11N Mini Wireless AP

User Manual

Version 1.0 | 2/11/2014

CONTENTS

Chapter 1 Introduction

Congratulations on your purchase of this outstanding 11N Mini Wireless AP. The Wireless AP is a 150M Mini Wireless AP/Repeater, fully complies with 802.11b/g/n specifications, adopting 1T1R architecture, up to 150Mbps data rate, you can connect notebook computer to a wireless network and access high-speed Internet connection which is beneficial for the such as HD video streaming and online gaming applications. The default mode is repeater which is especially useful for a large space to eliminate signal-blind corners. It is good choice for Large house, office, warehouse or other spaces where the existing wireless signal is weak. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

1.1 Features

- Compatible with IEEE 802.11b/g/n
- Wireless speed up to 150Mbps
- Internal power supply
- Travel-sized design, Ideal for home or travel use
- Support WPA and WPA2 to safeguard wireless network access security
- Supports AP, Router, Repeater operation modes

1.2 System Requirement

- An Ethernet-Based Cable or DSL modem
- An wireless network card on PC
- TCP/IP network protocol for each PC
- RJ45 Twisted-pair
- Microsoft IE (or Firefox or Netscape)

1.3 Environment

Operating Temperature: 0℃~40℃
Storage Temperature: -10℃~70℃
Operating Humidity: 10%~90% non-condensing
Storage Humidity: 5%~95% non-condensing

1.4 Package Contents

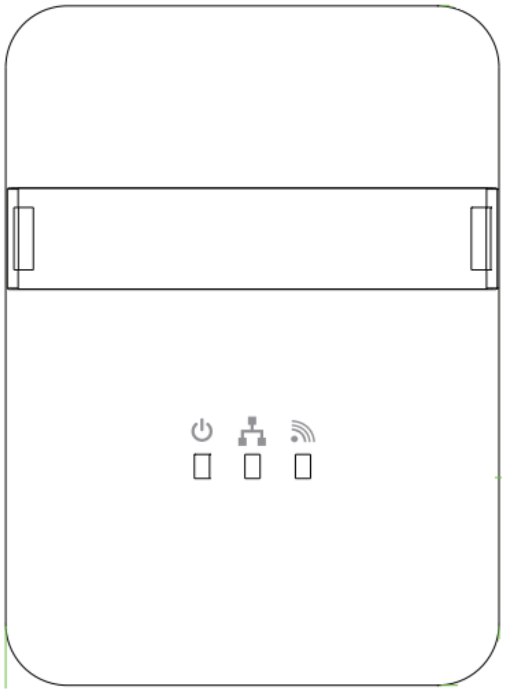
Please make sure you have the following in the box, if anything is missing, please contact your vendor.

- 11N Mini Wireless AP
- User Manual
- **RJ-45 Network Cable**
- Warranty Card

Chapter 2 Hardware Installation

2.1 Front Panel

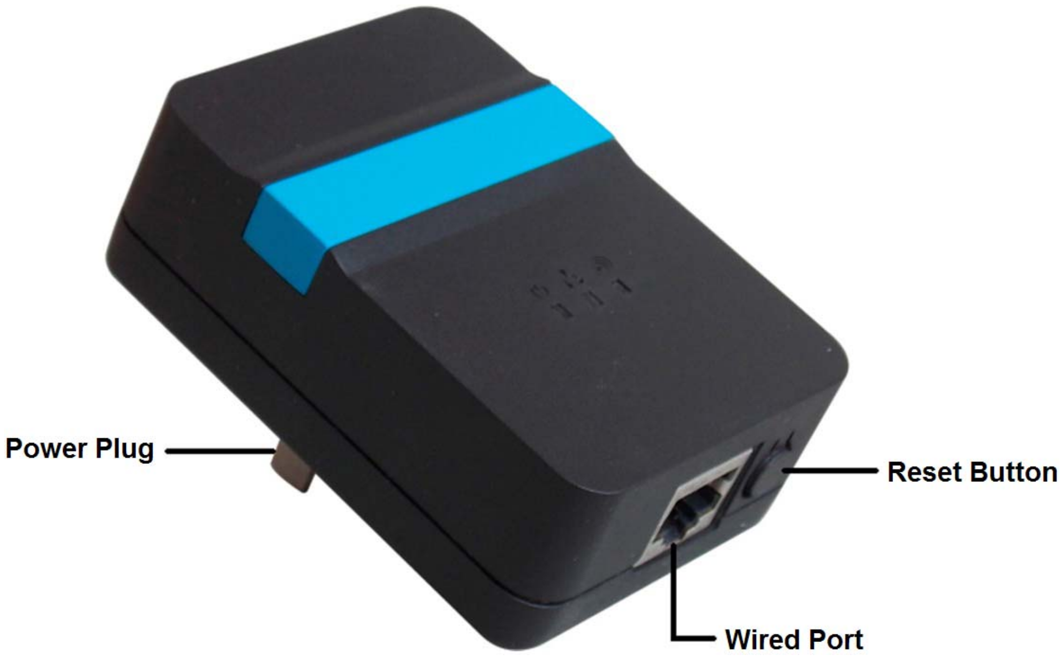
The front panel provides LED’s for device status. Refer to the following table for the meaning of each feature.



Name	Status	Indication
POWER	Off	Power is off.
	On	Power is on.
ETH (LAN/WAN)	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port but there is no activity.
	Flashing	There is an activity device linked to the corresponding port.
WLAN	Off	The Wireless function is disabled.
	On	The Wireless function is enabled.
	Flashing	Data is received or sent through the Wireless.

2.2 Physical Interface

There are three physical interfaces on this AP.



Interface	Description
Power Plug	A Power Plug for connecting the AP to a 100V~240V AC power socket.
Wired Port	A 10/100Mbps LAN/WAN Port for connecting the AP to the PC or the broadband device with a network cable.
Reset(WPS) Button	The Reset Button has two functions, WPS and Factory Default. When press it less than 2 seconds, it is WPS function, more than 5 seconds, the AP will restore to factory default.

2.3 Typical install

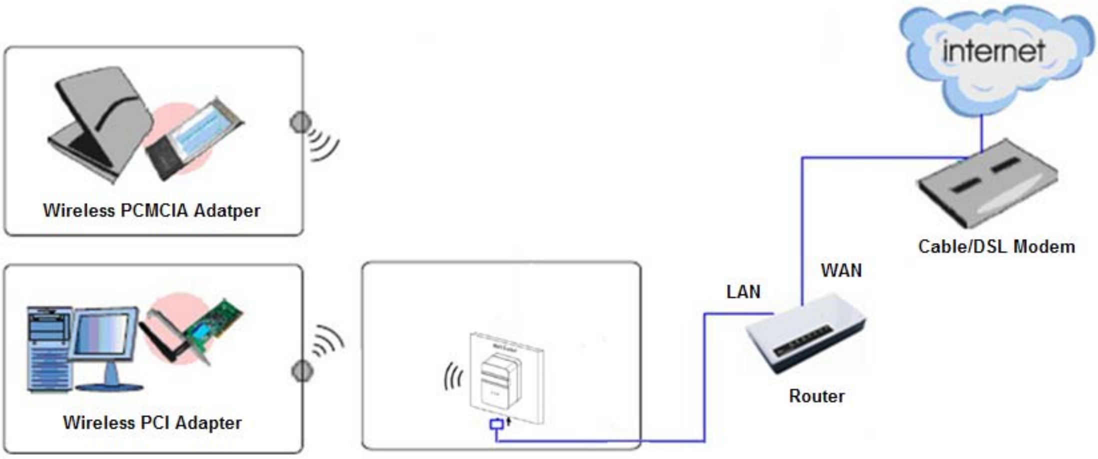
AP Mode:

As the supplement of wired LAN, Wireless AP enables the wired LAN to connect to the Internet wirelessly.

The default mode of Wireless AP is AP. Plug the power plug of Wireless AP in electrical wall socket and connect the Ethernet cable correctly, you can surf the Internet by connecting your PC(s) to The Router wirelessly.

To avoid the conflict of DHCP service with front-end devices, the DHCP server is default to be closed on this mode. If you want to login in the management page, please set your computer’s IP address manually.

As below picture, under this mode, wired port works as LAN, connects wired signal directly and turns the wired into wireless via AP device for the using of terminal wireless equipment.

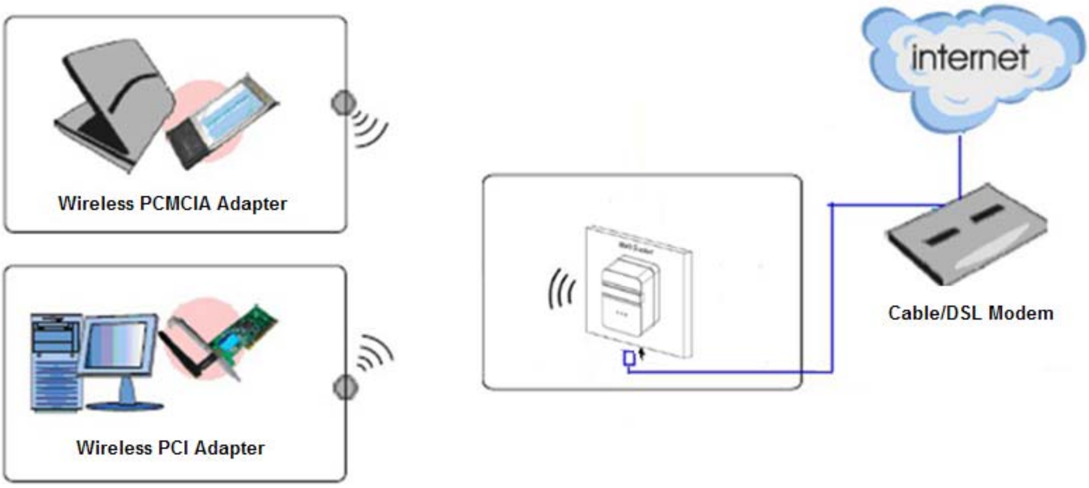


1. Connect the LAN port of Wireless AP to the wired network port with and Ethernet cable.
2. Plug the power plug of Wireless AP in electrical wall socket.
3. Power on the PC(s) and notebook(s).

Router Mode:

As a wireless router, Wireless AP enables multi-user to share Internet via DSL/Cable Modem.

As below picture, under this mode, wired port works as WAN, which can access network by using WI-FI Network, Cable/DSL Modem to be used by the lower extreme wireless device. DHCP server is default opened and it is recommended that the IP address and DNS server address obtained automatically.

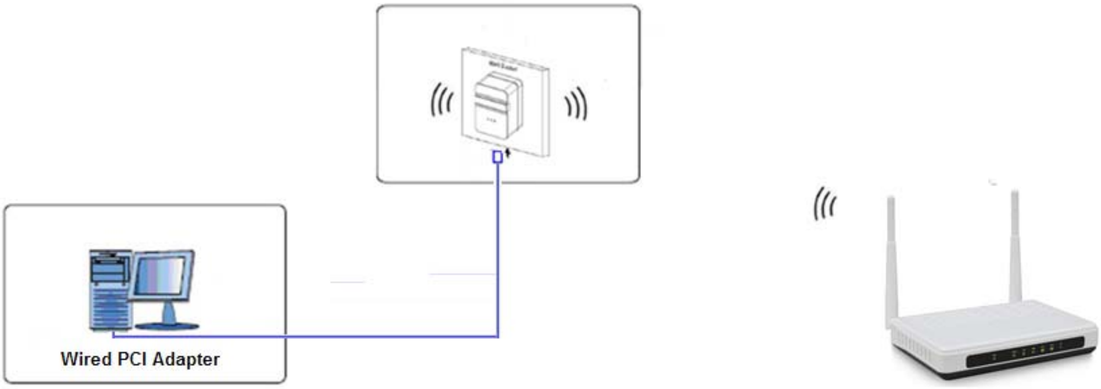


1. Connect the WAN port of Wireless AP to the LAN port on the DSL/Cable Modem.
2. Connect the WAN port on the DSL/Cable Modem to the wired Internet.
3. Plug the power plug of Wireless AP in electrical wall socket.
4. Power on the DSL/Cable Modem, PC(s) and notebook(s).

Wireless ISP Mode:

The Wireless AP is used as a wireless network card to connect the wireless network signal or wireless router.

As below picture, the only wired port works as LAN. Computer could connect to the device by wired way.



1. Connect the PC to the LAN port of Wireless AP with an Ethernet cable.
2. Plug the power plug of Wireless AP in electrical wall socket.
3. 3. Power on the PC.

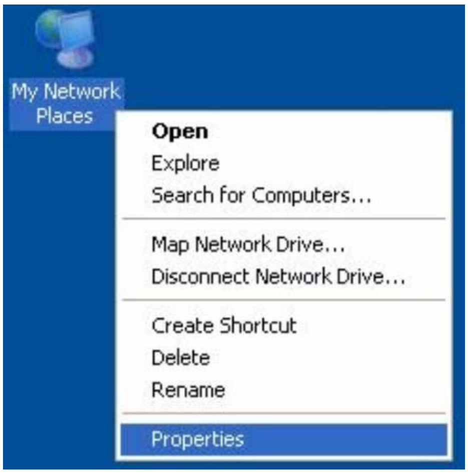
Chapter 3 TCP/IP Configuration

3.1 Set the Network Configurations

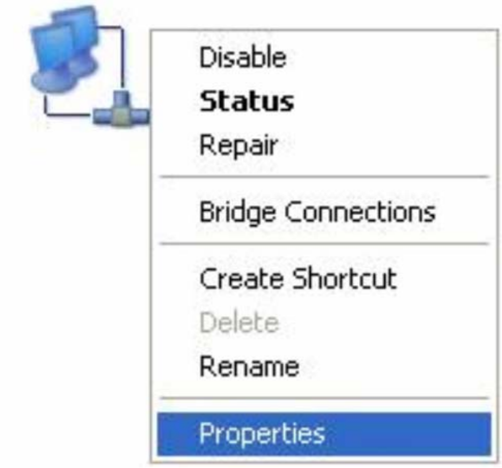
Under AP mode, you can proceed configuration by using the mode of wireless access or wired access.
Under Router mode, you can access device to process configuration by using the mode of wireless access.

