User's Guide

Model NO. CP300

Table of Contents

1. Product Introduction

Thank you very much for purchasing **TOTOLINK CP300 WLAN Broadband CPE**. This section will introduce the function and features of this device.

1.1 Overview

CP300 is WISP CPE Solution that specially designed for long distance wireless transmission. With two internal high gain antennas and advanced radio architecture, it can make the radio signal transmission coverage more extensive with a stable wireless connection and deliver up to 300Mbps data rate. Supported passive PoE makes the deployment more flexible. The outdoor protection design not only can prevent dust, water and lightning, but also adjust poor working environment. So no matter where you place it, in high or low temperature condition, it will work very well as normal.

1.2 Features

- Complies with IEEE802.11n and IEEE802.11g/b standards on 2.4G band.
- RF power up to 500mw.
- Adjustable transmission power.
- Two 11dBi internal antennas.
- Water-proof housing (IP65).
- 4 LED signal strength indications.
- Supports MAC based ACL and MAC filtering.
- Built-in DHCP server/client.
- Supports 64/128 bit WEP encryption and WPA-PSK, WPA2-PSK security.
- Repeater function allows more terminals to access Internet.
- Supports passive PoE power supply.
- Lightning protection design.
- Supports QoS bandwidth control.

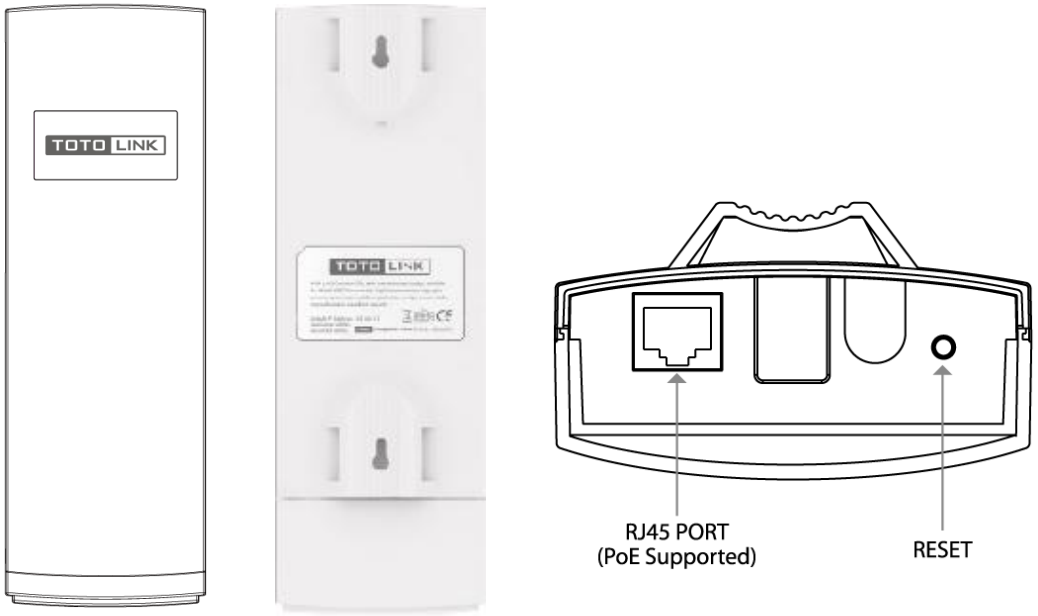
2. Hardware Installation

2.1 Typical Application

2.1.1 WISP

2.2 Appearance

2.2.1 Front and Rear Panel



Port and Button	Description
LAN	This port is used to connect with PoE injector by cable.
Reset	With the CPE powered on, press and hold the button for about 10 seconds, the CPE will reboot to factory default settings.

2.2.2 LED Description

LED Indicators	Description
POWER	The POWER LED will light blue when properly connected to a power source.
LAN	This Ethernet LED will light solid blue when an active Ethernet connection is made to the LAN port and flash when there is activity.
WLAN	This WLAN LED flash blue when the wireless function working.
Signal Strength	These LEDs display the signal strength.

2.3 Connecting the Device

- Connect the RJ45 port of PoE beside the power interface to computer using one cable.
- Connect the CP300 to the RJ45 port opposite the power interface on PoE using another cable.
- Connect the power supply with the PoE and plug it into an outlet.

Note: *if LED of PoE and CPE are lit, it means that you have connected them together successfully. If not, please check whether you have followed the instructions we gave above.*

You can check the following Figure 2.1 for reference:

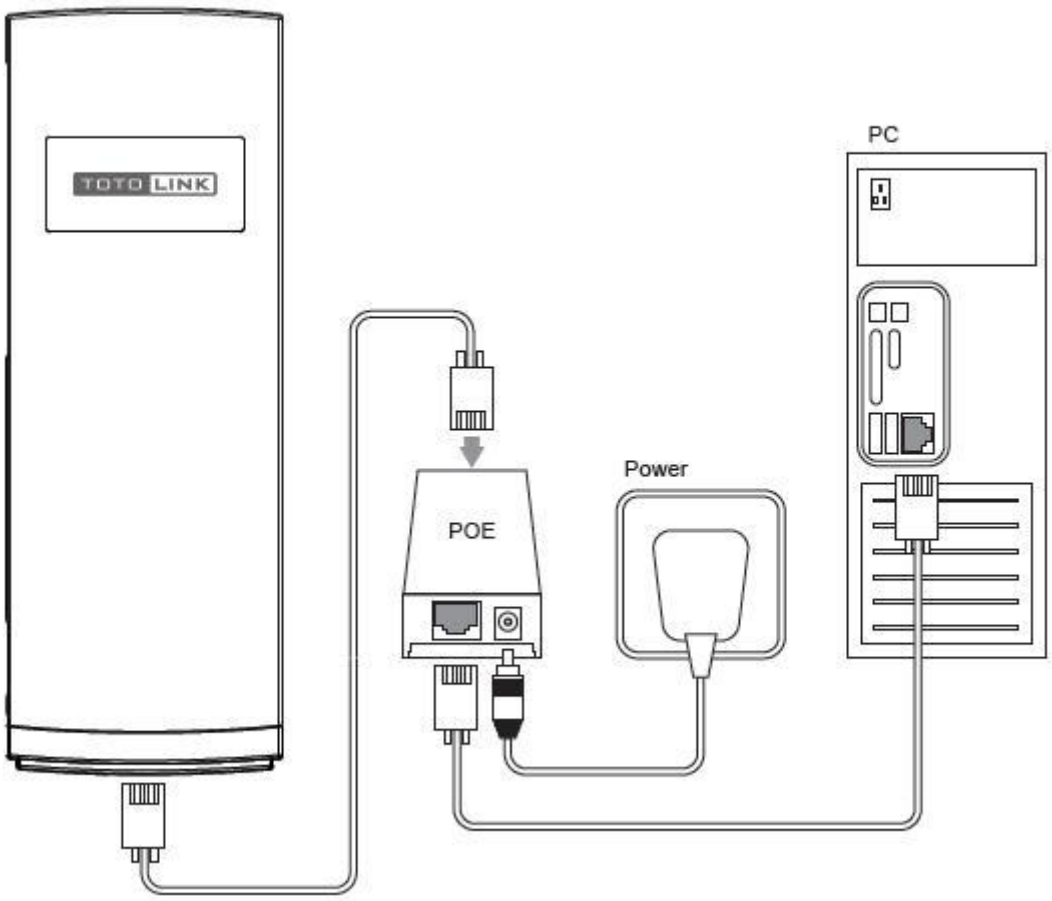


Figure 2.1 CPE Connection Graph

2.4 Set up the Computer

The default IP address of the CP300 WLAN Broadband CPE is 192.168.1.1, the default Subnet Mask is 255.255.255.0. Both of these parameters can be changed as you want. In this guide, we will use the default values for description. There are two ways to configure the IP address for your PC.

- **Configure the IP address manually**

Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" range from 2 to 254). The Subnet Mask is 255.255.255.0 and Gateway is 192.168.1.1 (CPE's default IP address).

- **Obtain an IP address automatically**

Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the PoE. Open a command prompt, and type in **ping 192.168.1.1**, then press **Enter.**

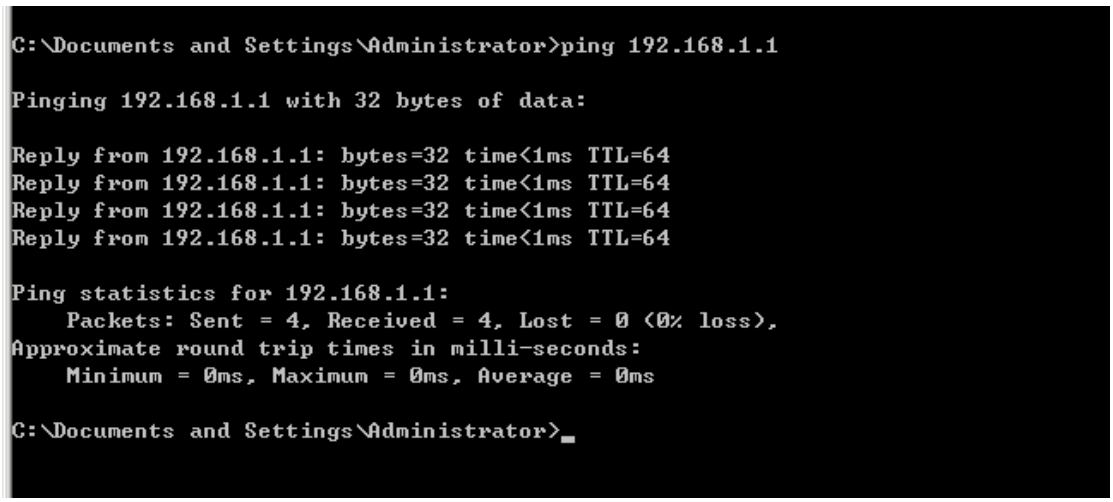


Figure 2.2 Success result of Ping command

If the result displayed is similar to that shown in Figure 2.2, it means that the connection between your PC and the PoE has been established.

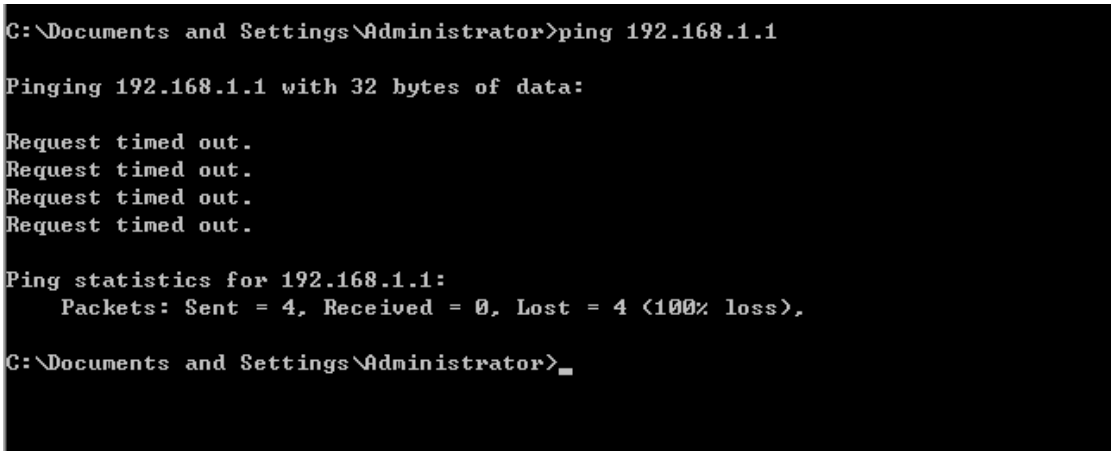


Figure 2.3 Failure result of Ping command

If the result displayed is similar to that shown in Figure 2.3, it means that your PC has not connected to the PoE successfully. Please check it following below steps:

1. Is the connection between your PC and the PoE correct?

If correct, the LED on the PoE, CPE and your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

Since the CPE's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

3. Configuration of Web Utility

After successful connection and setup, you can configure the Web interface of the WLAN bandwidth CPE now. This chapter describes how to configure some advanced settings for your Access Point through the web-based management page.

3.1 Login the Web Interface

Access the Web interface of the CPE by typing 192.168.1.1 in the address field of Web Browser. Then press **Enter** key.

