User’s Guide

Model NO. CP500

Table of Contents

1. Product Introduction

Thank you very much for purchasing **TOTOLINK CP500 WLAN Broadband CPE**. This section will introduce the function and features of this device.

1.1 Overview

CP500 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. The Router network mode also allows much more users to connect to internet. Powered by Passive PoE, CP500 makes the wires deployment more flexible. The outdoor protection design not only can prevent dust, water and lightning, but also can 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

- Supports IEEE802.11n and IEEE802.11a standards on 5G band.
- Supports Bridge/Router networking modes.
- RF power up to 300mw.
- Adjustable transmission power.
- Internal dual-polarization 14dBi antennas.
- Water-proof housing (IP65).
- Multi-frequency channels selectable.
- ACK timeout adjustable.
- Offers DHCP Leases/Route/Port Forward status display.
- Supports Ping Watchdog/Telnet Server/SSH Server/ Web Server/NTP Client.
- SNMP Agent makes the network more stable.
- 4LED signal strength indications.
- Supports MAC based ACL and MAC filtering.
- Supports 64/128 bit WEP encryption and WPA-PSK, WPA2-PSK security.
- Firewall/Traffic shaping.
- Link/Quality monitor/detection tools.
- Supports passive PoE.
- Lightning protection design.
- Supports Windows 8/ 7/ XP/ Vista, Linux and Mac OS.

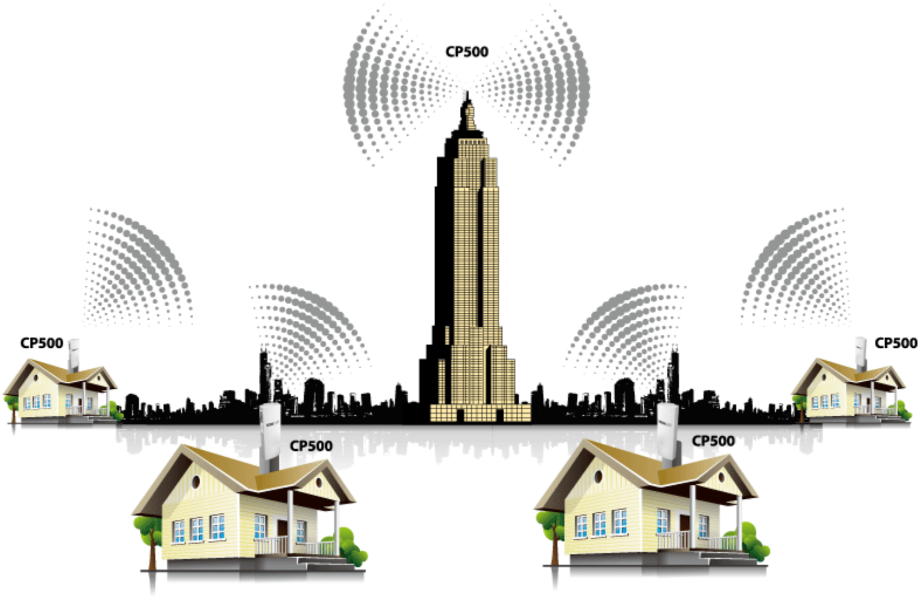
2. Hardware Installation

2.1 Typical Application

2.1.1 Point to Point

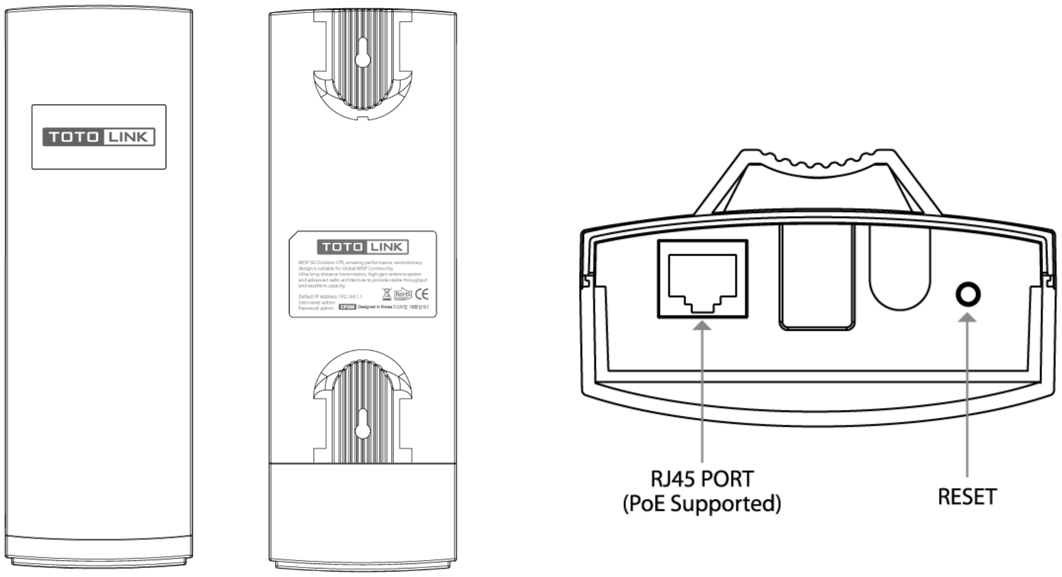
CP500
CP500

2.1.2 Point to Multi-Points



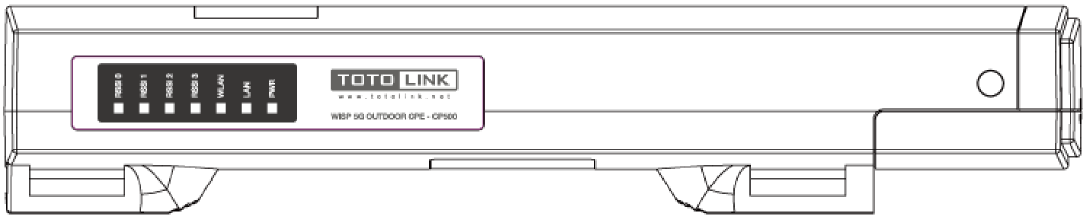
2.2 Appearance

2.2.1 Front and Rear Panel



Port and Button	Description
LAN	This port is used to connect PoE
Reset	Press this button, the device will restore to default factory settings.

2.2.2 LED Description



LED Indicators	Description
POWER	The POWER LED will light red when properly connected to a power source.
LAN	This Ethernet LED will light solid green when an active Ethernet connection is made to the LAN port and flash when there is activity.
WLAN	This WLAN LED flash green when the wireless function working.
Signal	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 CP500 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:

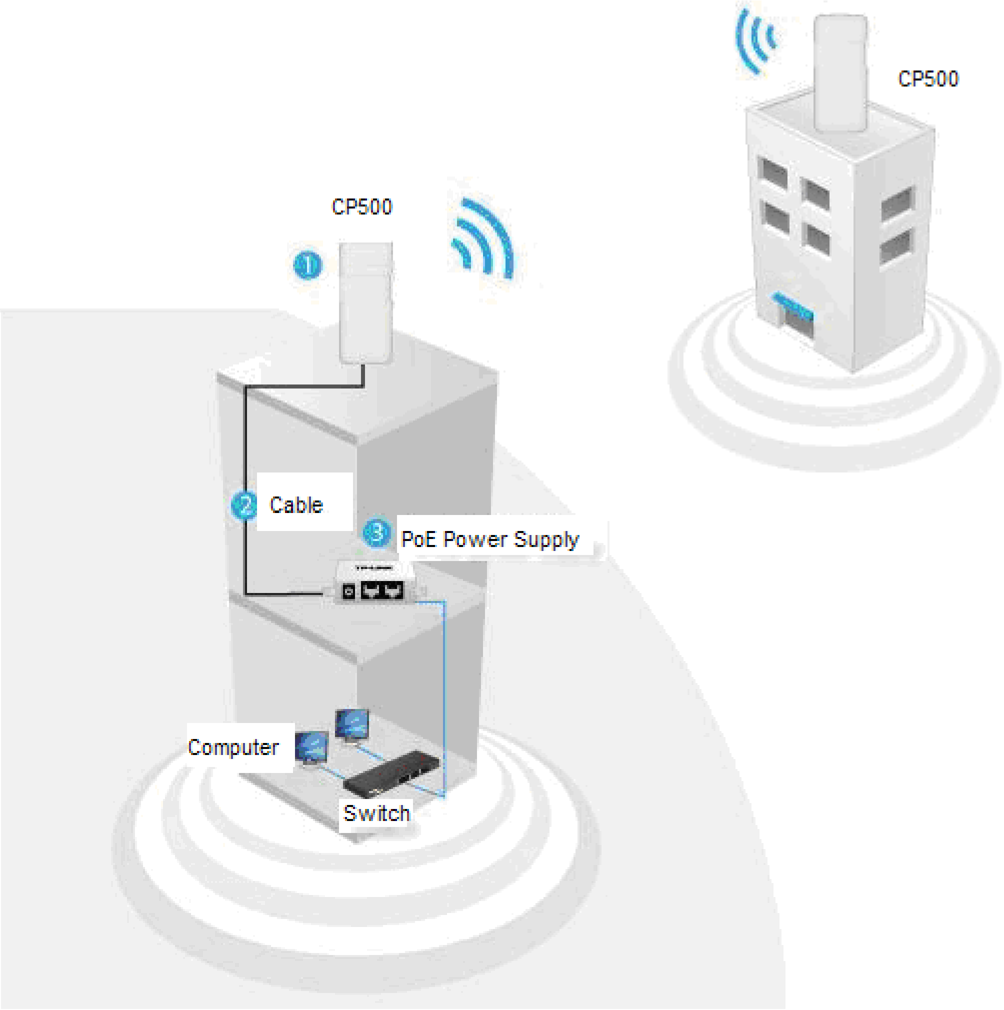


Figure 2.1 CPE Connection Graph

2.4 Set up the Computer

The default IP address of the CP500 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.

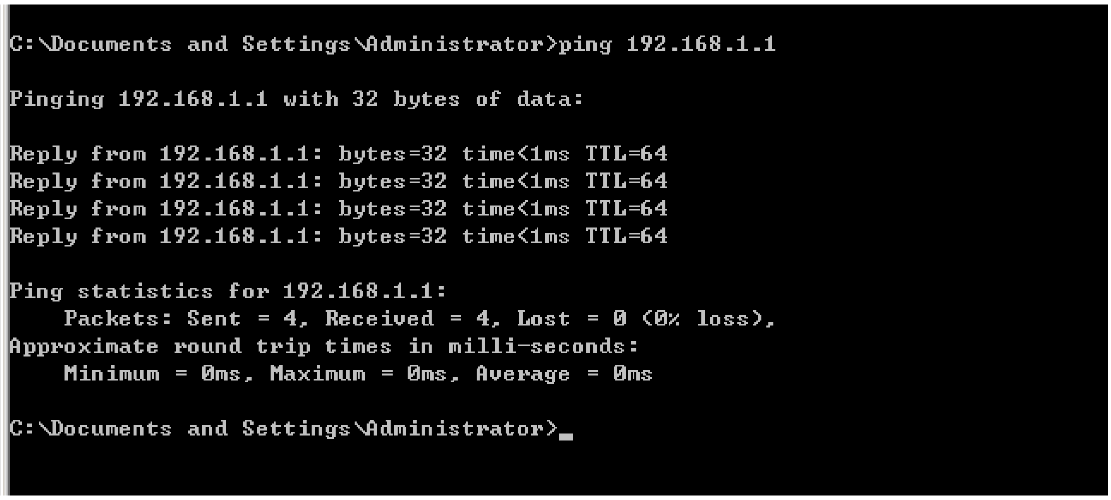
◆ **Configure the IP address manually**

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.

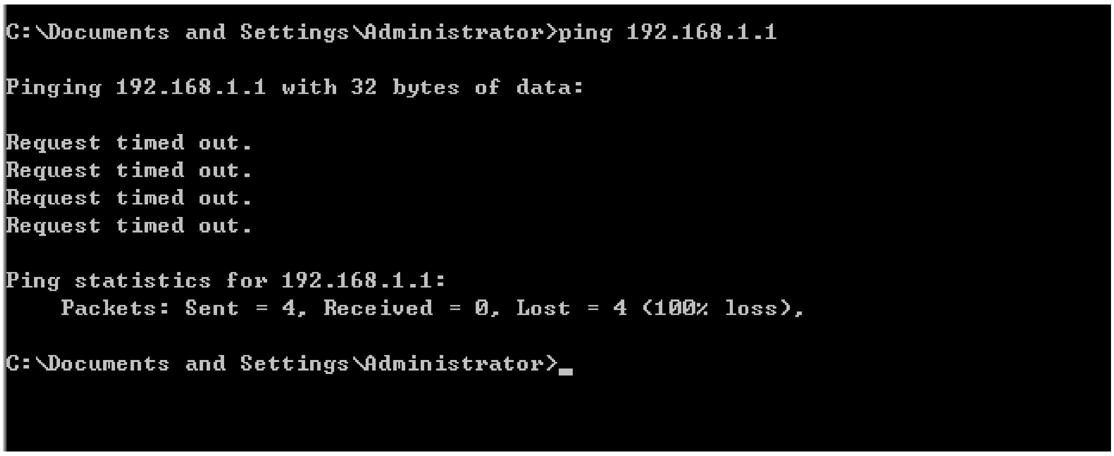
Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the PoE. Open a command prompt, and type in **ping 192.168.1.1**, then press **Enter.**



```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

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.



