use an external authentication server (e.g., RADIUS) and EAP just like IEEE 802.1X is using or pre-shared keys without need for additional servers. Wi-Fi calls these "WPA-Enterprise" and "WPA-Personal", respectively. Both mechanisms will generate a master session key for the Authenticator (AP) and Supplicant (client station).

802.1X: The original security mechanism of IEEE 802.11 standard was not designed to be strong and has proven to be insufficient for most networks that require some kind of security. Task group I (Security) of IEEE 802.11 working group has worked to address the flaws of the base standard and in practice completed its work in May 2004. The IEEE 802.11i amendment to the IEEE 802.11 standard was approved in June 2004 and published in July 2004.

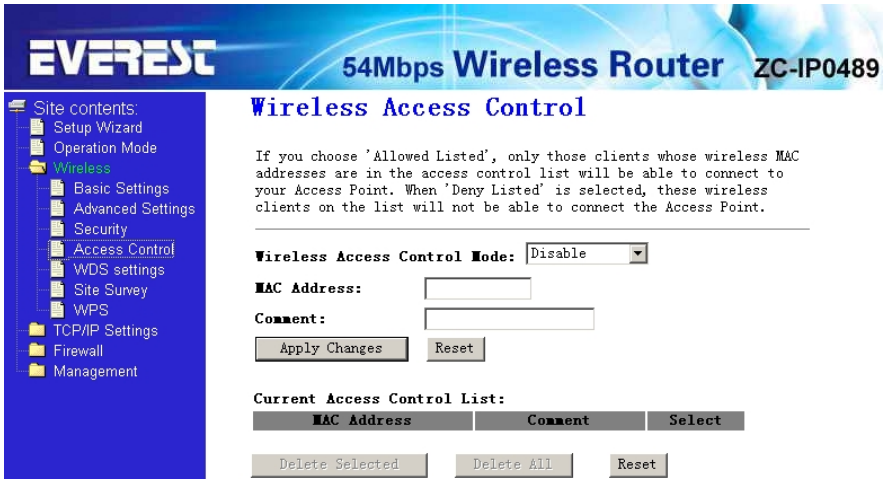
WPA Cipher suite/WPA2 Cipher suite:The encryption piece of WPA and WPA2 mandates the use of TKIP or, because it's considered to be more secure than TKIP, preferably AES encryption.

Pre-Shared Key Format: You can select PASSPHRASE or HEX(64 CHARACTERS).

Pre-Shared Key: You can input 128 characters key.

Authentication RADIUS Server:input Port and IP Address and Password.

