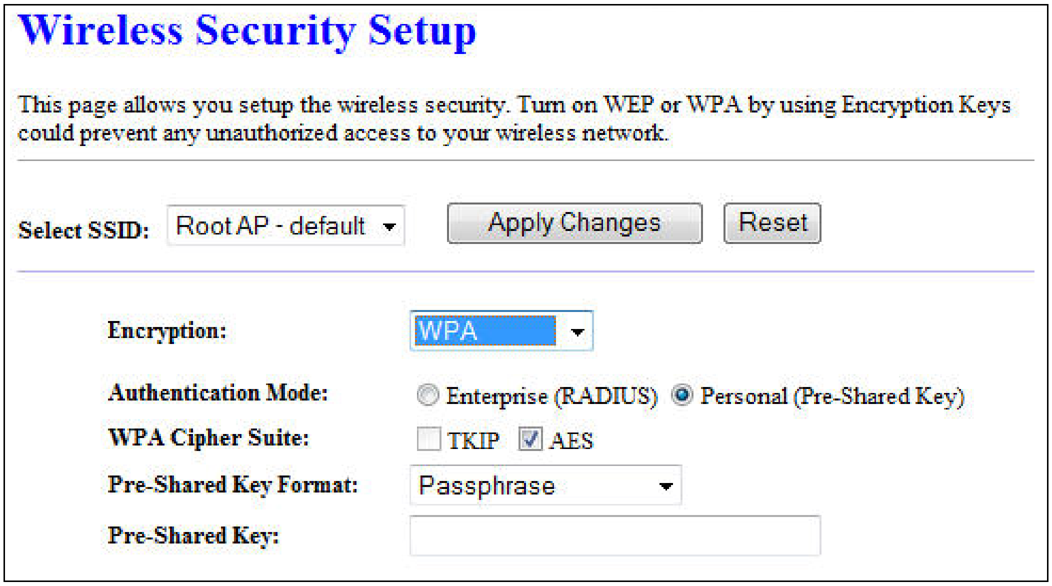
- WPA

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 ▾ [Apply Changes] [Reset]

Encryption: WPA ▾

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

WPA Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase ▾

Pre-Shared Key:

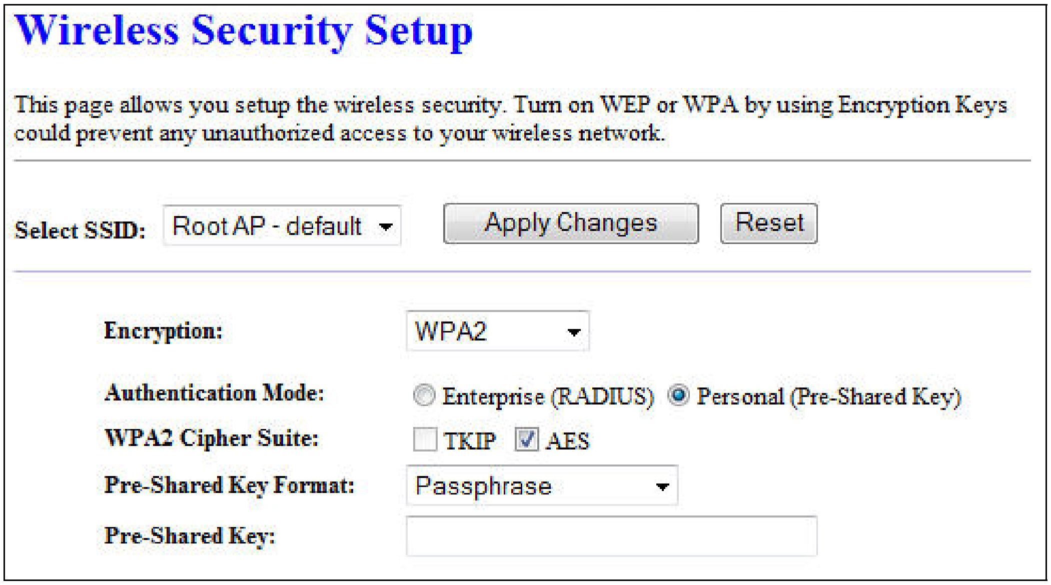
- WPA2

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

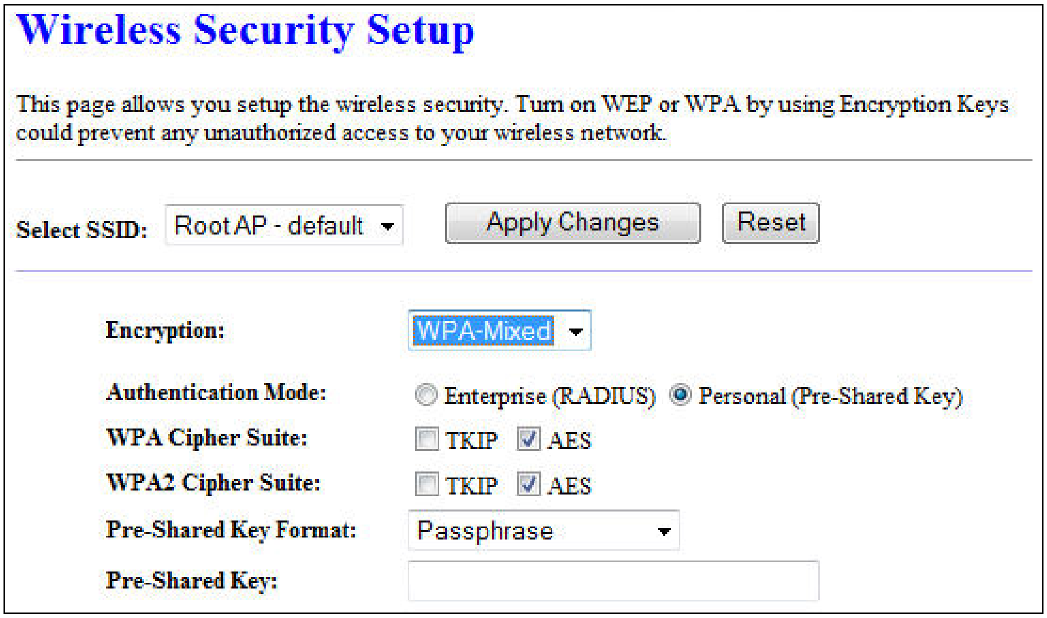
The router will detect automatically which Security type (WPA-PSK version 1 or 2) the client uses to encrypt.