After connecting device, operate according to below steps:

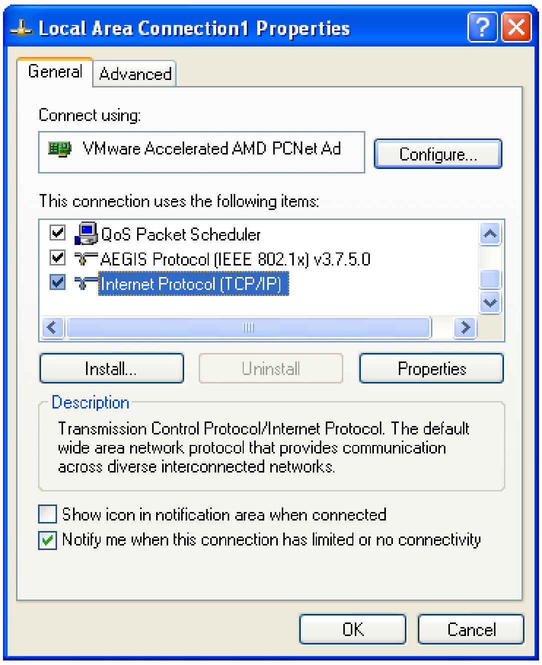
1. On your computer desktop right click **"My Network Places"** and select **"Properties"**.



2. Right click **"local Area Network Connection"** and select **"Properties"**.



3. Select **"Internet Protocol (TCP/IP)"** and click **"Properties"**.



Connect using:

VMware Accelerated AMD PCNet Ad

This connection uses the following items:

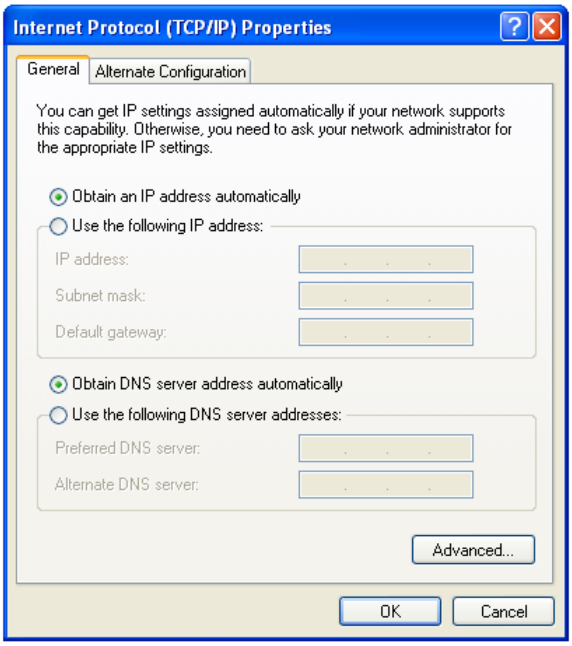
☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.7.5.0
☑ Internet Protocol (TCP/IP)

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

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

4. Select **"Obtain an IP address automatically"** or select **"Use the following IP address(S)"**.

A. Select **"Obtain an IP address automatically"** and **"Obtain DNS server address automatically"**. Click "OK".



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

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

B. **"Use the following IP address (S)"**

IP Address: 192.168.10.XXX :(XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.254

DNS Server: You need to input the DNS server address provided by you ISP. Otherwise, you can use the AP's default gateway as the DNS proxy server. Click "OK" to save the configurations.

Note: When your wireless AP is in AP mode, the equipment system DHCP function

will be automatic to shut down, you need to press the B method and set the IP.

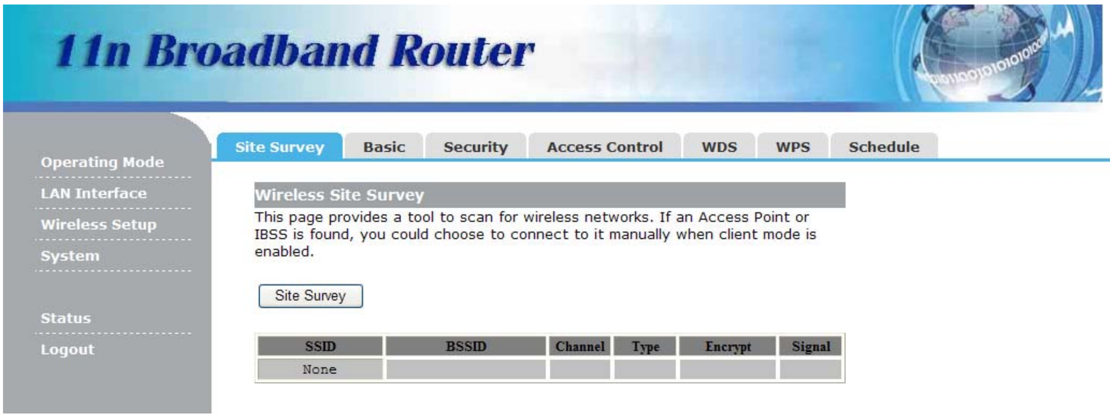
Click "OK" to save the configurations.

3.2 Getting Started

http://192.168.10.254/

To access the configuration pages, open a web-browser such as Internet Explorer and enter the IP address of the AP (**192.168.10.254**).
The Default User/Password: **admin**

If succeed, you can see the follow page.



Wireless Site Survey

This page provides a tool to scan for wireless networks. If an Access Point or IBSS is found, you could choose to connect to it manually when client mode is enabled.

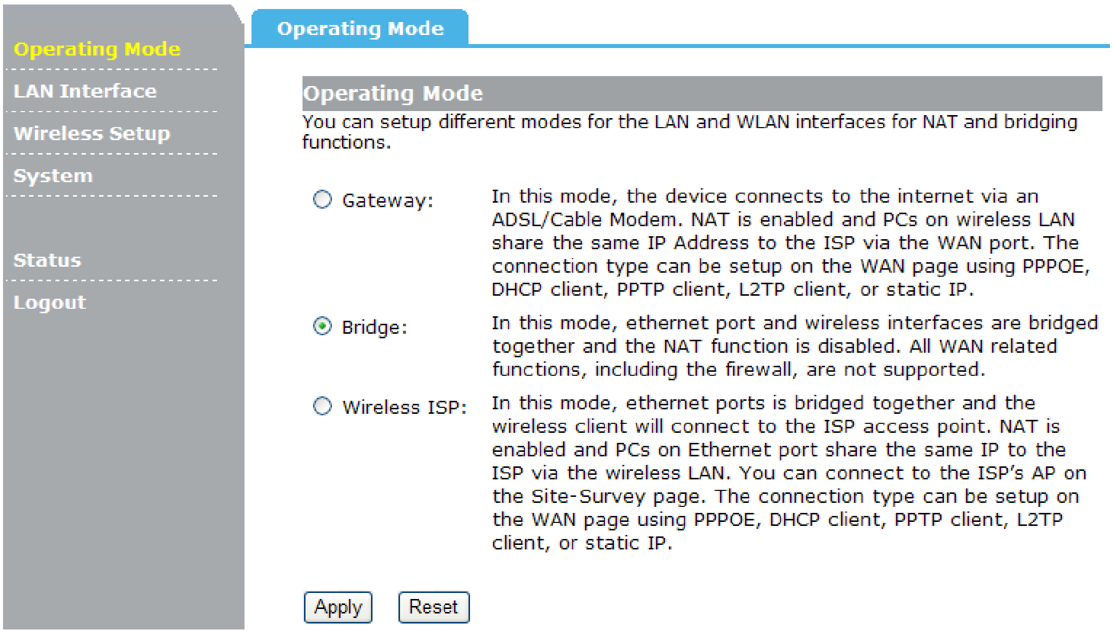
SSID	BSSID	Channel	Type	Encrypt	Signal
None					

Chapter 4 Configuring the AP

This chapter will show each Web page's key functions and the configuration way.

4.1 Operating Mode

The Wireless AP supports three operation modes, **Gateway**, **Bridge** and **Wireless ISP**. And each mode is suitable for different use, please choose correct mode.



Operating Mode

You can setup different modes for the LAN and WLAN interfaces for NAT and bridging functions.

○ Gateway: In this mode, the device connects to the internet via an ADSL/Cable Modem. NAT is enabled and PCs on wireless LAN share the same IP Address to the ISP via the WAN port. The connection type can be setup on the WAN page using PPPOE, DHCP client, PPTP client, L2TP client, or static IP.

● Bridge: In this mode, ethernet port and wireless interfaces are bridged together and the NAT function is disabled. All WAN related functions, including the firewall, are not supported.

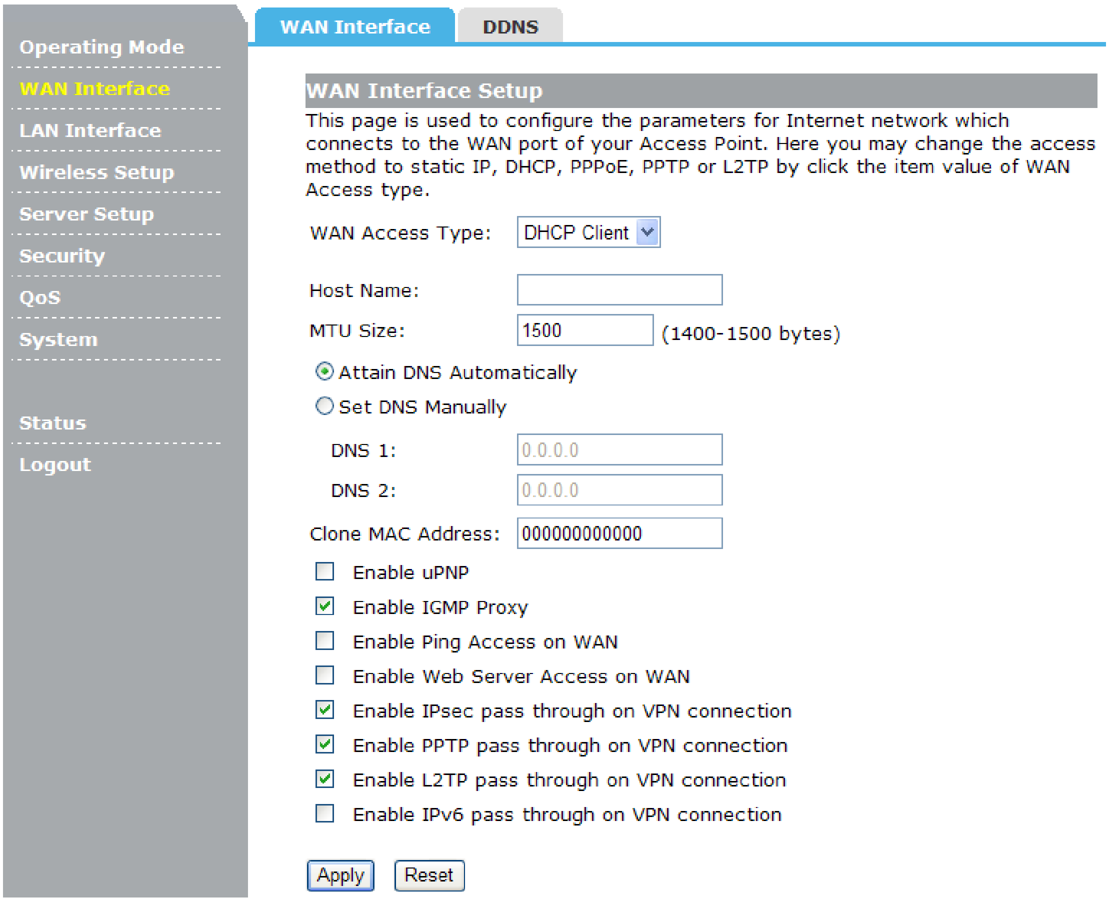
○ Wireless ISP: In this mode, ethernet ports is bridged together and the wireless client will connect to the ISP access point. NAT is enabled and PCs on Ethernet port share the same IP to the ISP via the wireless LAN. You can connect to the ISP's AP on the Site-Survey page. The connection type can be setup on the WAN page using PPPOE, DHCP client, PPTP client, L2TP client, or static IP.

4.2 WAN Interface

There are two submenus under the WAN Interface menu: **WAN Interface, DDNS**. Click any of them, and you will be able to configure the corresponding function.

4.2.1 WAN Interface

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



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: 1500 (1400-1500 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 0.0.0.0

DNS 2: 0.0.0.0

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

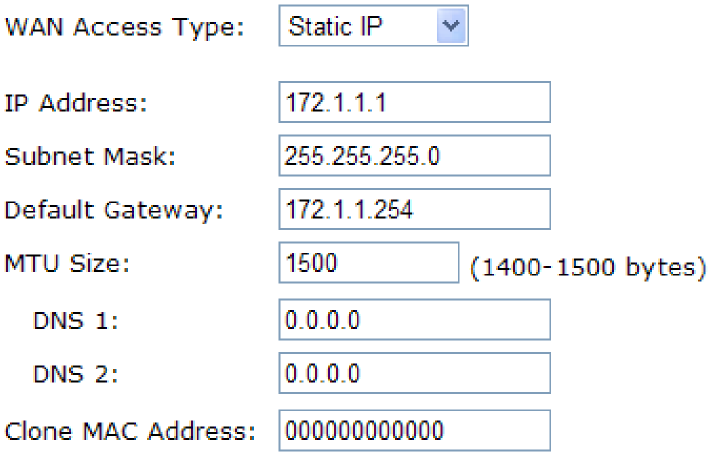
☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

□ Enable IPv6 pass through on VPN connection

Apply Reset

1. If you ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select *Static IP* option. The Static IP settings page will appear:



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: 0.0.0.0

DNS 2: 0.0.0.0

Clone MAC Address: 000000000000

IP Address / Subnet Mask: This is the AP's IP Address and Subnet Mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask.

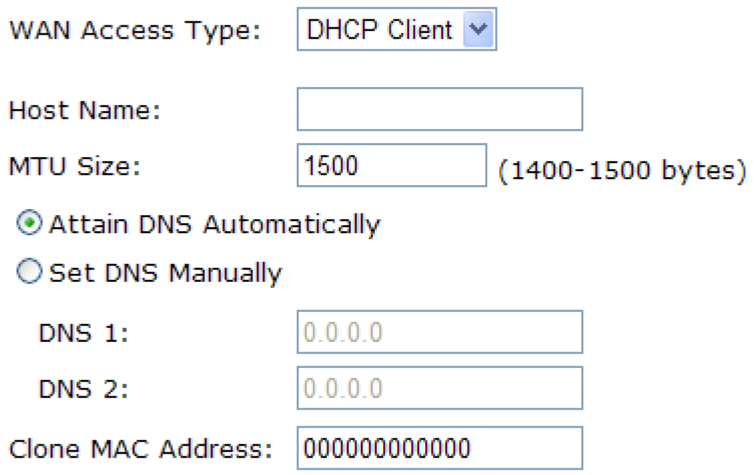
Gateway: Your ISP will provide you with the Gateway IP Address.

