Cerio Corporation

www.cerio.com.tw

CERIO Corporation

OW-215N2-X

500mW eXtreme Power 11Na 300Mbps +15dBi

Outdoor Bridge

User Manual

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

Table of Contents

1. Introduction 5
1.1 Overview 5
1.2 Package Content 5
1.3 Applications in Wireless Network 6
1.4 Features 7
1.5 Panel Function Description 9
1.6 Software Configuration 9
Example of Segment: (Windows 7) 10
Example of Segment: (Windows XP) 15
1.7 Wizard Setup 18
2. AP Mode Configuration 22
2.1 Choose Your Operating Mode (AP Mode) 22
2.2 External Network Connection 22
2.3 Configure OW-215N2-X LAN IP Address 22
2.4 Wireless General Setup 24
2.5 Configure Wireless Advanced Setup 26
2.6 Create Virtual AP – Virtual AP Setup 32
2.8 WDS Setup - Expand your Wireless Network 40
2.9 WDS Status 40
2.10 Associated Clients 41
3. WDS Mode Configuration 42
3.1 Choose Your Operating Mode (WDS Mode) 42
3.2 External Network Connection (Network Requirement) 42
3.3 Configure OW-215N2-X LAN IP Address 42
3.4 Wireless General Settings 44
3.5 Configure Wireless Advanced Setup 46
3.6 WDS Setup 52
3.7 WDS Status 53
4. Client Bridge + Repeater AP Mode Configuration 53
4.1 Chose Your Operating Mode(Client Bridge + Repeater AP) 53
4.2 External Network Connection (Network Requirement) 54
4.3 Configure OW-215N2-X LAN IP Address 54
4.4 Wireless General Setup 57
4.5 Configure Wireless Advanced Setup 58
4.6 Site Survey 64
4.7 Station Profile 65
4.8 Remote AP Status 67

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

4.9 Repeater AP Setup 67
4.10 Repeater AP MAC Filter Setup 71
5. CPE + AP Mode Configuration 73
5.1 Choose Your Operating Mode (CPE + Repeater AP Mode) 73
5.2 External Network Connection (Network Requirement) 73
5.3 Configure CPE(WAN) Setup 74
5.4 Configure OW-215N2-X LAN IP Address 78
5.5 Configure DDNS Setup 80
5.6 Wireless General Setup 81
5.7 Configure Wireless Advanced Setup 82
5.8 Site Survey 88
5.9 Station Profile 89
5.10 Remote AP Status 91
5.11 Repeater AP Setup 91
5.12 Repeater AP MAC Filter Setup 96
6. System Management 97
6.1 Configure Management 97
6.2 Configure System Time 100
6.3 Configure UPnP Setup by CPE mode 101
6.4 Configure SNMP Setup 101
7. Configure Advance Setup 103
7.1 DMZ by CPE mode 103
7.2 IP Filter by CPE mode 104
7.3 MAC Filter by CPE mode 106
7.4 Virtual Server by CPE mode 107
7.5 Parental Control by CPE mode 108
7.6 QoS 110
7.7 IP Routing by CPE mode 112
7.8 Time Policy 114
8. Configure Utilities Setup 115
8.1 Profile setting 115
8.2 Firmware Upgrade 116
8.3 Network Utility 117
8.4 PoE Bridge 118
8.5 Reboot 118
9. Configure Status 119
9.1 Overview 119
9.2 DHCP Client 119
9.3 Extra Info 120

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

9.4 Event Log 123
Appendix A. MCS Data Rate 124
Appendix B. Enabling UPnP in Windows XP 125

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

1. Introduction

1.1 Overview

CERIO OW-215N2-X Outdoor AP Bridge utilizes a 500mW high power with Aluminum Extrusion housing weatherproof. Flow Bandwidth support 802.11a/n of up to 300Mbps(Tx), 300Mbps(Rx) link rate. **And Build in lightning arrester (15kV ESD) OW-215N2-X** may connect to the WiFi mesh or WDS infrastructure and provides the subscriber with an Ethernet connection for a local access .to extend the range and increase the performance of our wireless network. The outdoor AP/bridge may connect to the **WiFi Mesh** or **WDS** infrastructure and provides the subscriber with an Ethernet connection for a local access. also with **included PoE power** and data are supplied to the unit using CAT5 Ethernet cable. Furthermore the **OW-215N2-X** have support PoE power supply function, and Support PoE Bridge, Can provide PoE Power to the next OW-215N2-X PoE unit .

CERIO OW-215N2-X 500mW eXtreme Power 11a/n Outdoor Access Point supports Multi operational modes, the **Pure AP mode / AP+WDS mode** and the **Pure WDS mode** and the **Client Bridge + Repeater AP Mode** and **WISP + Repeater AP mode** respectively with built-in remote management features simplify the deployment and reduce cost for continued maintenance of the outdoor bridge.

1.2 Package Content

OW-215N2-X Main Unit	x1
Power Adapter (Power Supply)	x1
PoE Injector	x1
Wall / Pole Mounting Bracket	x1
CD Manual	x1
Warranty Card	x1

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

1.3 Applications in Wireless Network

Smart of PoE Bridge application

CERIO OW-215N2-X 500mW eXtreme Power 11a/n Outdoor Access Point supports Design smart PoE Bridge function, the PoE Bridge function support provide next AP power. Can will be structure become very convenience. And the PoE bridge support CERIO WM-series AP or OW-series to be dual band budle wireless soultion.