Figure 3.1 IP address

Then it will require you to enter User Name and Password:

Figure 3.2 Login Windows

Enter **admin** for User Name and Password, both in lower case letters. Then click **Login** button or press **Enter** key.

> ***Note:*** *If the above screen does not prompt, it means that your web-browser has been set to using a proxy. Go to* ***Tools menu****>****Internet Options****>****Connections****>****LAN Settings****, in the screen that appears, cancel the* ***Using Proxy checkbox****, and click* ***OK*** *to finish it.*

Now you have logged into the web interface of the CPE. The first page you see is the MAIN page, see below:

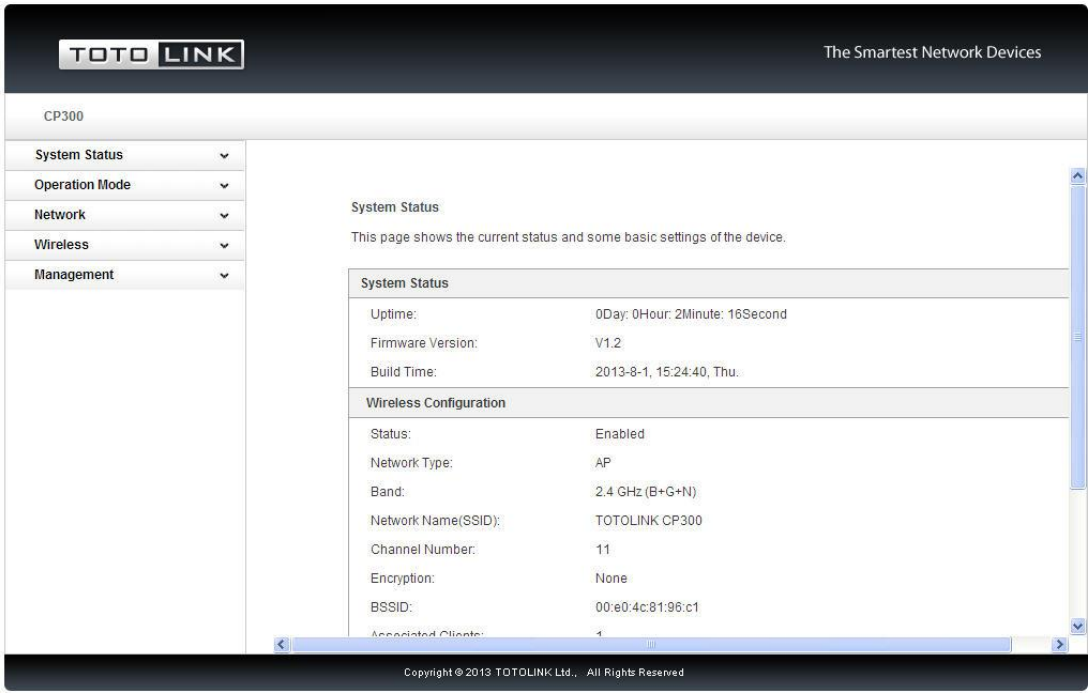


Figure 3.3 Login Interface

The setup interface will be different in different operation modes. By default, the operation mode is Bridge.

On the left, there is a navigation bar in Bridge mode. It contains the following items:

System Status: This page displays a summary of wireless status information, system status and LAN configuration.

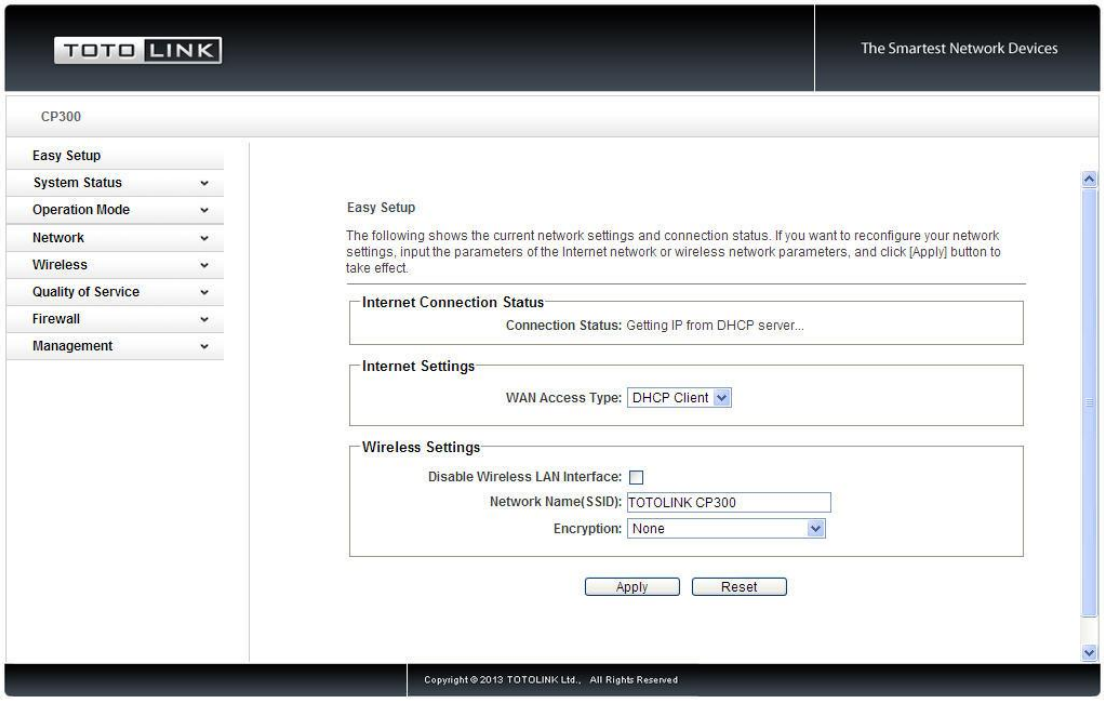
Network: You can configure the parameters for local area network which connects to the LAN port of your Access Point.

Wireless: This parameter contains the controls for a wireless network configuration.

Management: This page allows updating firmware, save/ reload settings, setup administrator. etc.

*In the Gateway mode, **Easy Setup**, **Quality of Service** and **Firewall** sections are added base on Bridge mode. What's more, **Dynamic DNS** is added in the Management part. Besides, Wireless ISP mode is almost the same as Gateway mode except of Easy Setup.*

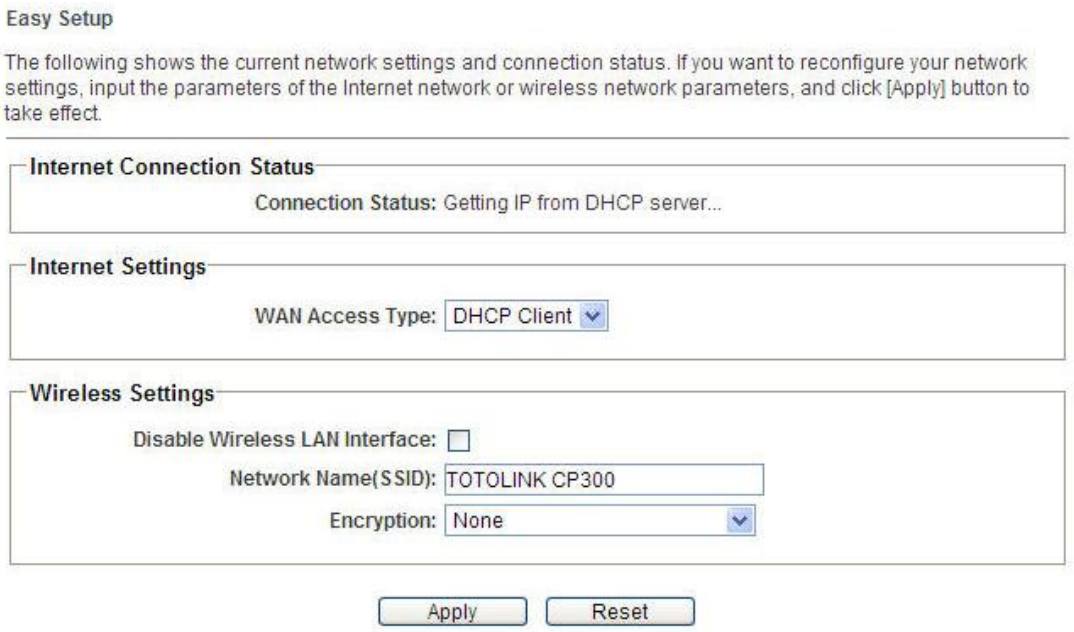
When you choose the Gateway mode, the main interface will change, see below:



3.2 Easy Setup

Note: Only in Gateway mode has easy setup part.

Easy Setup is provided as part of the web configuration utility. Users can simply finish the settings on this page to access Internet.



3.2.1 Internet Settings

This section is used to configure the parameters for Internet network which connects to the WAN port of your access point. You can choose the WAN connection type from the following three options. Otherwise, if the WAN connection type provided by your ISP is PPTP or L2TP, please go to **Network->WAN Setup** and configure the parameters refer to **3.5.3.4 PPTP**、 **3.5.3.5 L2TP**

3.2.1.1 DHCP Client

Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you choose this mode, you will get a dynamic IP address from your ISP automatically.

3.2.1.2 Static IP

If your ISP has provided a fixed IP that allows you to access Internet, please choose this option.

IP Address: the IP address provided by your ISP.

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it is provided by your ISP.

Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network. It is provided by your ISP.

DNS: Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. Here you can set the Primary and Secondary DNS addresses. This is provided by your ISP.

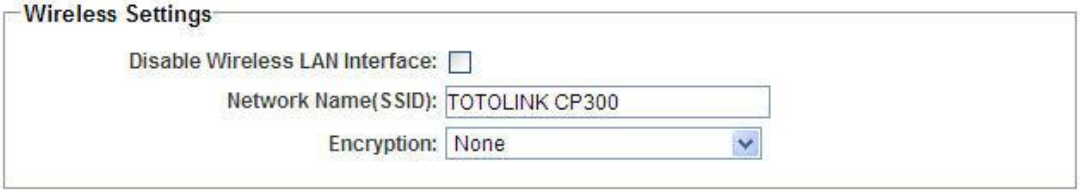
3.2.1.3 PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. It replied on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as wireless device or cable modem. All the users over the Ethernet can share a common connection. If you use ADSL virtual dial-up to connect Internet, please choose this option.

User Name: a specific valid ADSL user name provided by your ISP.
Password: the corresponding valid password provided by your ISP.
Confirm Password: please enter the password one more time for confirmation.

3.2.2 Wireless Settings

After the Internet Setting, you can also configure the Wireless parameters.



Disable Wireless LAN Interface: you can choose to disable the wireless function by checking this box.

Network Name (SSID): Service Set Identifier is used to identify your 802.11 wireless LAN. By default, it is TOTOLINK CP300.

Encryption: Here you can choose to set no encryption or select WEP, WPA-PSK, WPA2-PSK or WPA/WPA2-PSK**.** Here we recommend you choose WPA/WPA2-PSK, and you need to set the Key (encryption key) for this wireless LAN. See below:

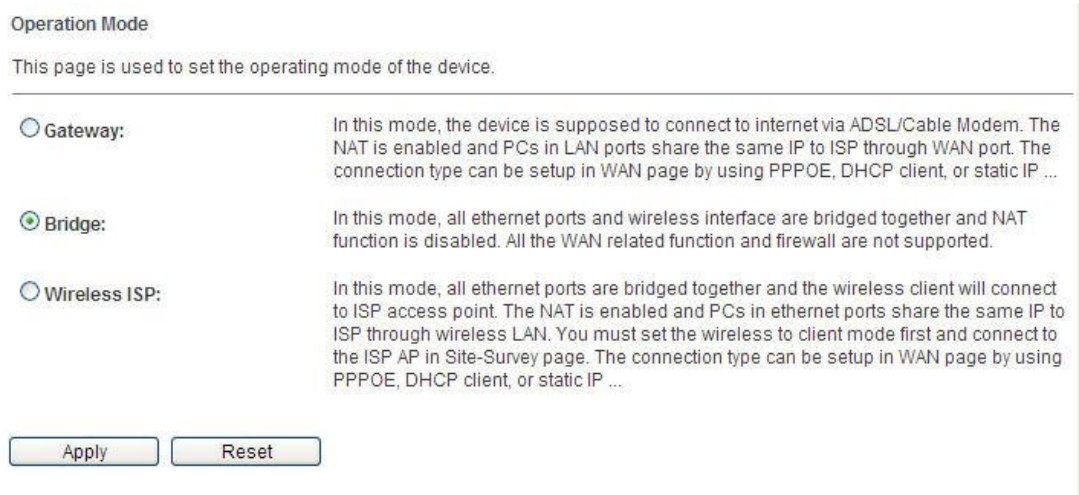
3.3 System Status

The System Status provides basic network settings of this router, including WAN (Bridge mode doesn't have this section), Wireless configuration and LAN. Also, you could get the current running firmware version or firmware related information from this presentation.