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: Your ISP will provide you with at least one DNS IP Address.

Clone Mac Address: You can configure the MAC address of the WAN.

2. If your ISP provides the DHCP service, please select *DHCP Client* option, and the AP's will automatically get IP parameters from your ISP. You can see the page as follows:



WAN Access Type: DHCP Client

Host Name:

MTU Size: 1500 (1400-1500 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 0.0.0.0

DNS 2: 0.0.0.0

Clone MAC Address: 000000000000

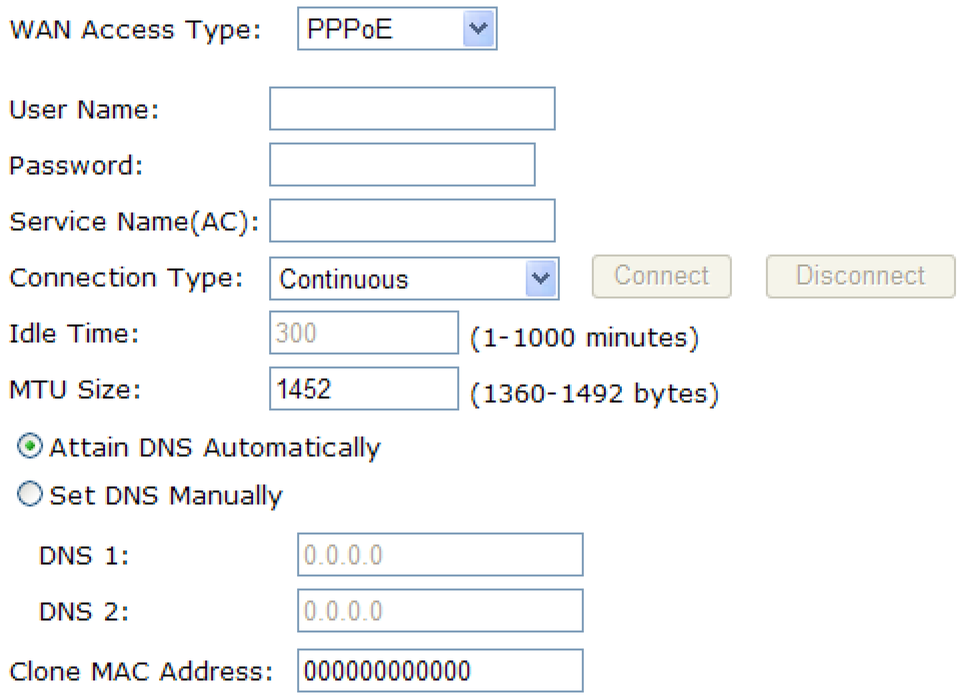
Host Name: This option specifies the Host Name of the AP.

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.

Set DNS Manually: If your ISP gives you one or two DNS addresses, select Set DNS Manually and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

Clone Mac Address: You can configure the MAC address of the WAN.

3. If your ISP provides a PPPoE connection, select *PPPoE* option. And you should enter the following parameters:



WAN Access Type: PPPoE

User Name:

Password:

Service Name(AC):

Connection Type: Continuous

Idle Time: 300 (1-1000 minutes)

MTU Size: 1452 (1360-1492 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 0.0.0.0

DNS 2: 0.0.0.0

Clone MAC Address: 000000000000

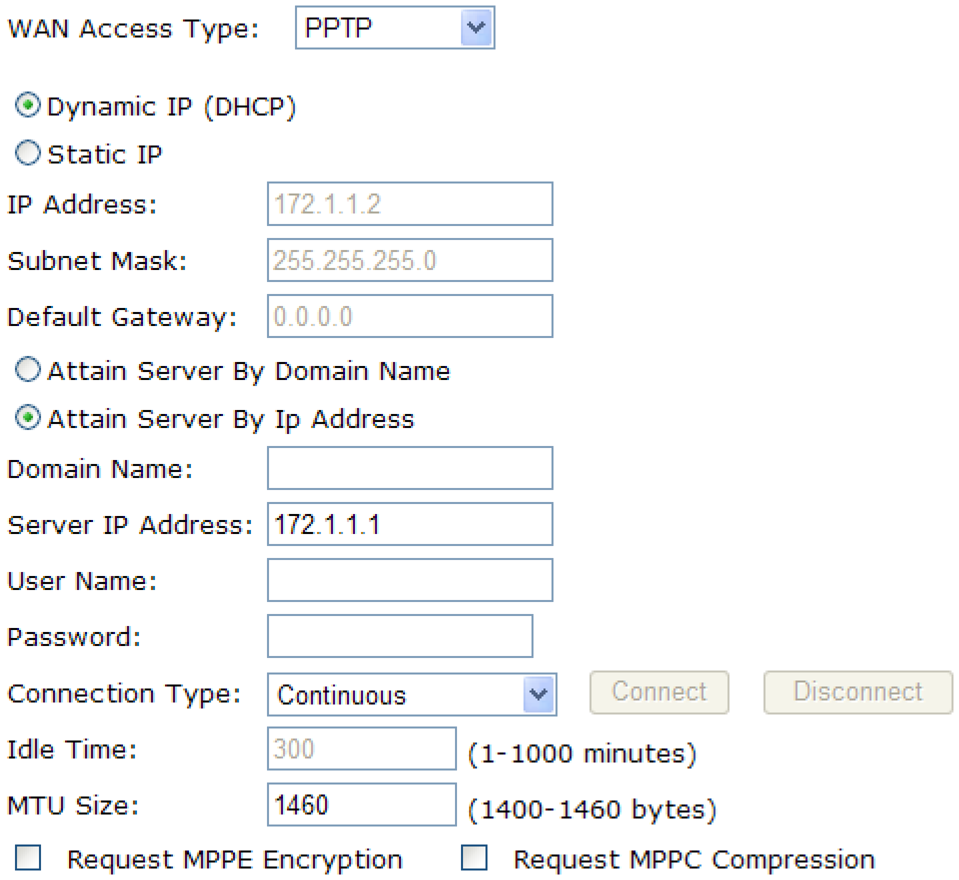
User Name / Password: Enter the User Name and Password you use when logging onto your ISP through a PPPoE connection.

Service Name(AC): The service name and AC (Access Concentrator) name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

Connection Type: There you can select Continuous, Connect on Demand or Manual.

Idle Time: You can configure the AP to disconnect from your Internet connection after a specified period of inactivity.

4. If your ISP provides a PPTP connection, select *PPTP* option. And you should enter the following parameters:



WAN Access Type: PPTP

● Dynamic IP (DHCP)

○ Static IP

IP Address: 172.1.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

○ Attain Server By Domain Name

● Attain Server By Ip Address

Domain Name:

Server IP Address: 172.1.1.1

User Name:

Password:

Connection Type: Continuous

Idle Time: 300 (1-1000 minutes)

MTU Size: 1460 (1400-1460 bytes)

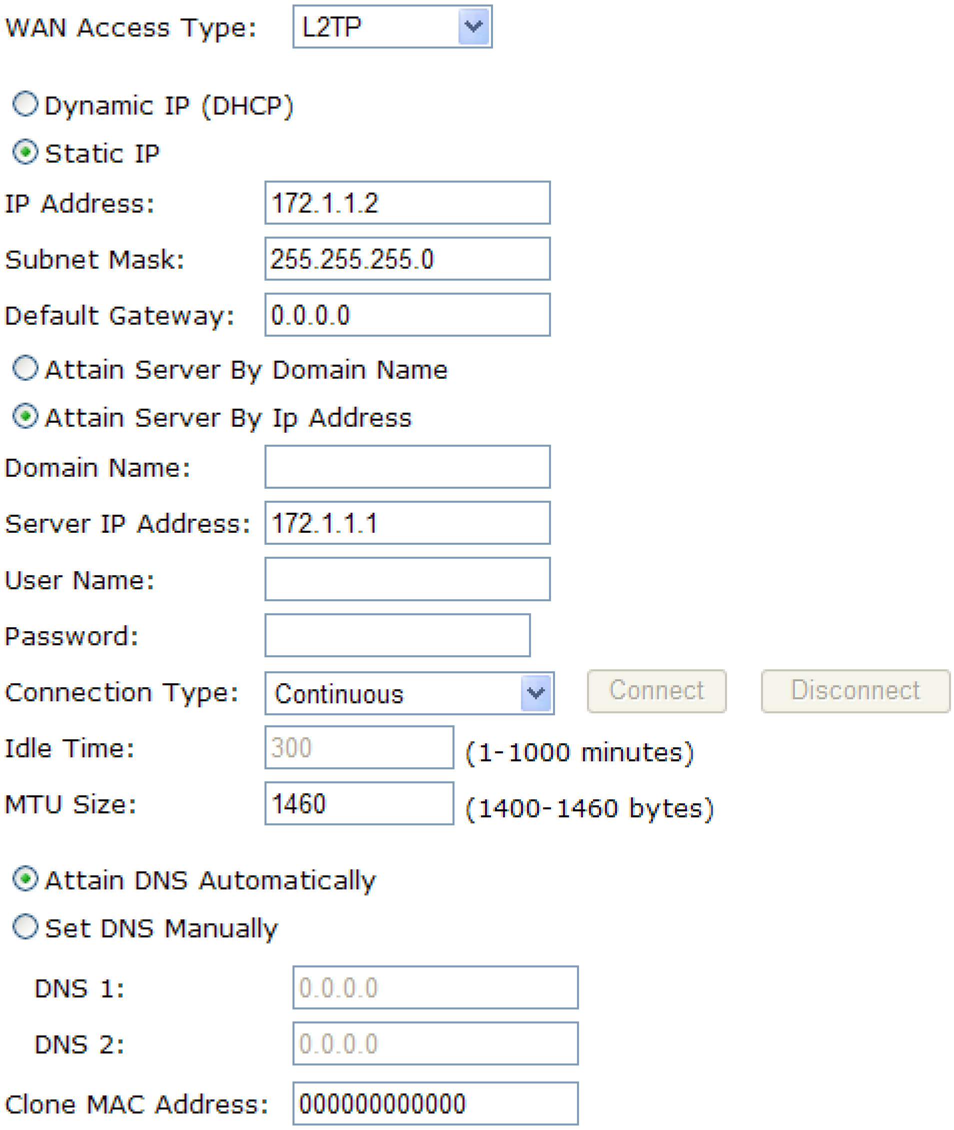
□ Request MPPE Encryption □ Request MPPC Compression

Dynamic IP (DHCP): Choose the IP address information provided by automatic acquisition ISP, or manual input.

Default Gateway: Enter the gateway IP provided by your PPTP Server.

User Name / Password: Enter the User Name and Password you use when logging onto your ISP through a PPTP connection.

5. If your ISP provides L2TP connection, please select *L2TP* option. And you should enter the following parameters:



WAN Access Type: L2TP

○ Dynamic IP (DHCP)
● Static IP

IP Address: 172.1.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0

○ Attain Server By Domain Name
● Attain Server By Ip Address

Domain Name:
Server IP Address: 172.1.1.1
User Name:
Password:
Connection Type: Continuous

Idle Time: 300 (1-1000 minutes)
MTU Size: 1460 (1400-1460 bytes)

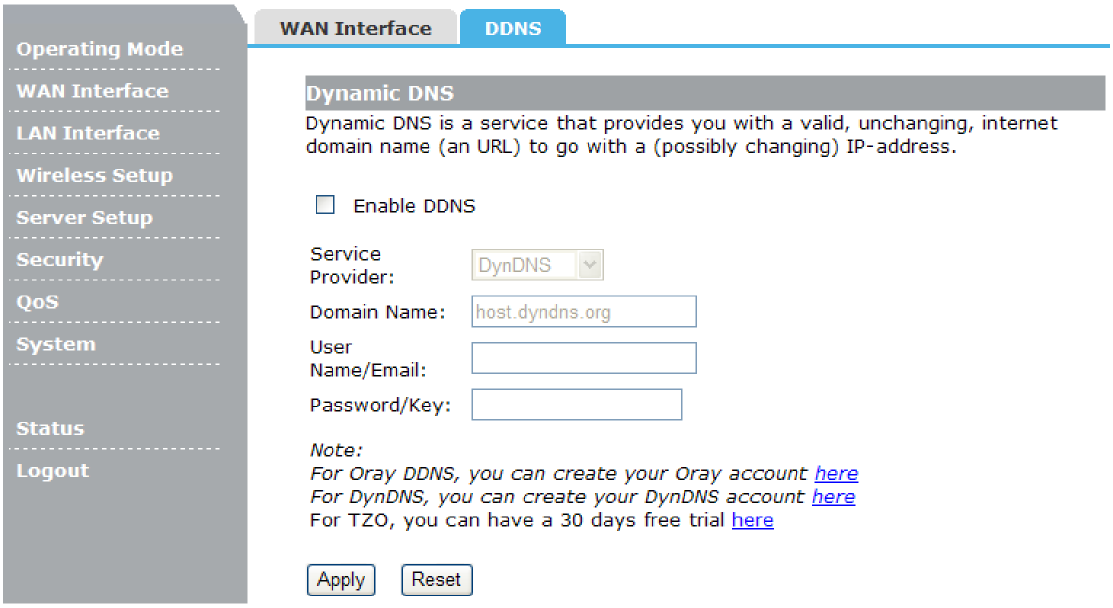
● Attain DNS Automatically
○ Set DNS Manually

DNS 1: 0.0.0.0
DNS 2: 0.0.0.0
Clone MAC Address: 000000000000

Dynamic IP (DHCP): Choose the IP address information provided by automatic acquisition ISP, or manual input.
Default Gateway: Enter the gateway IP provided by your L2TP Server.
User Name / Password: Enter the User Name and Password you use when logging onto your ISP through a L2TP connection.

4.2.2 DDNS

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



Dynamic DNS

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

□ Enable DDNS

Service Provider: DynDNS

Domain Name: host.dyndns.org

User Name/Email:

Password/Key:

Note:
For Oray DDNS, you can create your Oray account here
For DynDNS, you can create your DynDNS account here
For TZO, you can have a 30 days free trial here

Service Provider: Select one from the drop-down menu, such as DynDNS, OrayDDNS or TZO.