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

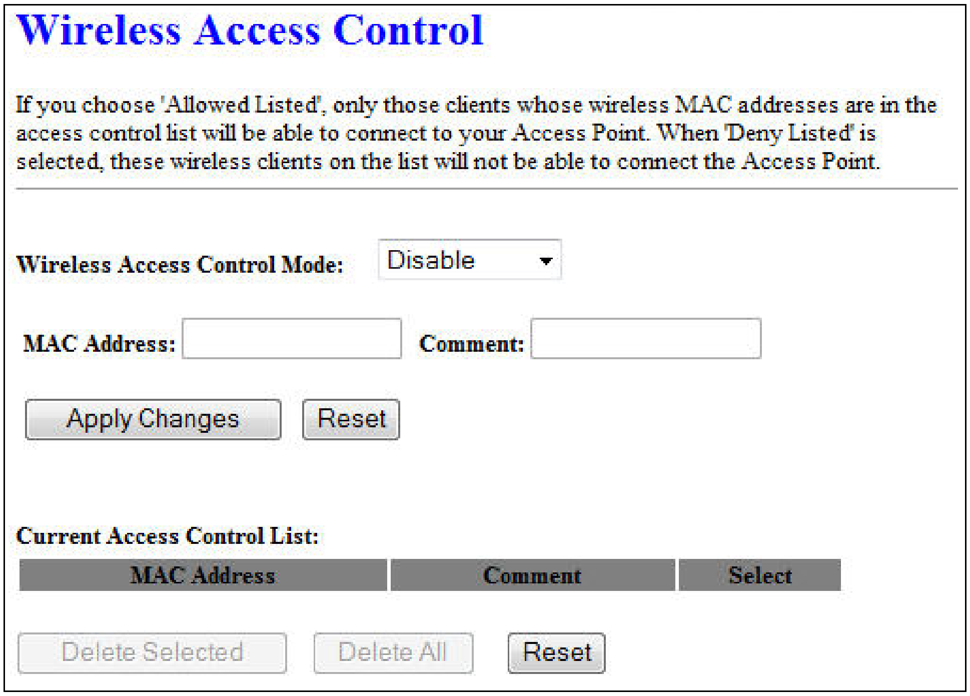
WPA2 Cipher Suite: □ TKIP ☑ AES

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 DA1101. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the DA1101.



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

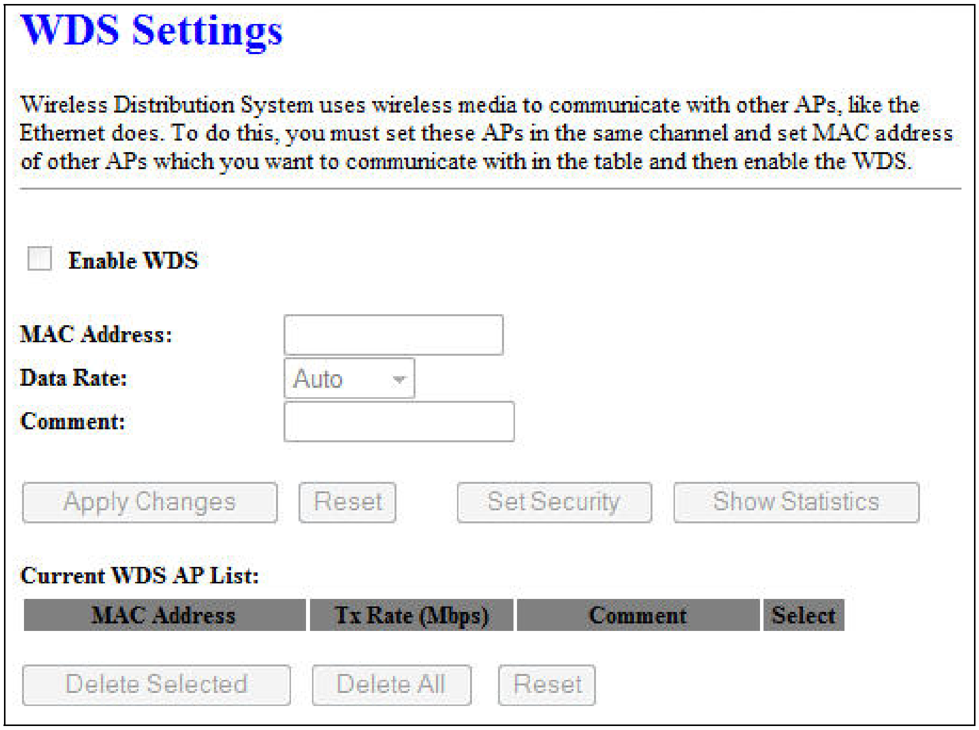
MAC Address: Comment:

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

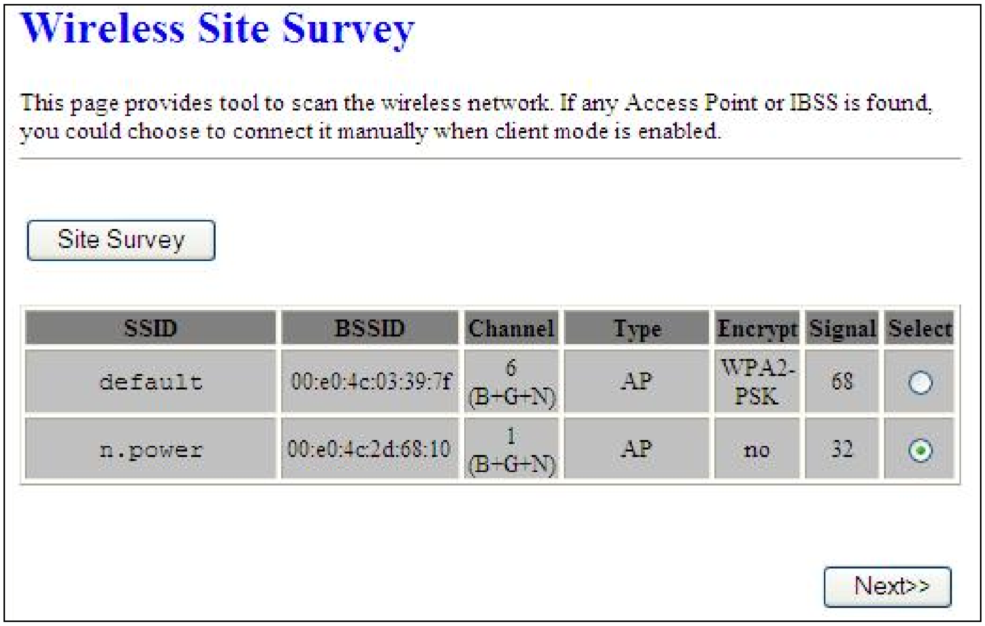
Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

Site Survey

This page provides tool to scan the wireless network. If any DA1101 or IBSS is found, you could choose to connect it manually when client mode is enabled.