```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>_
```

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?**

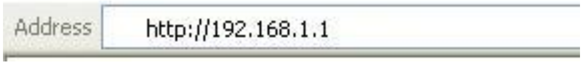
Since the CPE's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

3. Configuration of Web Utility

After successful connection and setup, you can configure the Web interface of the WLAN bandwidth CPE now.

3.1 Login the Web Interface

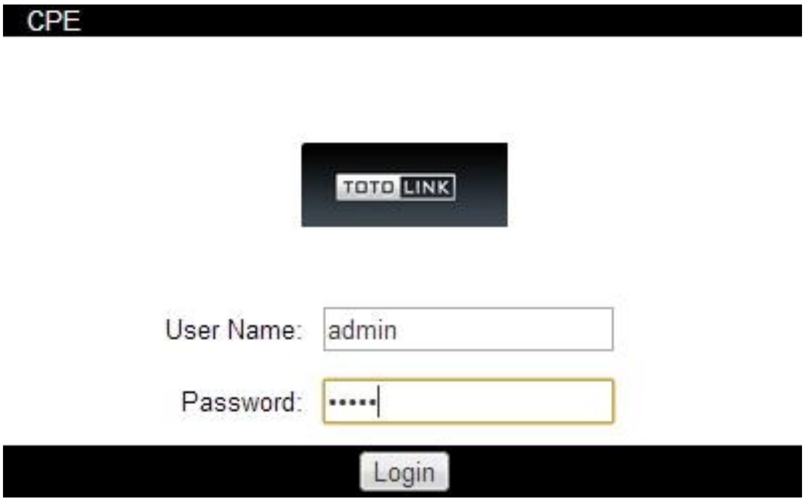
Access the Web interface of the CPE by typing 192.168.1.1 in the address field of Web Browser. Then press **Enter** key.



Address http://192.168.1.1

Figure 3.1 IP address

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



User Name: admin

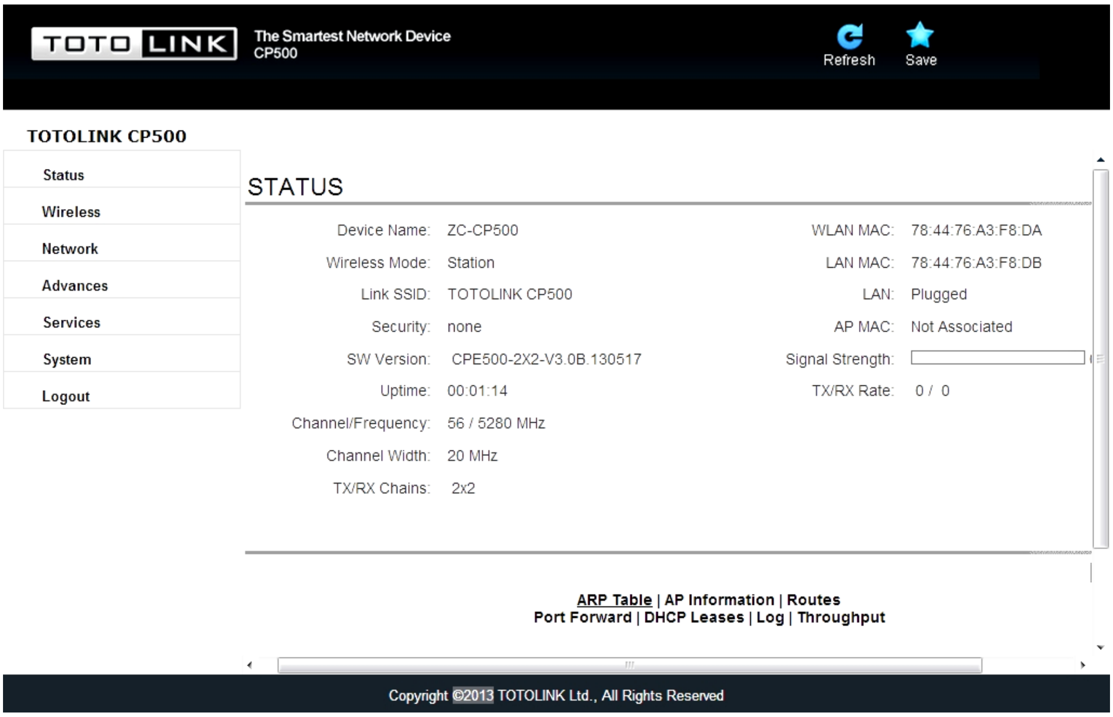
Password: •••••

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:


TOTO LINK
The Smartest Network Device
CP500
Refresh
Save
TOTOLINK CP500
Status
Wireless
Network
Advances
Services
System
Logout

STATUS

Device Name:	ZC-CP500	WLAN MAC:	78:44:76:A3:F8:DA
Wireless Mode:	Station	LAN MAC:	78:44:76:A3:F8:DB
Link SSID:	TOTOLINK CP500	LAN:	Plugged
Security:	none	AP MAC:	Not Associated
SW Version:	CPE500-2X2-V3.0B.130517	Signal Strength:	
Uptime:	00:01:14	TX/RX Rate:	0 / 0
Channel/Frequency:	56 / 5280 MHz		
Channel Width:	20 MHz		
TX/RX Chains:	2x2		

ARP Table | AP Information | Routes
Port Forward | DHCP Leases | Log | Throughput
Copyright ©2013 TOTOLINK Ltd., All Rights Reserved

Figure 3.3 Login Interface

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

Status: This page displays a summary of wireless status information, current values of basic configuration settings (depending on operating mode), network settings and information, traffic statistics of all the interfaces.

Wireless: This parameter contains the controls for a wireless network configuration, including basic settings that define operating mode, data rate and security options.

Network: You can configure the network mode on this parameter and configure network basic settings.

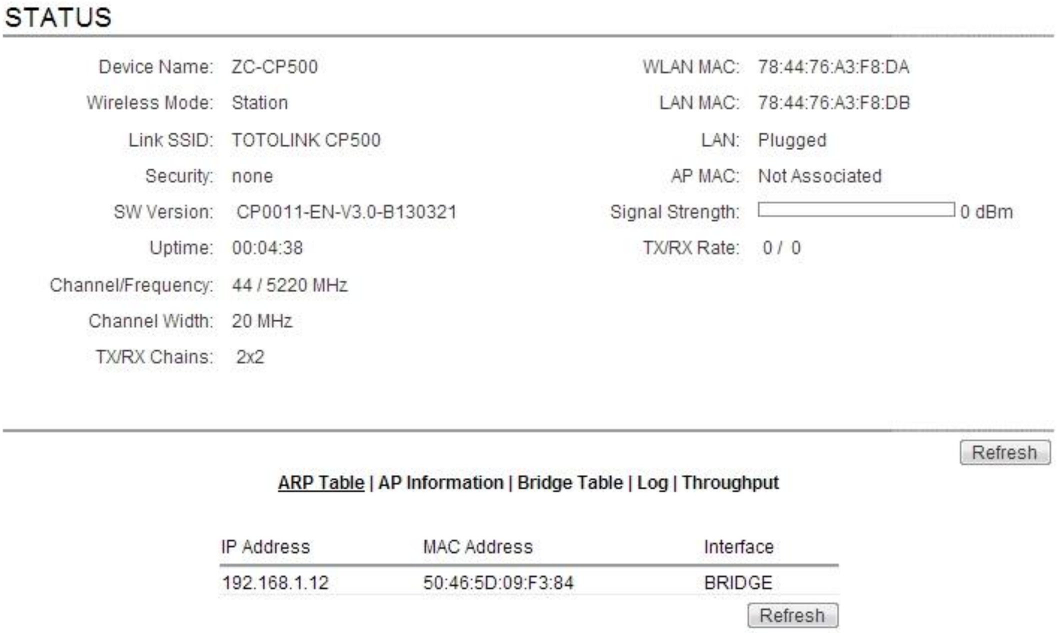
Advances: This page covers many advanced settings including Wireless, Ethernet, LED Thresholds and Traffic Shaping.

Services: This parameter allows you to configure the services supported by this CPE.

System: You can configure the system maintenance routines on this interface, dedicated for administrator account management, configuration backup and firmware upgrade.

Logout: This section allows you to logout immediately.

3.2 STATUS



STATUS

Device Name:	ZC-CP500	WLAN MAC:	78:44:76:A3:F8:DA
Wireless Mode:	Station	LAN MAC:	78:44:76:A3:F8:DB
Link SSID:	TOTOLINK CP500	LAN:	Plugged
Security:	none	AP MAC:	Not Associated
SW Version:	CP0011-EN-V3.0-B130321	Signal Strength:	0 dBm
Uptime:	00:04:38	TX/RX Rate:	0 / 0
Channel/Frequency:	44 / 5220 MHz		
Channel Width:	20 MHz		
TX/RX Chains:	2x2		

Refresh
ARP Table | AP Information | Bridge Table | Log | Throughput

IP Address	MAC Address	Interface
192.168.1.12	50:46:5D:09:F3:84	BRIDGE

Figure 3.4 Status of CP500

Device Name: displays the customizable name (ID). Device Name (Host Name) will be represented in registration screens of the CPE Operating Systems and discovery tools.

Wireless Mode: shows the radio interface operating mode. This device supports infrastructure wireless networking solution. AP (or AP+WDS) and Station (or Station +WDS) operating modes can be set depending on the network topology requirements.

Link SSID: is the name of the 802.11 Service Set (established by the “AP” or the “Station” are connected).

Security: This is the current security setting. "None" value is displayed if wireless security is disabled. WPA or WPA2 values are displayed if the corresponding wireless security method is used. More information is provided in the ***WIRELESS*** section.

SW Version: the current software version.

Uptime: This is the total running time the device has been running since last power up (reboot) or software upgrade. The time is expressed in days, hours, minutes and seconds.

Channel/Frequency: This is the operating frequency of the 802.11 Service Set (hosted by AP) the client is connected to. 802.11 Channel number corresponds to the operating frequency. More information about the supported channels is provided in the ***WIRELESS*** section. This device uses the radio frequency specified to transmit and receive data.