Wireless Configuration	
Status:	Enabled
Network Type:	AP
Band:	2.4 GHz (B+G+N)
Network Name(SSID):	TOTOLINK CP300
Channel Number:	9
Encryption:	None
BSSID:	00:e0:4c:81:96:c1
Associated Clients:	1
LAN Configuration	
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enabled
MAC Address:	00:e0:4c:81:96:c1

3.4 Operation Mode

This parameter specifies the operating network modes for the router. This router provides three modes: **Gateway**, **Bridge** and **Wireless ISP**. You could refer to the following description to choose the right one. Then click **Next**.



3.3.1 Gateway

Generally, this operating mode is selected by default as more and more users choose to access Internet by ADSL/Cable Modem. In this mode, the device works as a Software Router of the LAN, all clients will connect to Internet through this “agent”. If you choose this mode, PCs in four LAN ports share the same IP to ISP through WAN port. You can setup the connection type in WAN page by using PPPoE, DHCP client, PPTP client, L2TP client or Static IP.

3.3.2 Bridge

In Bridge mode the router forwards all the network management and data packets from

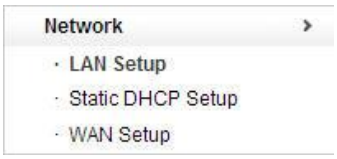
one network interface to the other without any intelligent routing. For simple applications this provides an efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belongs to the same network segment that has the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports.

3.3.3 Wireless ISP

It means Wireless Internet Service Provider. If you need to access Internet through Wi-Fi, you can choose this mode. For example, when you are in a hotel, airport or other public commercial place, you can select wireless ISP to connect to Internet. In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point.

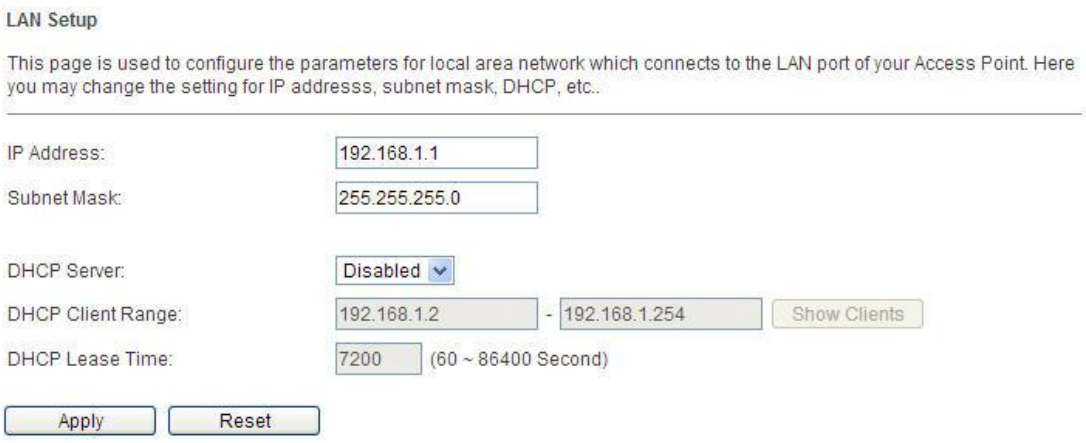
3.5 Network

Click the **Network** menu to show up all Network parameters you could set up. The picture on the left is the content in Bridge mode, while right one is in Gateway mode and Wireless ISP mode.



3.5.1 LAN Setup

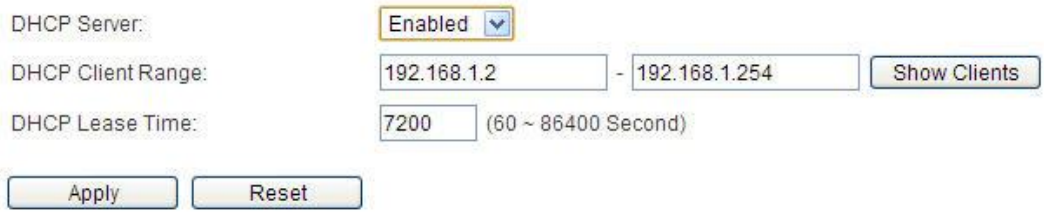
This page allows you to configure the LAN port and DHCP Server.



IP Address: this is the IP address to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

Subnet Mask: this is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

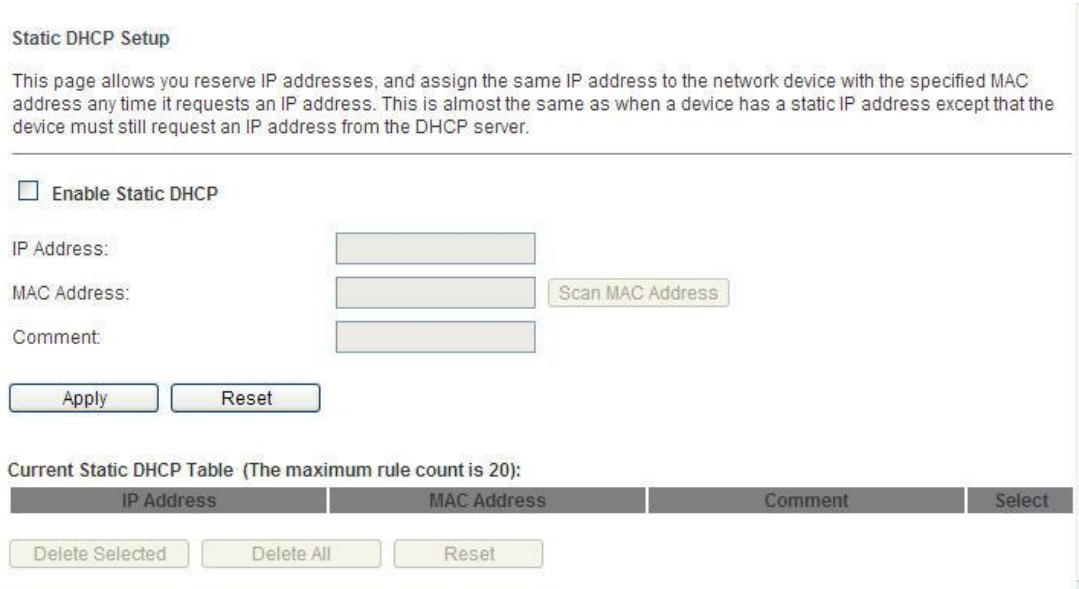
DHCP Server: if Enable this function, you need to define the range of assigned IP Address.



After you enabled the DHCP Server, Static DHCP Setup will appear in the subdirectory of the Network.

3.5.2 Static DHCP Setup

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.



Enable Static DHCP: you can choose to enable or disable this function.

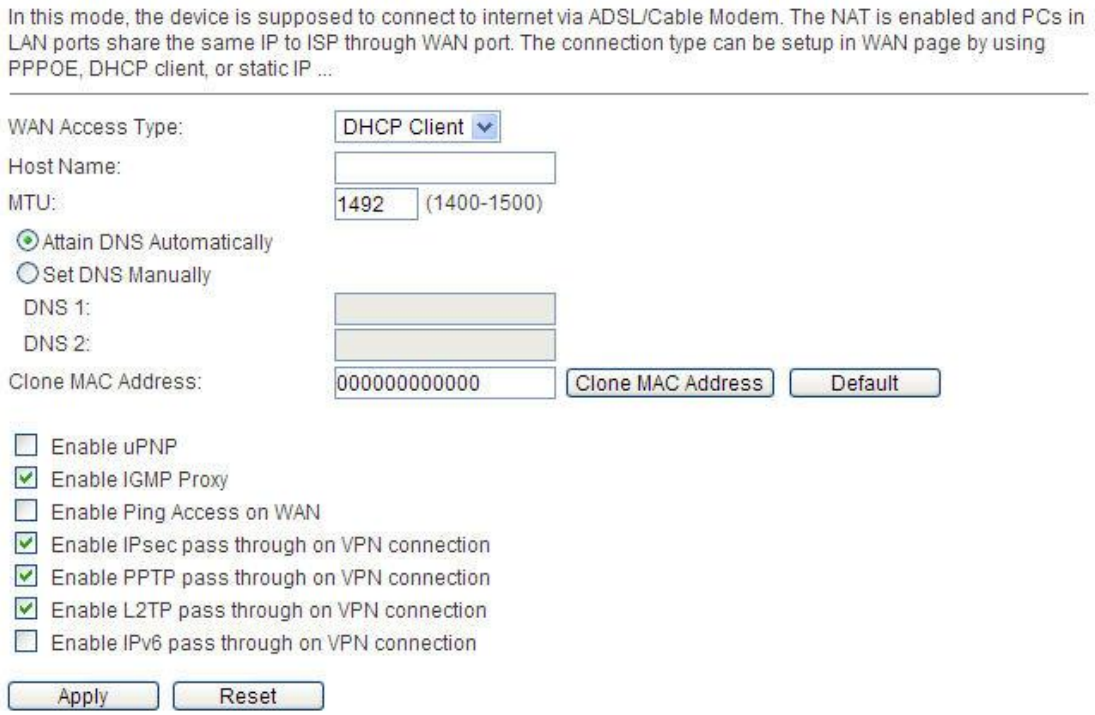
IP Address: shows the IP address of selected MAC address.

MAC Address: choose the MAC address that you want to bind.

Comment: enter the some description about this function.

3.5.3 WAN Setup

While you are in Gateway mode or Wireless ISP mode, the LAN port can be used as a WAN Port. You can setup access type and parameters in this section.



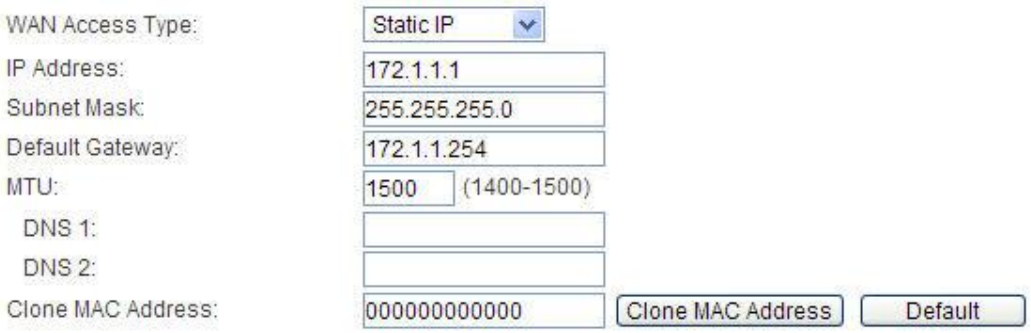
Enable UPnP: the UPnP (Universal Plug and play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows “Plug and Play” system. You can enable this function so that the router doesn’t need to work out which port need to be opened.

Enable IGMP Proxy: IGMP is the abbreviation of Internet Group Management Protocol. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. If you select this checkbox, the application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.

Enable Ping Access on WAN: enable users use Ping command to access WAN.