Wireless Site Survey

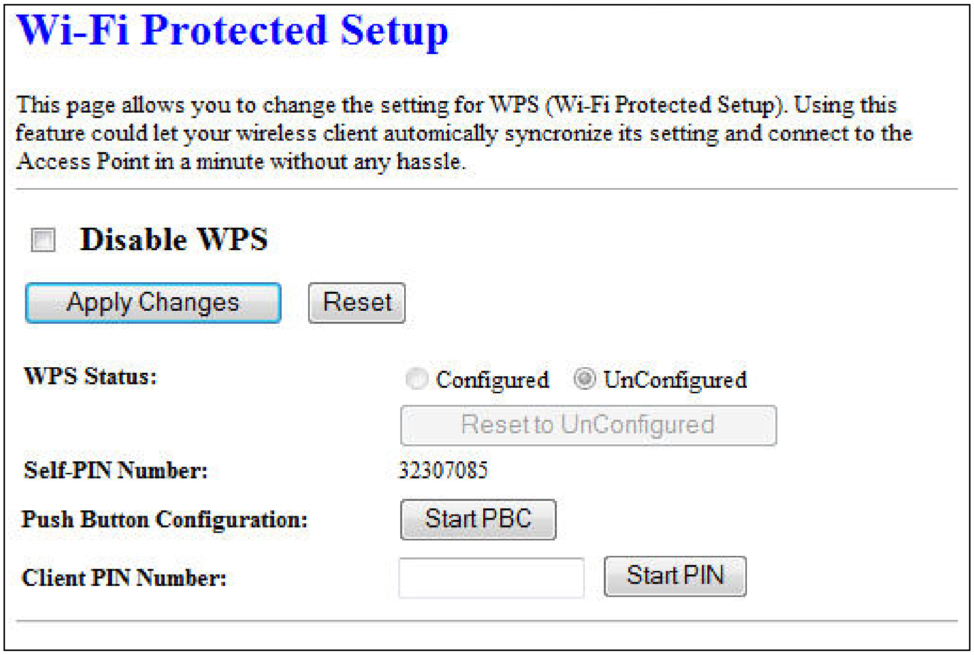
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

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

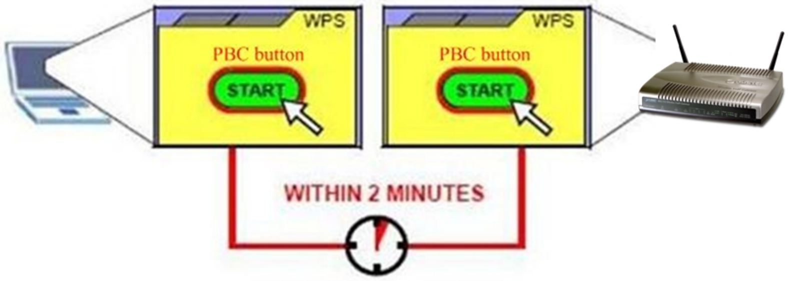
Push Button Configuration:

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.)

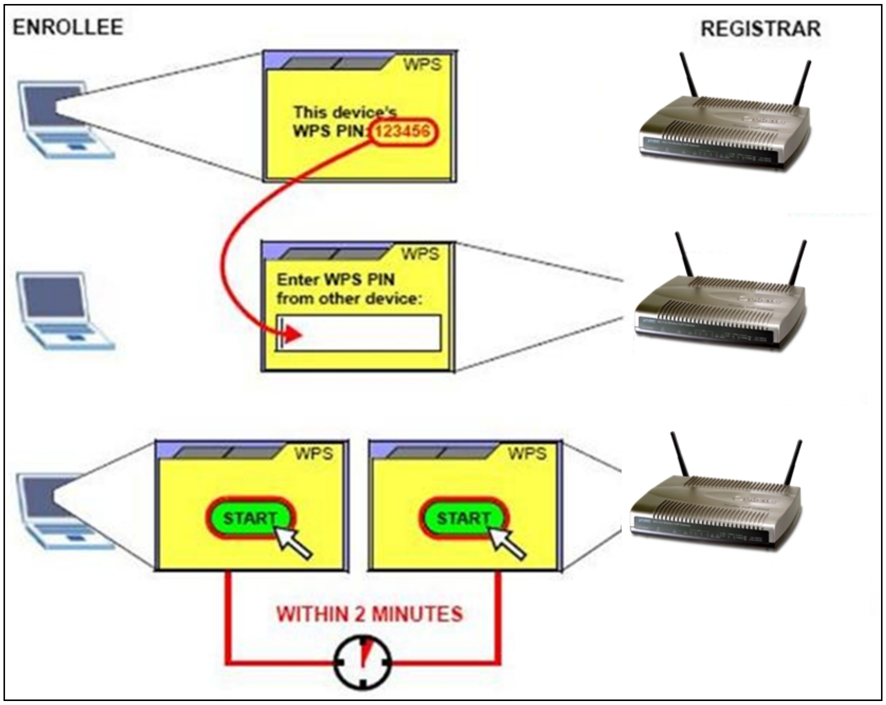
- PBC setup step:

1. Ensure you have set the security setting on DA1101 (as Registrar).
2. Click the WPS button on DA1101 (or the “Start PBC” button on the web interface of DA1101) and the other device (supports PBC function) in 2 minutes.
3. DA1101 (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 DA1101.
2. Click the “Start PIN” buttons on DA1101 and the other device in 2 minutes.
3. If you see the wireless client in the list, WPS-PIN setting is successful.



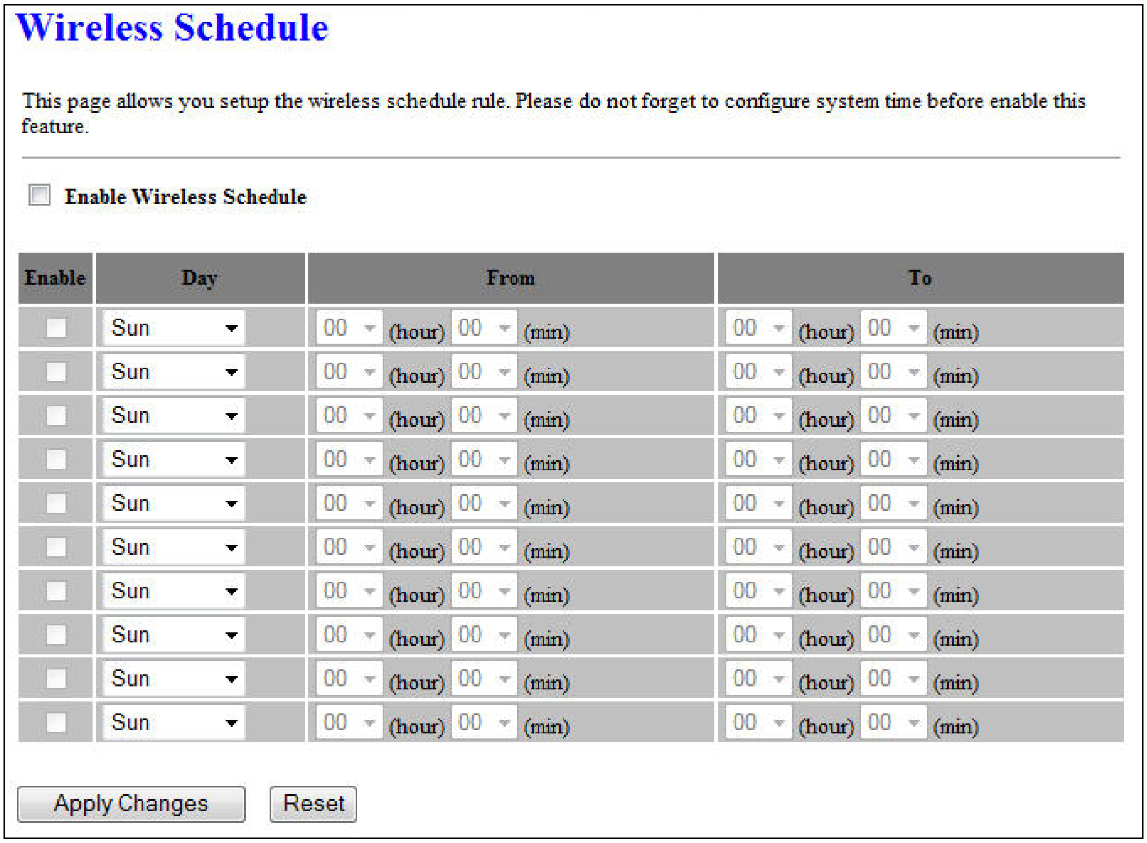
- PIN (as Enrollee) setup step:

1. Fill the PIN code of DA1101 into the other device (as Registrar).
2. Click the “Start PIN” buttons on DA1101 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**

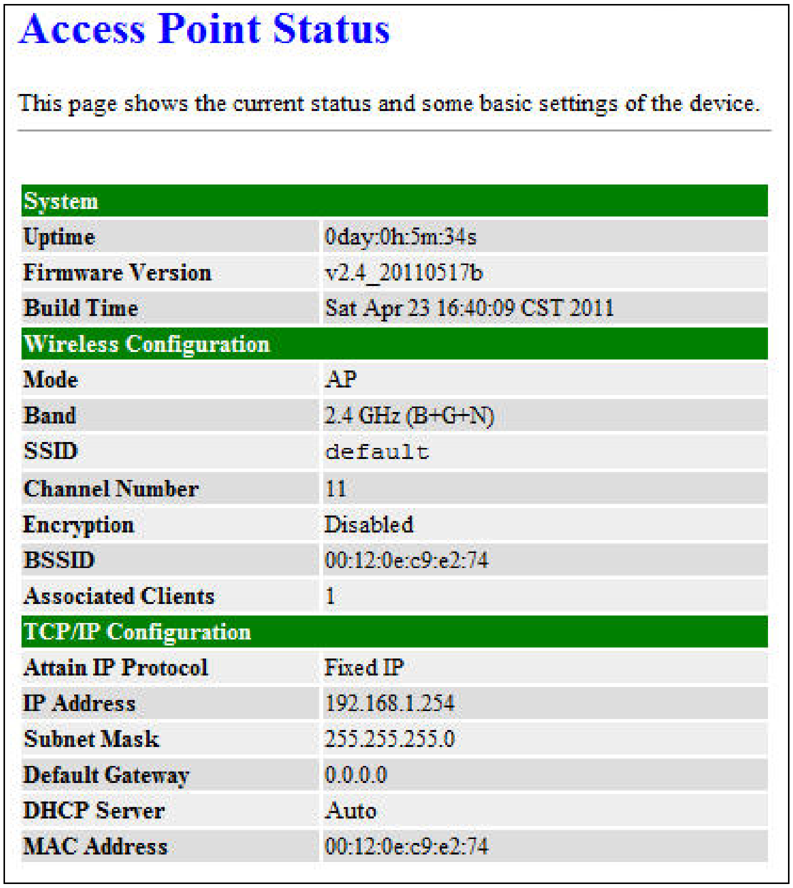
Enable	Day	From	To
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (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 DA1101.



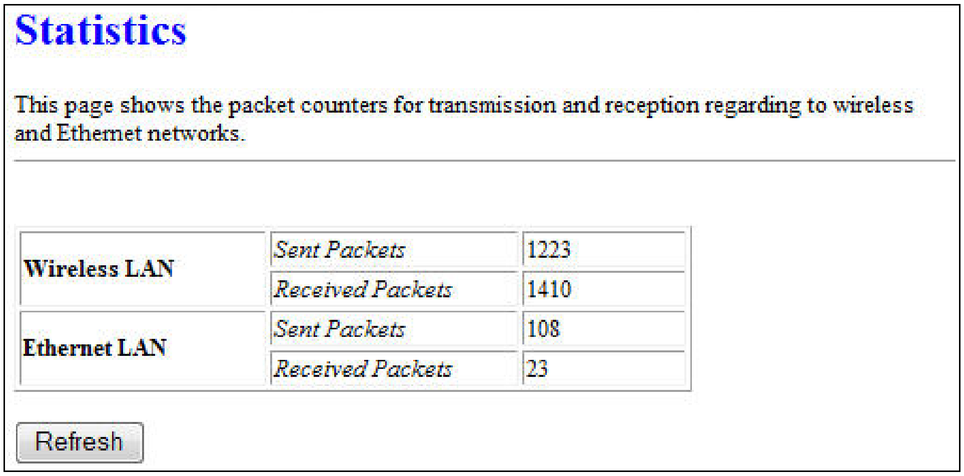
Access Point Status

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

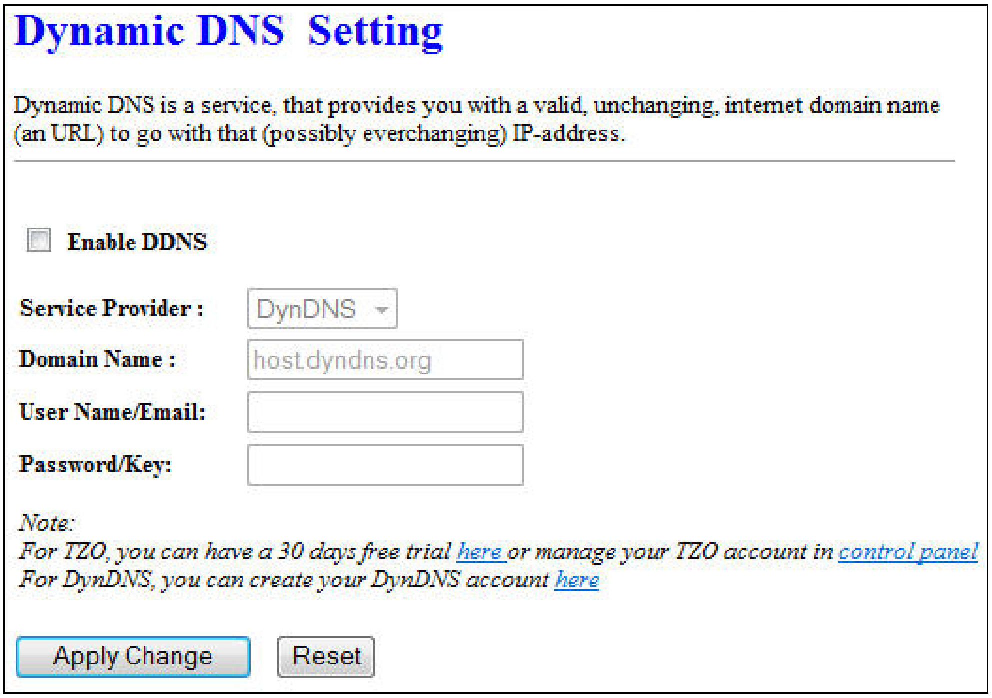
This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

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.