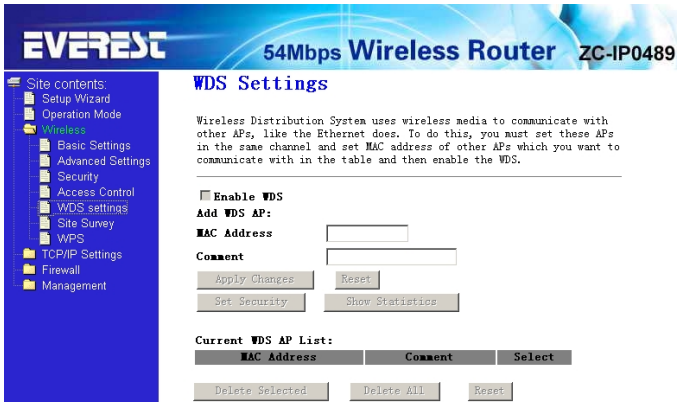
4.2.4 Wireless Access Control



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

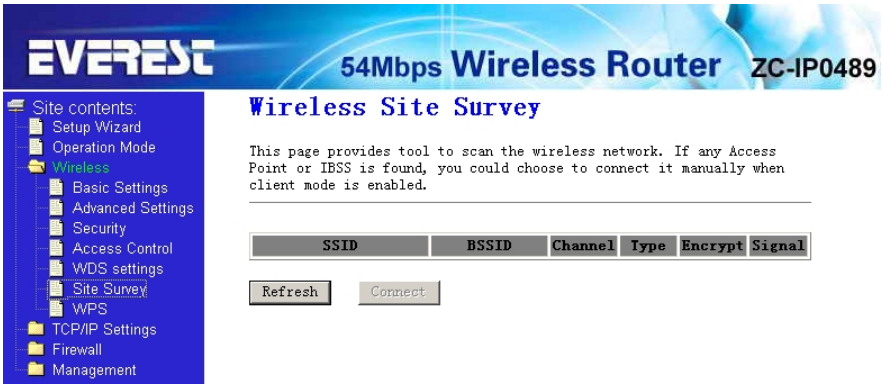
4.2.5 WDS Settings

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

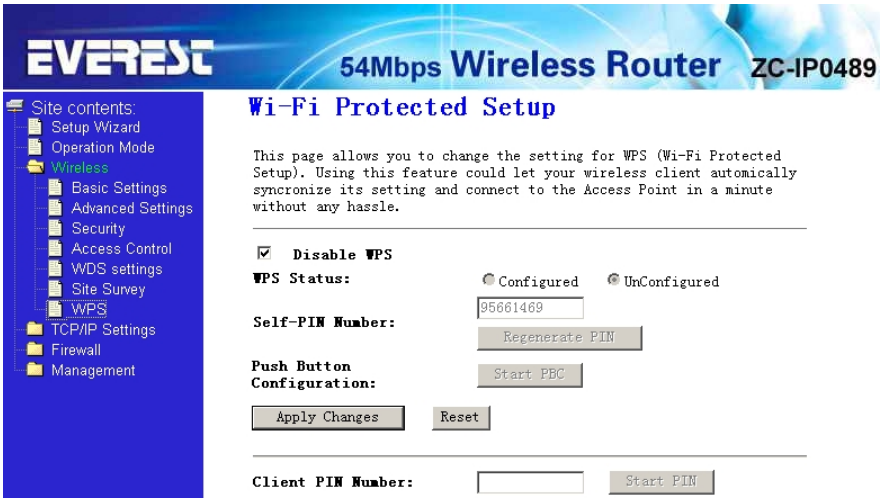


4.2.6 Wireless Site Survey

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



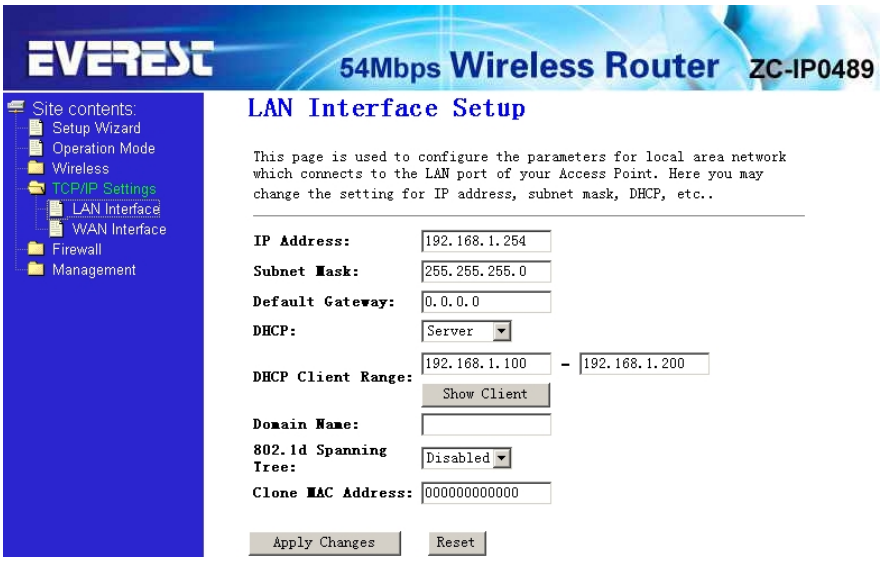
4.2.7 WPS Setting



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

4.3 TCP/IP Setting

4.3.1 LAN Setting Lan Interface setup



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

MAC Address - the physical address of the router, as seen from the LAN. The value can't be changed.

IP Address - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.254).

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

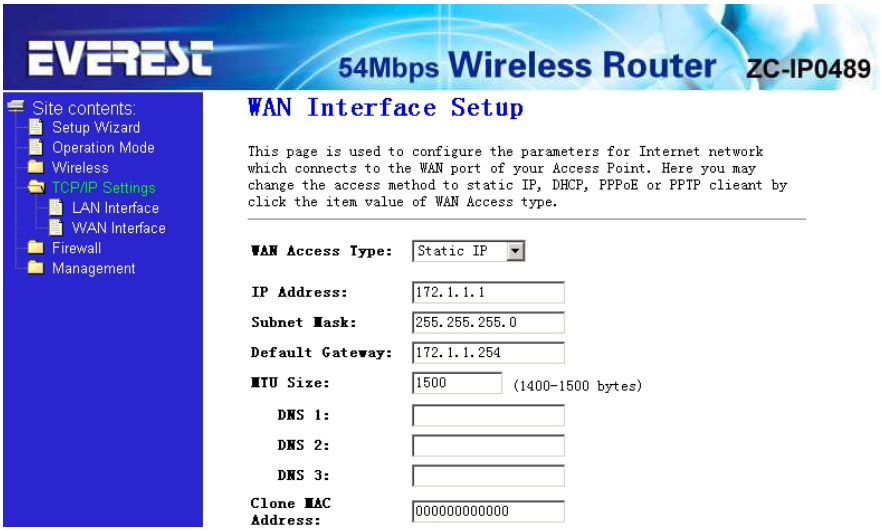
DHCP: You can select None,Client,Serve. The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN.

DHCP Client Range: This field specifies the first of the addresses in the IP address pool.