Domain Name: Enter the domain name (Such as host.dyndns.org).

User Name/Email: Enter the user name or email the same as the registration name.

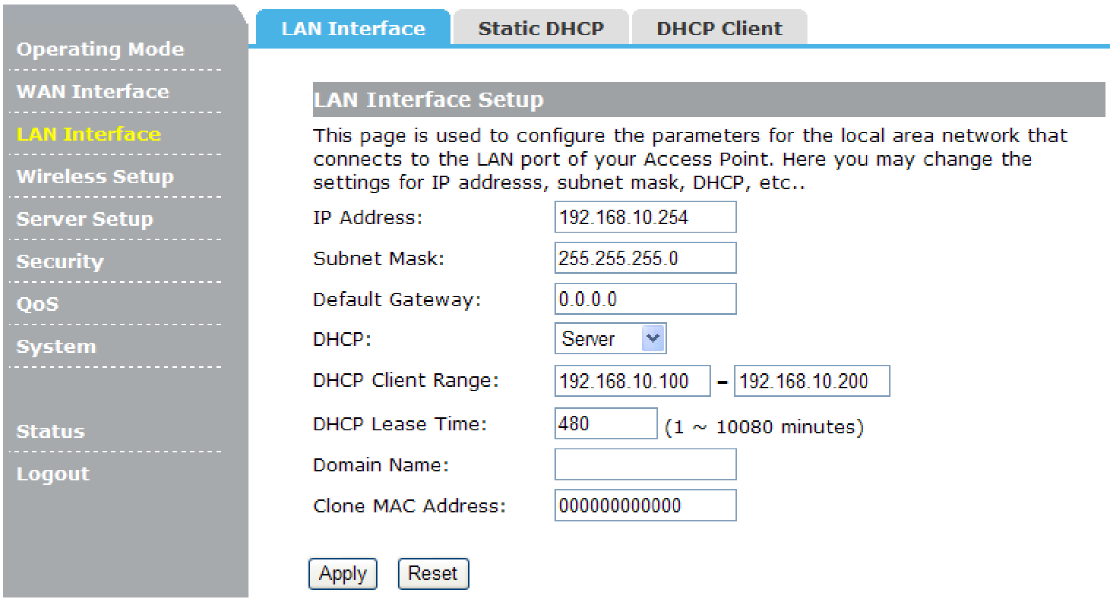
Password/Key: Enter the password you set.

4.3 LAN Interface

There are three submenus under the LAN Interface menu: **LAN Interface, Static DHCP, DHCP Client**. Click any of them, and you will be able to configure the corresponding function.

4.3.1 LAN Interface

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



LAN Interface Setup

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

IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Server

DHCP Client Range: 192.168.10.100 – 192.168.10.200

DHCP Lease Time: 480 (1 ~ 10080 minutes)

Domain Name:

Clone MAC Address: 000000000000

IP Address: Enter the IP address of your AP (**factory default: 192.168.10.254**).

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

Default Gateway: Enter the gateway IP address.

DHCP: Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.

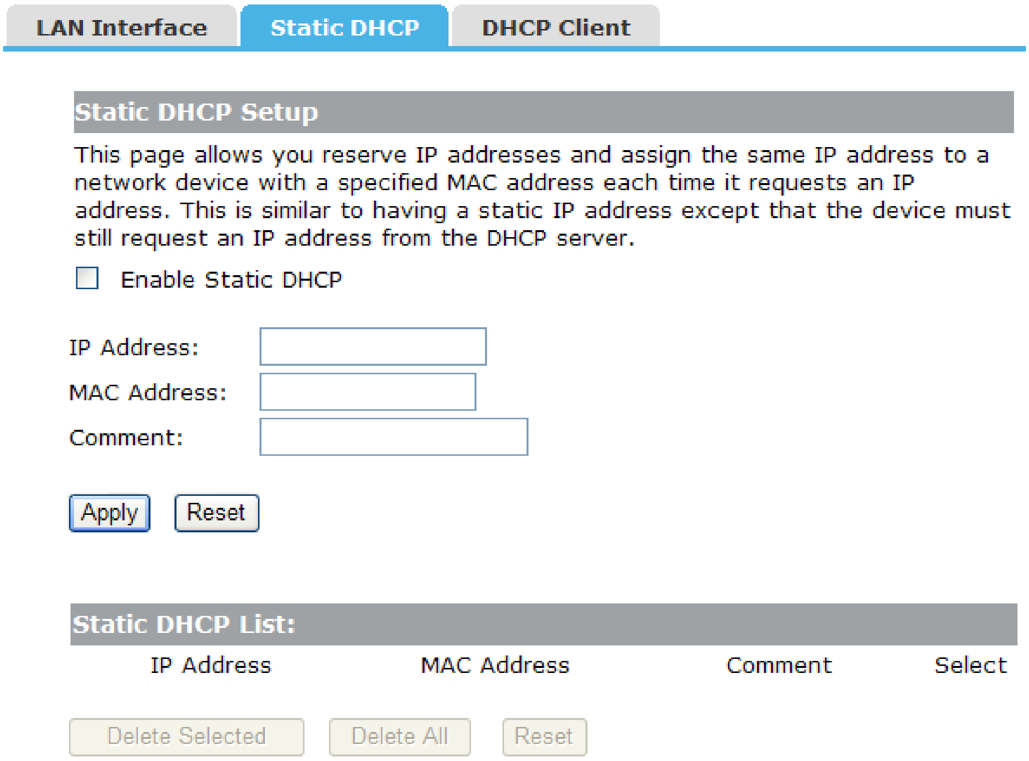
DHCP Client Range: Specify IP address for the DHCP Client Range.

DHCP Lease Time: The DHCP Lease Time is the amount of time a network user will be allowed connection to the AP with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.

Clone MAC Address: Input your MAC address should be cloned.

4.3.2 Static DHCP

This page 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.



Static DHCP Setup

This page allows you reserve IP addresses and assign the same IP address to a network device with a specified MAC address each time it requests an IP address. This is similar to having a static IP address except that the device must still request an IP address from the DHCP server.

□ Enable Static DHCP

IP Address:

MAC Address:

Comment:

Static DHCP List:

IP Address	MAC Address	Comment	Select

IP Address: Enter the IP address which needs to be bound.

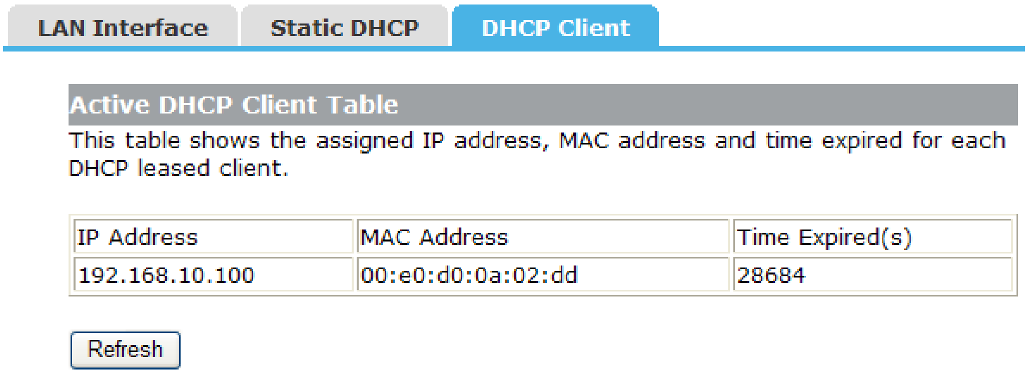
MAC Address: Enter the MAC address of the computer you want to assign the above IP address.

Comment: You can add some comment for this item.

Click **"Apply"** to add the entry in the list.

4.3.3 DHCP Client

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.



Active DHCP Client Table

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

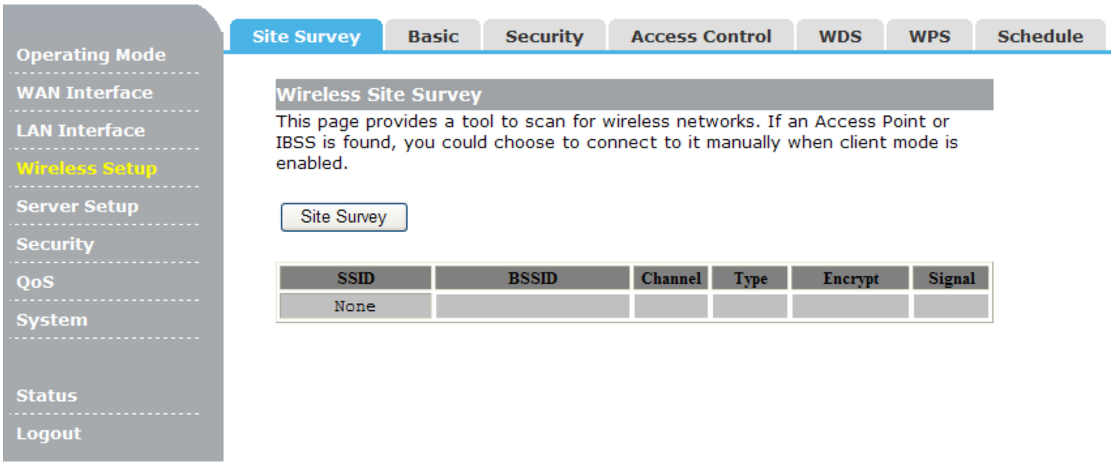
IP Address	MAC Address	Time Expired(s)
192.168.10.100	00:e0:d0:0a:02:dd	28684

4.4 Wireless Setup

There are seven submenus under the Wireless Setup menu: **Site Survey, Basic, Security, Access Control, WDS, WPS, Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.4.1 Site Survey

This page provides a tool to scan for wireless networks. If an Access Point or IBSS is found, you could choose to connect to it manually when client mode is enabled.



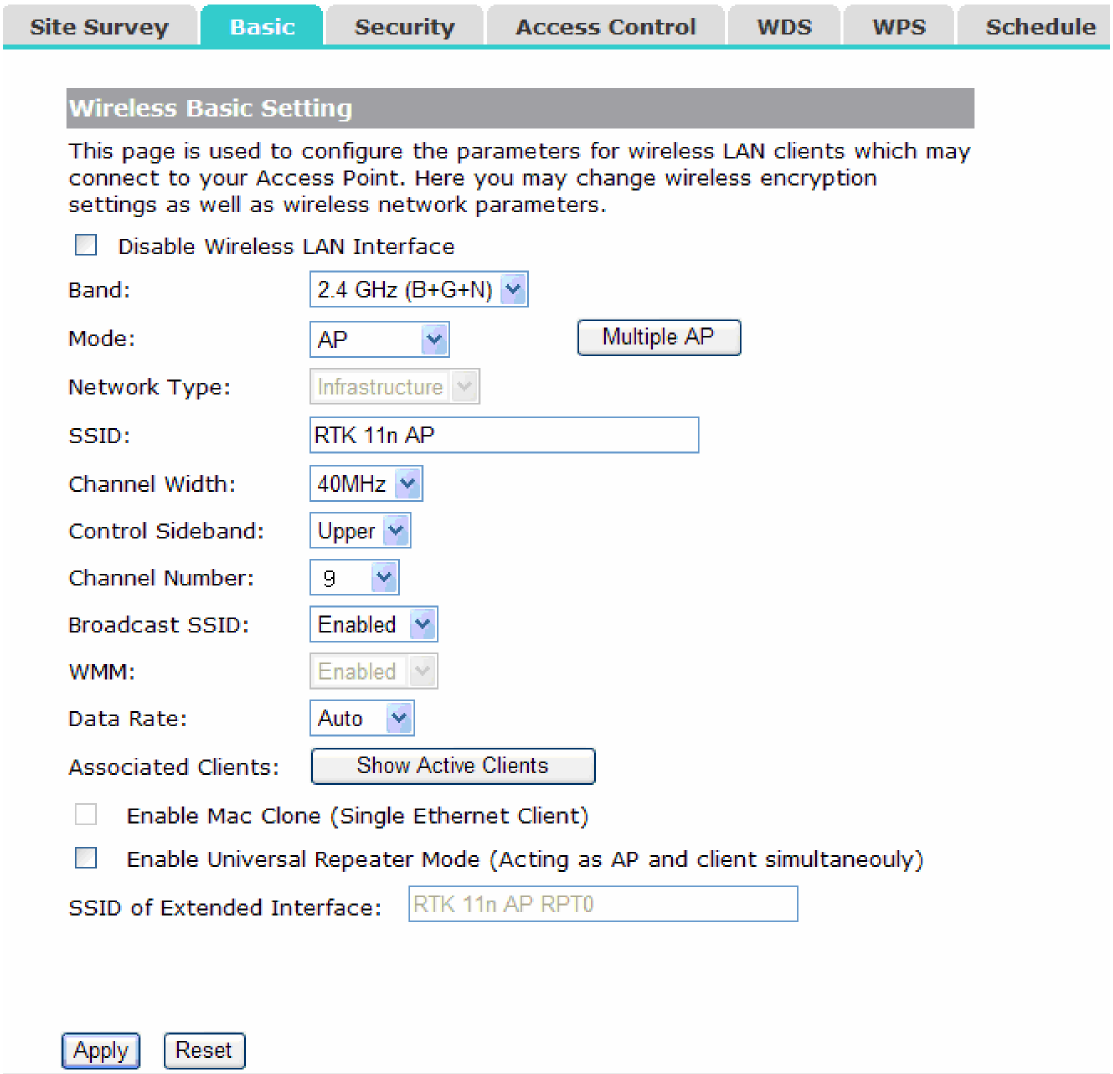
Wireless Site Survey

This page provides a tool to scan for wireless networks. If an Access Point or IBSS is found, you could choose to connect to it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal
None					

4.4.2 Basic

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless network parameters.



Wireless Basic Setting

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:	RTK 11n AP
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	9
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients

□ Enable Mac Clone (Single Ethernet Client)

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

SSID of Extended Interface: RTK 11n AP RPT0

Disable Wireless LAN Interface: Check this box to to disable the AP's wireless features; uncheck to enable it.

Band: Select one mode from the following. The default is 2.4GHz (B+G+N) mode.

Mode: Support AP, Client, WDS and AP+WDS mode.

Network Type: This type is only valid in client mode.

SSID: SSID (Service Set Identifier) is the unique name of the wireless network.

Channel Width: Select the channel width from the pull-down list. Select 40MHz if you use 802.11n or 802.11n mixed mode, otherwise 20MHz, it is default value.