Channel Width: This is spectral width of the radio channel used by powered device.CP500 supports 20 or 40MHz channel spectrum widths. In Station (or Station +WDS) mode, 20/40MHz is the value by default.

TX/RX Chains: displays the number of independent spatial data streams that this device is transmitting / receiving simultaneously within one spectral channel of bandwidth.

WLAN MAC: shows the MAC address of the CP500's WLAN (Wireless) interface.

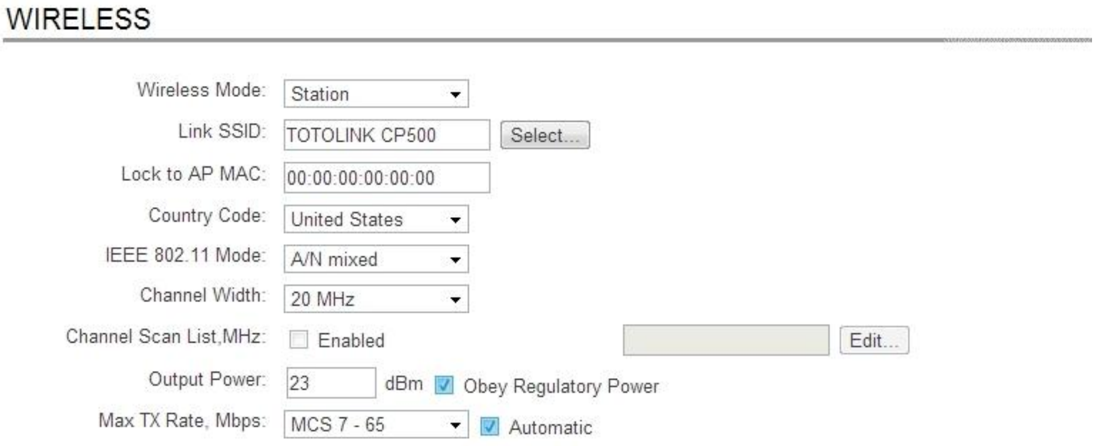
LAN MAC: displays the MAC address of the CP500's LAN (Ethernet) interface.

LAN: indicates the current status of the Ethernet port connection. This can alert system operator-technician that LAN cable is not plugged into device and there is no active Ethernet connection.

AP MAC: displays the MAC address of the Access Point where the device has associated while operating in Station mode (or Station +WDS). It is the MAC address of CP500's wireless interface itself if operating in Access Point mode. AP MAC is used as Basic Service Set Identifier (BSSID) in infrastructure type wireless networks.

3.3 WIRELESS

3.3.1 Wireless



WIRELESS

Wireless Mode: Station

Link SSID: TOTOLINK CP500 Select...

Lock to AP MAC: 00:00:00:00:00:00

Country Code: United States

IEEE 802.11 Mode: A/N mixed

Channel Width: 20 MHz

Channel Scan List,MHz: □ Enabled Edit...

Output Power: 23 dBm ☑ Obey Regulatory Power

Max TX Rate, Mbps: MCS 7 - 65 ☑ Automatic

Figure 3.5 Wireless Settings

Wireless Mode: specifies the operating mode of the device. The mode depends on the network topology requirements. There are 4 operating modes supported in CP500 software.

1. **Station:** This is a client mode, which can connect to an AP. It is common for a bridging application to an AP. In Station mode device acts as the Subscriber Station while connecting to the AP which is primary defined by the SSID and forwarding all the traffic to/from the network devices connected to the Ethernet interface.

2. **Station WDS**: WDS stands for Wireless Distribution System.

3. **Access Point**: This is an 802.11 Access Point.

4. **Access Point WDS**: WDS allows you to bridge wireless traffic between devices which are operating in AP mode. AP is usually connected to a wired network (Ethernet LAN) allowing wireless connection to the wired network. By connecting AP to one another in an Extended Service Set using the WDS, distant Ethernets can be bridged into a single LAN.

> ***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.*

Link SSID: Service Set Identifier used to identify your 802.11 wireless LAN should be specified while operating in *Access Point* or *Access Point WDS* mode. All the client devices within range will receive broadcast messages from the access point advertising this SSID.

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

IEEE 802.11 Mode: This is the radio standard used for operation of your CP500 powered device. By default, it is A/N Mixed.

Channel Width:

20MHz – is the standard channel spectrum width (selected by default).

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

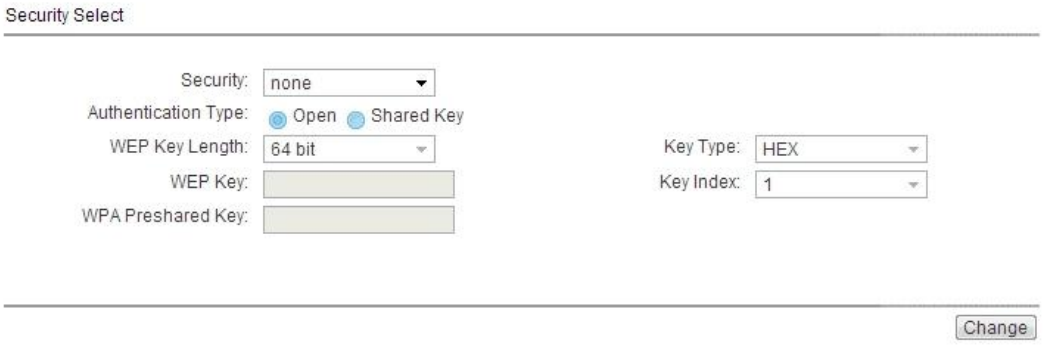
Channel Scan List, MHz: select the wireless channel while operating in AP mode. Multiple frequency channels are available to avoid interference between nearby access points. The channel list varies depending on the selected country code, IEEE 802.11 mode and Channel Spectrum Width and Channel Shifting option.

Output Power: This will configure the maximum average transmit output power (in dBm) of the wireless device. The output power at which wireless module transmits data can be specified using the slider. When entering output power value manually, the slider position will change according to the entered value.

Max TX Rate, Mbps: This defines the data rate (in Mbps) at which the device should transmit wireless packets. If the **Best (automatic)** option is selected, then the *rate algorithm* will select the best data rate depending on the link quality conditions. You can fix a specific data rate between MCS 0 and MCS 7 (or MCS15 for 2x2 chains devices) also. Use **Best (automatic)** option if you are having trouble getting connected or losing data at a higher rate. In this case the lower data rates will be used by device automatically. If you select 20MHz Channel Spectrum width the maximum data rate is MCS7 (65Mbps) or MCS15 (150Mbps). If you select 40MHz Channel Spectrum width the maximum data rate is MCS7 (150Mbps) or MCS15 (300Mbps).