Wireless Architecture Mode

Pure AP Mode & AP/ AP+WDS Mode

- It can be deployed as a tradition fixed wireless Access Point
- It allow wireless clients or Stations(STA) to access
- This enables the wireless interconnection of Access Point in an IEEE802.11 network. and accept wireless clients at the same time

Pure WDS Mode

- This enables the wireless interconnection of Access Point in an IEEE802.11 network
- It allows a wireless network to be expanded using multiple access point without the need for a wired backbone to link them
- This also be referred to as repeater mode It cannot allow wireless clients or Stations (STA) to access

Client Bridge + Repeater AP Mode

- It can be used as an Client Bridge + Repeater AP to receive wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers.
- In this mode, **OW-215N2-X** is enabled with DHCP Server functions. The wired clients of OW-215N2-X are in the same subnet from Main Base Station and it accepts wireless connections from client devices, You can disabled the mode extend repeater AP function, will be do to “AP Client ” function.

CPE + Repeater AP Mode

- It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers

- In the CPE mode, **OW-215N2-X** is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to OW-215N2-X are in different subnet from those connected to Main Base Station, and, in CPE mode, it does not accept wireless association from wireless clients.

1.4 Features

- Operation Modes : AP Mode, WDS Mode, Client Bridge + Repeater AP Mode and WISP Repeater + AP Mode
- 500mW at 5Ghz Output High Power
- IEEE 802.11a/n 2Tx / 2Rx Design, Bandwidth of up to 300Mbps(Tx), 300Mbps(Rx) link rate
- Maxmum Security with 802.1X, WAP, and WPA2
- Support Over load current protection for the board design . and 3 LEDs Wireless Signal Strength
- Weater-Proof RJ45 Connector, Integragted Power over Ethernet (PoE)
- Support PoE Bridge by LAN Port function.
- Build in lightning arrester (15kV ESD)
- Support 8 Multiple-BSSID. And Support IEEE802.11f IAPP
- Support Static Routing and RIP and OSPF Dynamic Routing by CPE mode.
- Support Layer-7 Protocol Filter and Content Filter by CPE mode.
- QoS(Quality of Service) for bandwidth management and traffic prioritization
- Support IEEE802.1d Spanning Tree
- Integragted IGMP v1/v2/v3 snooping functions and Support Web management and SNMP MIB-II
- Built-in software interface allows for communicating with CERIO AM-Series AP Management
- WLAN Switch or Access Controller of network management servers.

Networking by CPE mode.

- Support Static IP, Dynamic IP(DHCP Client) and PPPoE on WiFi WAN Connection
- Support VPN Pass Throughput (PPTP , IPSec , L2TP) and MAC Cloning
- Proxy DNS ,Dynamic DNS ,NTP Client
- Virtual DMZ, Virtual Server (IP / Port Forwarding) and
- Support IP / MAC Filter and Support Bandwidth trafic Shaping

Wireless Feature

- Transmission power control : Layer 1~9
- Channel selection : Manual or Auto
- No of associated clients per AP : 32
- Setting for max no associated clients : Yes
- Support 8 virtual BSSID and associated clients per AP to 32 and the Pure WDS Max. 8

- Setting for transmission speed
- Dynamic Wireless re-transmission
- IEEE 802.11i Preauth (PMKSA Cache)
- IEEE 802.11h - TPC(Transmission Power Control)
- IEEE 802.11d -Multi country roaming
- Channel Bandwidth setting : 20MHz or 20/40MHz
- HT Tx/Rx Stream selection : 1 or 2
- Short Slot support

Authentication/Encryption (Wireless Security)

- Blocks client to client discovery within a specified VLAN
- WEP 64/128 bit /EAP-TLS + Dynamic WEP , EAP-TTLS + Dynamic WEP
- PEAP/MSPEAP + Dynamic WEP
- WPA-PSK/TKIP,WPA-802.1x/TKIP, 802.11i WPA2-PSK/CCMP/AES 128/256bit,
- WPA2 (802.1x /CCMP / AES 128/256bit), No. of registered RADIUS servers : 1
- Setting for TKIP/CCMP/AES 128/256bit (ASCII 63 & HEX 64)key's refreshing period
- Hidden SSID broadcast support, and VLAN assignment on BSSID
- Access Control list (ACL) by MAC Address

Quality of Service

- Download and Upload traffic control and support Traffic Analysis and Statistics
- Packet classifications via DSCP (Differentiated Services Code Point) and Support IEEE802.11e WMM
- Control Policy by IP/IP Ranges/ MAC/ Service , Layer-7 Protocol Support
- No. of Max. Policy setting : 10
- DiffServ/TOS , IEEE 802.11p/COS, IEEE 802.1Q Tag VLAN priority control

Parental Control by CPE mode

- Blocking Control Policy by IP Range / MAC Group / Port / Layer-7 Protocol
- URL Blocking