802.1d Spanning Tree: The IEEE 802.1D Spanning Tree Algorithm (STA) ,loop prevention and redundant link configuration. You can select disable or enable.if your mode was set WDS or AP+WDS, this item should be set “enable”

Clone MAC Address:you can enter a MAC,Then click clone.

4.3.2WAN 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, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type,User name, password, Service: you can refer to **3.2 Quick Installation Guide.**

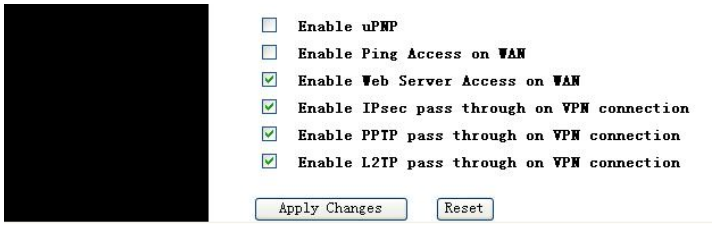
Connection Type:you can select **continous o, connect on demand, manual.**

Idle time: when **connection type** is **connect on demand,**you can set idle time.

MTU Size: The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1492 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

DNS: You can select Attain DNS Automatically or Set DNS Manually

Clone MAC Address: if you wang clone, input MAC Address



Enable UpnP: The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

Enable L2TP pass through on VPN connection:

Enable IPsec pass through on VPN connection:

Enable PPTP pass through on VPN connection:

4.4 Firewal

4.4.1 Port Filtering

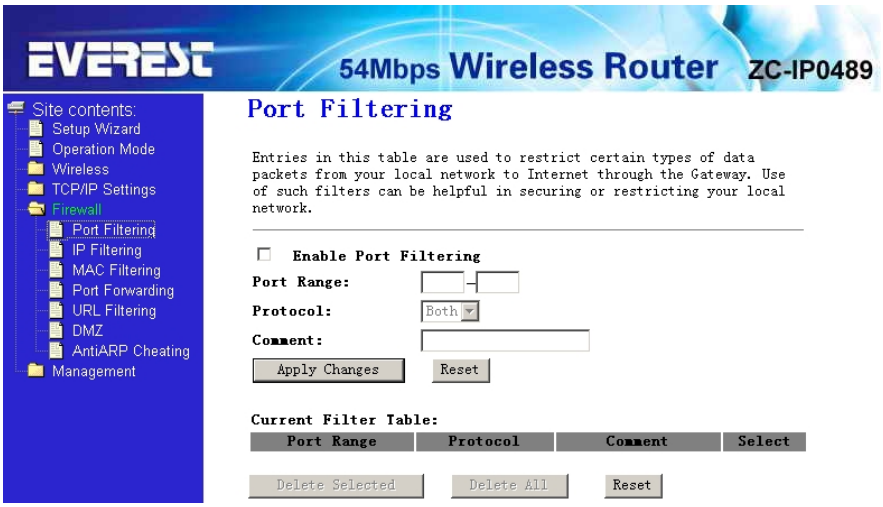
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port filtering: select it, you can modify port filter.

Port range: input the filter port, for eaample 20-220

Protocol: you can select both,TCP,UDP

Cuurrent filter table: The list of port filter.



4.4.2 IP Filtering

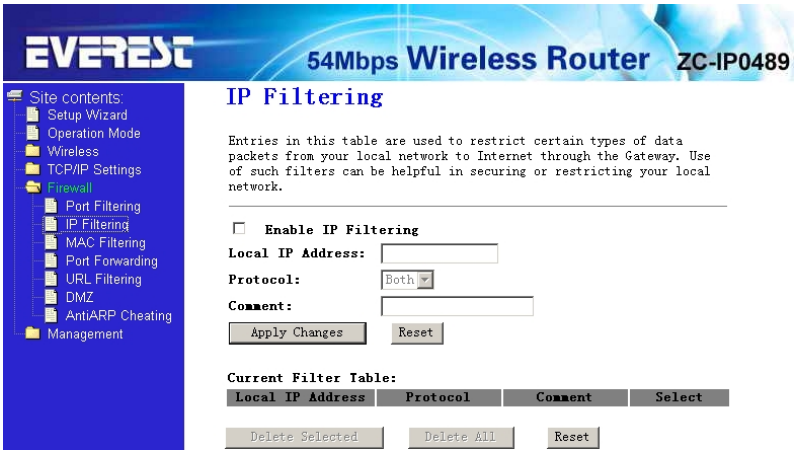
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering: select it, you can modify IP filter.

Local IPAddress:input the IP Address,for example:192.168.1.23.

Protocol: you can select both,TCP,UDP

Cuurrent Filter table: The list of IP filter.