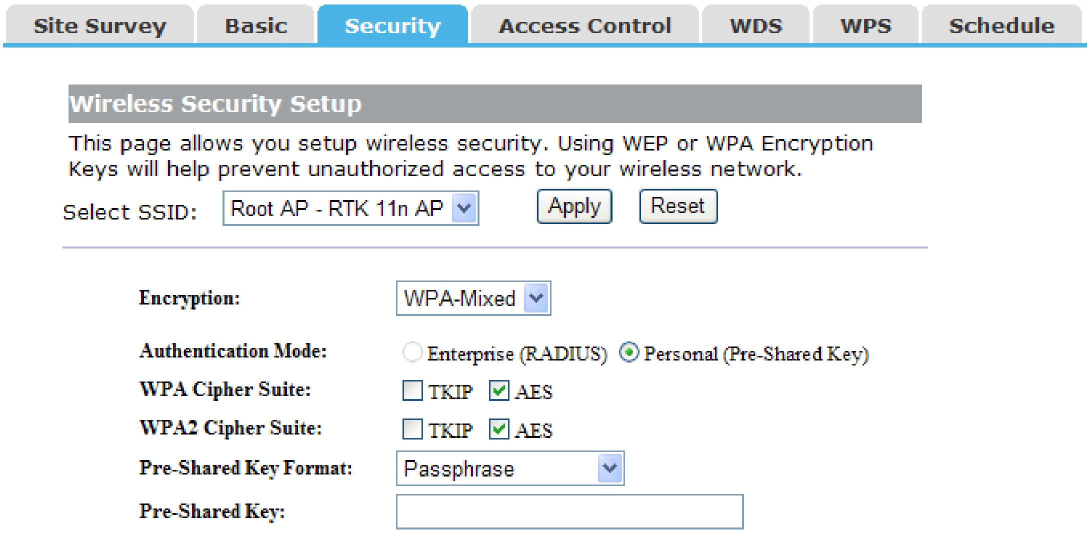
Channel Number: Indicates the channel setting for the AP.

Broadcast SSID: Select "Enable" to enable the device's SSID to be visible by wireless clients. The default is enabled.

WMM: It will enhance the data transfer performance of multimedia data when they're being transferred over wireless network.

4.4.3 Security

This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.



Wireless Security Setup

This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.

Select SSID: Root AP - RTK 11n AP

Encryption: WPA-Mixed

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

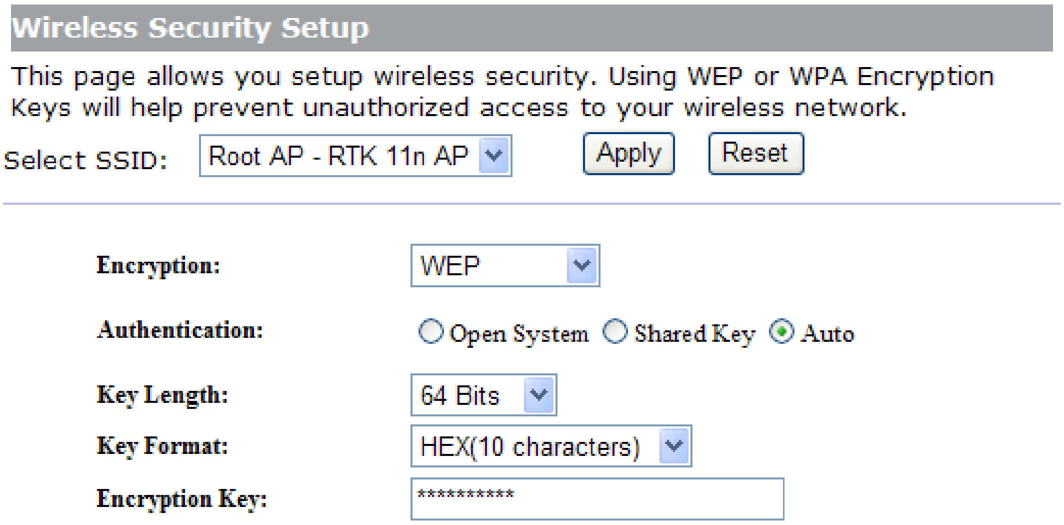
WPA Cipher Suite: □ TKIP ☑ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

The following picture shows how to set the WEP security.



Wireless Security Setup

This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.

Select SSID: Root AP - RTK 11n AP

Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

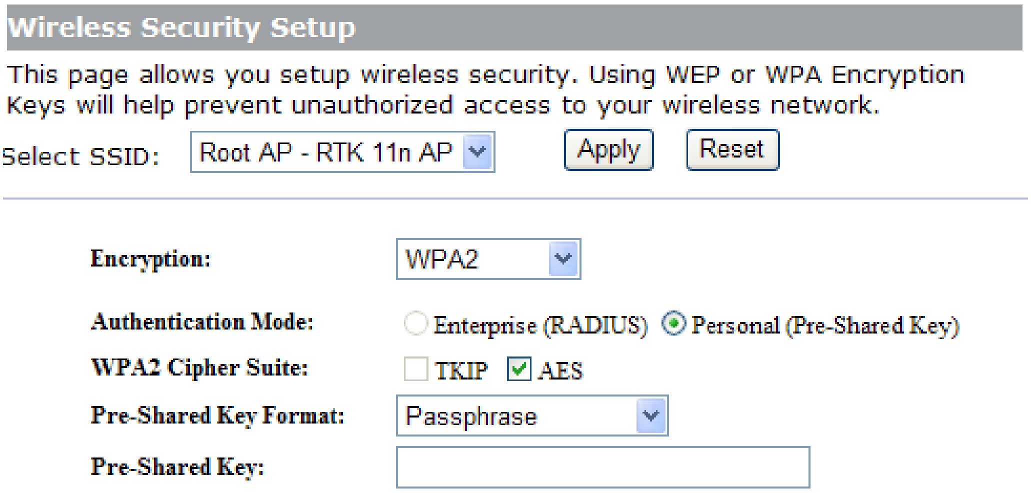
Key Length: 64 Bits

Key Format: HEX(10 characters)

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

Key length: WEP supports 64 Bits or 128 Bits security key.
Key Format: User can enter key in ASCII or Hex format.
Encryption Key: Enter the key, its format is limited by the Key format, ASCII or Hex.

The following picture shows how to set WPA-PSK security, you can select WPA (TKIP), WPA2 (AES) and Mixed mode.



Wireless Security Setup

This page allows you setup wireless security. Using WEP or WPA Encryption Keys will help prevent unauthorized access to your wireless network.

Select SSID: Root AP - RTK 11n AP [Apply] [Reset]

Encryption: WPA2

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

WPA2 Cipher Suite: □ TKIP ☑ AES

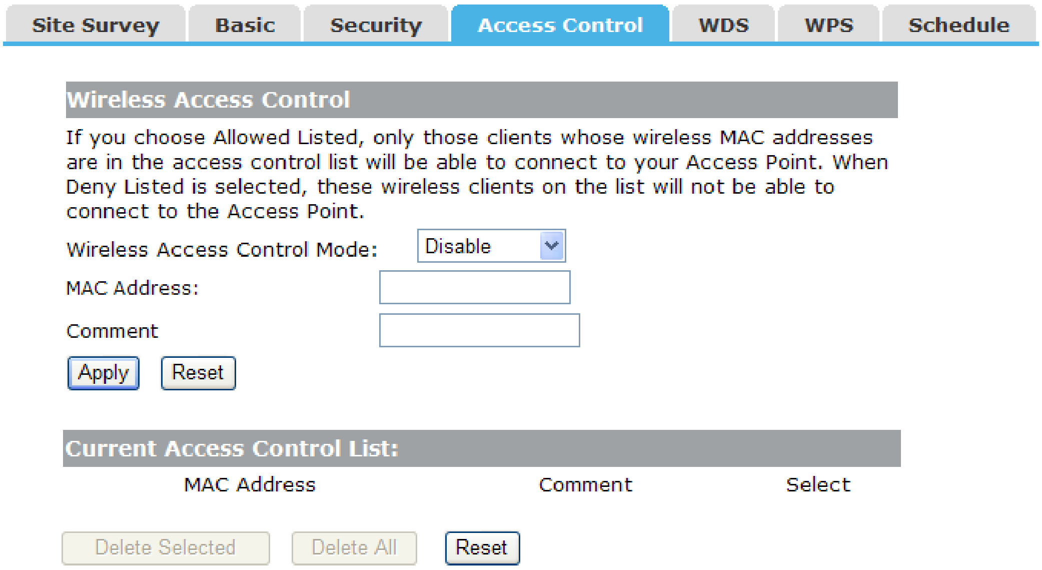
Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Pre-Shared Key Format: Specify the format of the key, pass phrase or hex.
Pre-Shared Key: Enter the key here, its format is limited by the key format.

4.4.4 Access Control

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the AP, which depend on the station's MAC addresses.



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 to the Access Point.

Wireless Access Control Mode: Disable

MAC Address:

Comment

[Apply] [Reset]

Current Access Control List:

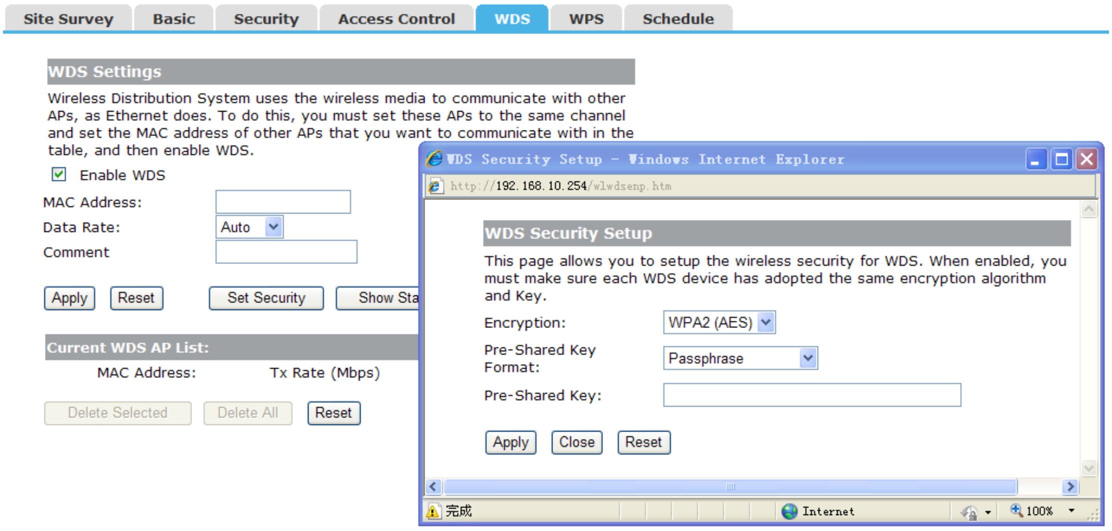
MAC Address	Comment	Select

[Delete Selected] [Delete All] [Reset]

Mode: 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. The MAC Address format is 001122334455.

4.4.5 WDS

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, firstly you must set AP Mode to WDS or AP+WDS in basic setting, then enable WDS function and set another AP MAC which you want to communicate with. The WDS supports PSK security mode. Of course in order to make APs work, you have to keep them the same channel and security mode.



WDS Settings

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

☑ Enable WDS

MAC Address:

Data Rate: Auto

Comment

Current WDS AP List:

MAC Address: Tx Rate (Mbps)

Delete Selected
Delete All
Reset
WDS Security Setup - Windows Internet Explorer
http://192.168.10.254/wlwdsenp.htm

WDS Security Setup

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

Encryption: WPA2 (AES)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Enable WDS: Check this box to enable WDS function.

MAC Address: Enter the remote AP MAC address.

Comment: You can add some comment for this item.

Set Security: Set WDS security.

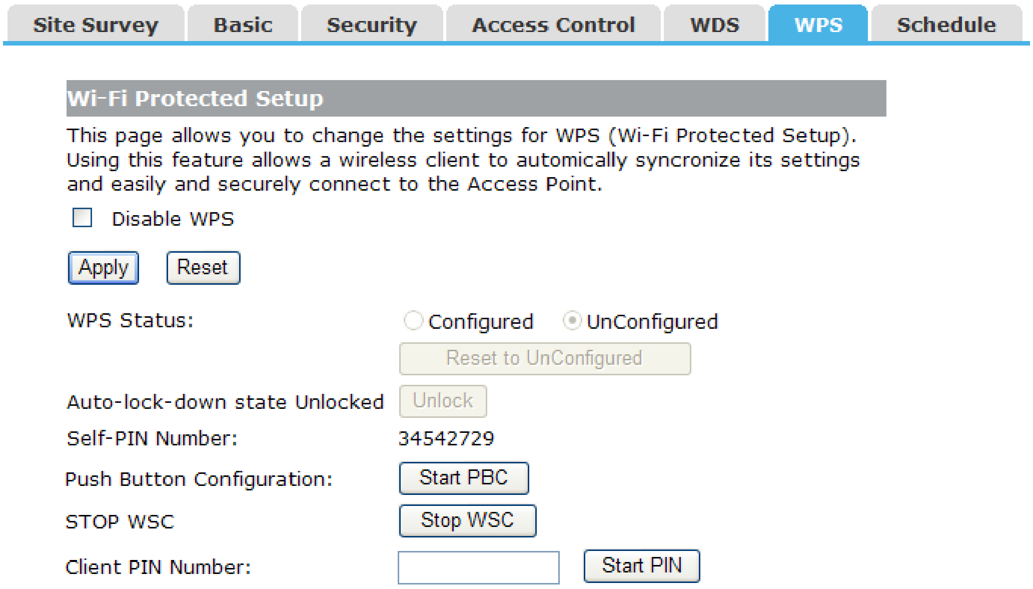
Encryption: You may select None or WPA2 (AES).

Pre-Shared Key Format: You can select Passphrase or HEX(64 Characters).

Pre-Shared Key: Pre-shared key(PSK) is a method to set encryption keys. Commonly used in Wi-Fi Protected Access.

4.4.6 WPS

WPS is designed to ease set up of security Wi-Fi networks and subsequently network management. This AP supports WPS features for AP mode, AP+WDS mode, and Infrastructure-Client mode.



Wi-Fi Protected Setup

This page allows you to change the settings for WPS (Wi-Fi Protected Setup). Using this feature allows a wireless client to automically syncronize its settings and easily and securely connect to the Access Point.