Management

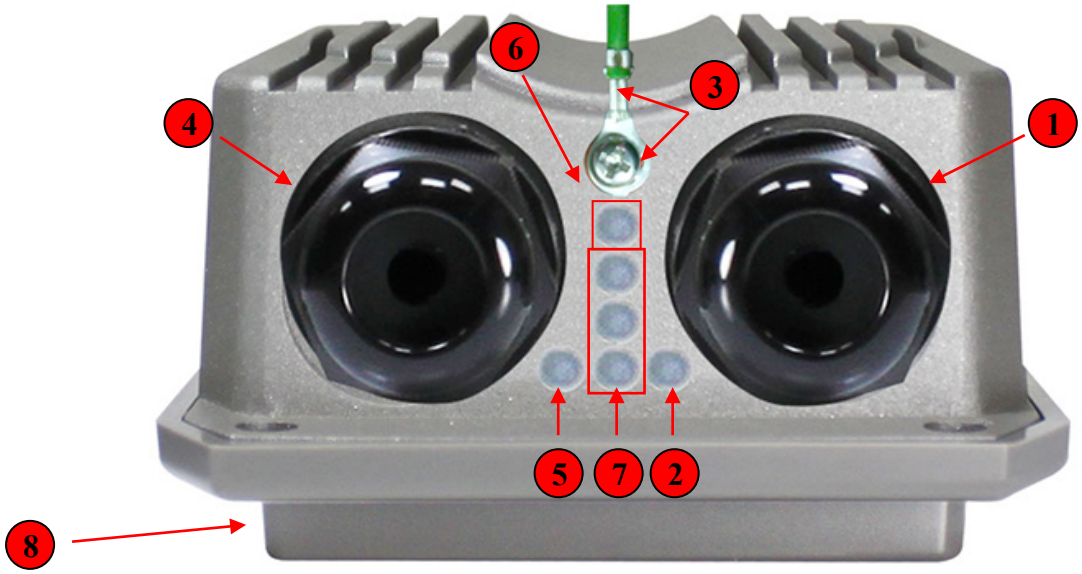
- Web-Based management interface, Intuitive Web Management Interface, Administrative Access : HTTP and HTTPS and support CLI access via Telnet and SSH
- Support Firmware Upgrade via Web , Reset to Factory Defaults,
- Support SNMP v1/v2c/v3 , MIB II
- UPnP (Universal Plug and Play) by CPE mode.
- NTP Time Synchronization

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- SNMP Traps to a List of IP Address
- Support Event log

1.5 Panel Function Description

There is several LED indicators on the front of the **OW-215N2-X**. Please refer to the definitions below :



(1) The Ethernet connect of LAN2 Port / PoE out
(2) The LED indicator of LAN2 Port
(3) At in Reset button , and Support Ground connection
(4) The Ethernet connect of LAN1 Port(PoE in)
(5) The LED indicator of LAN2 Port
(6) Power LED
(7) The three LED's for strong or weakly indicator on signal bridge, and the three LED's only support "**Client Bridge + Repeater AP** and **WISP + Repeater AP modes**".
(8) Built-in 15dBi Directional Antenna

1.6 Software Configuration

OW-215N2-X supports web-based configuration. Upon the completion of hardware installation, **OW-215N2-X** can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- **Default IP Address**: 192.168.2.254
- **Default Subnet Mask**: 255.255.255.0
- **Default Username and Password**

MODE	AP , WDS , (WISP / Client Bridge)+ Repeater AP	
Management Account	Root Account	Admin Account
Username	root	admin
Password	default	admin

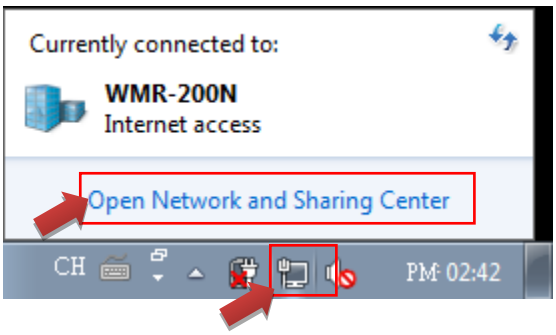
- **IP Segment Set-up for Administrator's PC/NB**

Set the IP segment of the administrator's computer to be in the same range as **OW-215N2-X** for accessing the system. Do not duplicate the IP Address used here with IP Address of **OW-215N2-X** or any other device within the network.

Example of Segment: (Windows 7)