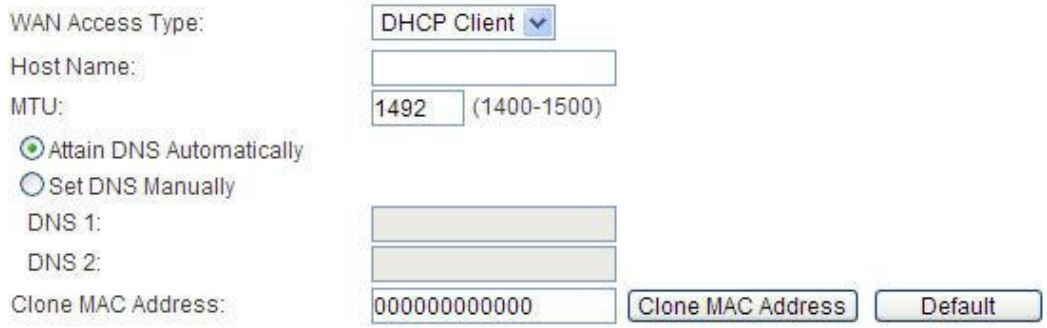
3.5.3.1 Static IP

If your ISP has provided a fixed IP that allows you to access Internet, please choose this option. These parameters we have introduced in Easy Setup, please refer to **3.3.1.2 Static IP**



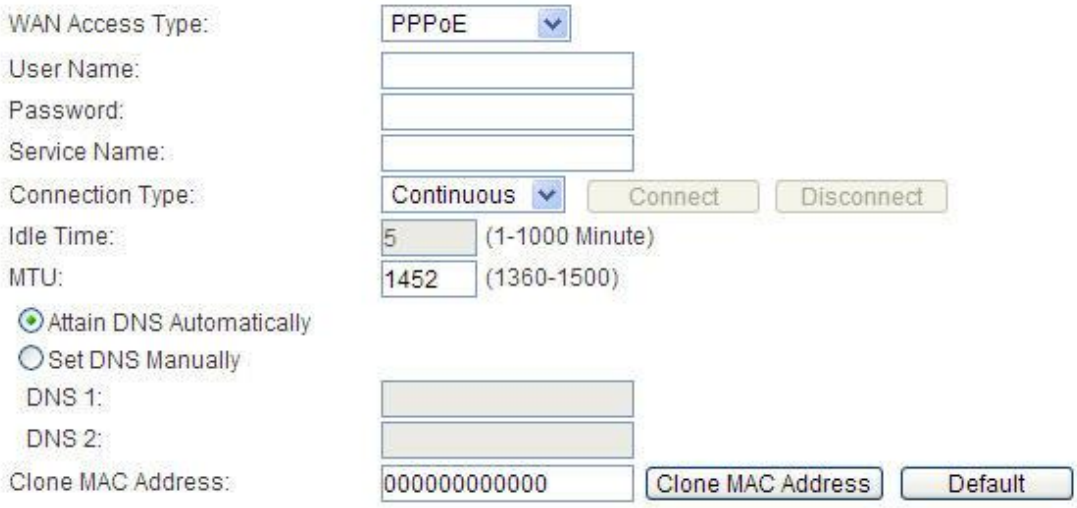
3.5.3.2 DHCP Client

Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you choose this mode, you will get a dynamic IP address from your ISP automatically.



3.5.3.3 PPPoE

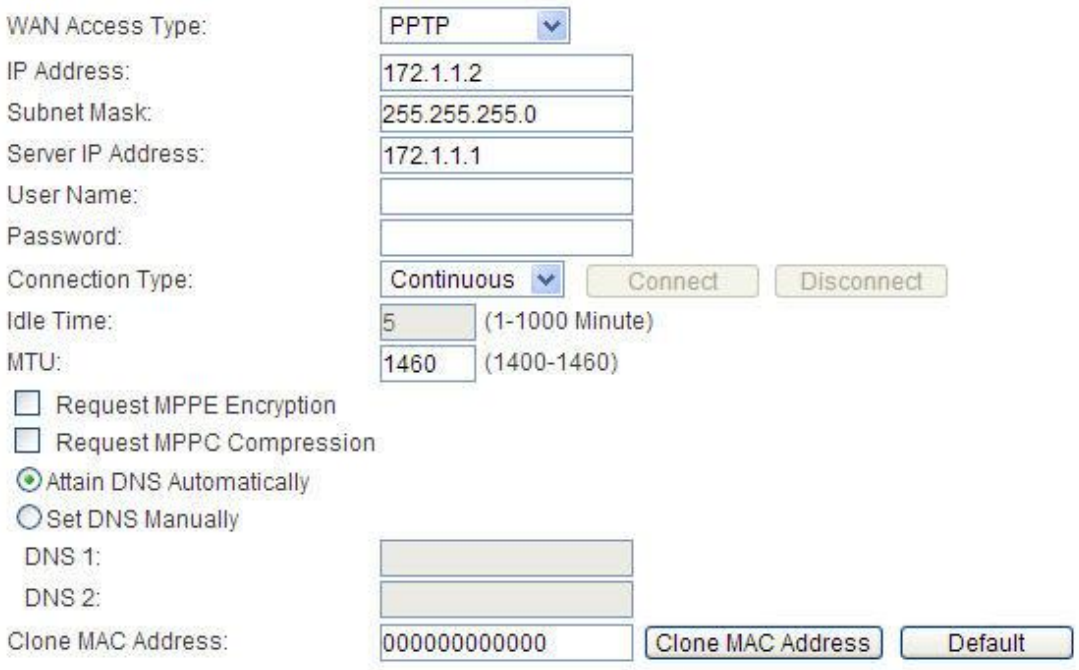
Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. It replied on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as wireless device or cable modem. All the users over the Ethernet can share a common connection. If you use ADSL virtual dial-up to connect Internet, please choose this option.



User Name: a specific valid ADSL user name provided by your ISP.
Password: the corresponding valid password provided by your ISP.
Confirm Password: please enter the password one more time for confirmation.

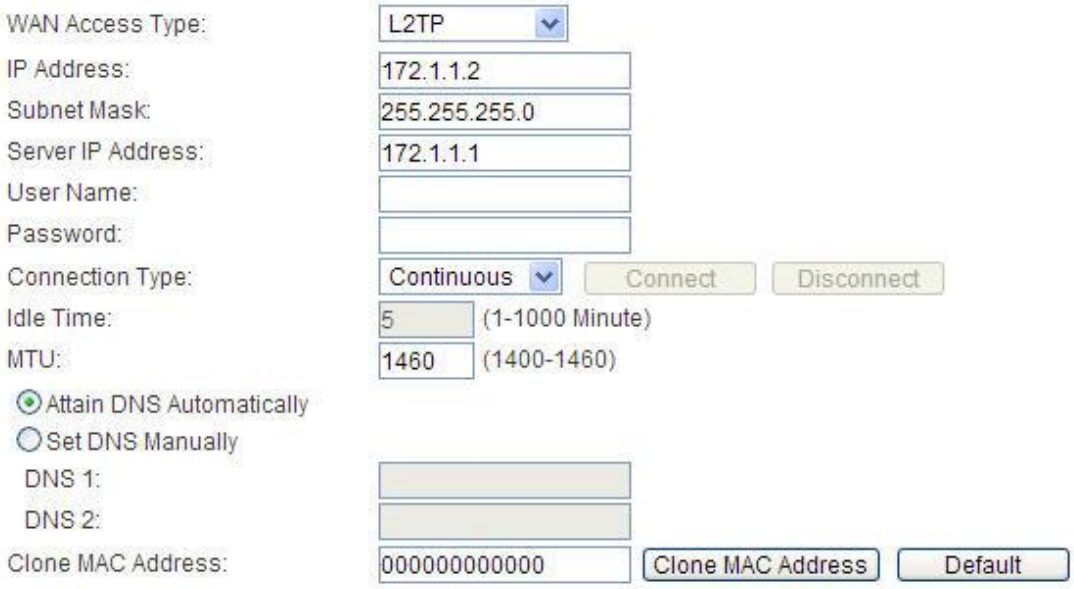
3.5.3.4 PPTP

PPTP means Point to Point Tunneling Protocol is a VPN connection that only applies in Europe. If you choose one of them, please type in all the information that your ISP provided for this protocol:



3.5.3.5 L2TP

L2TP means Layer 2 Tunneling Protocol is a VPN connection that only applies in Europe, Middle East and Africa (MEA) regions. If you choose one of them, please type in all the information that your ISP provided for this protocol:

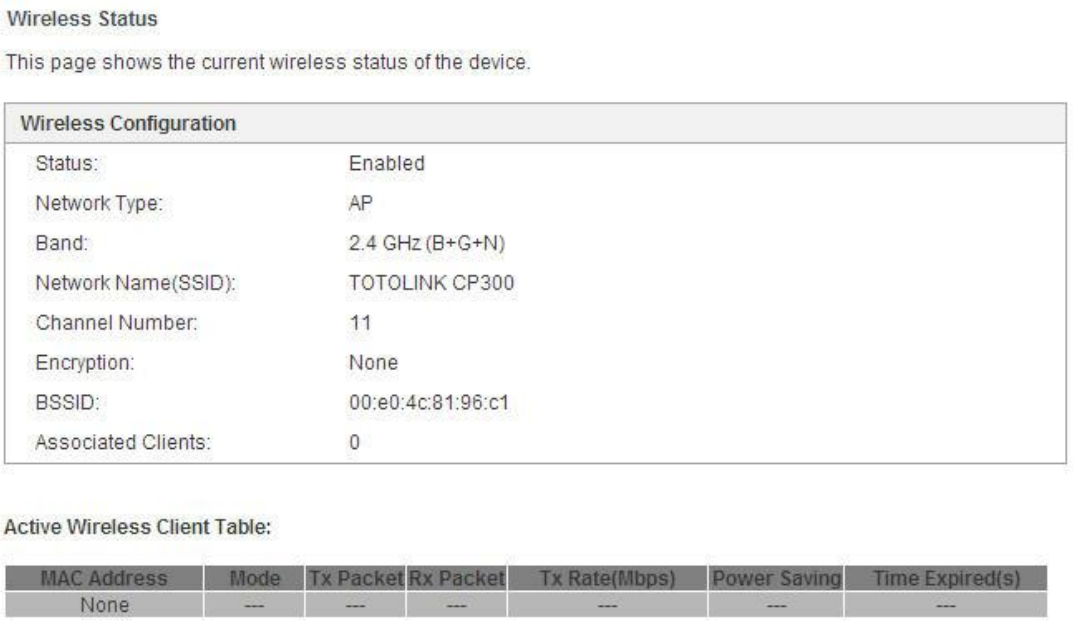


3.6 Wireless

The general wireless settings, such as 802.11 modes, SSID and data rates can be configured in this section. Also some more advanced settings can be setup here.

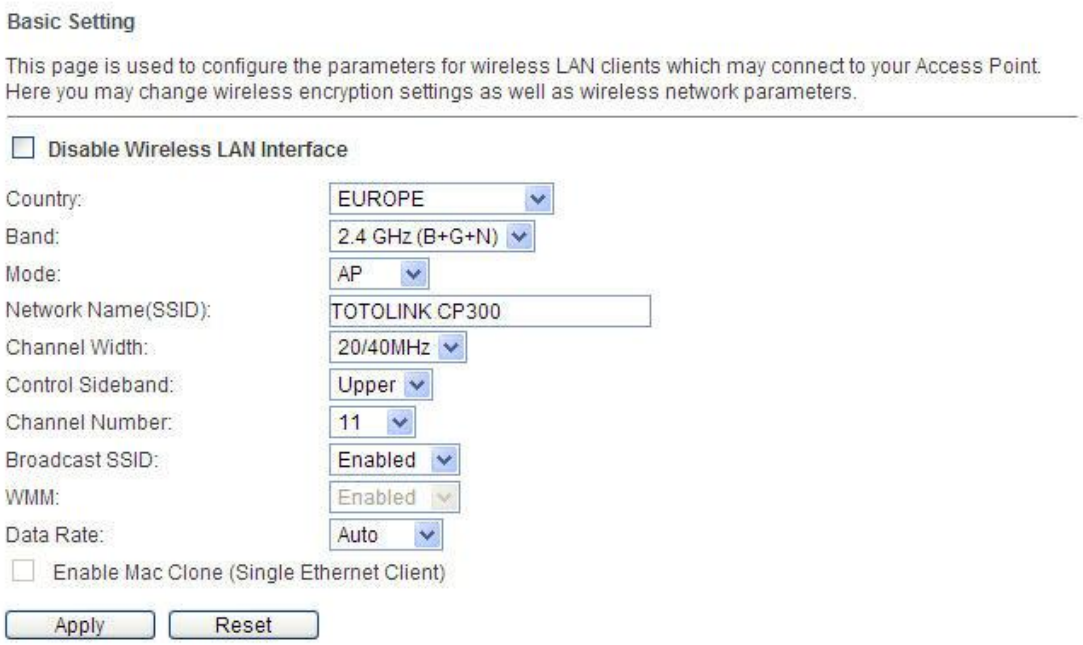
3.6.1 Wireless Status

This page displays the current Wireless Interface configuration of the router.



3.6.2 Basic Setting

On this page, you could configure the parameters for Wireless LAN clients that may connect to your Access Point.



Country: Different countries will have different power levels and possible frequency selections.