☐ Disable WPS

WPS Status: ○ Configured ● UnConfigured

Auto-lock-down state Unlocked

Self-PIN Number: 34542729

Push Button Configuration:

STOP WSC

Client PIN Number:

Disable WPS: Check this box and clicking “Apply” will disable WPS function. WPS is turned on by default.

WPS Status: When AP’s settings are factory default, it is set to open security and un-configured state, some registers such as Vista WCN can configure AP. Otherwise If it already shows “Configured”, it means that the AP has setup its security.

Self-PIN Number: It is AP’s PIN.

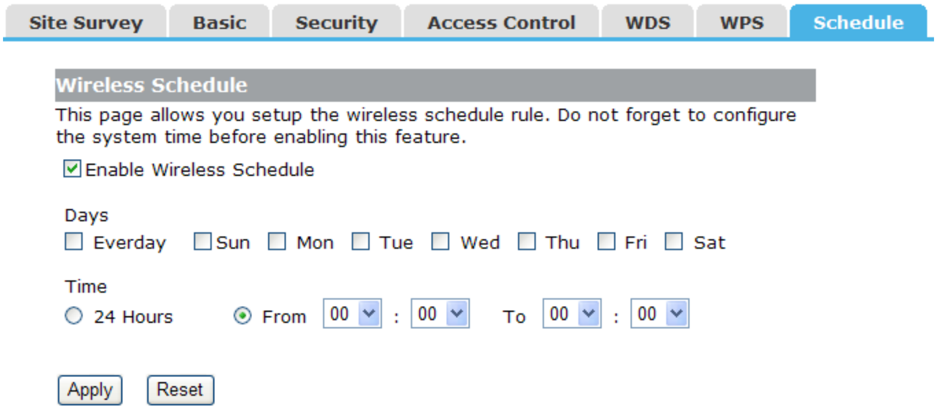
Start PBC: Clicking this button will invoke the Pus Button Configuration of WPS. If one station wants to connect to the AP, it must click its PBC button in two minute.

Note: This AP also has a hardware button, it is same button with reset. When click this button less than two seconds, the AP will run PBC function, during this time, the station can connect to the AP by its software or hardware WPS button. By the way, click this button exceed 5 seconds, the AP will restore factory default.

Client PIN Number: The length of PIN is limited to four or eight numeric digits. If the AP and Station input the same PIN and click “Start PIN” button in two minutes, they will establish connection and setup their security key.

4.4.7 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. Do not forget to configure the system time before enabling this feature.

☑ Enable Wireless Schedule

Days

☐ Everday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time

○ 24 Hours ● From 00 : 00 To 00 : 00

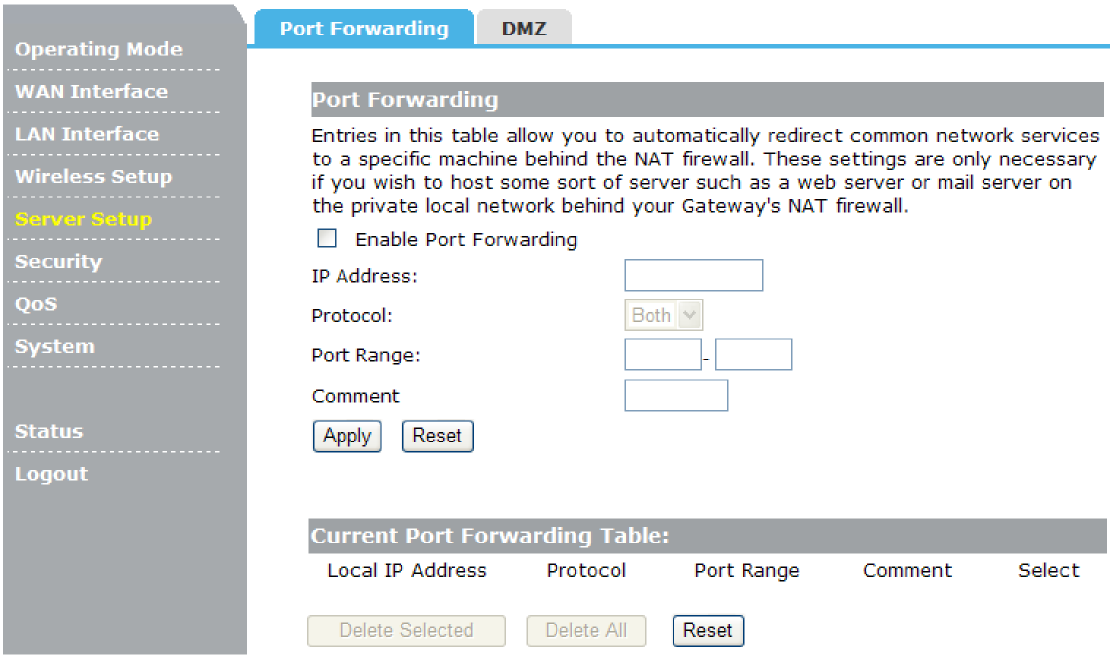
Enable Wireless Schedule: Check this box will enable Wireless Schedule function.

4.5 Server Setup

There are two submenus under the Server Setup menu: **Port Forwarding, DMZ**. Click any of them, and you will be able to configure the corresponding function.

4.5.1 Port Forwarding

If you configure the AP as Virtual Server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP port number), the AP redirects the external service request to the appropriate server.



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 such as 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

Apply Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Delete Selected Delete All Reset

Enable Port Forwarding: Check this box will enable Port Forwarding function.

IP Address: That external User accesses the AP will redirect to this local IP.

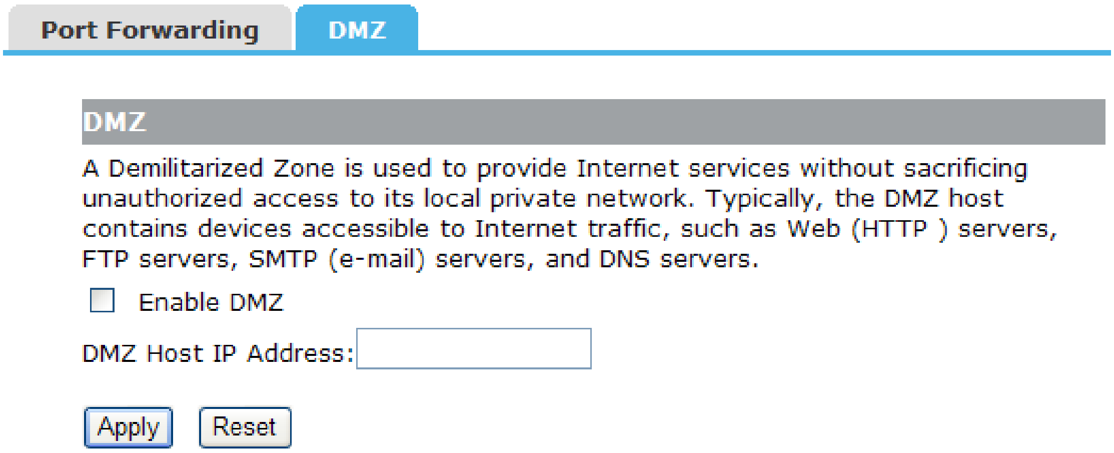
Protocol & Port Range: The packet with this protocol and port will be redirected to the local IP.

Comment: You can add some comment for this item.

Current Port Forwarding Table: The table shows all you have configured. You can delete one or all.

4.5.2 DMZ

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router.



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 this box will enable DMZ function.

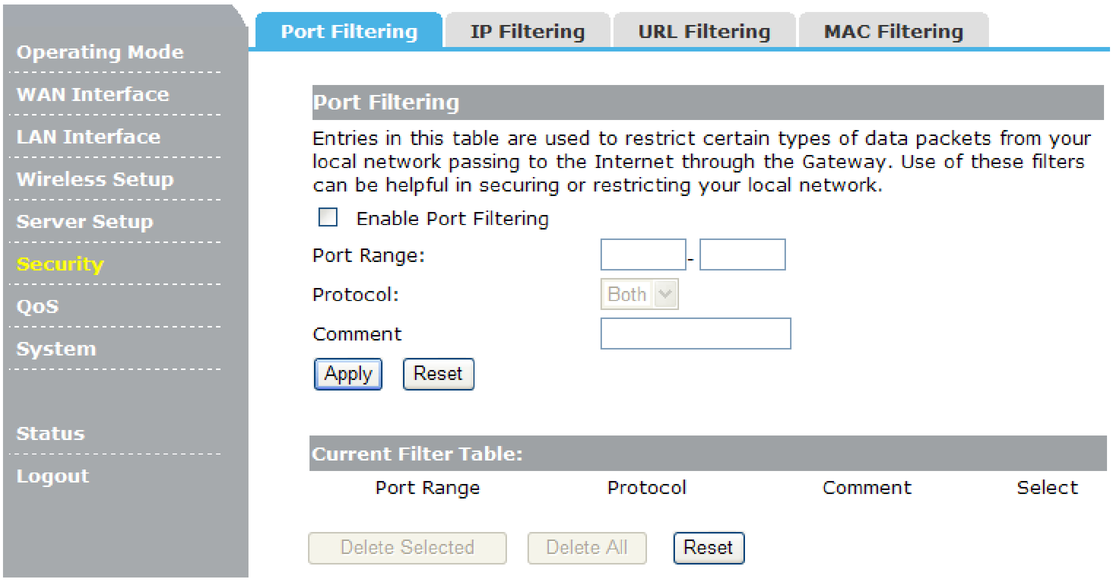
DMZ Host IP Address: To expose one PC to the Internet, select Enable DMZ and enter the computer's IP address in the DMZ Host IP Address field.

4.6 Security

There are four submenus under the Security menu: **Port Filtering, IP Filtering, URL Filtering, MAC Filtering**. Click any of them, and you will be able to configure the corresponding function.

4.6.1 Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network passing to the Internet through the Gateway. Use of these 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 passing to the Internet through the Gateway. Use of these 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 this box will enable Port Filtering function.

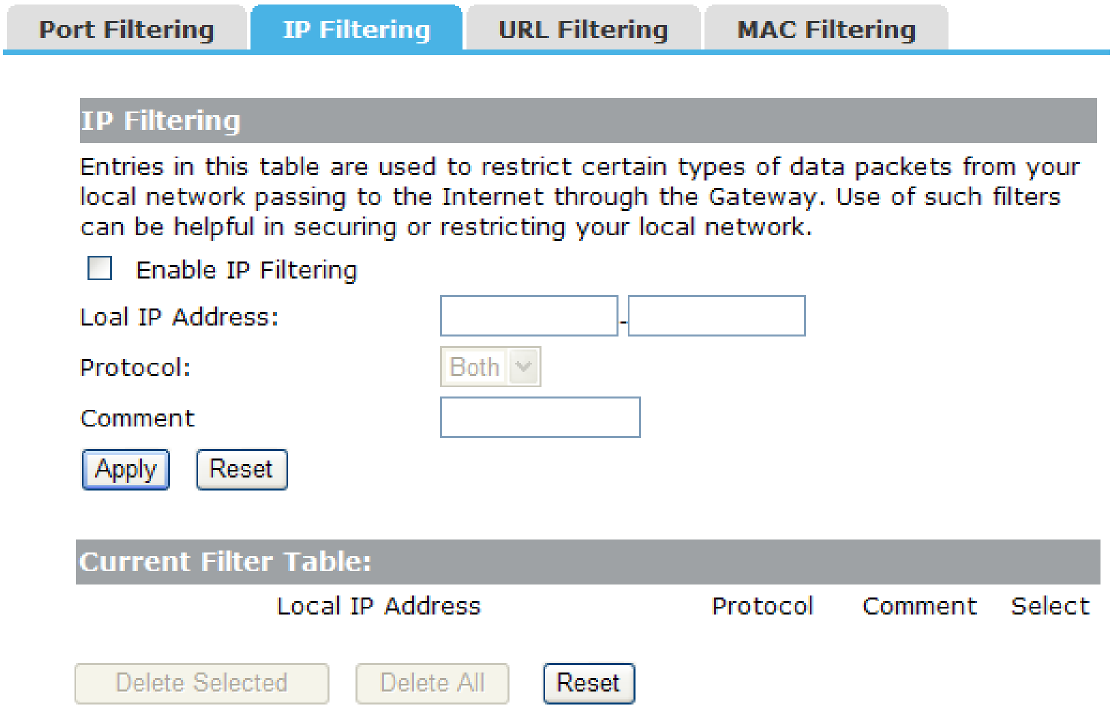
Port Range: The port range that you want to filter.

Protocol: The protocol that you want to filter, either TCP, UDP, or Both.

Comment: You can add some comment for this item.

4.6.2 IP Filtering

The IP Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses.



IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network passing to the 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 ______

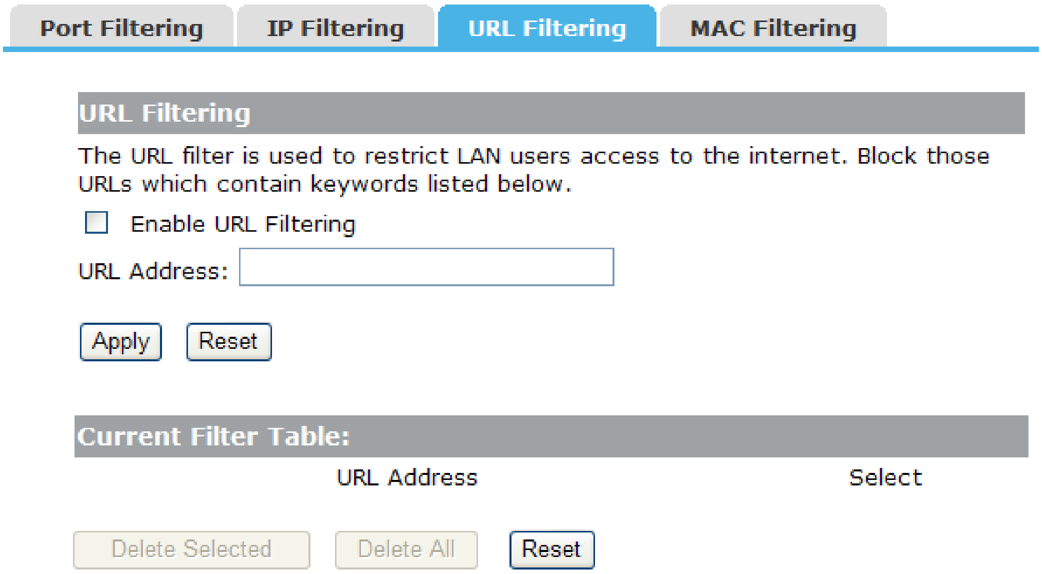
Current Filter Table:

Local IP Address	Protocol	Comment	Select

Enable IP Filtering: Check this box will enable IP Filtering function.
Local IP Address: The Local IP address range that you want to filter.
Protocol: The protocol that you want to filter, either TCP, UDP, or Both.
Comment: You can add some comment for this item.