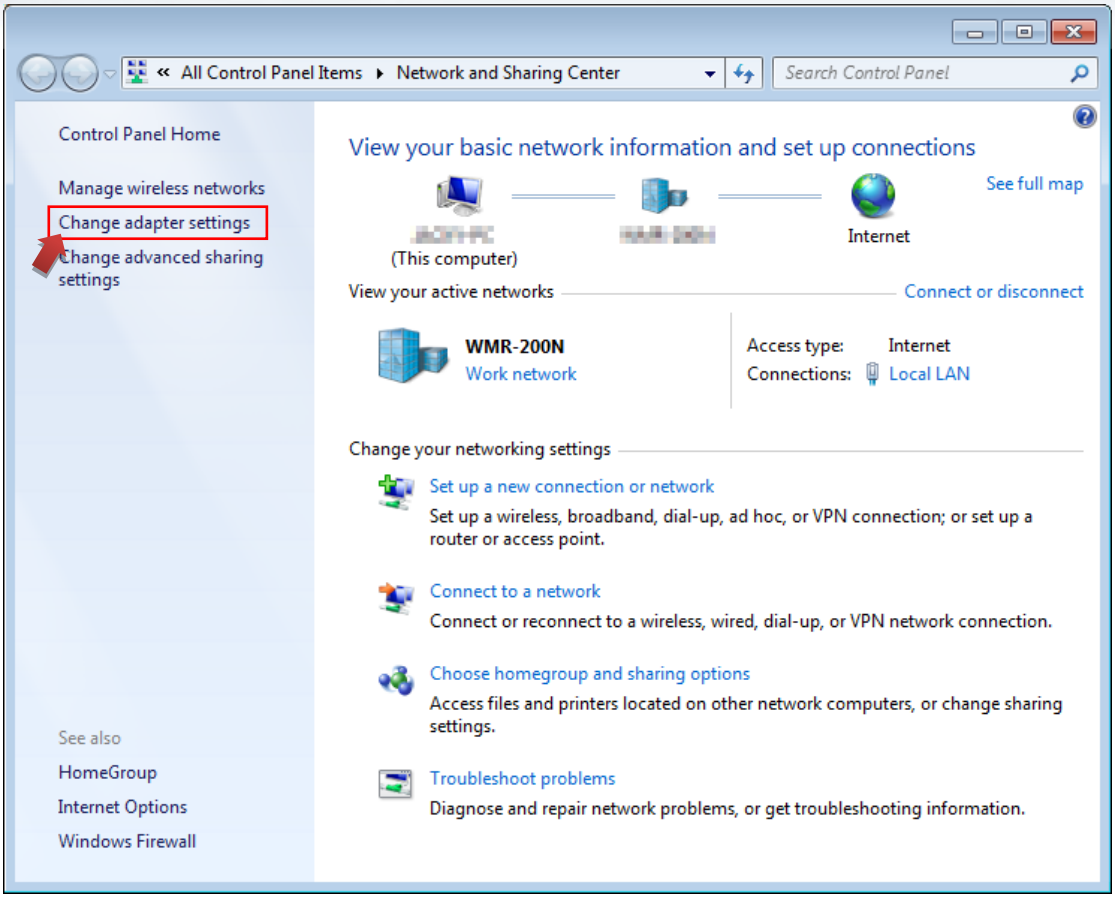
Step 1 :

Please click on the computer icon in the bottom right window, and click **"Open Network and Sharing Center"**



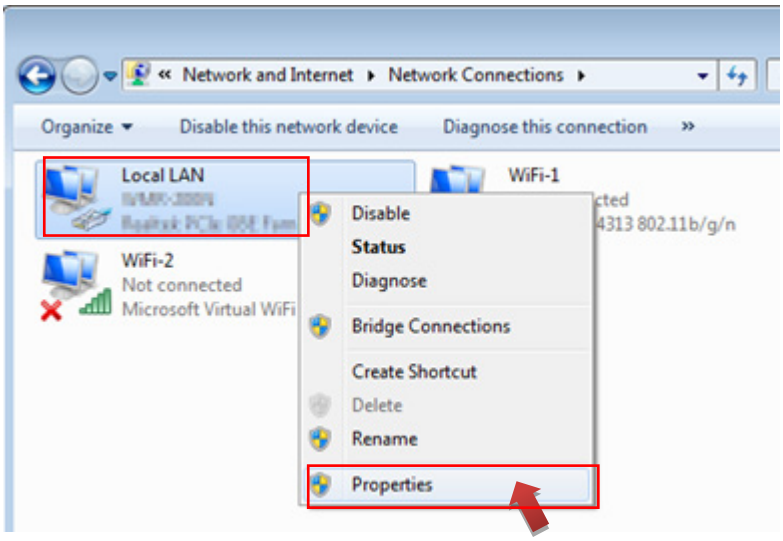
Step 2 :

In the Network and Sharing Center page, Please click on the left side of **"Change adapter setting"** button



Step 3 :

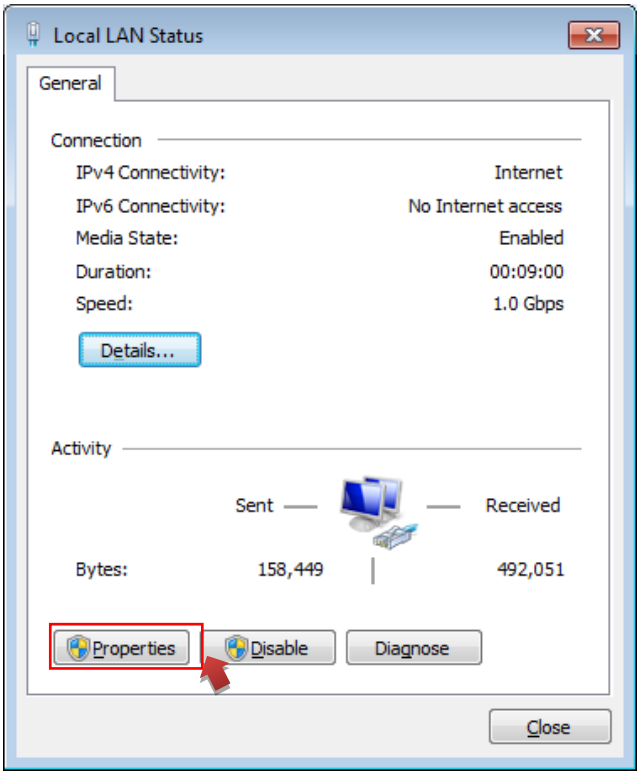
In **“Change adapter setting”** Page. Please find Local LAN and Click the right button on the mouse and Click **“Properties”**



Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

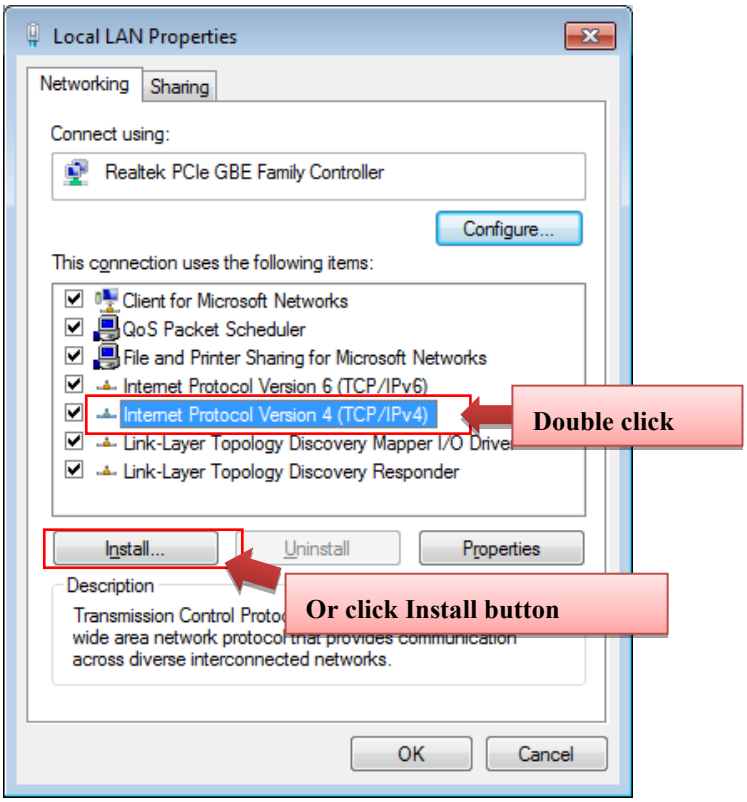
Step 4 :

In **"Properties"** page, please Click **"Properties"** button to TCP/IP setting



Step 5 :

In Properties page to setting IP address, please find **"Internet Protocol Version 4 (TCP/IPv4)"** and double click or click **"Install"** button.



Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

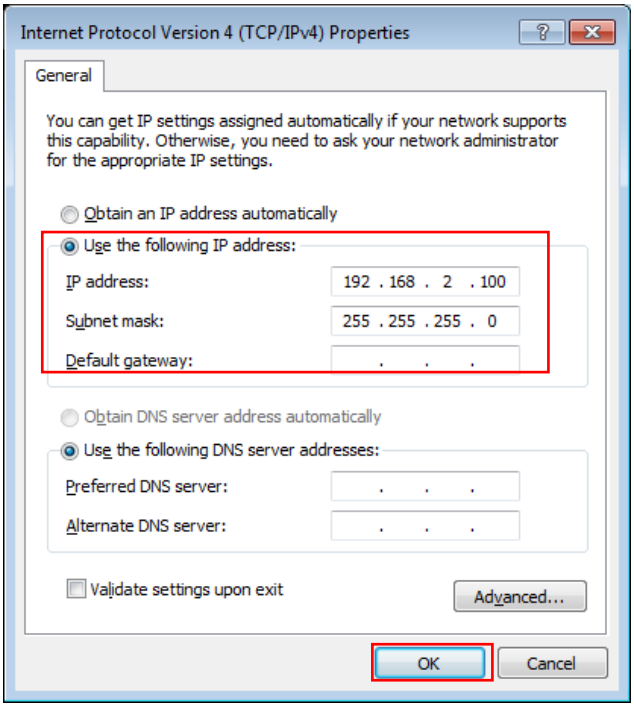
Step 6 :