3.3.2 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).



Security Select

Security: none

Authentication Type: ● Open ○ Shared Key

WEP Key Length: 64 bit

Key Type: HEX

WEP Key:

Key Index: 1

WPA Preshared Key:

Figure 3.6 Wireless Security Select

Security: you can select None, WEP, WPA, WPA (TKIP), WPA (AES), WPA2, WPA2 (TKIP) and WPA2 (AES).

Authentication Type: you can choose to share this wireless network with others by Sharedkey or keep it open.

WEP: Wired Equivalent Protocol.

WPA: (Wi-Fi Protected Access) WPA is an intermediate solution for the security issues. It uses Temporal Key Integrity Protocol (TKIP) to replace WEP.

WPA-AES: enable WPA security mode with AES support only. Wi-Fi Protected Access - WPA (IEEE 802.11i/D3.0) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

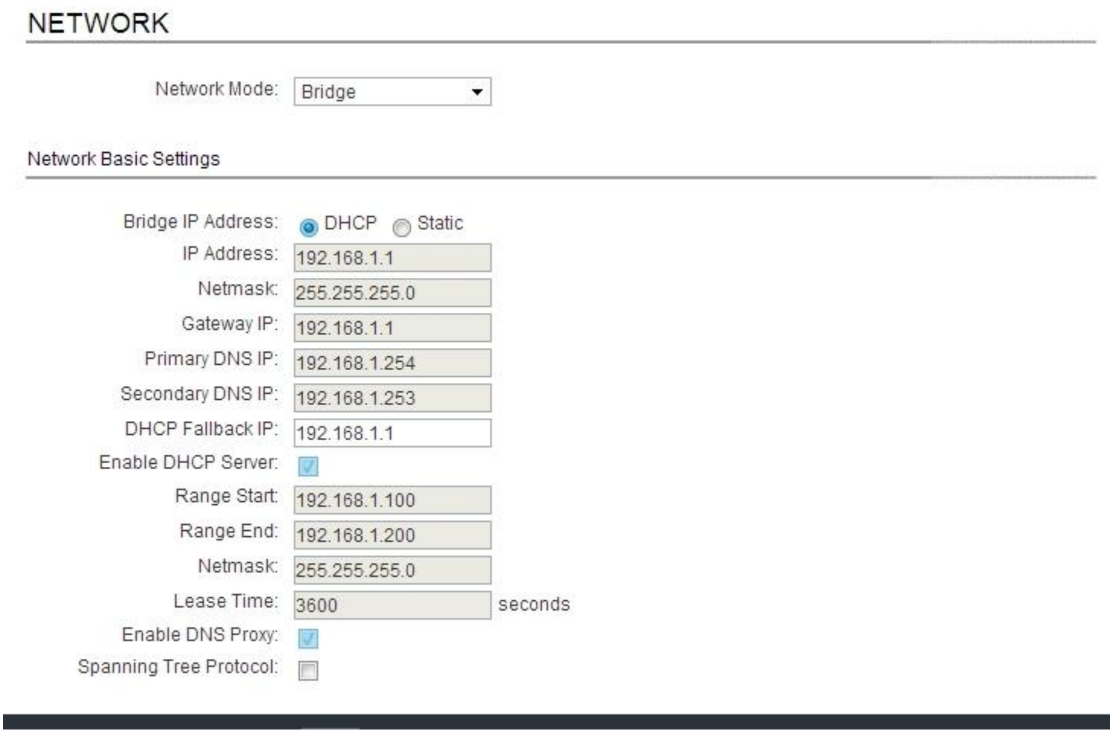
WPA2-AES: enable WPA2 security mode with AES support only. Wi-Fi Protected Access 2 - WPA2 (IEEE 802.11i) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

3.4 NETWORK

CP500 supports two network modes: Bridge and Router. Please choose one according to your needs and provide the required information.

3.4.1 Bridge Mode

Since this CPE only has one LAN port, you can access this CPE by two methods: connect to bridge mode by cable, or connect to it wirelessly. If you choose Bridge mode, please provide following information:



NETWORK

Network Mode: Bridge

Network Basic Settings

Bridge IP Address: ● DHCP ○ Static
IP Address: 192.168.1.1
Netmask: 255.255.255.0
Gateway IP: 192.168.1.1
Primary DNS IP: 192.168.1.254
Secondary DNS IP: 192.168.1.253
DHCP Fallback IP: 192.168.1.1
Enable DHCP Server: ☑
Range Start: 192.168.1.100
Range End: 192.168.1.200
Netmask: 255.255.255.0
Lease Time: 3600 seconds
Enable DNS Proxy: ☑
Spanning Tree Protocol: □

Figure 3.7 Bridge Mode Network Settings

Bridge IP Address: there are two modes supported.

DHCP: choose this option to obtain the IP address, Gateway and DNS address dynamically from DHCP server.

Static: set the Static IP address by yourself.

IP Address: settings should consist with the address space of the network segment where CP500 device located. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space.

Netmask: 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 192.0.0.x to 223.255.255.x.

Gateway IP: is the IP address of the host router which 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. CP500 will direct all the packets to the gateway if the destination host is not within the local network. (Applicable for Static mode only)

Primary DNS IP: server IP is mandatory. It is used by the *DNS Proxy* and for the device management purpose.

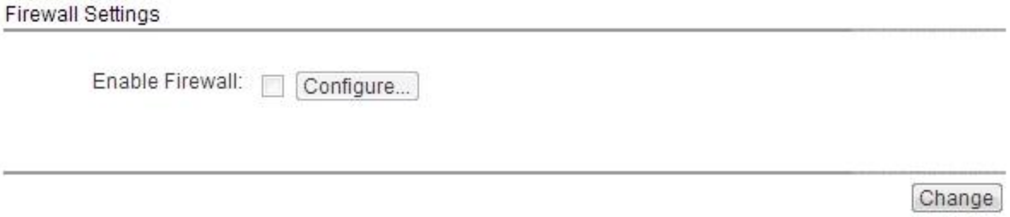
Secondary DNS IP: server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

DHCP Fallback IP: In case the external network interface of the router is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid

DHCP server, it will fall back to the static IP address listed here.

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

Firewall Settings: click Configure button to configure firewall parameters.



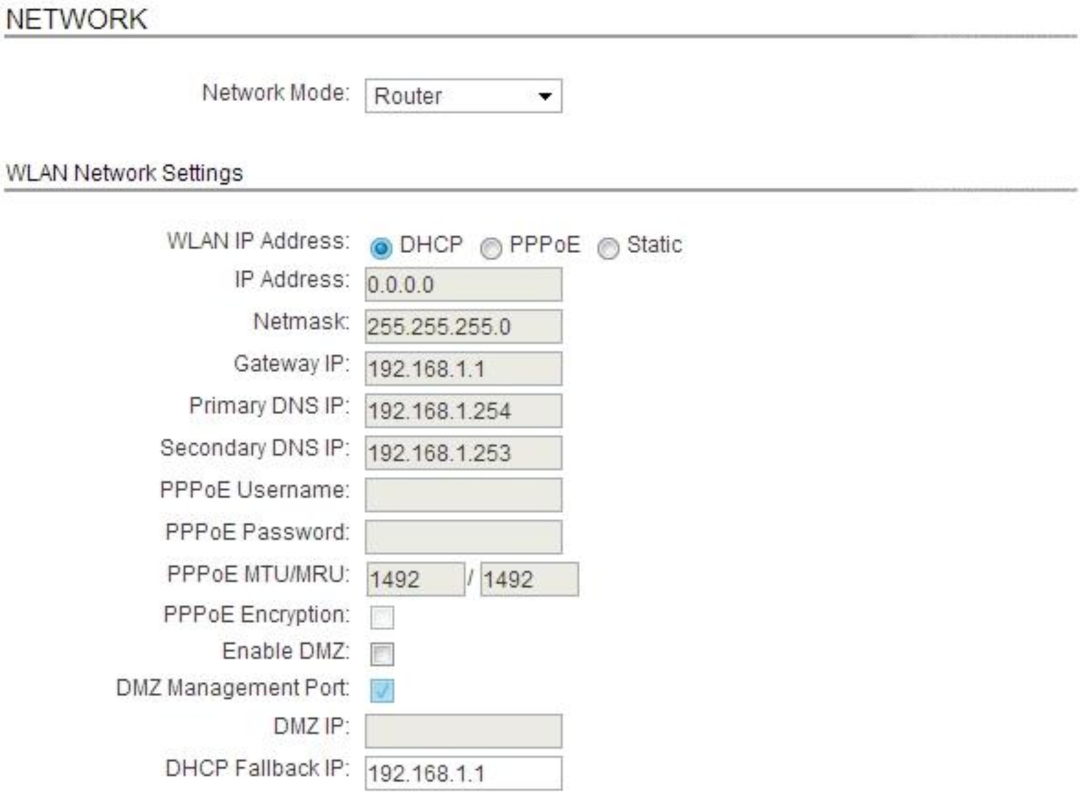
Firewall Settings

Enable Firewall: □

Figure 3.8 Firewall Settings

3.4.2 Router Mode

If you choose this mode, it means you use this CPE as a router. And you need to finish the following settings, detailed information please refer to **Bridge Mode.**



NETWORK

Network Mode: Router

WLAN Network Settings

WLAN IP Address: ● DHCP ○ PPPoE ○ Static

IP Address: 0.0.0.0

Netmask: 255.255.255.0

Gateway IP: 192.168.1.1

Primary DNS IP: 192.168.1.254

Secondary DNS IP: 192.168.1.253

PPPoE Username:

PPPoE Password:

PPPoE MTU/MRU: 1492 / 1492

PPPoE Encryption: □

Enable DMZ: □

DMZ Management Port: ☑

DMZ IP:

DHCP Fallback IP: 192.168.1.1

Figure 3.9 Router WLAN Settings

IP Address: is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purpose.

Netmask: is the network address space identifier for the particular IP.