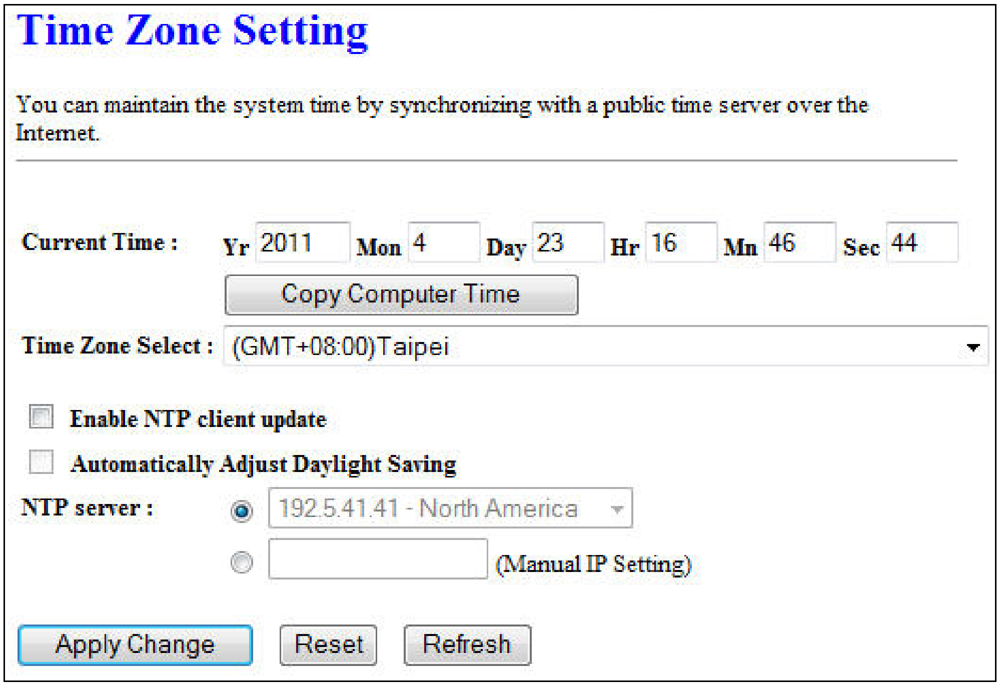
Step 4. Type the User Name/Email for your DDNS account.

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

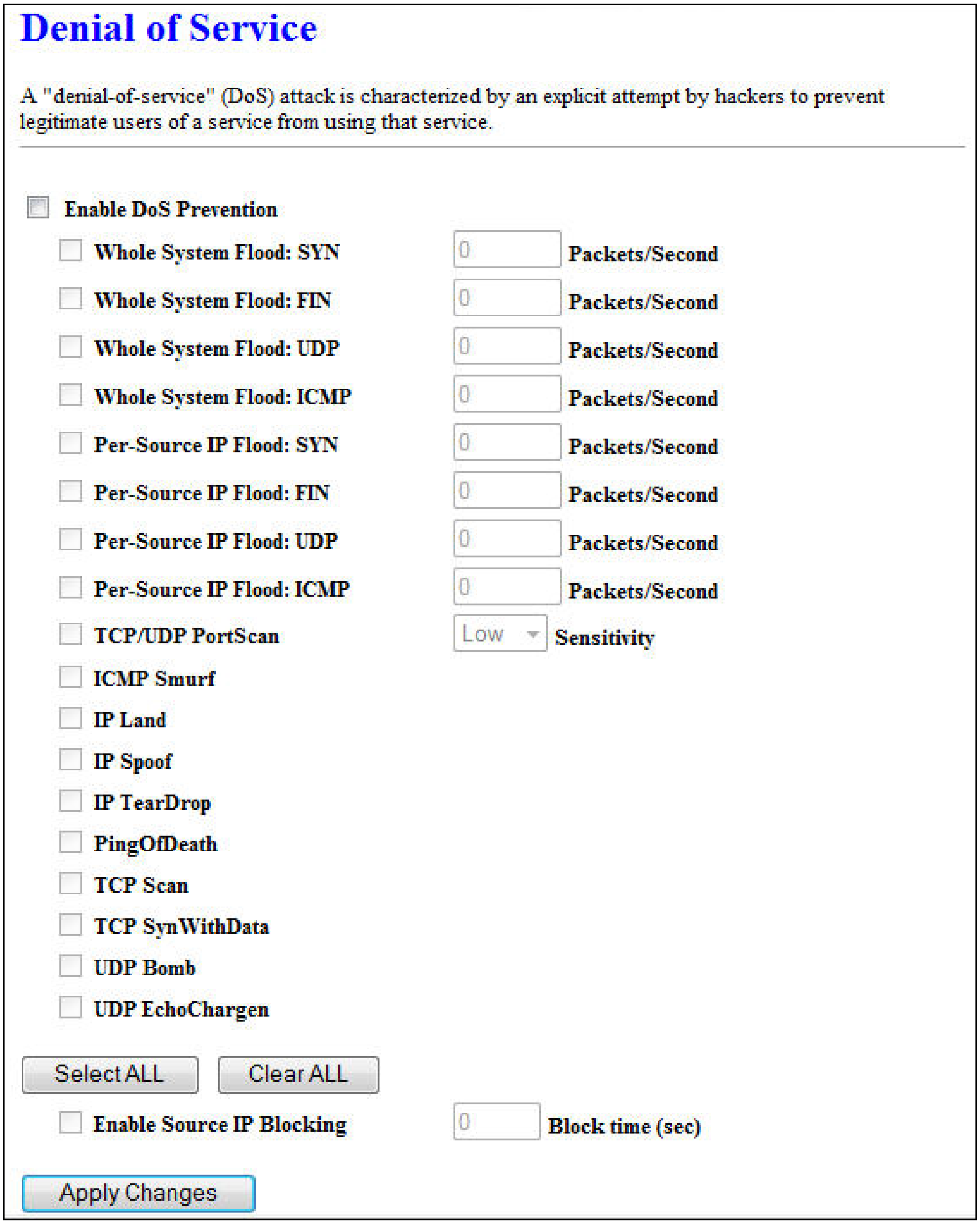
NTP server : ● 192.5.41.41 - North America

○ (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, the DA1101 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