Select **“Use the following IP address”**, and fix in IP Address : 192.168.2.X

ex. The X is any number by 1 to 253

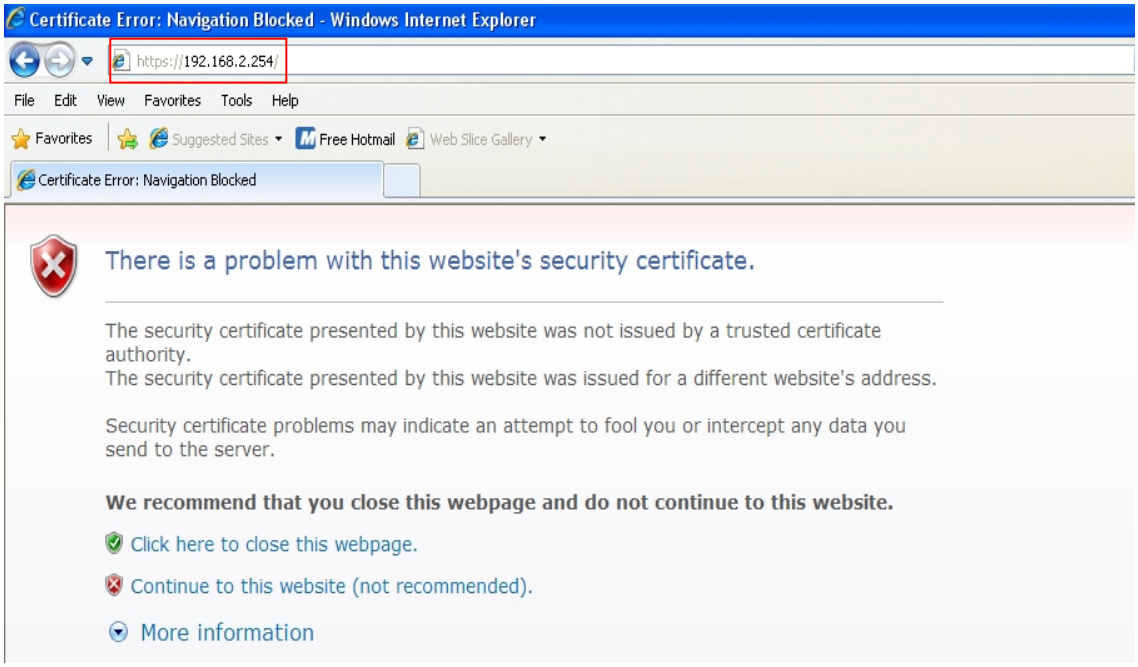
Subnet mask : 255.255.255.0

And Click **"OK"** to complete the fixed computer IP setting



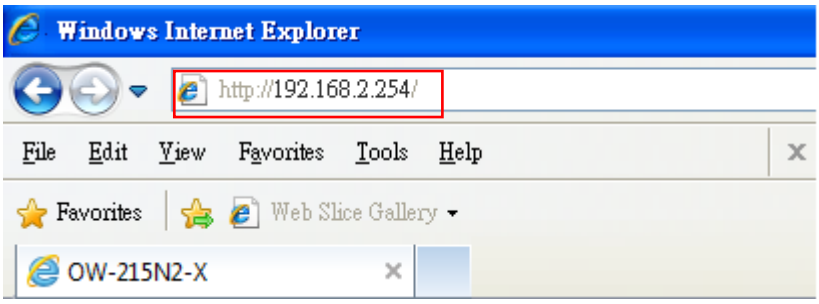
Open Web Browser

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (https://192.168.2.254). There will be a “Certificate Error”, because the browser treats system as an illegal website.



Click **"Continue to this website"** to access the system's WMI. The system's Overview page will appear.

Launch as web browser to access the web management interface of system by entering the default IP Address, http://192.168.2.254, in the URL field, and then press Enter. Browser will pop up "login" page. Please key in username and password into the system on OW-215N2-X.



The system manager Login Page then appears.

Enter **"root"** as User name and **"default"** as Password, and then click OK to login to the system.