4.6.3 URL Filtering

The URL filter is used to restrict LAN users access to the internet.



URL Filtering

The URL filter is used to restrict LAN users access to the internet. Block those URLs which contain keywords listed below.

□ Enable URL Filtering

URL Address: ______

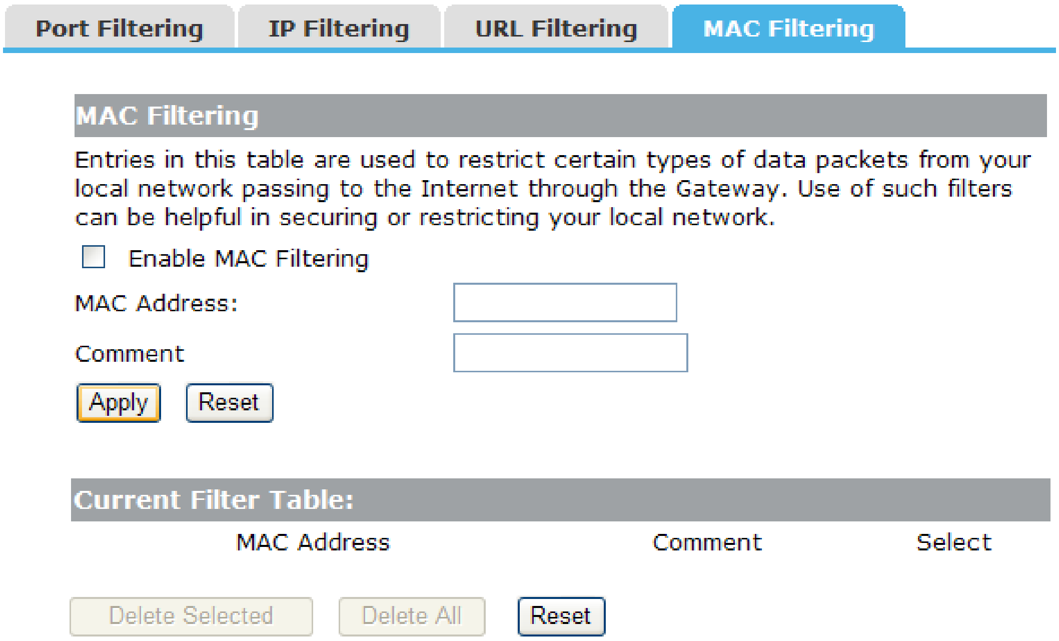
Current Filter Table:

URL Address	Select

Enable URL Filtering: Check this box will enable URL Filtering function.
URL Address: The URL Address that you want to filter.

4.6.4 MAC Filtering

The MAC Filtering feature allows you to control access to the Internet by users on your local network based on their MAC address.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network passing to the 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

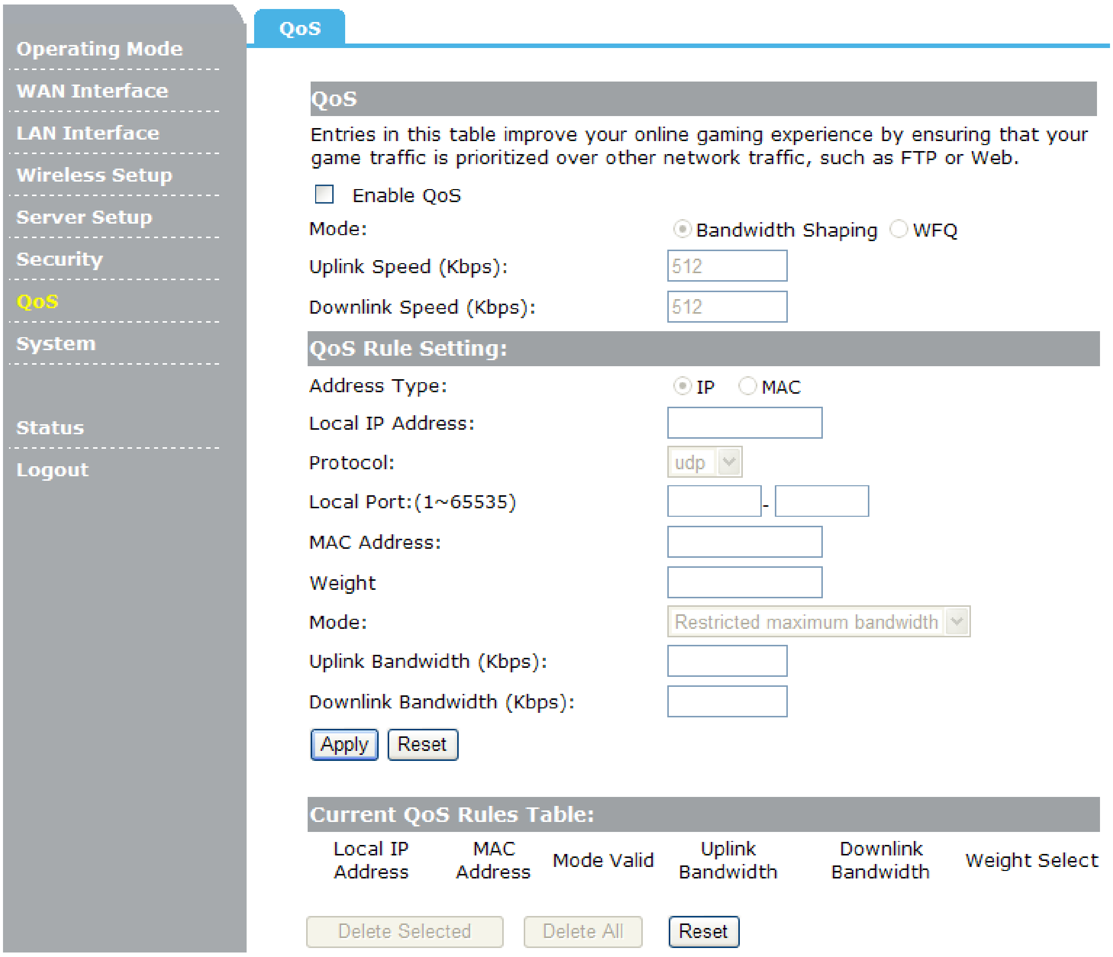
Enable MAC Filtering: Check this box will enable MAC Filtering function.
MAC Address: The MAC address that you want to filter.
Comment: You can add some comment for this item.

4.7 QoS Setup

The QoS helps improve your network gaming performance by prioritizing applications. By default the bandwidth control are disabled and application priority is not classified automatically.

In order to complete this settings, please follow the steps below.

1. Enable this function.
2. Enter the total speed or choose automatic mode.
3. Enter the IP address or MAC address user want to control.
4. Specify how to control this PC with this IP address or MAC address, priority and its up/down speed.
5. Click Apply button to add this item to control table.



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

Mode: ● Bandwidth Shaping ○ WFQ

Uplink Speed (Kbps): 512

Downlink Speed (Kbps): 512

QoS Rule Setting:

Address Type: ● IP ○ MAC

Local IP Address:

Protocol: udp

Local Port:(1~65535) -

MAC Address:

Weight

Mode: Restricted maximum bandwidth

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Current QoS Rules Table:

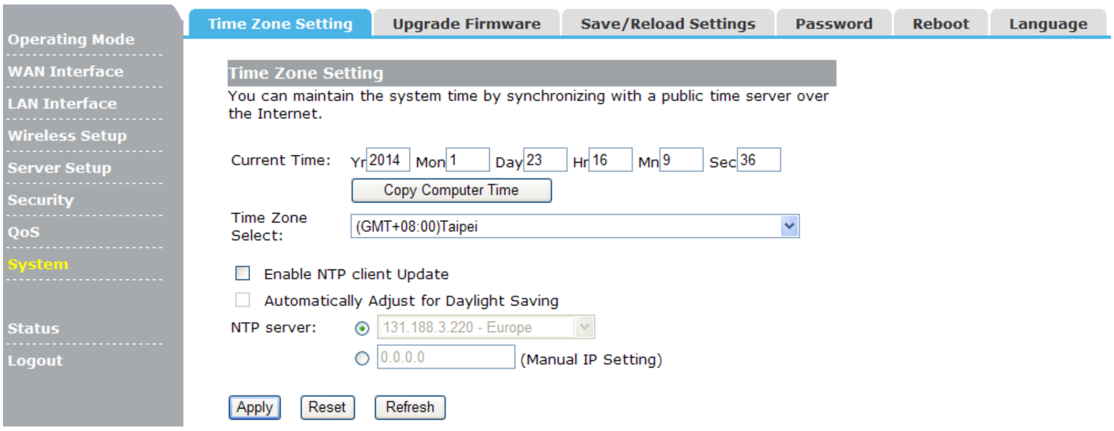
Local IP Address	MAC Address	Mode Valid	Uplink Bandwidth	Downlink Bandwidth	Weight Select

4.8 System

There are six submenus under the System menu: **Time Zone Setting, Upgrade Firmware, Save/Reload Settings, Password, Reboot, Language**. Click any of them, and you will be able to configure the corresponding function.

4.8.1 Time Zone

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 2014 Mon 1 Day 23 Hr 16 Mn 9 Sec 36

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

□ Enable NTP client Update

□ Automatically Adjust for Daylight Saving

NTP server: ● 131.188.3.220 - Europe

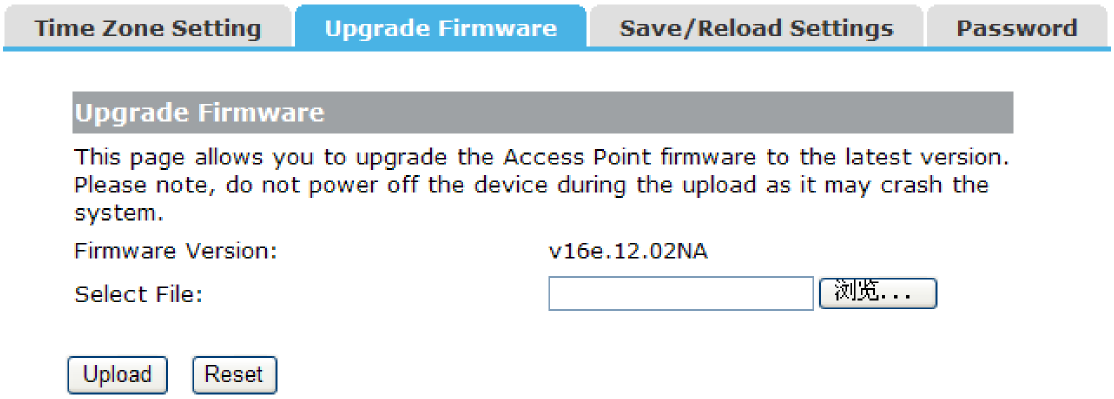
○ 0.0.0.0 (Manual IP Setting)

Time Zone select: Select your local time zone from this pull down list.

NTP Server: Select the NTP Server, then the AP will get the time form the NTP Server preferentially.

4.8.2 Upgrade Firmware

You can upgrade latest Firmware in this page.



Upgrade Firmware

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

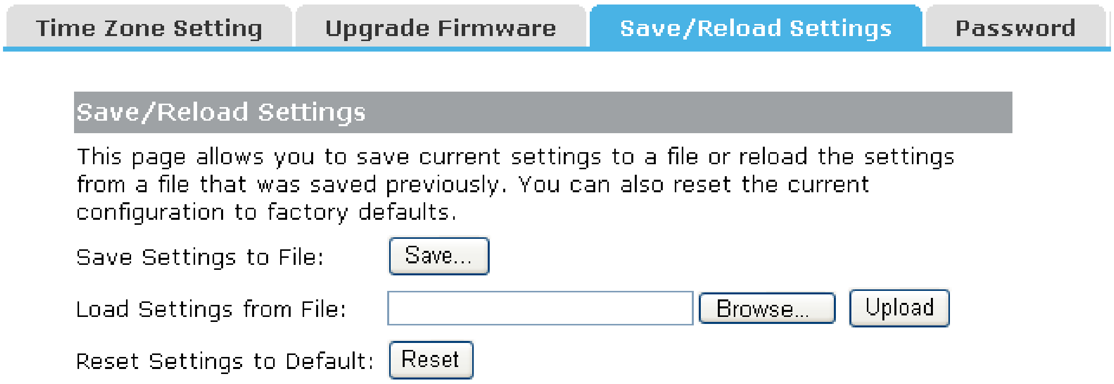
Firmware Version: v16e.12.02NA

Select File:

Firmware Version: This displays the current firmware version.

4.8.3 Save/Reload Settings

You can backup or restore the system configuration in this page.



Save/Reload Settings

This page allows you to save current settings to a file or reload the settings from a file that was saved previously. You can also reset the current configuration to factory defaults.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Save Settings to File: Get the AP's settings and store it in your local computer.

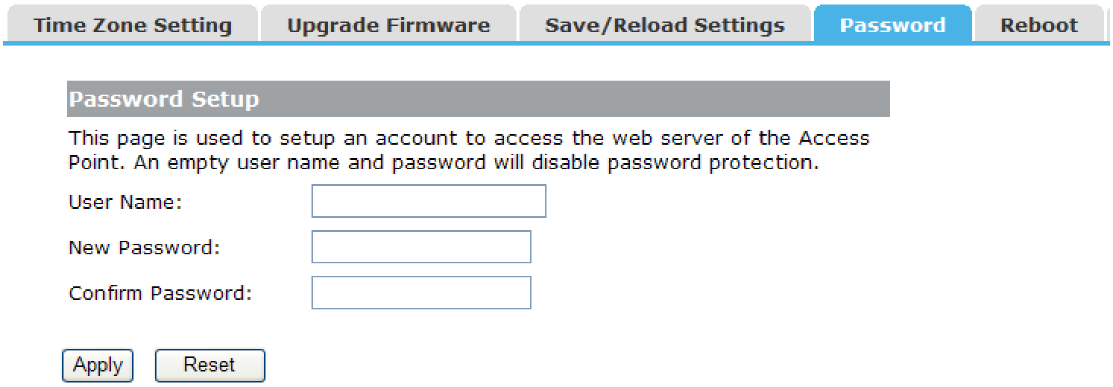
Load Settings from File: Restore the settings from the file you backup before from your local computer, the AP will go to the former settings.