4.4.3 MAC Filtering

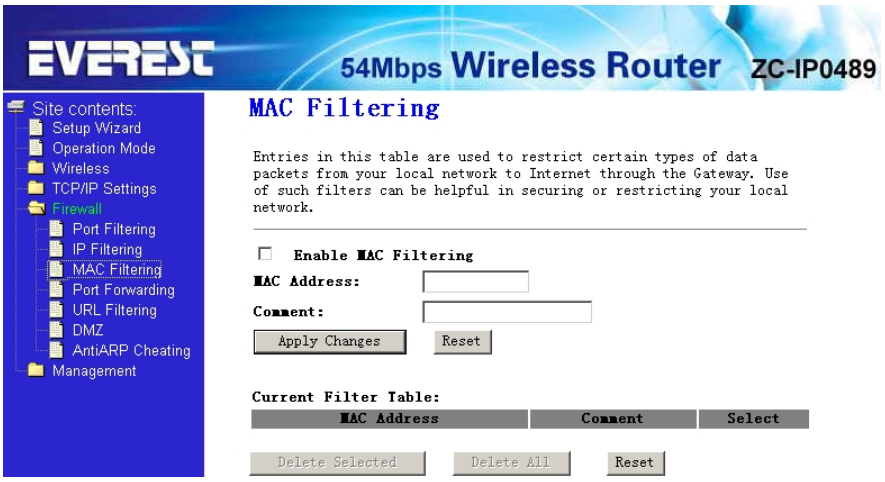
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network

Enable MAC Filtering: select it,you can modify MAC filter.

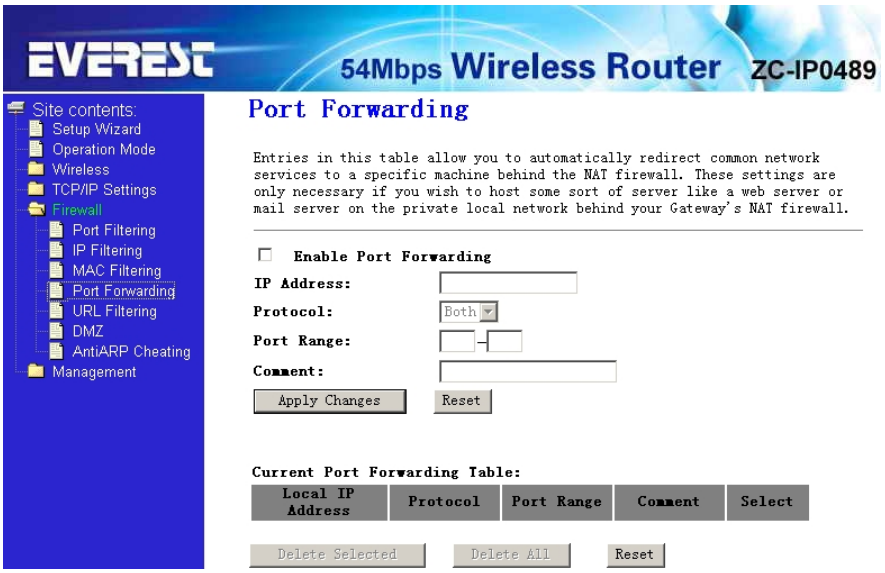
MACAddress:type the MACAddress,for

example:00:e0:4e:3f:2d:c5.

Cuurrent Filter table: The list of MAC filter.



4.4.4 Port Forwarding



Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable MAC Address:select it,you can modify MAC Address Filtering..

IP Address: The IP Address of the PC running the service application

Protocol - The protocol used for this application, either **TCP**, **UDP**, or **both** (all protocols supported by the router).

Port Range- The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is Start port, YYY is End port).

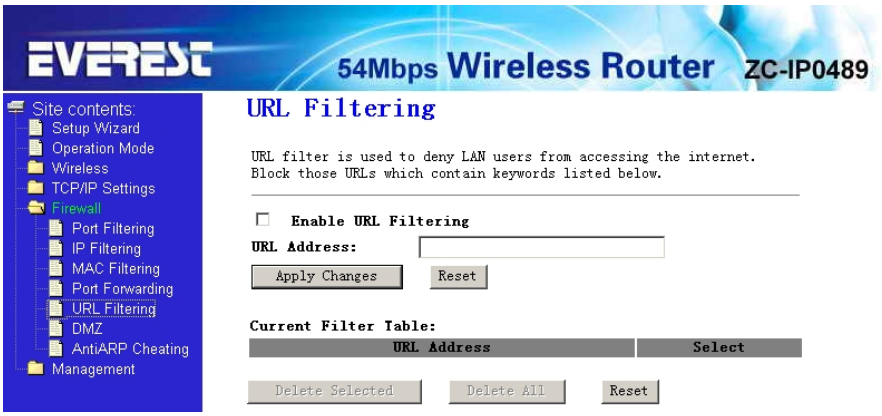
Current Port Forward Table: port forward services already list.

4.4.5 URL Filtering

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

Enable URL : select it, you can edit URL, For example:xxx.com

Click **apply changes**.