Band: In fact, this option allows you to choose the radio standard for operation of your Router. 802.11b and 802.11g are old 2.4GHz mode, while 802.11n (2.4GHz and/or 5GHz) is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM)

modulation. Here, you can choose the last one 2.4GHz (B+G+N), this mode offers better compatibility.

Mode: specifies the operating mode of the device. The mode depends on the network topology requirements. There are 3 operating modes supported in CP300 software.

1. **AP**: This mode allows users with laptop to surf Internet by wireless connection. It's designed to add wireless function for existed wired router which is just suitable for home and small offices.

2. **Client**: If you choose this mode, the Channel Number and Channel Width can't be edited.

3. **WDS**: Wireless Distribution System means connecting multiple wireless networks to one. It will use two or more wireless bandwidth Router/AP connecting with each other to expand wireless signal to longer distance. This mode is suitable for medium-size networks like school and enterprise network.

Note: *Access Point operating in WDS mode and all the WDS Peers must operate on the same frequency channel; use the same channel spectrum width and security settings.*

Network Name (SSID) — Service Set Identifier used to identify your 802.11 wireless LAN should be specified while operating in AP or AP+WDS mode. All the client devices within the range will receive broadcast messages from the access point advertising this SSID.

Channel Width---This is the spectral width of the radio channel. Supported wireless channel spectrum widths: (20/40MHZ is selected by default)

20MHz is the standard channel spectrum width.

40MHz is the channel spectrum with the width of 40MHz.

Control Sideband---This function is to control the sideband of the radio channel.

Upper: By default, it is Upper, and the Channel Number is 11.

Lower: If you choose Lower, the Channel Number will change to Auto automatically and you can't change the Control Sideband at the same time. The selectable Channel Number now will range from 1 to 9. Only when you choose other Channel Number you will activate the Control Sideband again. If you choose Upper, the Channel Number selectable will range from 5 to 13.

Channel Number---this option provides selectable channel numbers.

Broadcast Network Name: enable this function allows others to search for this router's SSID.

WMM: WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data.

Data Rate: This defines the data rate (in Mbps) at which the device should transmit wireless packets. You can fix a specific data rate between MCS 0 and MCS 7 also. It is recommended to use Auto option, especially if you are having trouble getting connected or losing data at a higher rate.

MCS means Modulation Coding Scheme**.** Before 802.11n standard emerges, most

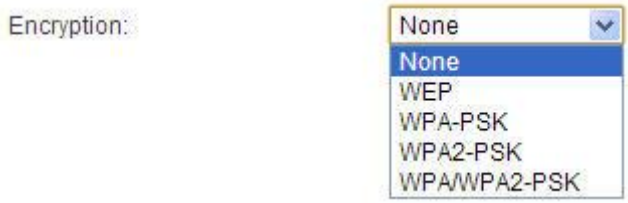
Access Points complies with 802.11a/b/g standards and the data rate ranges from 1Mbps to 54Mbps, including only 12 possible physical speed. But when it comes to 802.11n technology, the physical speed can be affected by many factors, such as modulation type, coding rate, space flow quantity, whether 40MHz banding and so on. Combining these factors together will create a lot of selectable physical speed. Thus, 802.11n proposes the term MCS. You can consider this term to be a whole combination of these factors and every digit represents a combination.

Enable MAC Clone (Single Ethernet Client): MAC address is the physical address of your computer's network card. Generally, every network card has one unique Mac address. Since many ISPs only allow one computer in LAN to access Internet, users can enable this function to make more computers surf Internet.

Note: *only if you choose Client Mode, you can do this operation.*

3.6.3 Security Select

This section allows you setup the security. You can select None WEP WPA WPA (TKIP), WPA (AES) WPA2 WPA2 (TKIP) and WPA2 (AES).

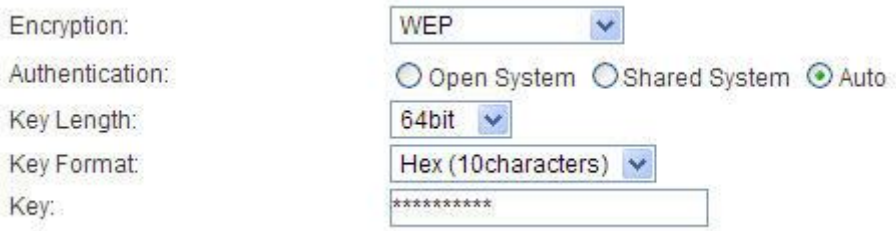


Encryption: you can select None, WEP, WPA, WPA-PSK, WPA2-PSK and WPA/WPA2-PSK.

3.6.3.1 WEP

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encryption data being transferred over your wireless network. WEP is the oldest security algorithm, and

there are few applications that can decrypt the WEP key in less than 10 minutes.



Key Length: 64-bit/128-bit, by default it is 64-bit.

64-bit—For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x414234445.)

128-bit—For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D).

Key Format: If you choose 64 bit, there will be two Key Formats selectable: ASCII (5 characters) and Hex (10 characters). If 128-bit, the Key Formats should comply with ASCII (13 characters) or Hex (26 characters)

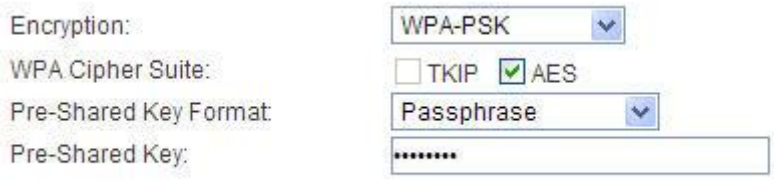
Key: Please refer to Key Length to set this parameter.

3.6.3.2 WPA-PSK/WPA2-PSK

Wi-Fi Protected Access (WPA) is the most dominating security mechanism in industry. It is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x. WPA2 means Wi-Fi Protected Access 2, it is the current most secure method of wireless security and required for 802.11n performance. Please set one Encryption key (password) for your wireless network to prevent being occupied by others.

TKIP--Temporal Key Integrity Protocol is one cipher for data encryption supported by WPA.

AES--Advanced Encryption Standard is another cipher for data encryption supported by WPA.

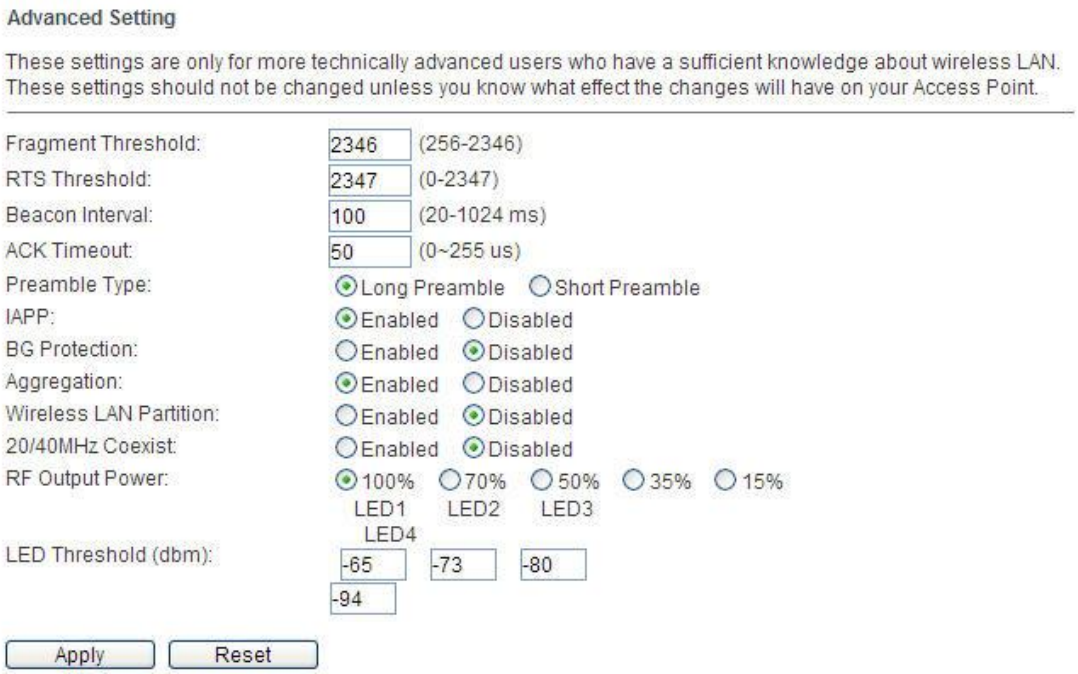


Pre-Shared Key Format/Pre-Shared Key: This is a pre-defined key used for encryption during data transmission. It has two formats: Passphrase and Hex (64 characters). Then you need to enter the Pre-Shared Key, either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as “0x321253abcde…”).

3.6.3.3 WPA/WPA2-PSK

This option mixes WPA/WPA2 together. It will provide the best security for your router.

3.6.4 Advanced Setting



Fragment Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes. Setting the Fragment Threshold too low may result in poor network performance. The use of fragment can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However, lower values of the Fragment Threshold will result in lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes. The default value is 2347, which means that RTS is disabled.

RTS/CTS (**Request to Send/Clear to Send**) are the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden

terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

System uses **Request to Send/Clear to Send** frames for the handshake that provide collision reduction for an access point with hidden stations. The stations are sending a RTS frame first while data is sent only after a handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provide clear media for the requesting station to send the data. CTS collision control management has a time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Beacon Interval: by default, it is set to 100ms. Higher Beacon interval will improve the device's wireless performance and is also power-saving for client side. If this value set lower than 100ms, it will speed up the wireless client connection.

ACK Timeout: the acknowledgments affect long distance links in that the transmitter waits for a limited amount of time before retrying. If the ACK timeout is set too short, the transmitter will start retransmitting before an ACK could have possibly been received and this retransmission may well actually interfere with an ACK that is "on it's way". If, conversely, the ACK timeout is set too long, the transmitter waits unnecessarily long before retransmitting in the case no ACK is received. This represents lost time and thus reduces the throughput of the link.

Preamble Type: this option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses shot preamble with 56 bit sync filed instead of long preamble with 128 bit sync filed. However, some original 11b wireless network devices only support long preamble. By default, Long Preamble is selected.

IAPP： Inter-Access Point Protocol is designed for the enforcement of unique association throughout an ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period. It is enabled by default.

BG Protection: Background Protection, it is disabled by default.

Aggregation: A part of the 802.11n standard. It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header. It is enabled by default.

Frames- determine the number of frames combined on the new larger frame.

Bytes- determine the size (in **Bytes**) of the larger frame.

Wireless LAN Partition: divides the WLAN to several parts.

20/40MHz Coexist: enable this function will make the device select the channel with better performance automatically. It is disabled by default.

RF Output Power: you can select the output power of the wireless device. The default

value is 100%. It will deliver the best performance of the device.

LED Thresholds, dBm: specify the marginal value of Signal Strength (dBm) which will switch on LEDs indicating signal strength:

LED 1 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -65dBm.

LED 2 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -73dBm.

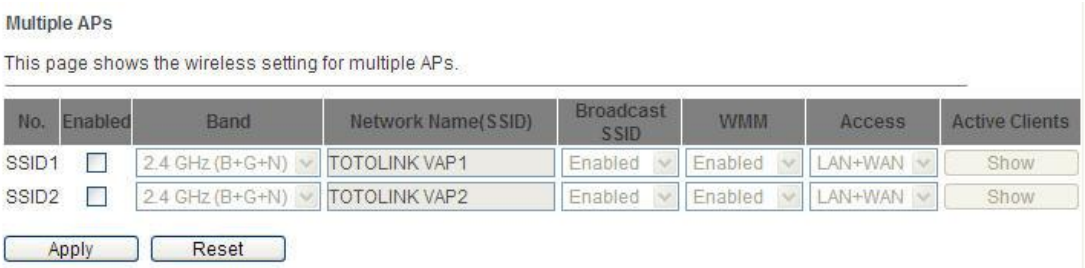
LED 3 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -80dBm.

LED 4 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -94dBm.