The OW-215N2-X system login default As follows

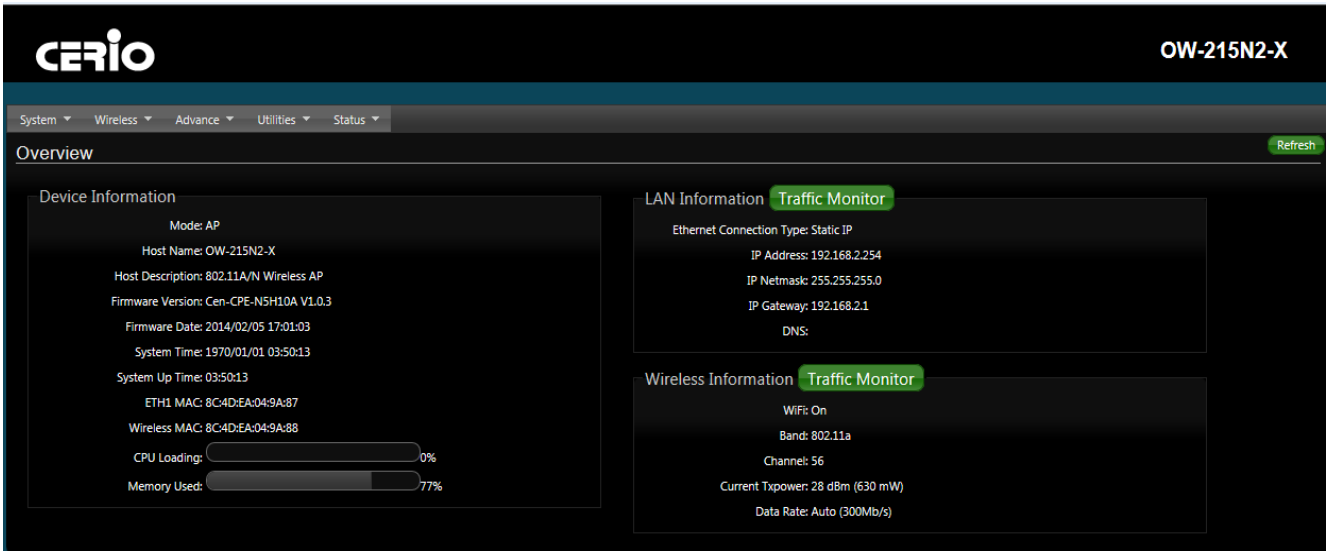
User Name : **root**

Password : **default**

Cerio Corporation

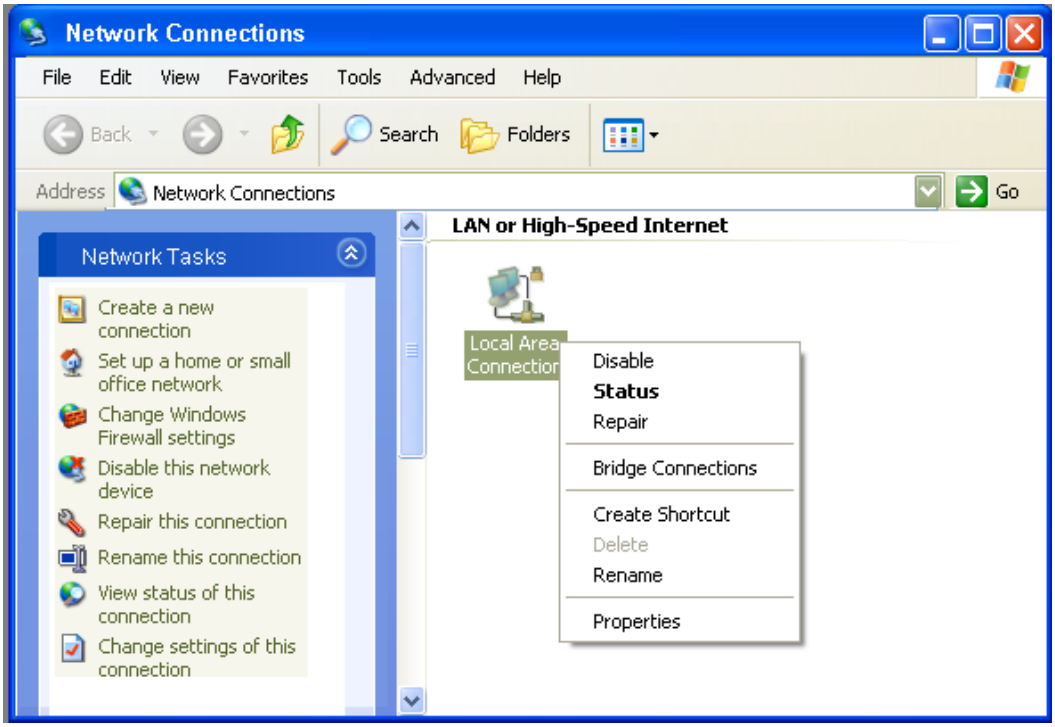
www.cerio.com.tw

The OW-215N2-X System screen



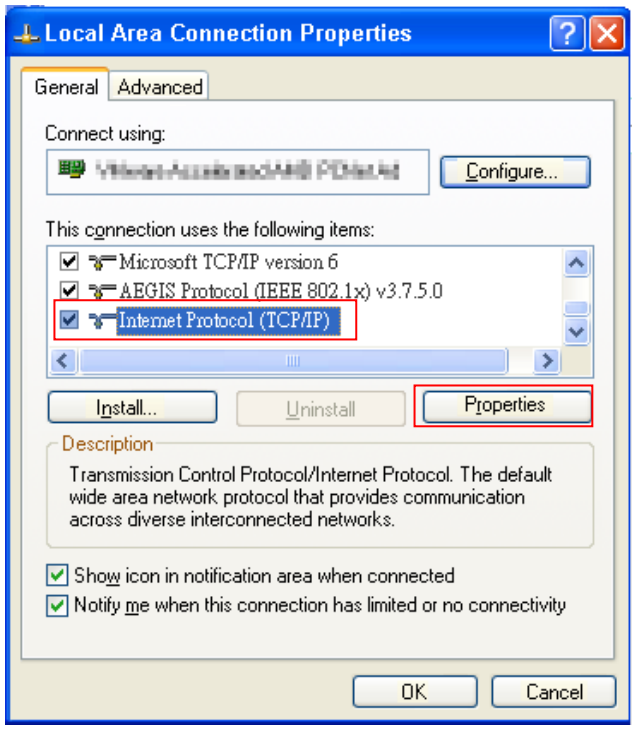
Example of Segment: (Windows XP)

- Click **Start** -> **Settings** -> **Control Panel**, and then "**Control Panel**" window appears. Click on "**Network Connections**", and then "**Network Connections**" window appears.
- Click right on "**Local Area Connection**", and select **Properties**.

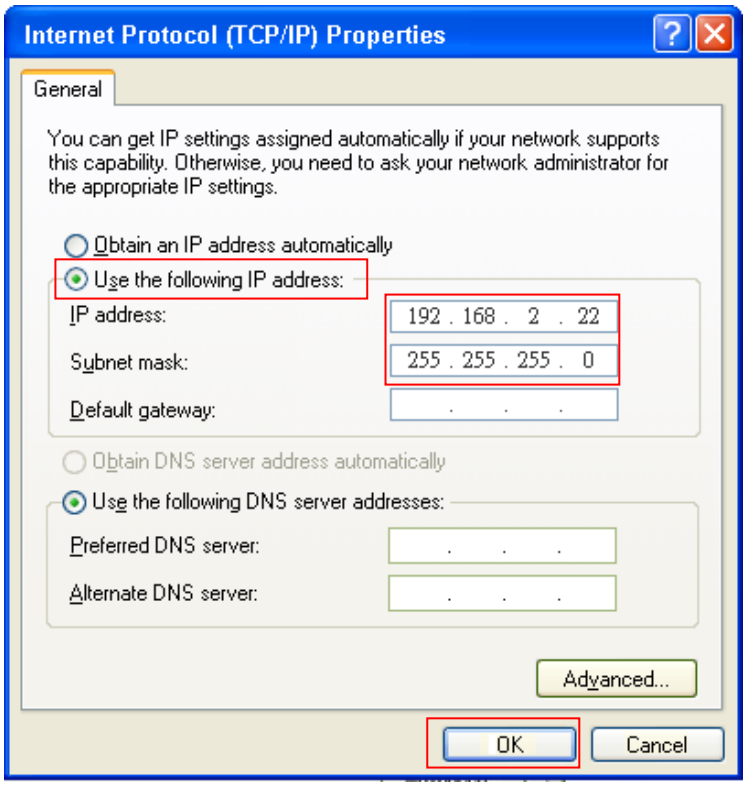


Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- In "**Local Area Connection Properties**" window, select "**Internet Protocol (TCP/IP)**" and click on **Properties** button.