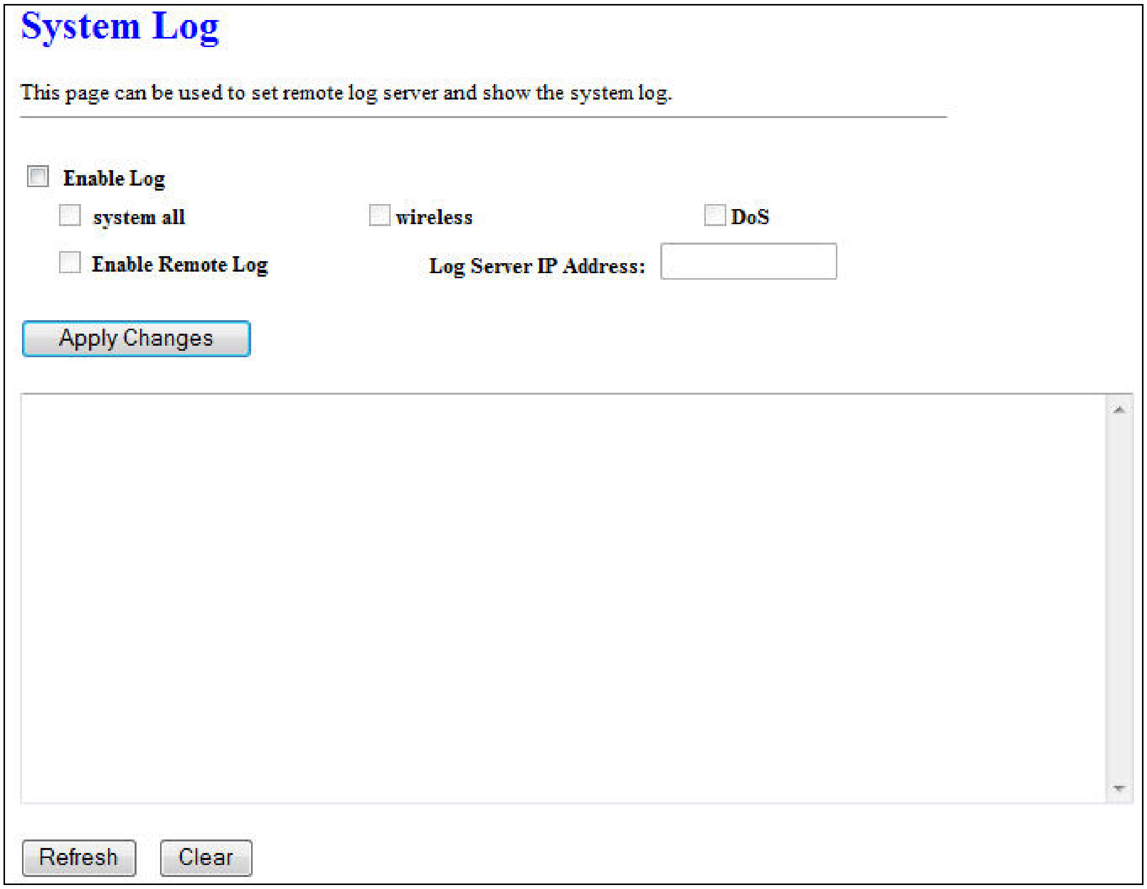
☐ UDP Bomb

☐ 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

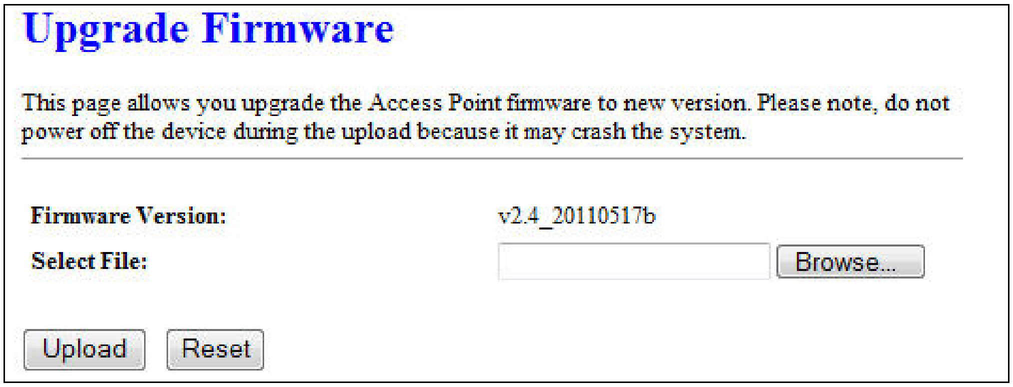
□ system all □ wireless □ DoS

□ 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 DA1101 firmware to new version. Please note, do not power off the device during the upload because it may crash the system.



Upgrade Firmware

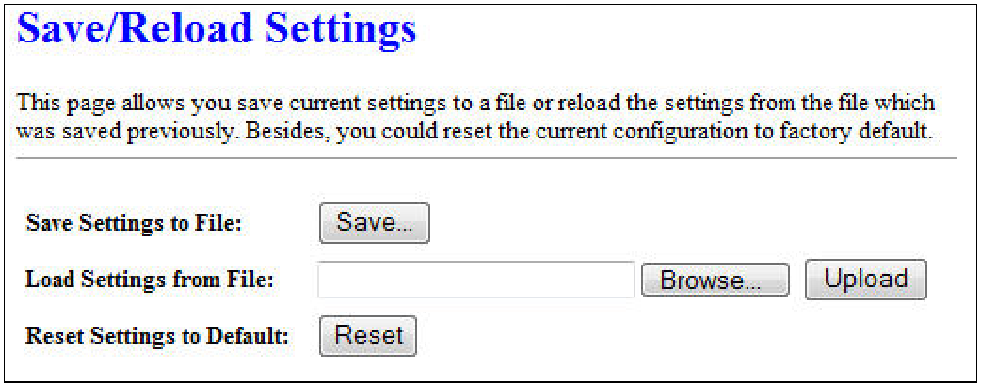
This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

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:

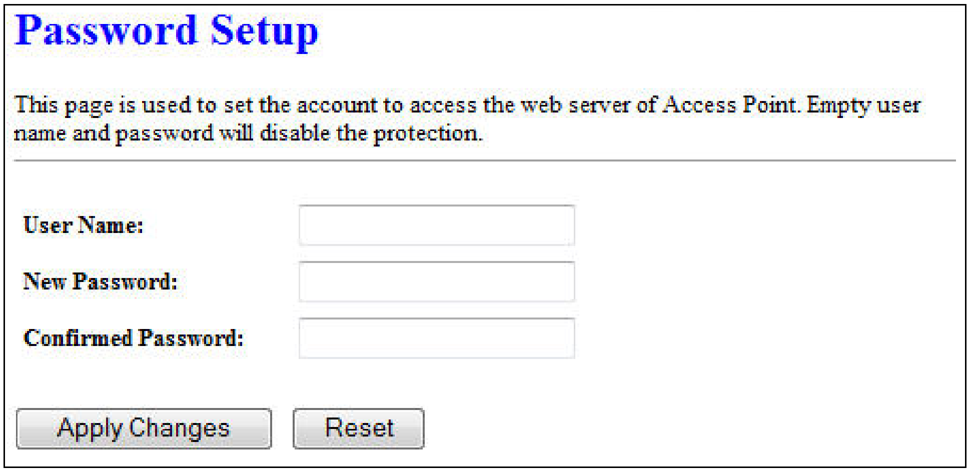
Load Settings from File:

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 DA1101. 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:

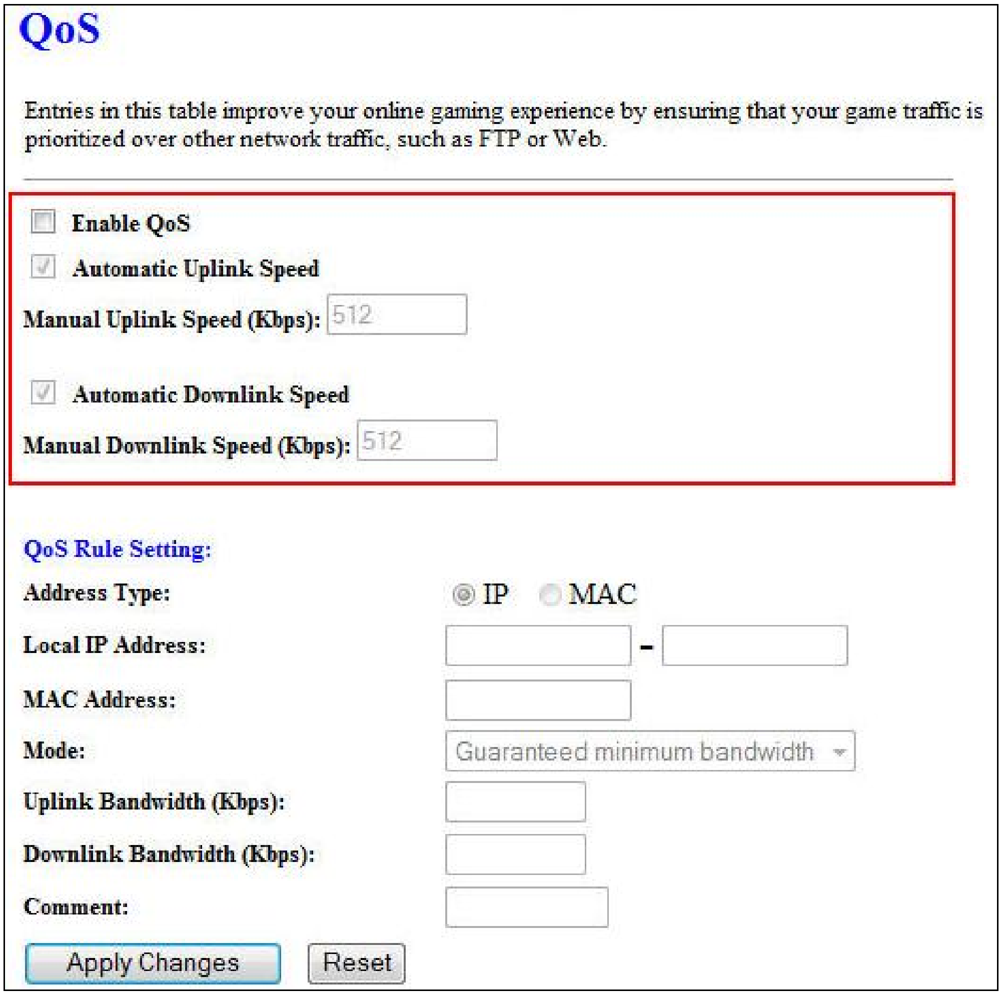
User Name	Enter user name.
New Password	Input password for this user.
Confirmed Password	Confirm password again.

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):

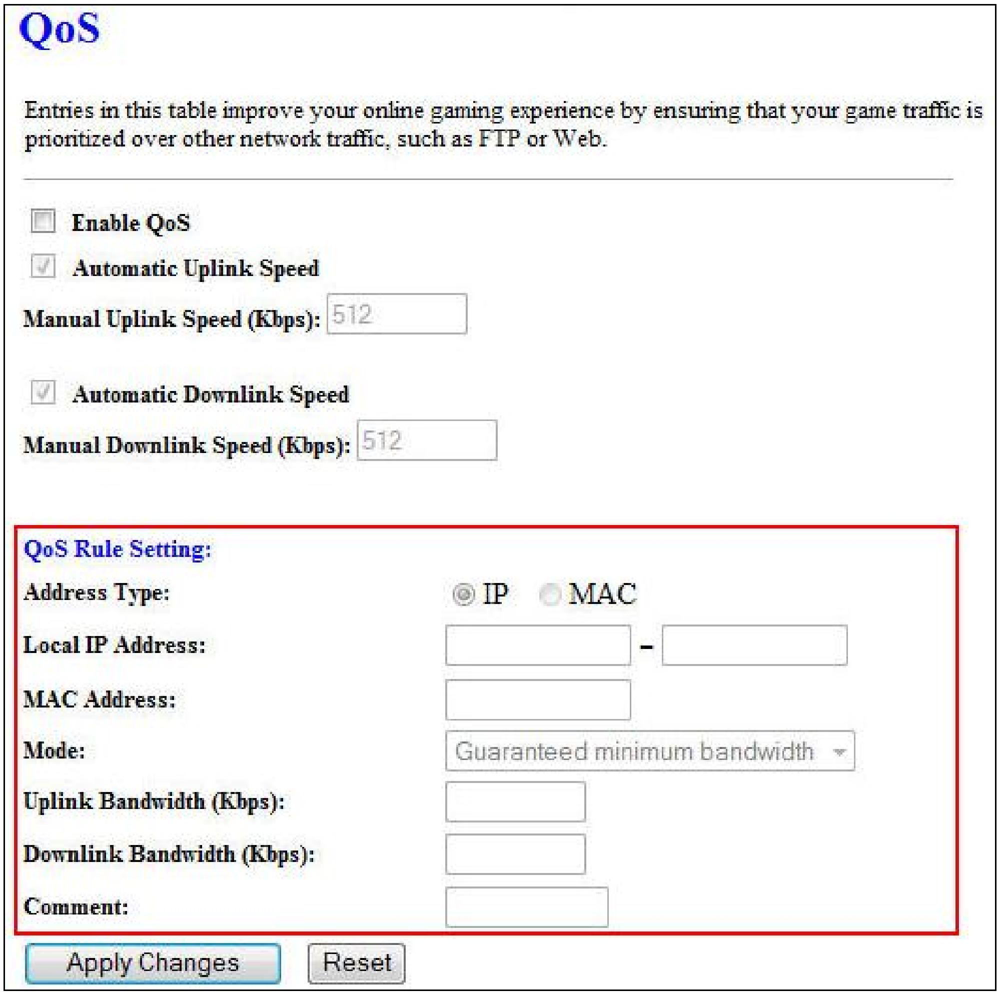
Downlink Bandwidth (Kbps):

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:	