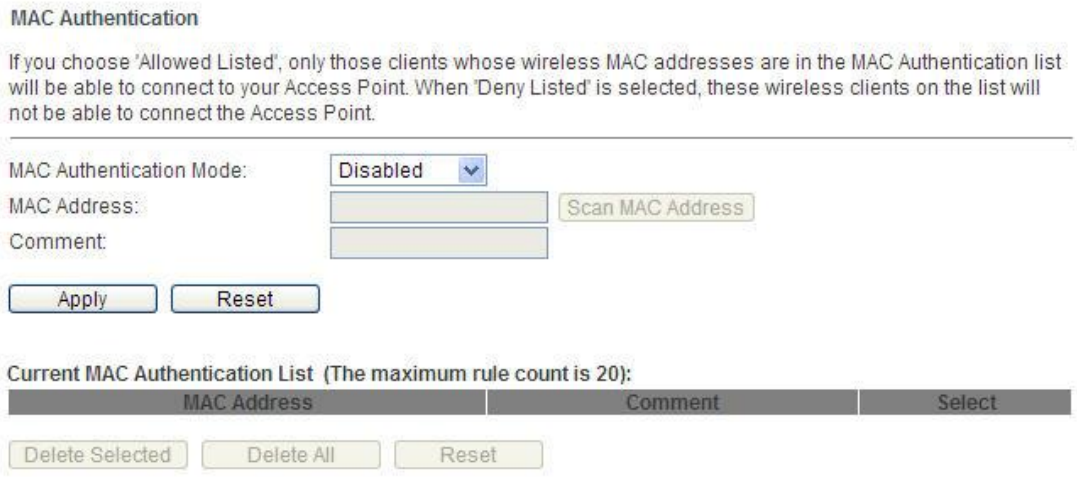
Configuration example: if the Signal Strength (displayed in the *Main* page) fluctuates around -63 dBm, the LED Thresholds can be set to the values -70, -65, -62, -60.

3.6.5 Multiple APs

This router allows you to set two SSIDs while you are in AP mode or WDS mode. You can set two different SSID so that it is very convenient for users who want to set up extra wireless networks for guests or friends with better access control.



3.6.6 MAC Authentication



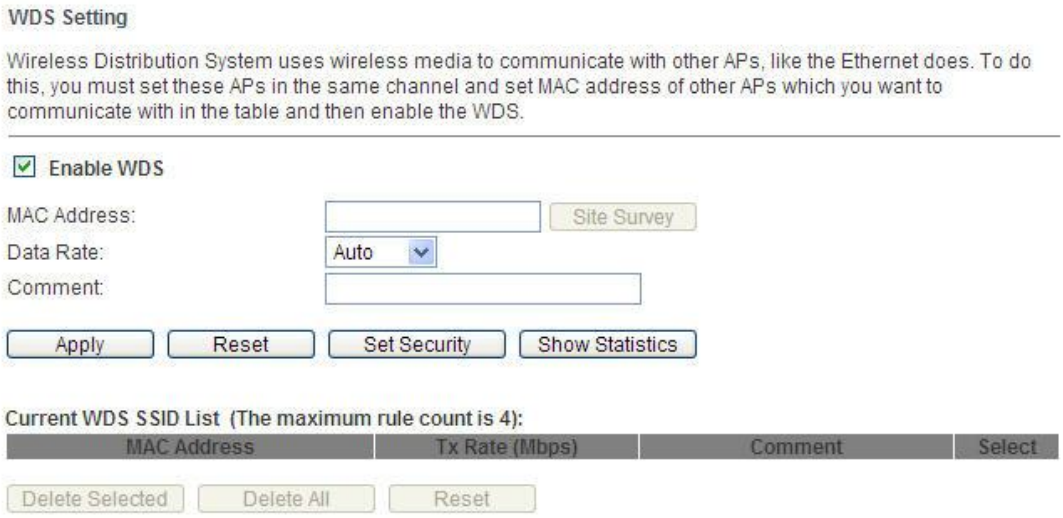
MAC Authentication Mode: you can select to allow or deny the listed MAC address to

connect to your router.

MAC Address: enter the MAC address.
Comment: describe the reason why you want to use MAC Authentication. Just few words are saved there usually.

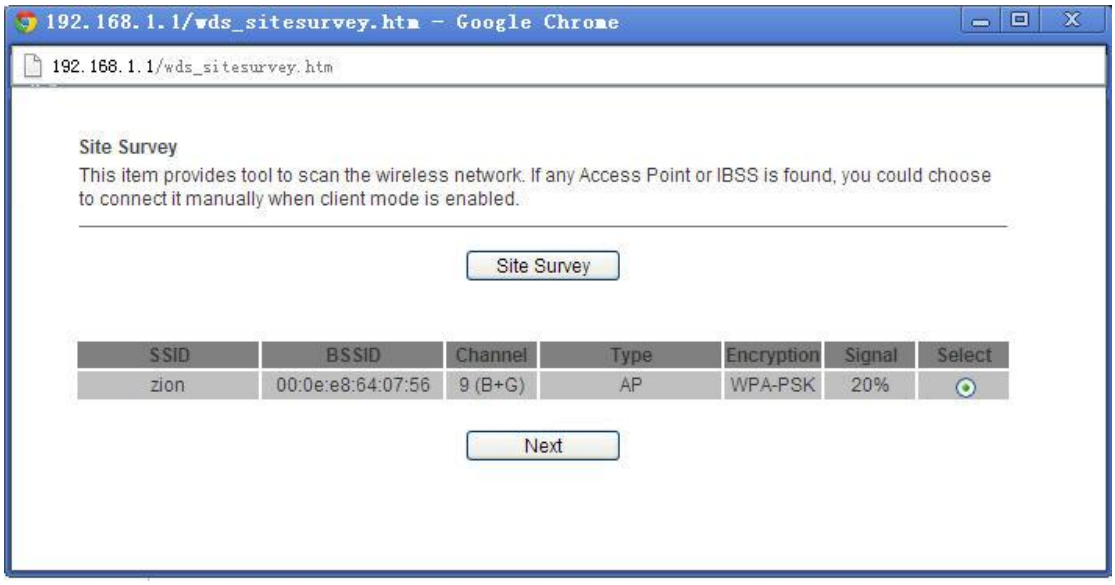
3.6.7 WDS Setting

Wireless Distribution System means connecting multiple wireless networks to one. It will use two or more wireless bandwidth Router/AP connecting with each other to expand wireless signal to longer distance. This mode is suitable for medium-size networks like school and enterprise network.

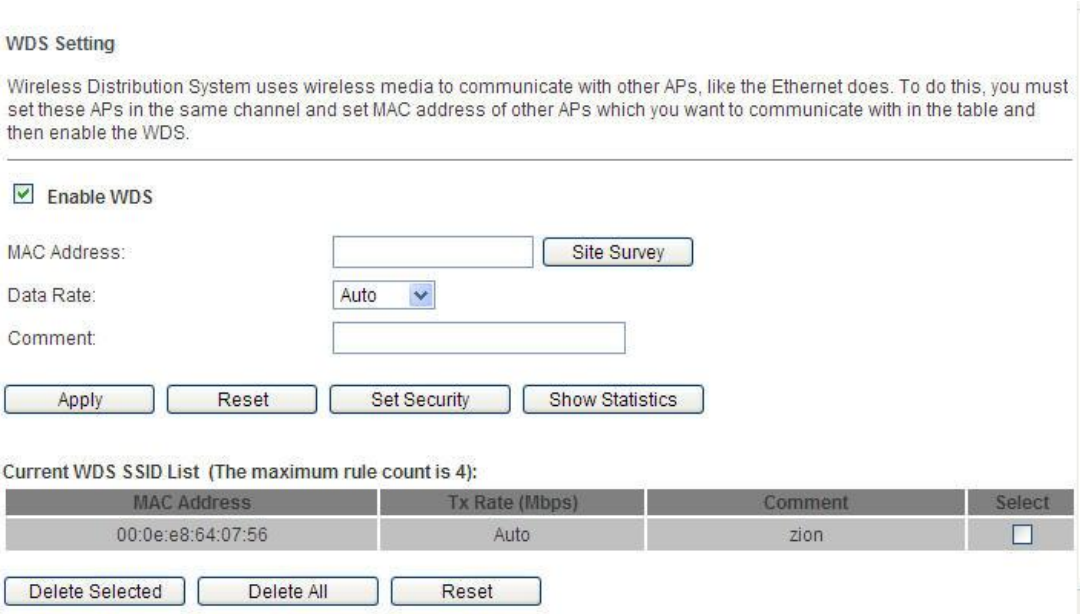


Enable WDS: tick out to enable the WDS function.
After enable WDS function, click **Set Security** Button, it will come to the WDS security setting interface. There are four encryption types for you to choose, respectively none, 64 /128bit WEP and WPA2 (AES), you can setup encryption refer to the introduction before.

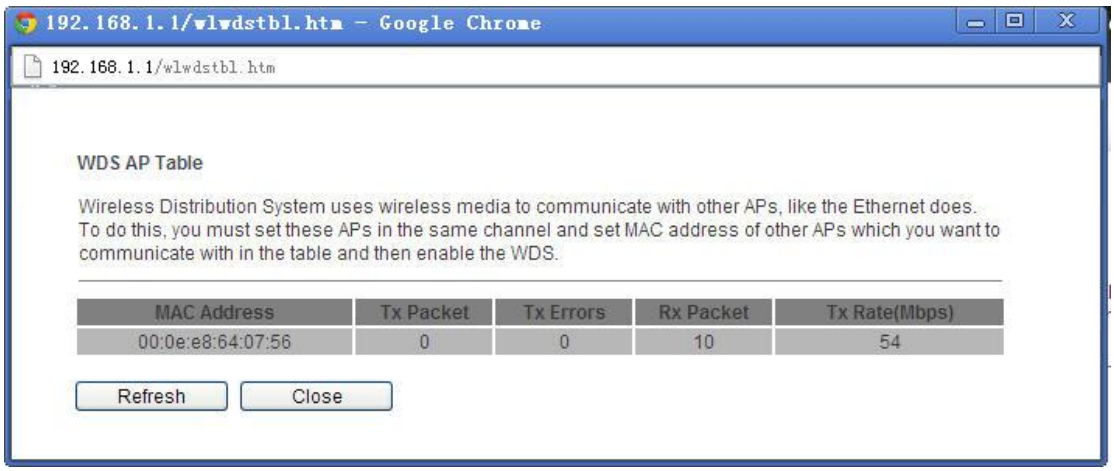
After encryption setup completed, please click Site Survey after MAC Address Bar. Then the windows as below show will pop up. Choose **Select** to connect to the access point which you want to connect with and click **Next**.



Click **Apply** to make configuration work out you can see detailed information in Current WDS SSID List.



When you click **Show Statistics** Button, the WDS AP table will pop up. This page shows you detailed transmission/receiving packets.



3.6.8 WPS Setting

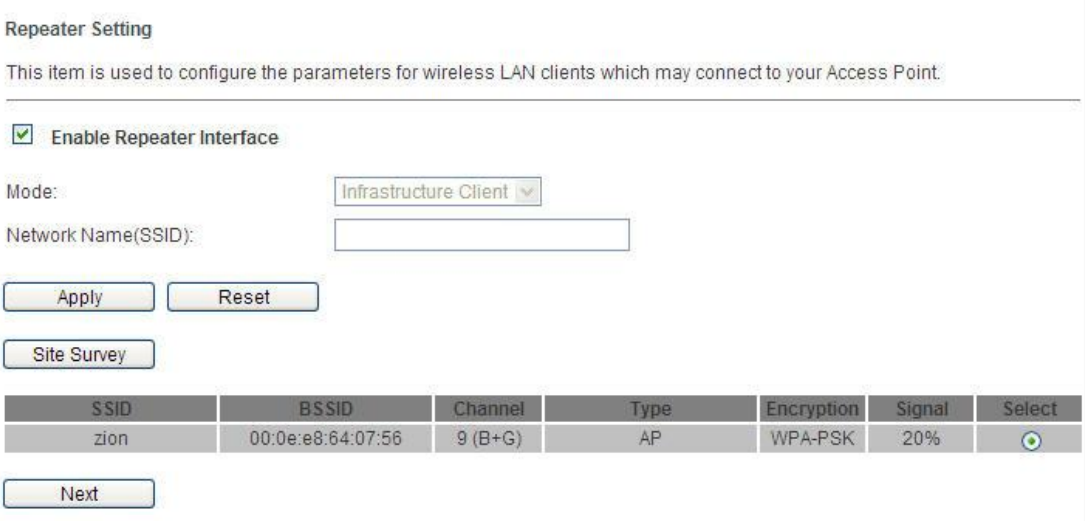
WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2. It is enabled by default.