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on it's local network while CP500 powered device is operating in *AP/AP WDS* wireless mode and in the contrariwise direction in "Station/Station WDS" mode.

Enable DHCP Server: enable this function to get IP address dynamically.

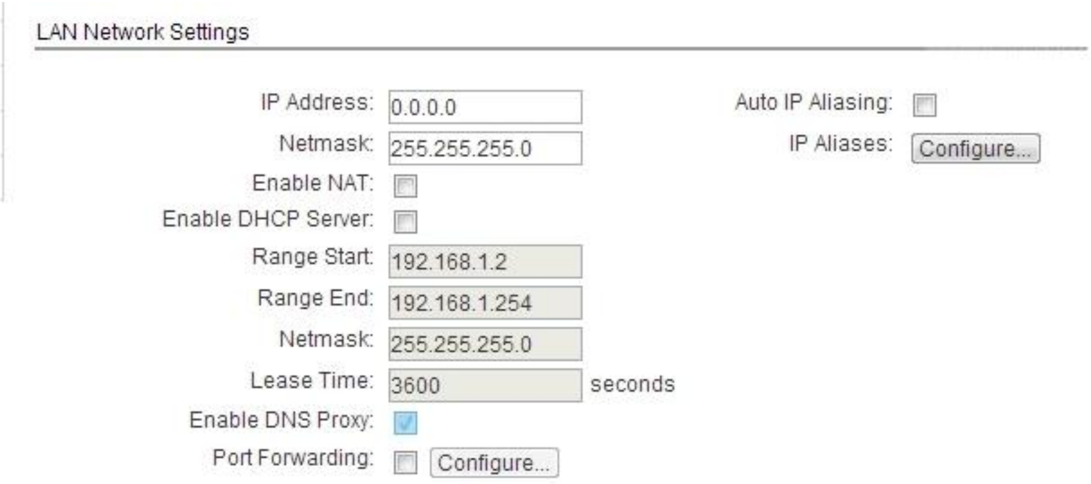
Range Start/Range End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.

Netmask: 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 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

Enable DNS Proxy: The DNS Proxy forwards the Domain Name System requests from the hosts which reside in the internal network to the DNS server while CP500 powered device is in operating in *Router* mode. Valid *Primary DNS Server IP* needs to be specified for *DNS Proxy* functionality. Internal network interface IP of CP500 powered device should be specified as the DNS server in the host configuration in order *DNS Proxy* should be able to get the DNS requests and translate domain names to IP addresses afterwards.

Port Forwarding: Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for number of applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port.



LAN Network Settings

IP Address: 0.0.0.0

Netmask: 255.255.255.0

Enable NAT: □

Enable DHCP Server: □

Range Start: 192.168.1.2

Range End: 192.168.1.254

Netmask: 255.255.255.0

Lease Time: 3600 seconds

Enable DNS Proxy: ☑

Port Forwarding: □ Configure...

Auto IP Aliasing: □

IP Aliases: Configure...

Figure 3.10 Router LAN Settings

LAN IP Address: CP500 supports three methods.

PPPoE Username: if choose PPPoE, you need to provide the username to connect to the server (must match the configured on the PPPoE server)

PPPoE Password: password to connect to the server (must match the configured on the PPPoE server).

PPPoE MTU/MRU: the size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP tunnel; (MTU/MRU default value: 1492).

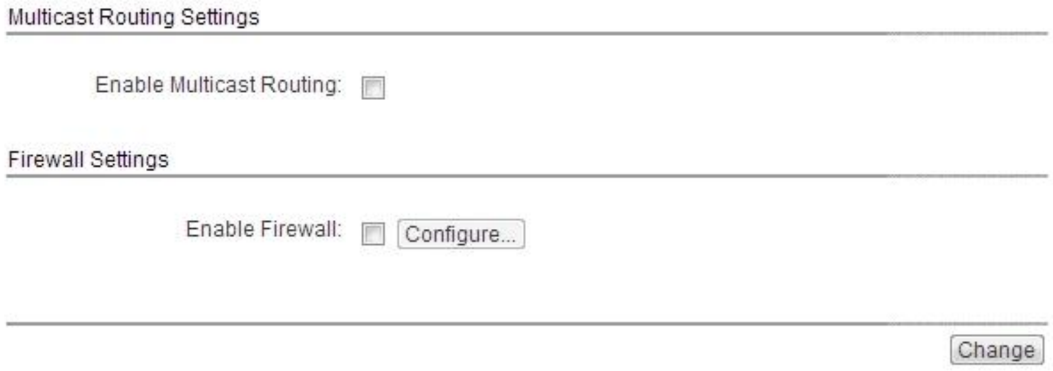
PPPoE Encryption: enable the MEEP Cryptography.

Enable DMZ: The Demilitarized zone (DMZ) 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.

DMZ Management Port: Web Management Port for CP500 device (TCP/IP port 80 by default) will be used for the host device if *DMZ Management Port* option is enabled.

DMZ IP: connected to the internal network host, specified with the DMZ IP will be accessible from the external network.

Multicast Routing Settings: you can choose to enable this function. With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts which need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however CP500 provides the multicast traffic pass-through functionality.



Multicast Routing Settings

Enable Multicast Routing: □

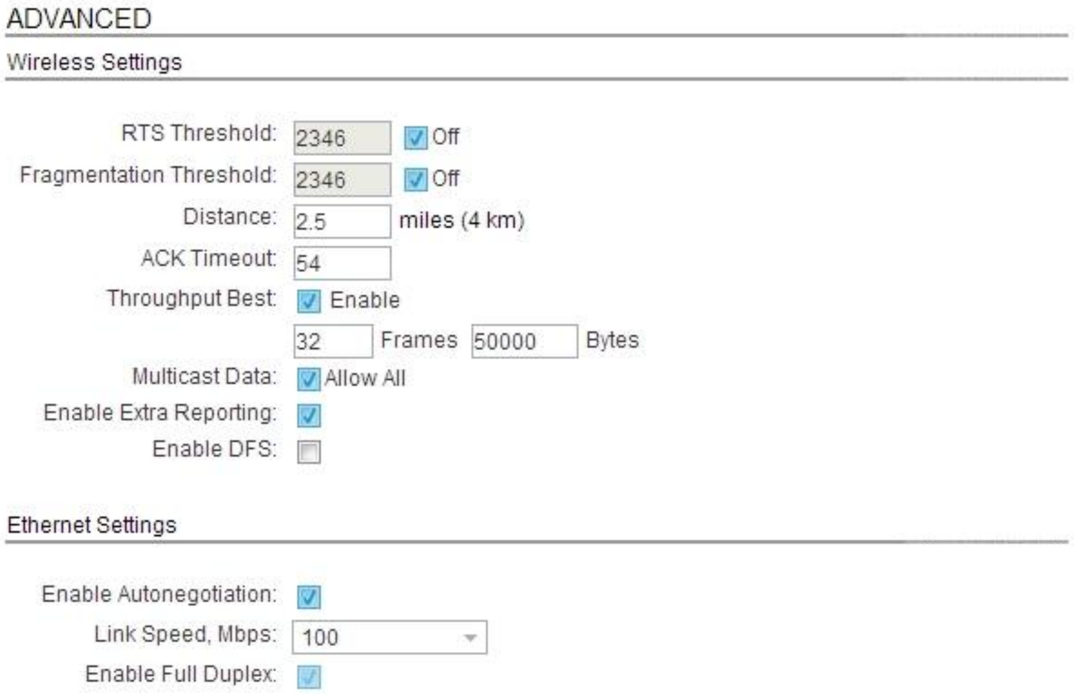
Firewall Settings

Enable Firewall: □

Figure 3.11 Multicast Routing Settings

3.5 ADVANCED

3.5.1 Wireless Settings



ADVANCED

Wireless Settings

RTS Threshold: 2346 ☑ Off

Fragmentation Threshold: 2346 ☑ Off

Distance: 2.5 miles (4 km)

ACK Timeout: 54

Throughput Best: ☑ Enable

32 Frames 50000 Bytes

Multicast Data: ☑ Allow All

Enable Extra Reporting: ☑

Enable DFS: □

Ethernet Settings

Enable Autonegotiation: ☑

Link Speed, Mbps: 100

Enable Full Duplex: ☑

Figure 3.12 Wireless Settings

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2346bytes, or word “off”. The default value is 2346 which means that RTS is disabled.

Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word “off”. Setting the *Fragmentation Threshold* too low may result in poor network performance.

Distance: specify the distance value in miles (or kilometers) using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout: specify the *ACK Timeout*. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set *timeout* it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the *timeout* is set too short or too long, it will result poor connection and throughput performance.

Throughput Best: A part of the 802.11n standard (or draft-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.

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

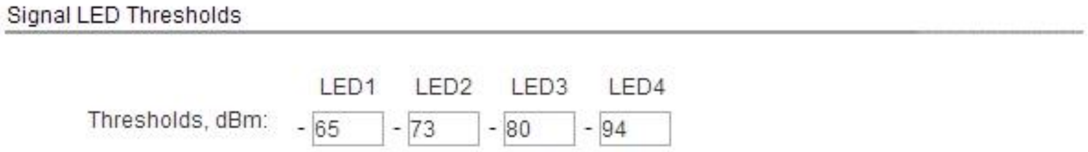
Bytes--- determines the size (in Bytes) of the larger frame.

Multicast Data: This option allows all the Multicast packet pass-through functionality. By default this option is disabled.