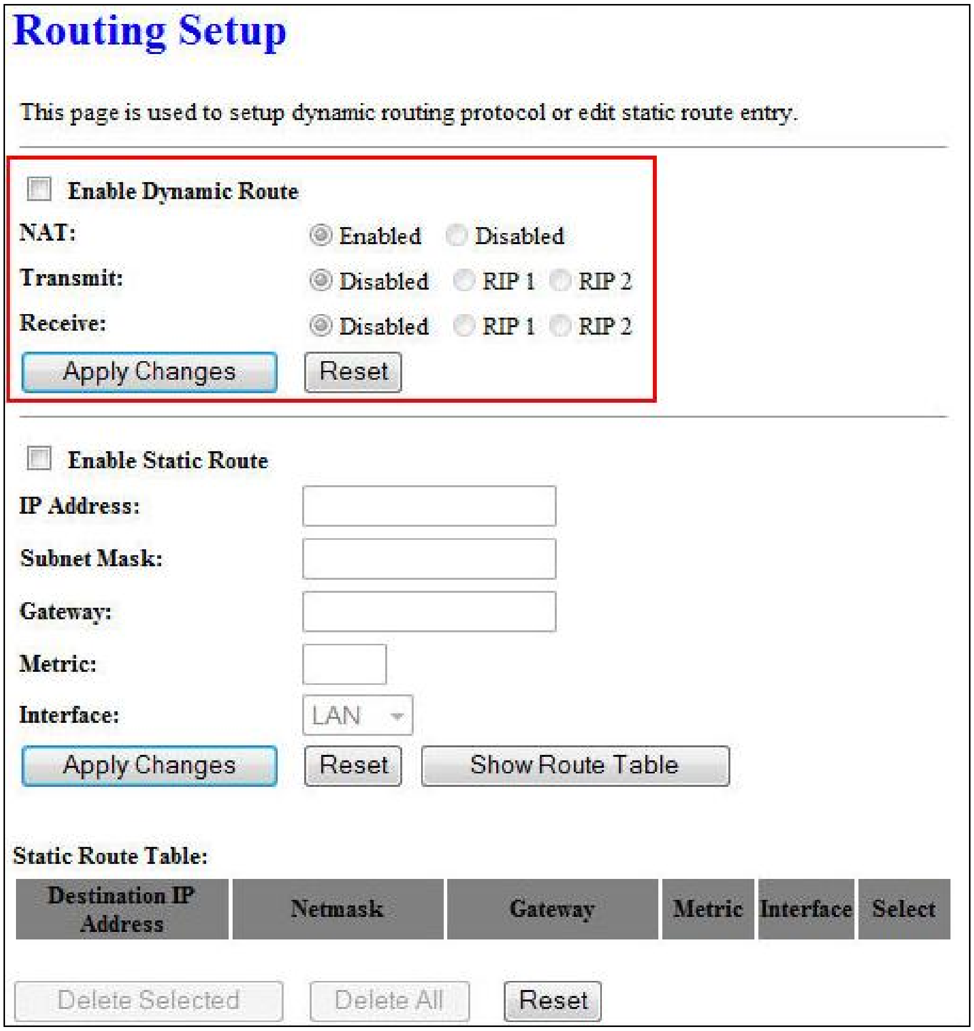
Address Type	Select IP or MAC address type.
Local IP Address MAC Address	Depend on the address type that selected, user can enter the IP address or MAC address of client to set up the bandwidth of the transmission.
Mode	Select Guaranteed minimum bandwidth or Restricted maximum bandwidth modes.
Uplink 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

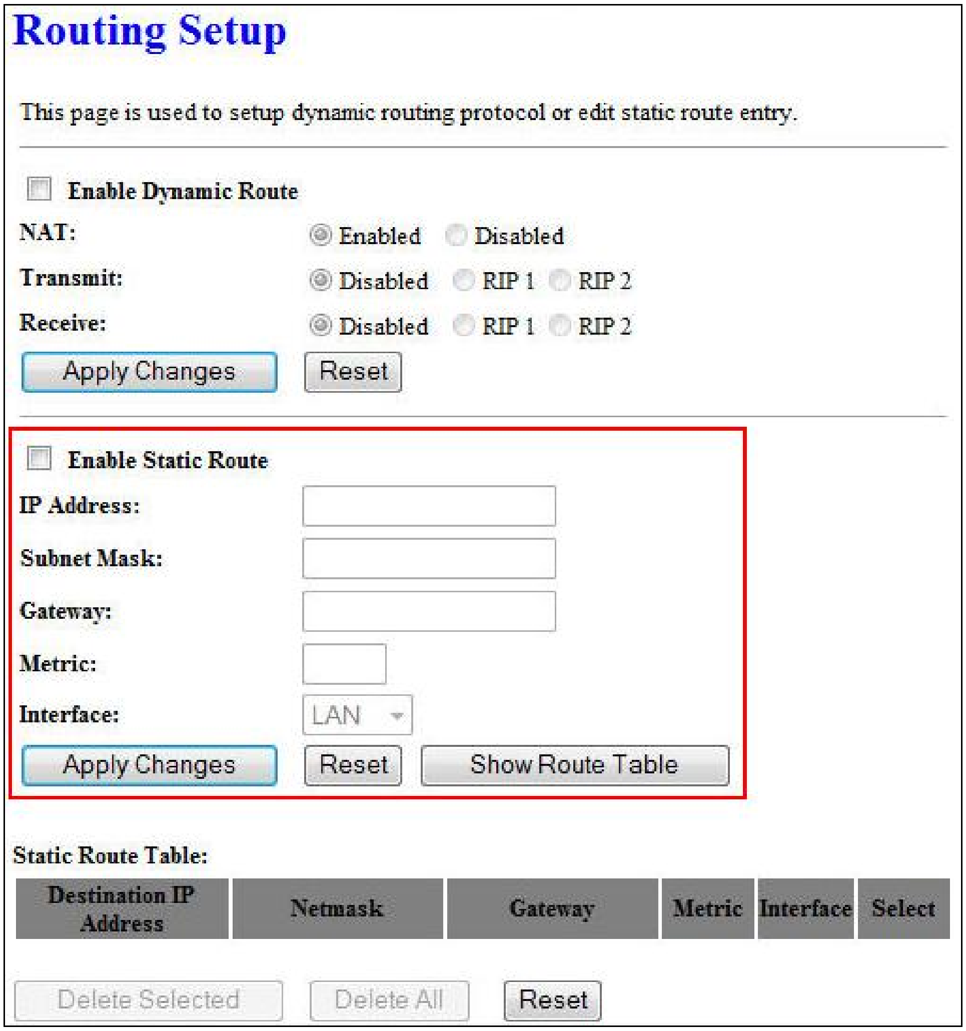
Static Route Table:

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 DA1101 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 DA1101 login username and / or password

A1:

1.) Restore DA1101 to its factory default settings by pressing the "Reset" button of the device for 10 seconds or more.

Appendix B DA1101 Specifications

Product	802.11n Wireless DA1101
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	