Reset Settings to Default: Restore the system settings to factory default.

4.8.4 Password

To ensure the AP's security, you will be asked for your password when you access the AP's Web-based Utility. The default user name and password is **"admin"**.

This page will allow you to add or modify the User name and password.



Password Setup

This page is used to setup an account to access the web server of the Access Point. An empty user name and password will disable password protection.

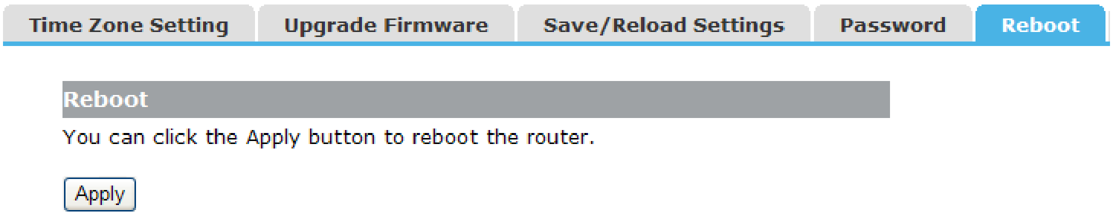
User Name:

New Password:

Confirm Password:

4.8.5 Reboot

You can reboot device via clicking the Apply button.

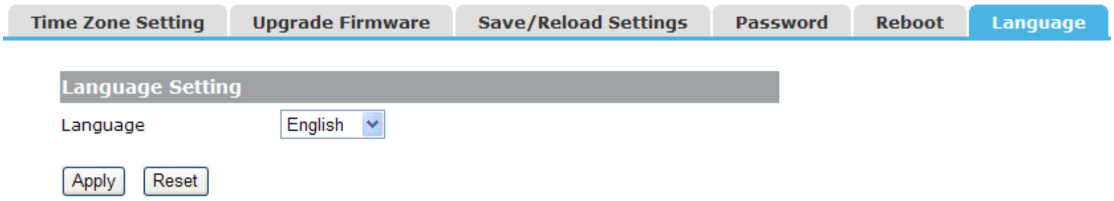


Reboot

You can click the Apply button to reboot the router.

4.8.6 Language

You can select correspondent language.



Language Setting

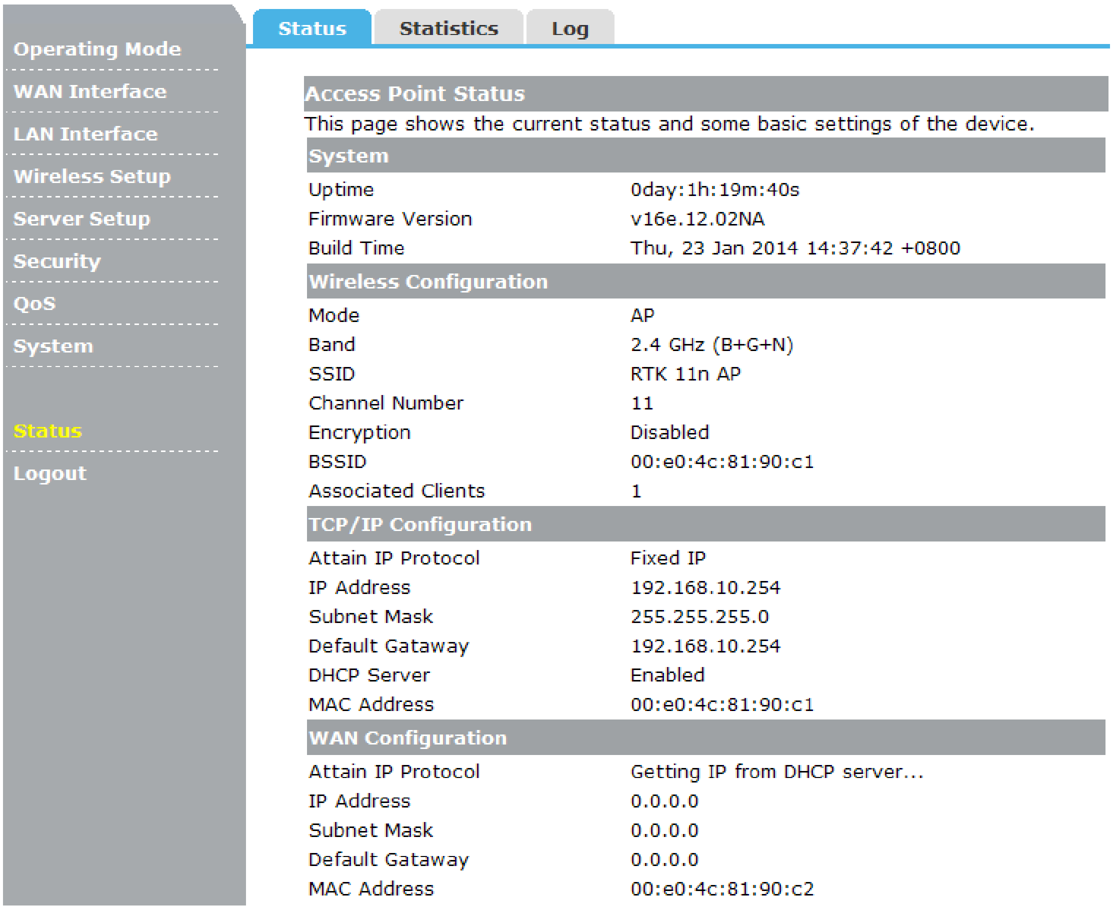
Language English

4.9 Status

There are three submenus under the Status menu: **Status, Statistics, Log**. Click anyone, you will see the following status.

4.9.1 Status

The Status page provides the current status information about the AP.



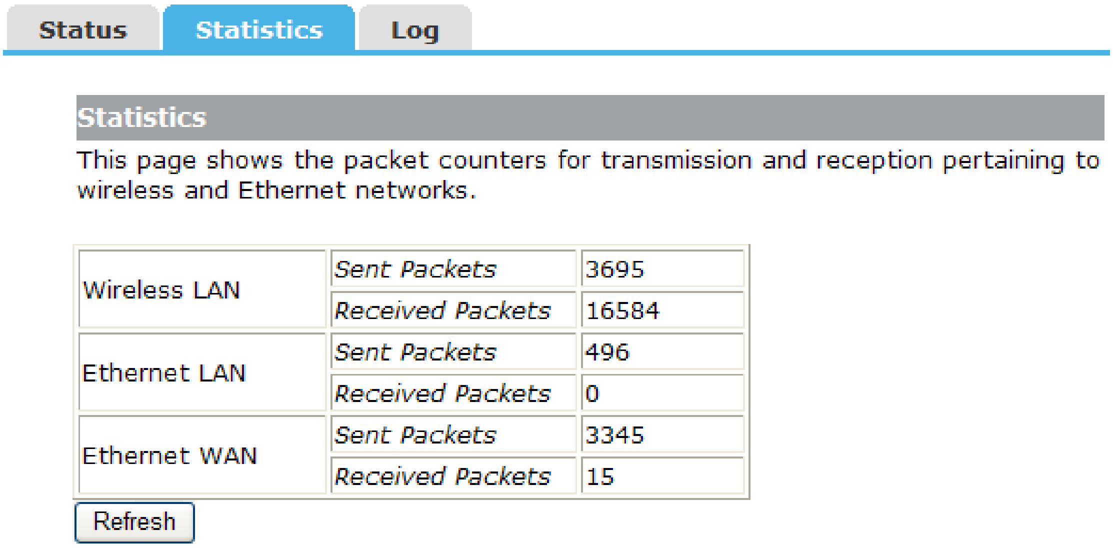
Access Point Status

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

System	
Uptime	0day:1h:19m:40s
Firmware Version	v16e.12.02NA
Build Time	Thu, 23 Jan 2014 14:37:42 +0800
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	RTK 11n AP
Channel Number	11
Encryption	Disabled
BSSID	00:e0:4c:81:90:c1
Associated Clients	1
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.10.254
Subnet Mask	255.255.255.0
Default Gataway	192.168.10.254
DHCP Server	Enabled
MAC Address	00:e0:4c:81:90:c1
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gataway	0.0.0.0
MAC Address	00:e0:4c:81:90:c2

4.9.2 Statistics

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



Statistics

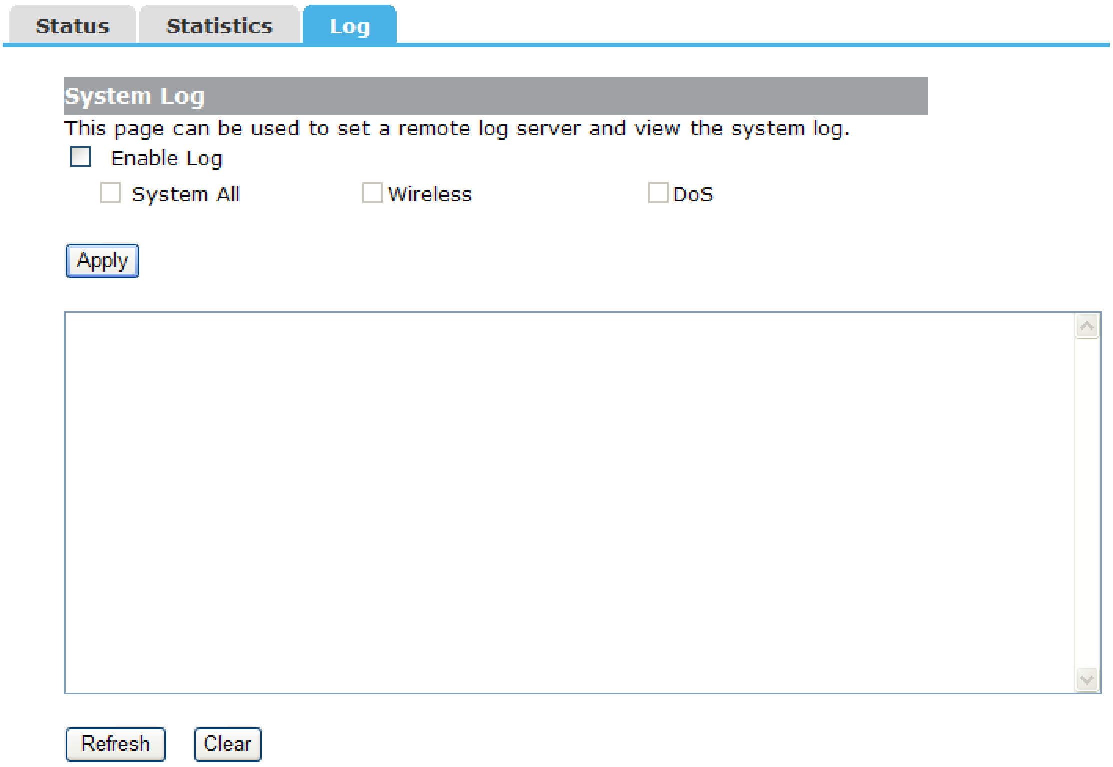
This page shows the packet counters for transmission and reception pertaining to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	3695
	Received Packets	16584
Ethernet LAN	*Sent Packets*	496
	Received Packets	0
Ethernet WAN	*Sent Packets*	3345
	Received Packets	15

Refresh: Click this button to refresh the data.

4.9.3 System Log

The page shows the system log. Click the “Refresh” to update the log. Click “Clear” to clear all shown information.



System Log

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

□ Enable Log

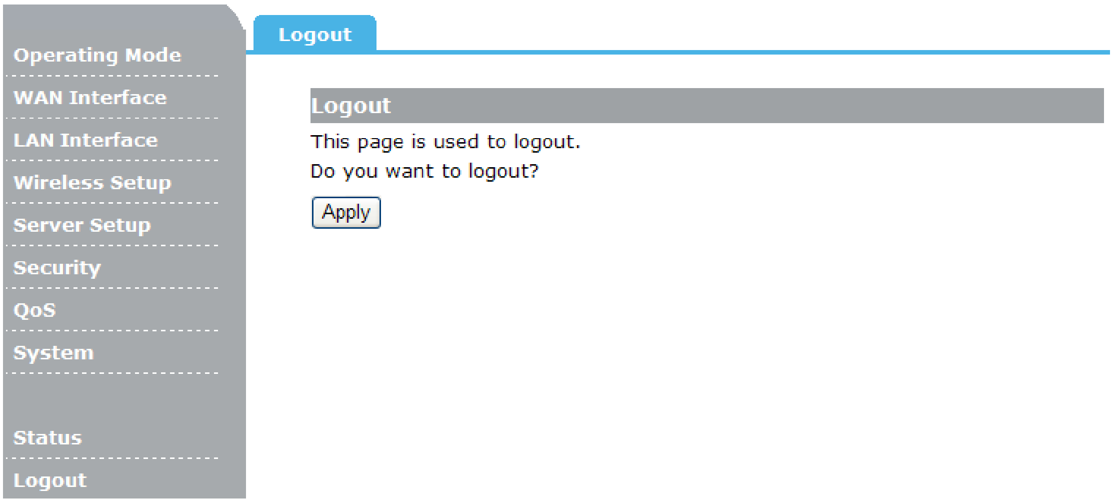
□ System All □ Wireless □ DoS

Refresh: Click this button to update the log.

Clear: Click this button to clear the current shown log.

4.10 Logout

This page is used to logout.



Logout

This page is used to logout.

Do you want to logout?

FCC RF EXPOSURE INFORMATION:

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.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

RF Exposure: A distance of 20 cm shall be maintained between the antenna and users, and the transmitter module may not be co-located with any other transmitter or antenna.

EU regulatory conformance

The equipment named above is confirmed to comply with the requirements setout in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (2004/108/EC), Low-voltage Directive (2006/95/EC) and R&TTE (1999/5/EC). The equipment passed the test which was performed according to the following European standards:

•ETSI EN 301 489-1 V1.9.2 (2011-09)
•ETSI EN 301 489-17 V2.2.1 (2012-09)
•ETSI EN 300 328 V1.8.1 (2012-06)
•EN 62311: 2008
•EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013