Enable Extra Reporting: this feature will report additional information (i.e. Host Name) in the 802.11 management frames. This information is commonly used for system identification and status reporting in discovery utilities and Router operating systems.

Enable DFS: *DFS* is the part of the IEEE 802.11h wireless standard. *Enable DFS* option allows to enable/disable DFS support (applicable for M5 series only). DFS may be mandatory in some regulatory domains and should be tuned according to the regulations of the selected country. Please consult compliance guide and official regulations authorities for further explanation of compliance requirements for the country where CP500 based device is installed.

3.5.2 Signal LED Thresholds



Signal LED Thresholds

	LED1	LED2	LED3	LED4
Thresholds, dBm:	- 65	- 73	- 80	- 94

Figure 3.13 Signal LED Thresholds

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

LED 1 (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -94dBm.

LED 2 (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -80dBm.

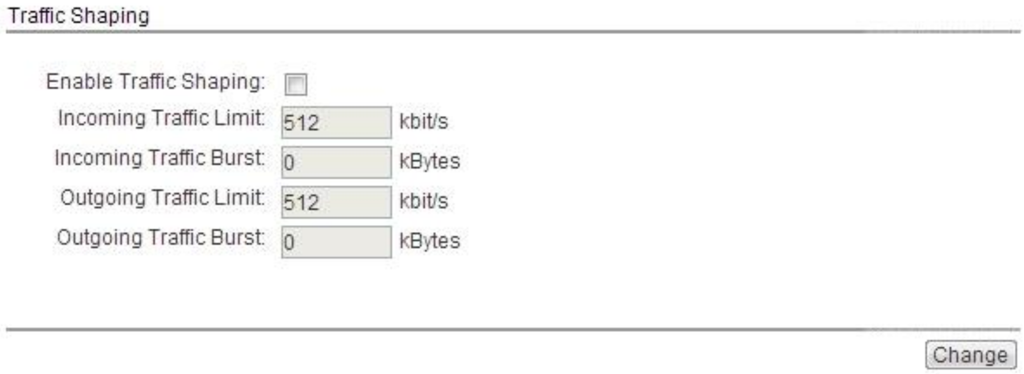
LED 3 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -73dBm.

LED 4 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -65dBm.

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.

Note: *sign "-" character should not be used for the Signal Strength value specification.*

3.5.3 Traffic Shaping



Traffic Shaping

Enable Traffic Shaping: ☐
Incoming Traffic Limit: 512 kbit/s
Incoming Traffic Burst: 0 kBytes
Outgoing Traffic Limit: 512 kbit/s
Outgoing Traffic Burst: 0 kBytes

Figure 3.14 Traffic Shaping

Enable Traffic Shaping: enable this function allows you to set the incoming/outgoing transmission data rate by yourself.

Incoming Traffic Limit: set the data rate limit for incoming traffic. By default it is 512kbit/s.

Incoming Traffic Burst: set the data rate burst for incoming traffic. By default it is 0kbit/s.

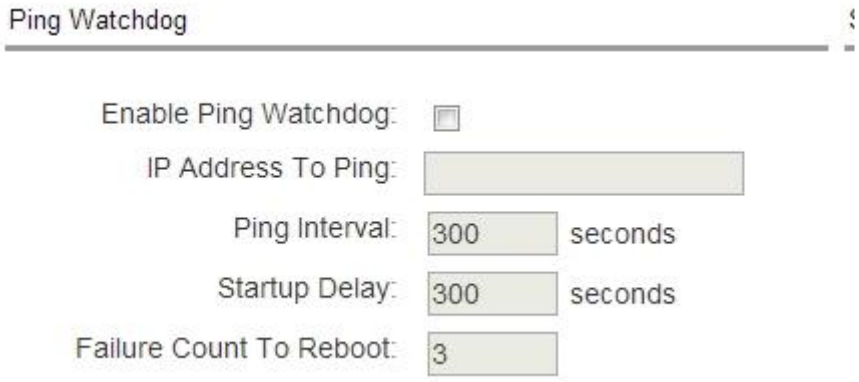
Outgoing Traffic Limit: set the data rate limit for outgoing traffic. By default it is 512kbit/s.

Outgoing Traffic Burst: set the data rate burst for outgoing traffic. By default it is 0kbit/s.

3.6 SERVICES

3.6.1 Ping Watchdog

The ping watchdog sets CP500 device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the device will automatically reboot. This option creates a kind of "fail-proof" mechanism.



Ping Watchdog

Enable Ping Watchdog: ☐
IP Address To Ping:
Ping Interval: 300 seconds
Startup Delay: 300 seconds
Failure Count To Reboot: 3

Figure 3.15 Ping Watchdog

Enable Ping Watchdog: control will enable Ping Watchdog Tool.

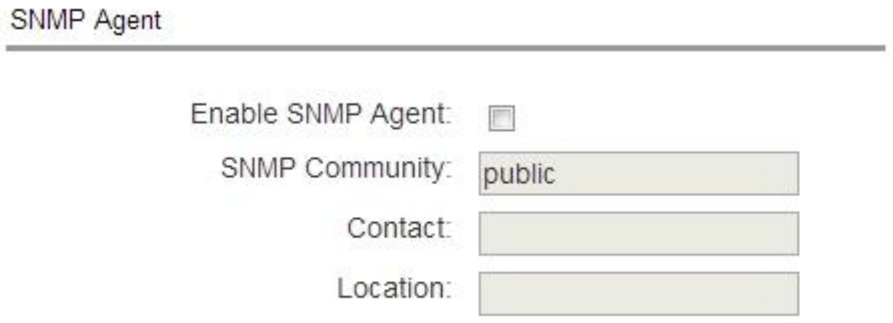
IP Address To Ping: specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

Ping Interval: specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. The default value is 300 seconds.

Startup Delay: specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The default value is 300 seconds. The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted.

Failure Count To Reboot: specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device. The default value is 3.

3.6.2 SNMP Agent



SNMP Agent

Enable SNMP Agent: □

SNMP Community: public

Contact:

Location:

Figure 3.16 SNMP Agent

Enable SNMP Agent: control will enable SNMP Agent.

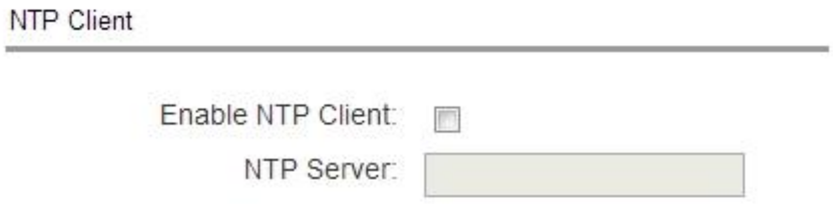
SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access. CP500 supports SNMP v1. The default SNMP Community is *public*.

Contact: specify the identity or the contact who should be contacted in case emergency situations arise.

Location: specify the physical location of the device.

3.6.3 NTP Client

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the CP500 system time. *System Time* is reported next to the every *System Log* entry while registering system events if *Log* option is enabled.



NTP Client

Enable NTP Client: □

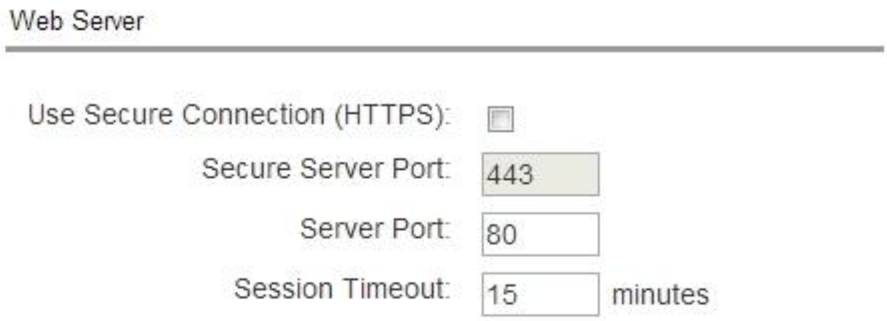
NTP Server:

Figure 3.17 NTP Client

Enable NTP Client: control will enable NTP client.

NTP Server: specify the IP address or domain name of the NTP Server.

3.6.4 Web Server



Web Server

Use Secure Connection (HTTPS): □

Secure Server Port: 443

Server Port: 80

Session Timeout: 15 minutes

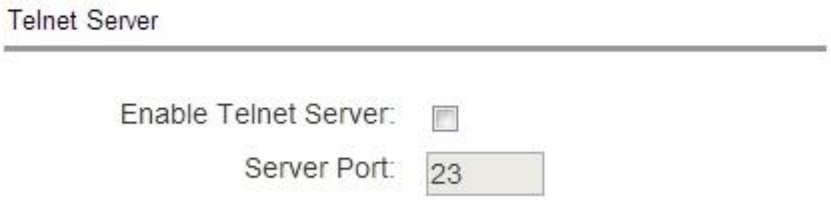
Figure 3.18 Web Server