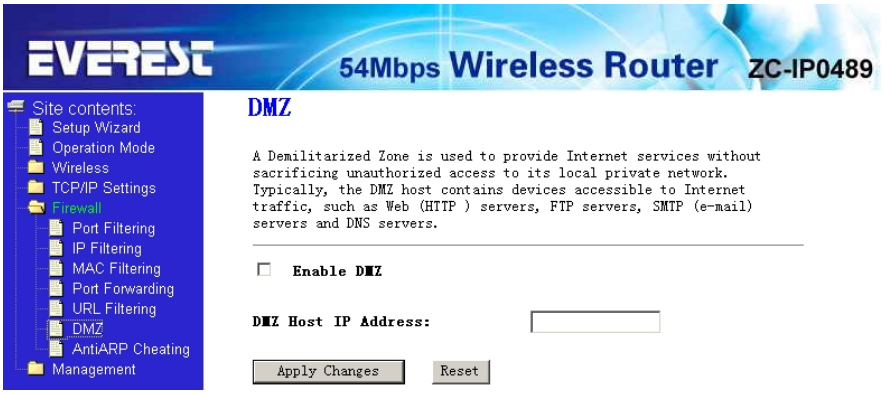
4.4.6 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function.

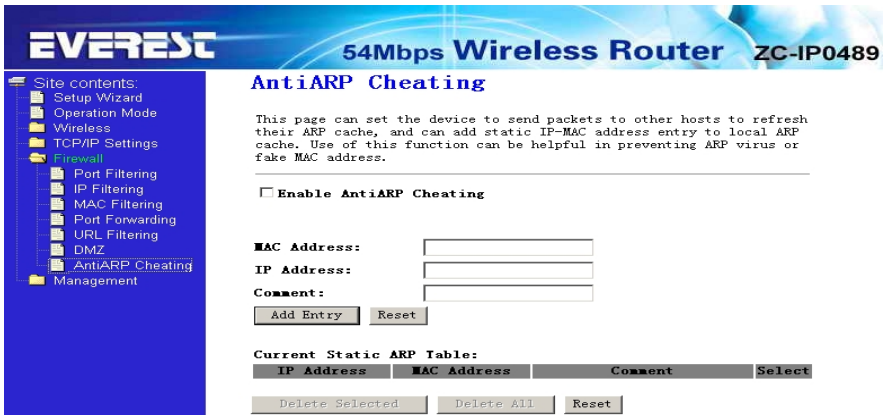
DMZ Enable: Select it, DMZ can be edit..

DMZ Host IP Address:input IP Address.for example 192.168.1.34.

Click **apply changes**,complete set DMZ.



4.4.7 AntiARP Cheating

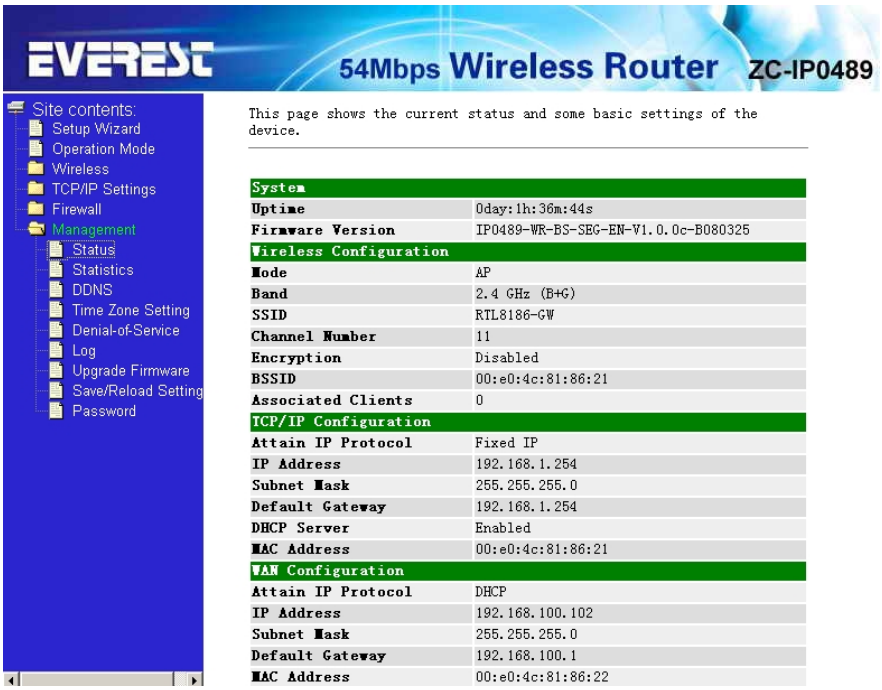


This page can set the device to send packets to other hosts to refresh their ARP cache, and can add static IP-MAC address entry to local ARP cache. Use of this function can be helpful in preventing ARP virus or fake MAC address