WPS Status: Display related system information for WPS. If the wireless security (encryption) function of the CPE is properly configured, you can see **Configured** chosen.
Self-PIN Number: it will show the PIN Number of your device.
Push Button Configuration: click Start PBC button to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes.)
Client PIN Number: please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Current Key Info: If the wireless security (encryption) function of the router is properly configured, you can see the encryption information on the list.

3.6.9 Repeater Setting

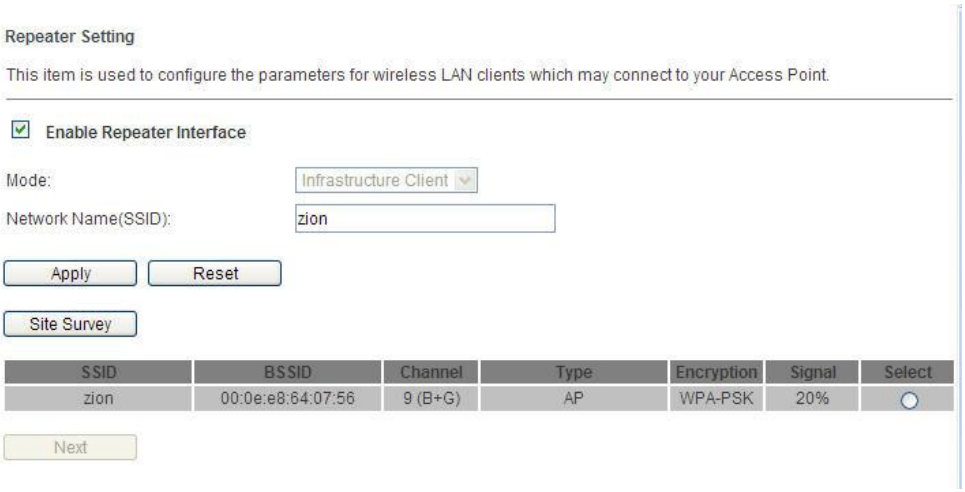
Repeater methods can help you to expand the wireless coverage and allow more terminals to access Internet.

Enable Repeater Interface: tick out to enable the repeater function.
After repeater function is enabled, the setting interface is changed, see below.



Choose **Select** to connect to the upper AP and click Next, then it will come to encryption setting interface. Enter the Pre-Shared Key of the upper AP and click **Connect**.

After encryption setting completed, please come back to the repeater interface and click **Apply** to finish Repeater settings.



3.7 Quality of Service

In Gateway mode or Wireless ISP mode, QoS is provided for a better management. Quality of Service can be also called QoS simply. Deploying QoS management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network. Since numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, we need QoS to control the bandwidth use. On this page, you could set the QoS rules.

Enable QoS: you can choose to enable this function or not.

Manual Uplink Speed: you can set the uplink speed for all LAN PCs.

Manual Downlink Speed: you can set the downlink speed for all LAN PCs.

Address Type: bandwidth control on IP or MAC, please choose the proper one according

to your need.

IP Address: if you choose IP address, please enter the IP address range.

Mac Address: if you choose MAC address type, please enter the MAC address, or click Scan MAC Address button to view valuable MAC Address.

Uplink Bandwidth: type in the uplink bandwidth.

Downlink Bandwidth: type in the downlink bandwidth.

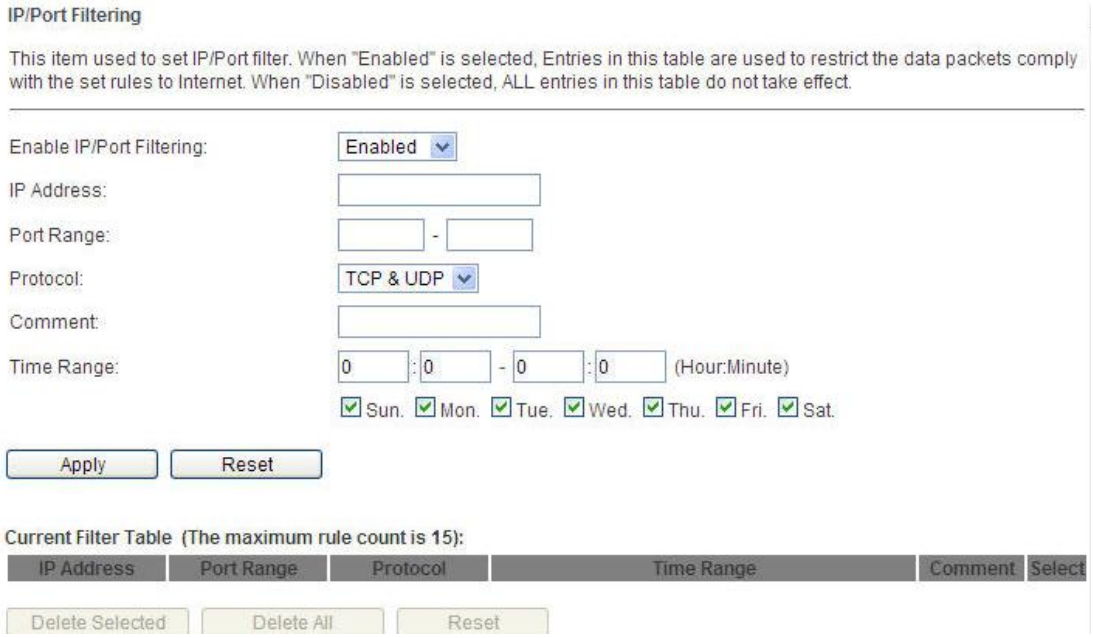
Comment: describe the reason. Just few words are saved there usually.

Current QoS Rules Table: shows the detailed QoS rules you have set.

3.8 Firewall

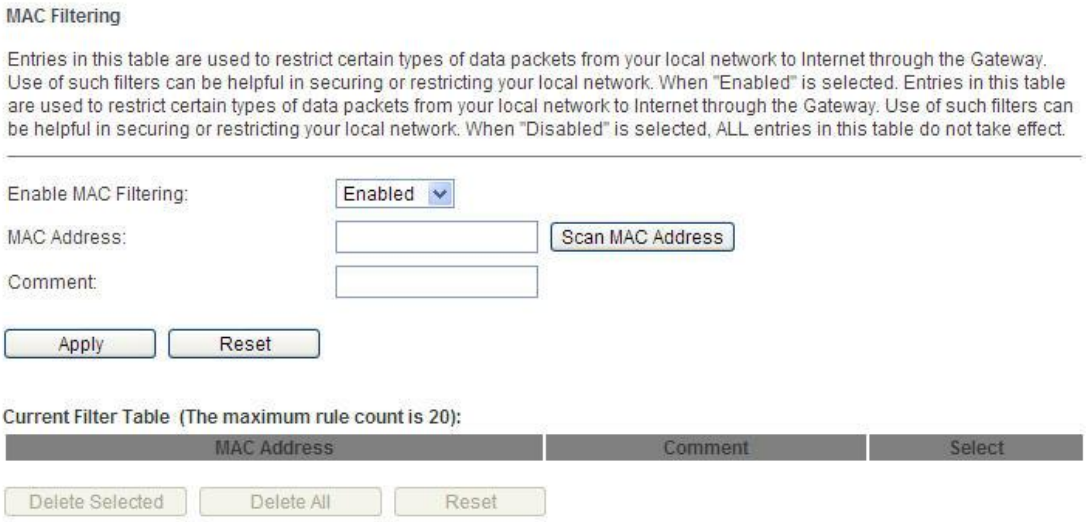
While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of this router helps to protect you local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

3.8.1 IP/Port Filtering



Enable IP/Port Filtering: you can select this checkbox to enable Port Filtering function.
IP Address: the IP address that you want to filter.
Port Range: the port range that you want to filter.
Protocol: choose which particular protocol type should be filtered. Here you can choose UDP/TCP.
Comment: describe the reason why you want to filter these ports. Just few words are saved there usually.
Time Range: enter the time range and select the date a week when you want the IP/Port Filtering works.
Current Filter Table: this table will list the detailed information about the ports that will be filtered.

3.8.2 MAC Filtering

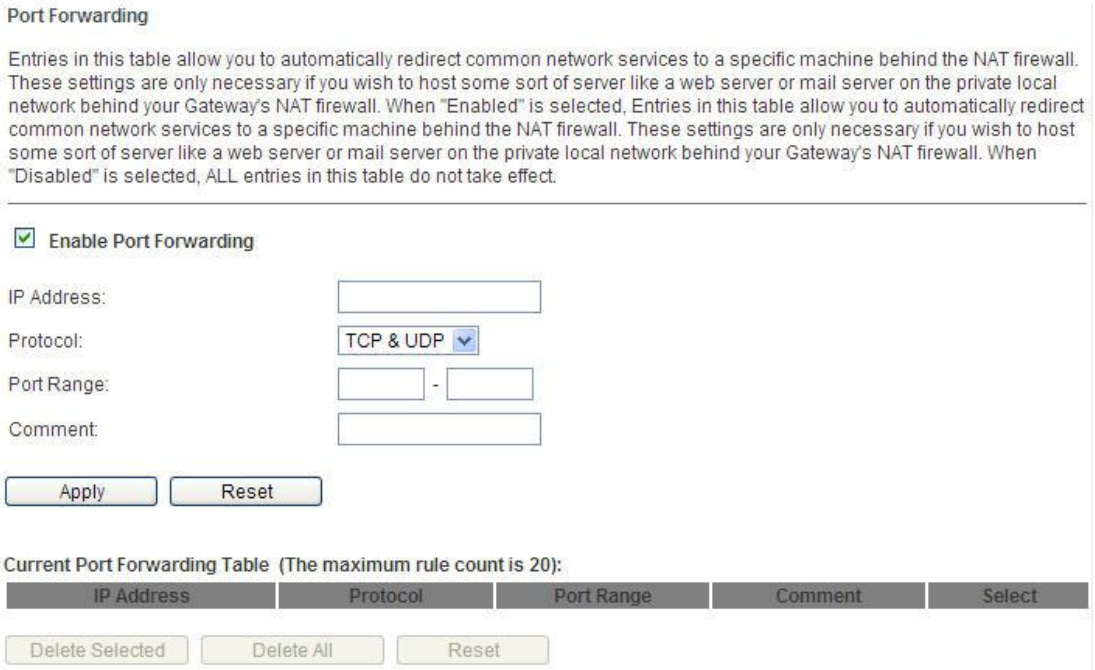


Enable MAC Filtering: you can check the box to enable MAC Filtering function.
MAC Address: the MAC address that you want to filter.
Comment: describe the reason why you want to filter the MAC address. Just few words are saved there usually.
MAC Filter Table: this table will list the detailed information about the MAC addresses that will be filtered.

3.8.3 URL Filtering

Enable URL Filtering: you can select this checkbox to enable URL filtering function.
URL Address: type in the keywords contained in URLs that you don't allow LAN users to access.
URL Filter Table: this table will list the detailed information about the keywords contained in URLs that you don't allow LAN users to access.

3.8.4 Port Forwarding



Port Forwarding creates a transparent tunnel through a firewall/NAT, granting an access from the WAN side to the particular network service running on the LAN side. 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: you can select this checkbox to enable Port Forwarding function.

I**P Address:** enter the Port's IP address.

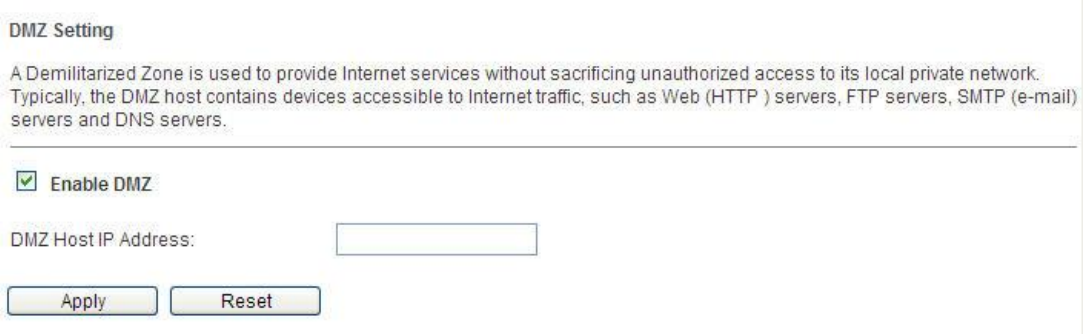
Protocol: choose which particular protocol type should be forwarding. Here you can choose Both/UDP/TCP.