Use Secure Connection (HTTPS): If checked Web server will use secure HTTPS mode. HTTPS mode is unchecked by default.

Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.

Server Port: Web Server TCP/IP port setting while using HTTP mode.

3.6.5 Telnet Server



Telnet Server

Enable Telnet Server: □

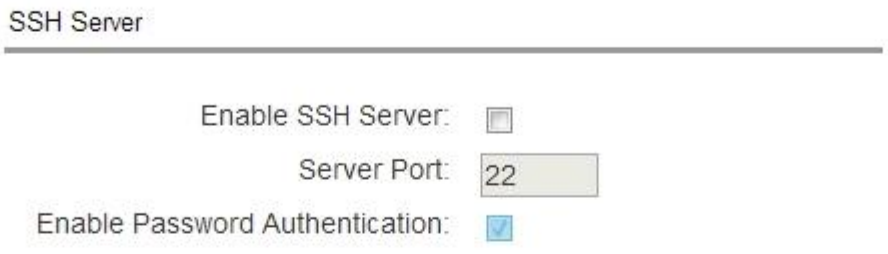
Server Port: 23

Figure 3.19 Telnet Server

Enable Telnet Server: you can enable this function to access telnet server.

Server Port: type in the telnet server port here. By default, it is 23.

3.6.6 SSH Server



SSH Server

Enable SSH Server: ☐

Server Port: 22

Enable Password Authentication: ☑

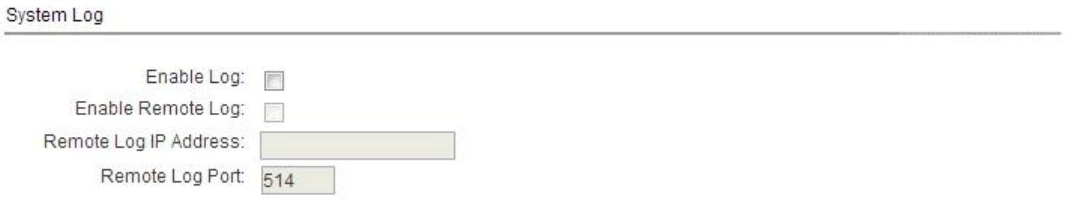
Figure 3.20 SSH Server

Enable SSH Server: SSH means Secure Share. It is the most secure protocol specially used for remote login and other web service.

Server Port: type in the SSH server port here. By default, it is 22.

Enable Password Authentication: by default, it is checked.

3.6.7 System Log



System Log

Enable Log: ☐

Enable Remote Log: ☐

Remote Log IP Address:

Remote Log Port: 514

Figure 3.21 System Log

Enable Log: This option enables the registration routine of the *System Log* messages. By default it is disabled.

Enable Remote Log: enables the *System Log* remote sending function while *System log* messages are sent to a remote server specified by the *Remote Log IP Address* and *Remote Log Port*.

Remote Log IP Address is the host IP address where *System Log* messages should be sent. Remote host should be configured properly to receive *System Log* protocol messages.

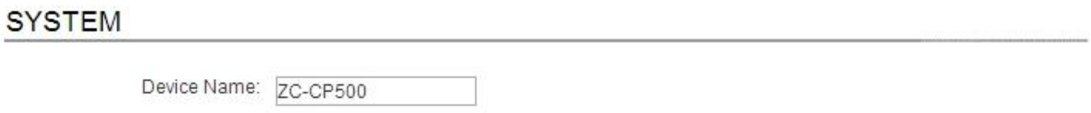
Remote Log Port: is the TCP/IP port of the host *System Log* messages should be sent. "514" is the default port for the commonly used system message logging utilities.

3.7 SYSTEM

The System Page contains Administrative options. This page enables administrator to reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator’s credentials.

3.7.1 Device name

In this section you can modify the device name.

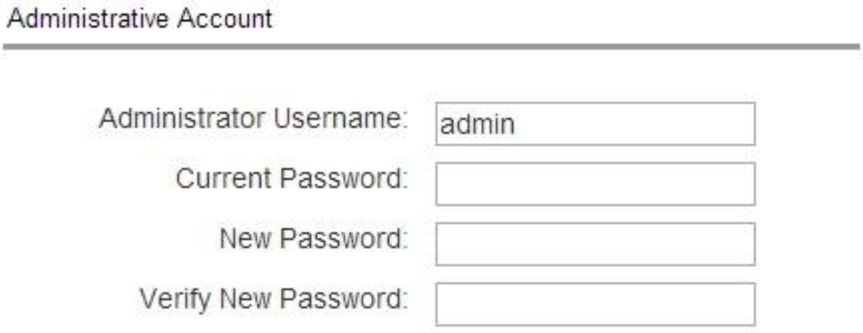


SYSTEM

Device Name: ZC-CP500

3.7.2 Administrative Account

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.



Administrative Account

Administrator Username: admin

Current Password:

New Password:

Verify New Password:

Figure 3.22 Administrative Account

Administrator Username: specifies the name of the system user.

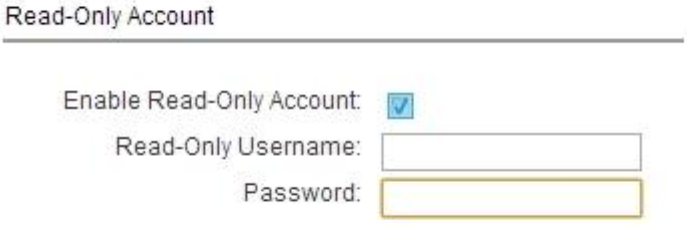
Current Password: administrator is required to enter a current password. It is required for *Password* or *Administrator Username* change routine.

New Password: new password used for administrator authentication should be specified.

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

3.7.3 Read-Only Account

In this section you can enable the read-only account, and configure the username and password to protect your device from unauthorized access. The default option is disabled.



Read-Only Account

Enable Read-Only Account: ☑

Read-Only Username:

Password:

Figure 3.23 Read-Only Account

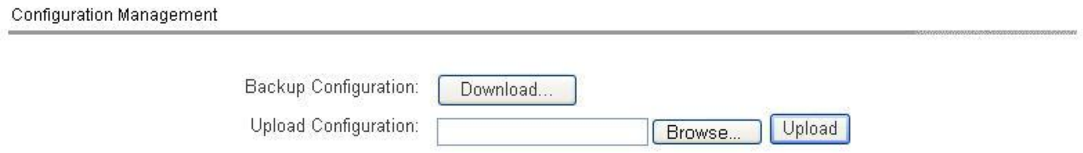
Enable Read-Only Account: This option activates the read-only account.

Read-Only Username: specifies the name of the system user.

Password: new password used for read-only administrator authentication should be specified.

3.7.4 Configuration Management

CP500 configuration is stored in plain text file (*.cfg file). Use the Configuration Management section controls to backup, restore or update the system configuration file:


Configuration Management

Backup Configuration:

Upload Configuration:

Figure 3.24 Configuration Management

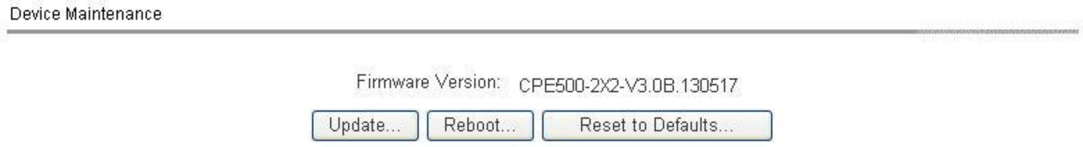
Backup Configuration: click **Download** button to download the current system configuration file.

Upload Configuration: click **Browse** button to navigate to and select the new configuration file or specify the full path to the configuration file location.

Activating the **Upload** button will transfer new configuration file to the system.

3.7.5 Device Maintenance

This section 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. Besides, you could reset the current configuration to factory default.


Device Maintenance

Firmware Version: CPE500-2X2-V3.0B.130517

Figure 3.25 Device Maintenance