4.5 Management

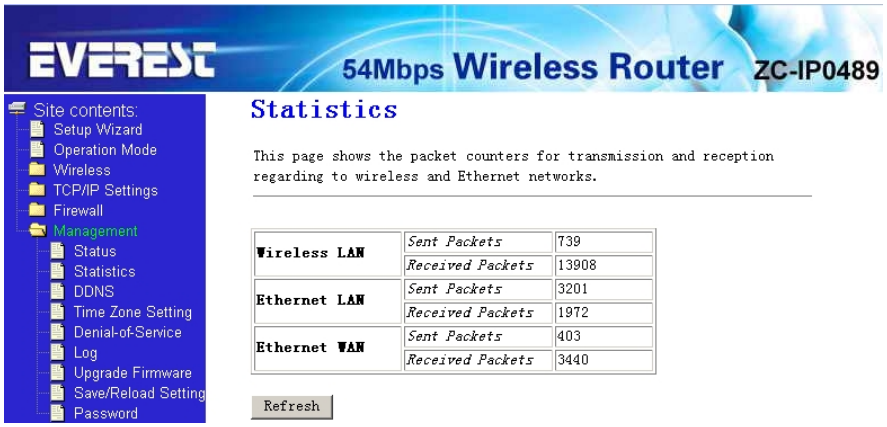
4.5.1 Status

This page shows the current status and some basic settings of the device. you can check system Information, LAN Interface Information, WAN Interface Information.

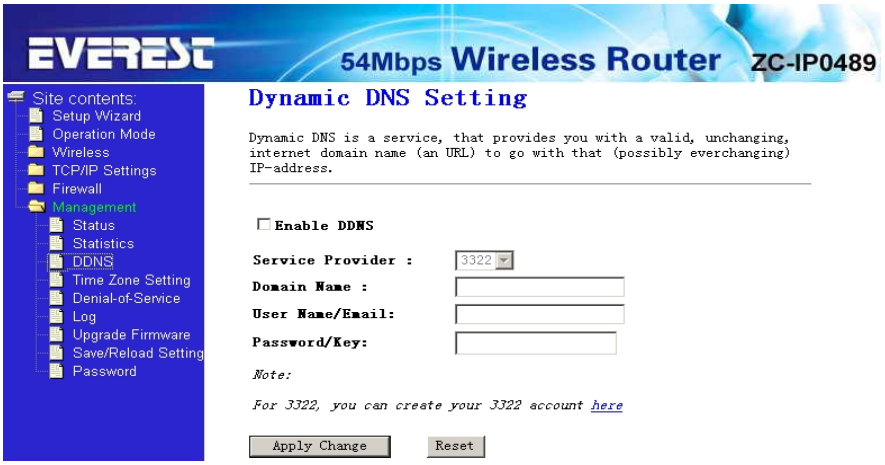


4.5.2 Statistics

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



4.5.3 Dynamic DNS Setting



Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

1. Type your **dervice provider.**
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. **Domain Name -** the domain names are displayed here. Click **Apply Changes** to logout the DDNS service.

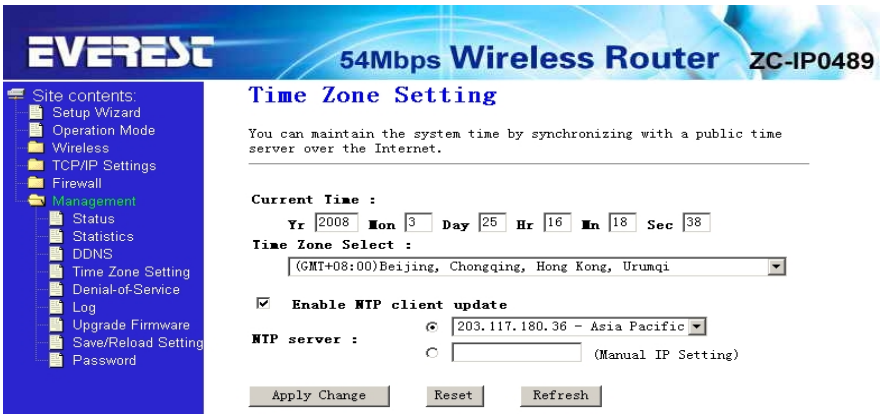
4.5.4 Time Zone Setting

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

Current time: type the date and time.

Time Zone Select: Select your local time zone from this pull down list.
Enable NTP client update:select it, you can get the time from **NTP.**
NTP server :select a server from list.

Click the **Apply changes** get the time from Internet if you have connected to Internet.