Port Range: set the range that the port forward to.

Comment: describe the reason why you want to use port forward function. Just few words are saved there usually.

Port Forwarding Table: this table will list the detailed information about the ports that will be forwarded.

3.8.5 DMZ



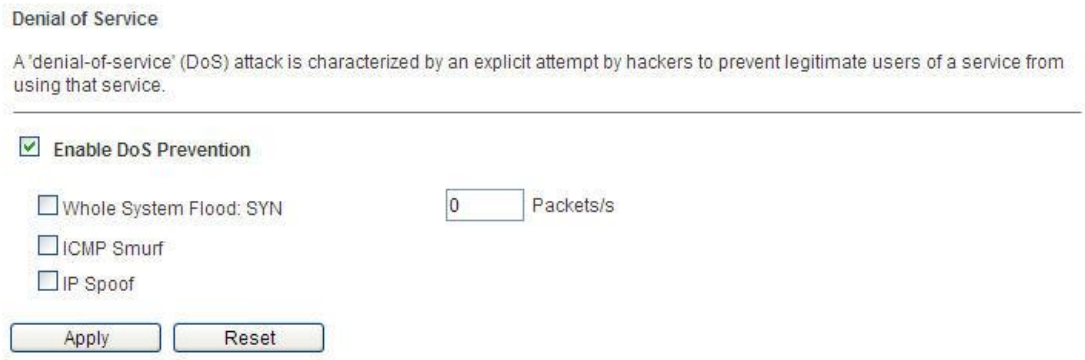
DMZ means Demilitarized Zone. It can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.
Enable DMZ: you can select this checkbox to Enable DMZ function.
DMZ Host IP Address: type in the IP address of the DMZ host.

3.8.6 Denial-of-Service

The DoS Prevention functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The DoS Prevention function enables the router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also this router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the CPE will activate its defence mechanism to mitigate in a real-time manner.

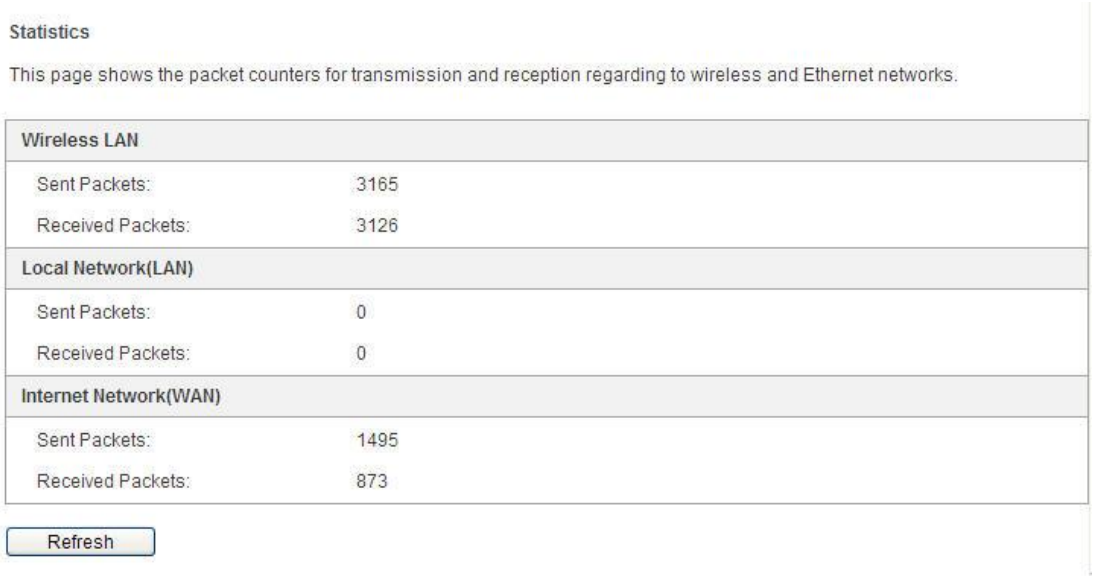


3.9 Management

For system management, there are several items that you have to know the way of configuration: Statistics, Time Zone Setting, Remote Management, System Log, Upgrade Firmware, Save/Reload Configuration and Administrator Settings.
The picture on the left is the content in Bridge mode, while the picture on the right side is in Gateway mode and Wireless ISP mode. The only difference is the Dynamic DNS Setting section.

3.9.1 Statistics

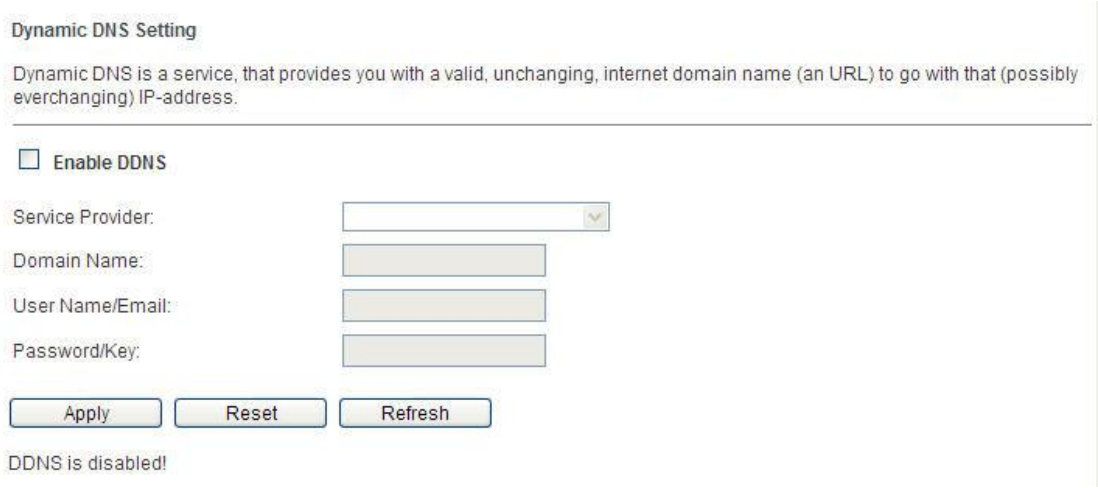
This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks. While it is in the Bridge mode, it is only Wireless LAN and Local Network LAN sections.



3.9.2 Dynamic DNS Setting

Dynamic Domain Name System is also called DDNS simply. The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service from the DDNS service providers. This router supports two service providers: DynDNS and NO-IP.



You could choose to enable or disable DDNS function. If you enable DDNS, you need to provide below information:

Service Provider: choose one service provider where you have applied for free DDNS service.

Domain Name: type in the host name you registered from the DDNS provider.

User Name/Email: enter the User Name or Email you registered from the DDNS provider.

Password/Key: enter the Password or Key you set for the User Name.

3.9.3 Time Zone Setting

This page allows you to maintain the system time by synchronizing with a public time server over the Internet.

Current Time: shows the current time based on your time zone.

Time Zone Select: select the Time Zone where the router is located.

Enable NTP Client Update: tick out to enable NTP Client Update.

Automatically Adjust Daylight Saving: if the Time Zone you choose implements daylight saving time, please select this option.

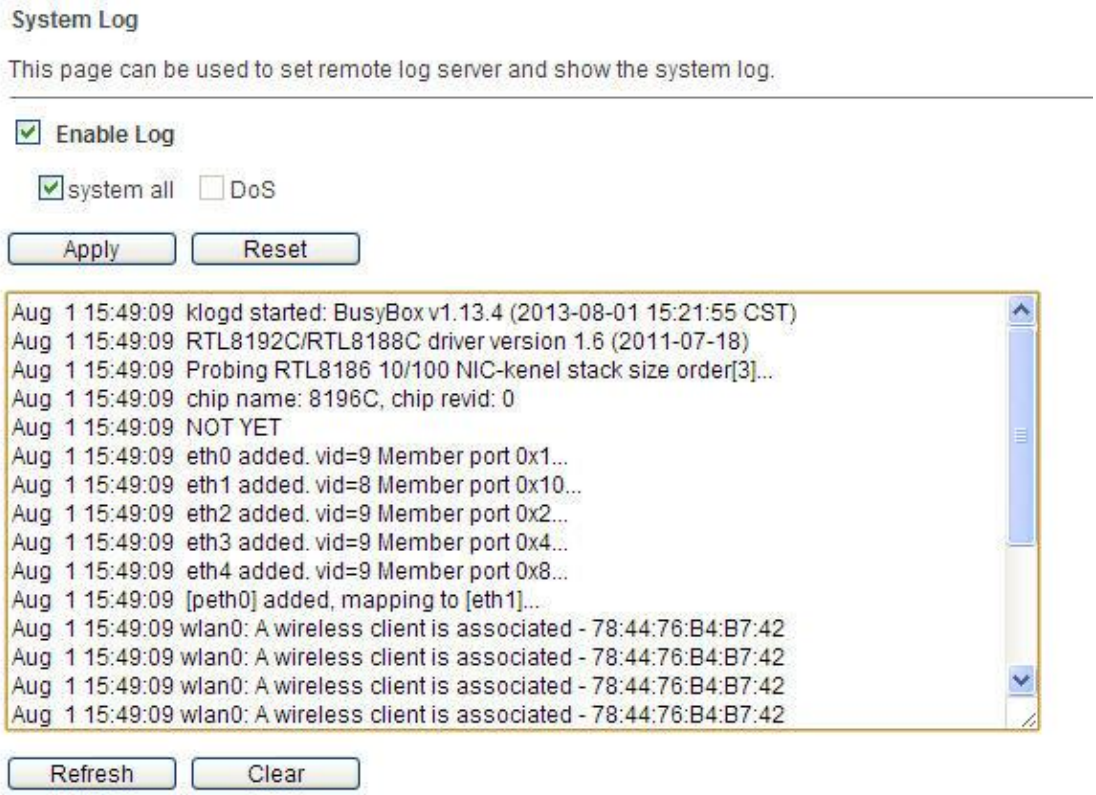
NTP Server: NTP means Network Time Protocol which is used to make the computer time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption.

3.9.3 Remote Management

You could choose to enable or disable Remote Management.

3.9.4 System Log

This page can be used to set remote log server and show the system log. After enable system log, you can choose system all or DoS



3.9.5 Upgrade Firmware

This page allows you to 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.

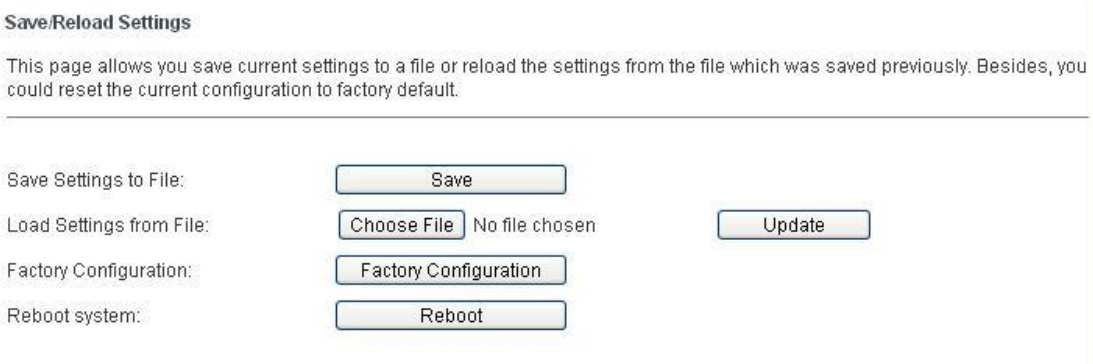
Firmware Version: shows the current firmware version.

Select File: click **Choose File** to select the firmware version you want to upgrade on your computer.

Click **Upgrade** to upgrade the firmware version.

3.9.6 Save/ Reload Setting

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



Save Setting to File: click **Save** button to download the current settings of the Access Point to your computer.

Load Settings from File: if you want to reload the settings from the file saved before, you could click **Choose File** button to choose the right file then click **Update** button.

Factory Configuration: this **Factory Configuration** button is provided to allow you to restore the router settings to the default factory settings.

Reboot System: click **Reboot** to reboot this device.

3.9.7 Administrator

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup.

User Name: enter the User Name you login.

New Password: new password is used for administrator authentication.

Confirmed Password: new password should be re-entered to verify its accuracy.

Note: *password length is 8 characters maximum, characters after the 8th position will be truncated.*