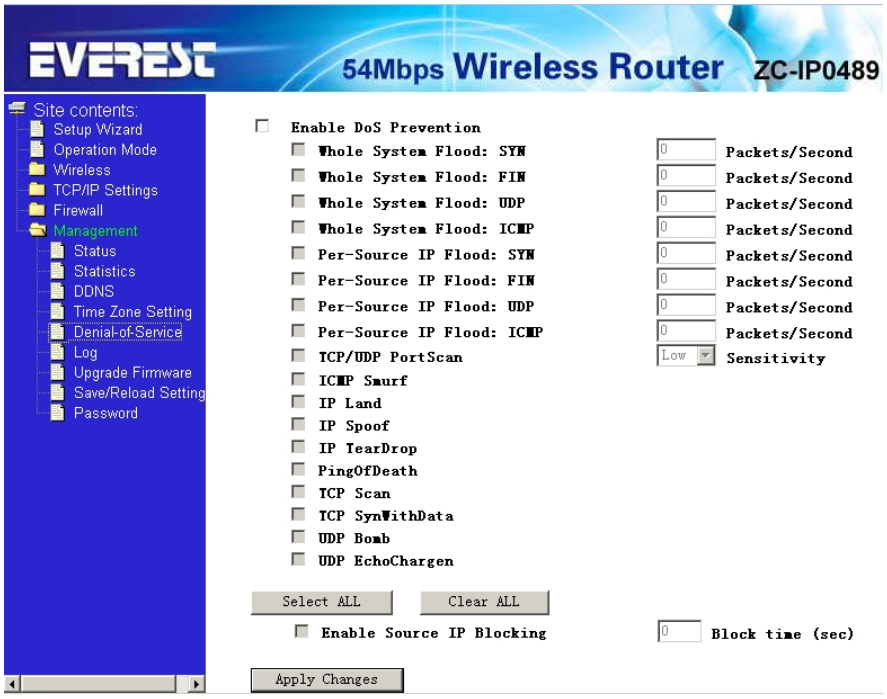
4.5. 5 Denial of Service

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

Enable DOS Prevention:select it, you can modify DOS Prevention.

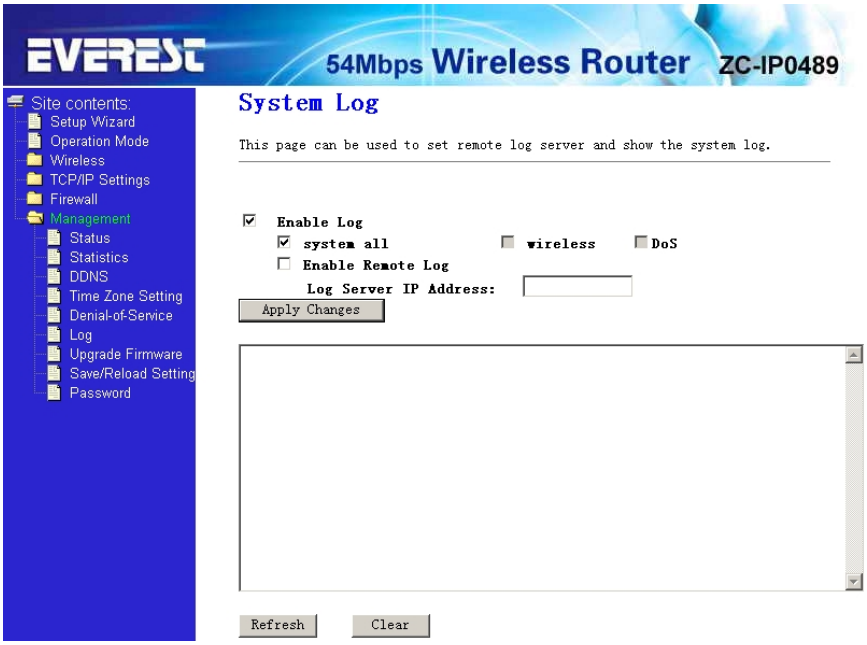
Enable Source IP Blocking: you can input source IP Blocking time

Click apply changes,DOS take effect.



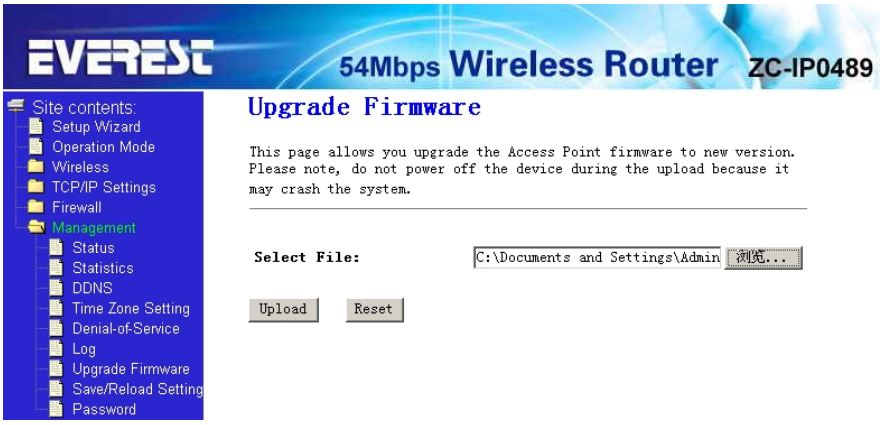
4.5.6 Log

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



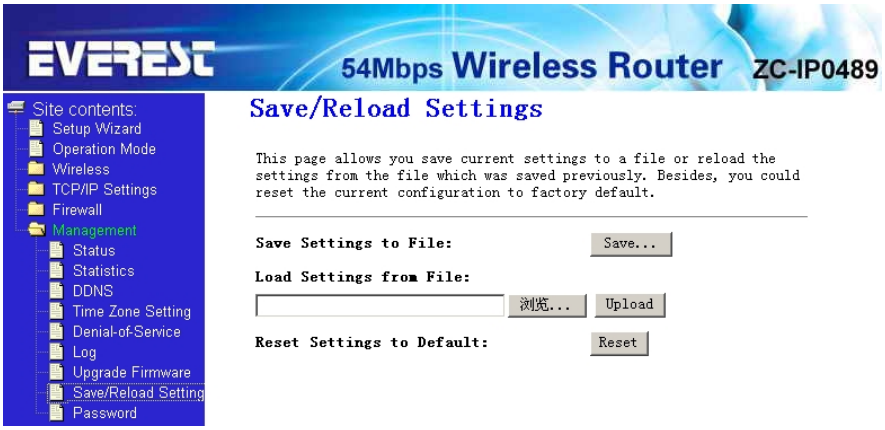
4.5.7 Upgrade Firmware

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



4.5.8 Save/Reload settings

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



4.5.9 Password setup

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

Appendix 1: FAQ

1. **How do I configure the router to access Internet by ADSL users?**
   1) First, configure the ADSL modem configured in RFC1483 bridge model.
   2) Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL modem.
   3) Login to the router, click the “TCP/IP settings” menu on the left of your browser, and click

"WAN Interface" submenu. On the WAN page, select “PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.

4) If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “Manual” for Internet connection mode. Type an appropriate number for Time to avoid wasting paid time. Otherwise, you can select “continous” for Internet connection mode.

2.How do I configure the router to access Internet by Ethernet users?

1) Login to the router, click the “TCP/IP Settings” menu on the left of your browser, and click "LAN Interface" submenu. On the WAN page, select “DHCP” for "Client", finish by clicking “apply changes”.

2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires MAC register, login to the router and click the "TCP/IP Setting" menu link on the left of your browser, and then click "LAN Interface", if your PC’s MAC address is proper MAC address,type your PC’s MAC address will fill in the "Clone MAC Address" field. Or else,The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "apply changes" button. It will take effect after rebooting.

3.I want to use Netmeeting, what do I need to do?

1) If you start Netmeeting as a sponsor, you don’t need to do anything with the router.
2) If you start as a responsor, you need configure Virtual Server or DMZ Host.
3) How to configure Virtual Server: Login to the router, click the “Forwarding” menu on the left of your browser, and click " port foward" submenu. On the "port forward " page, enter “1720” into the blank below the “Service Port”, and your IP address below the IP Address, assuming 192.168.1.25469 for an example, remember to “supply changes”.
4) How to enable DMZ Host: Login to the router, click the “firewall settings” menu on the left of your browser, and click " DMZ" submenu. On the "DMZ" page, click “Enable DMZ” radio and type your IP address into the “DMZ Host IP Address” field, using 192.168.1.25469 as an example, remember to click the "Apply changes” button.

4. The wireless stations cannot connect to the router.

1) Make sure the "Disable Wireless LAN Interface " is not select.
2) Make sure that the wireless stations' SSID accord with the router's SSID.
3) Make sure the wireless stations have right KEY for encryption when the router is encrypted.
4) If the wireless connection is ready, but you can’t access the router, check the IP Address of your wireless stations.

Appendix 2: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b and 802.11g
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Radio Data Rate	54/48/36/24/18/12/9/6/11/5.5/3/2/1Mbps
Power Supply	9V~ 800mA

LEDs	Power, M1, WLAN, 1,2,3,4

Environmental and Physical	
Operating Temp.	0℃~40℃ (32℉~104℉)
Operating Humidity	10% - 95% RH, Non-condensing
Dimensions (W×D×H)	7.9×4.7×1.2 in. (201×120×31.10 mm)

Appendix 3: Glossary

802.11b - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

802.11g - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.

DMZ (**De**m**i**litarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such anternet gaming or videoconferencing.

DNS (**D**omain **N**ame **S**erver) **-** An Internet Service that translates the names of websites into IP addresses.

Domain Name - A descriptive name for an address or group of addresses on the Internet.

DoS (**D**enial **o**f **S**ervice) **-** A hacker attack designed to prevent your computer or network from operating or communicating.

DSL (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.

ISP (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet

MTU (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.

NAT (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

SSID - A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

WEP (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or

128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

Wi-Fi - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

Federal Communication Commission Interference Statement

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

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

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.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.