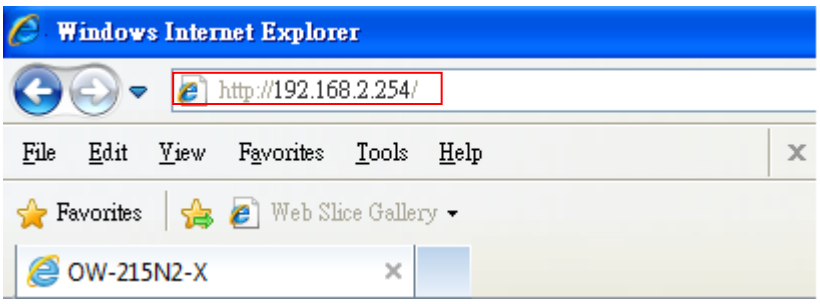
- Select "**Use the following IP address**", and type in



Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

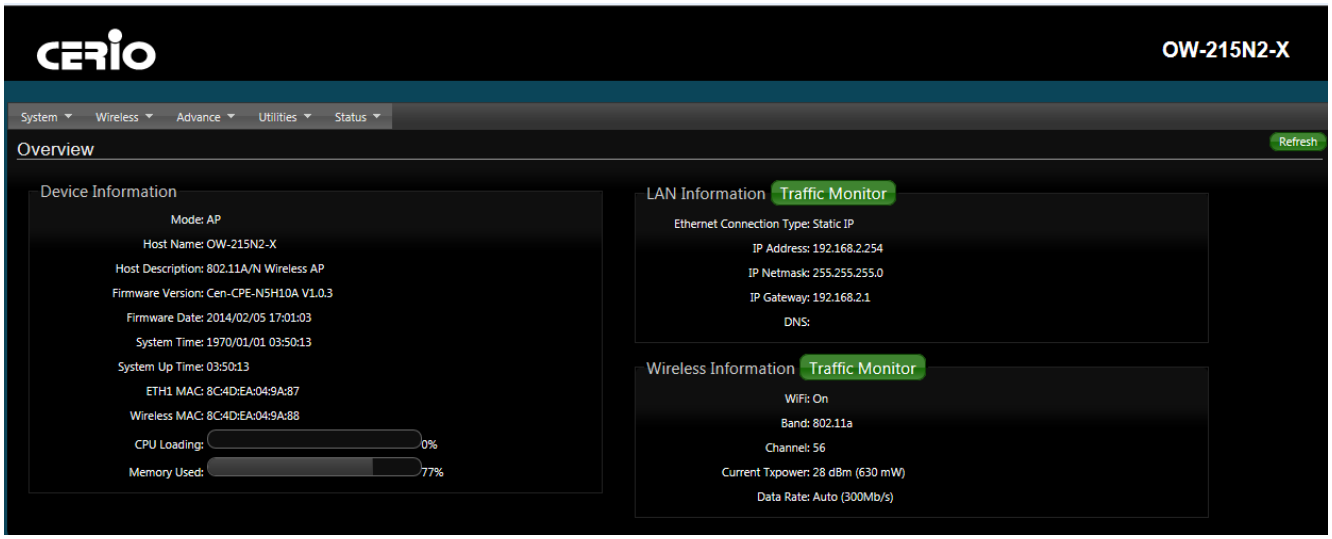
➢ **Launch Web Browser**

Launch as web browser to access the web management interface of system by entering the default IP Address, http://192.168.2.254, in the URL field, and then press Enter.



➢ **System Login**

➢ System Overview page will appear after successful login.



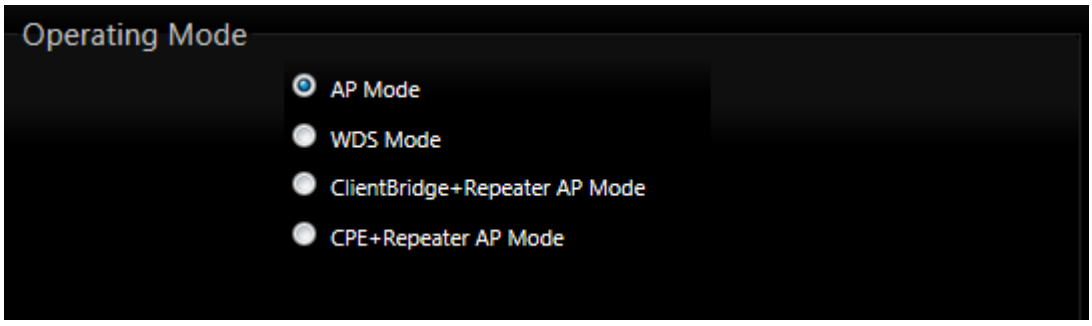
1.7 Wizard Setup

The setup wizard is designed to be an 'easy to use' utility that allows quick modification of the **OW-215N2-X** UI Web-based GUI interface settings . The wizard should take no longer than 5 minutes to use.

This is purely because the wizard has been designed for a quick and easy setup aimed at all users. More advanced users can configure the remaining settings using the advanced settings options from the setup menu.

➢ **Chose Your Operating Mode**

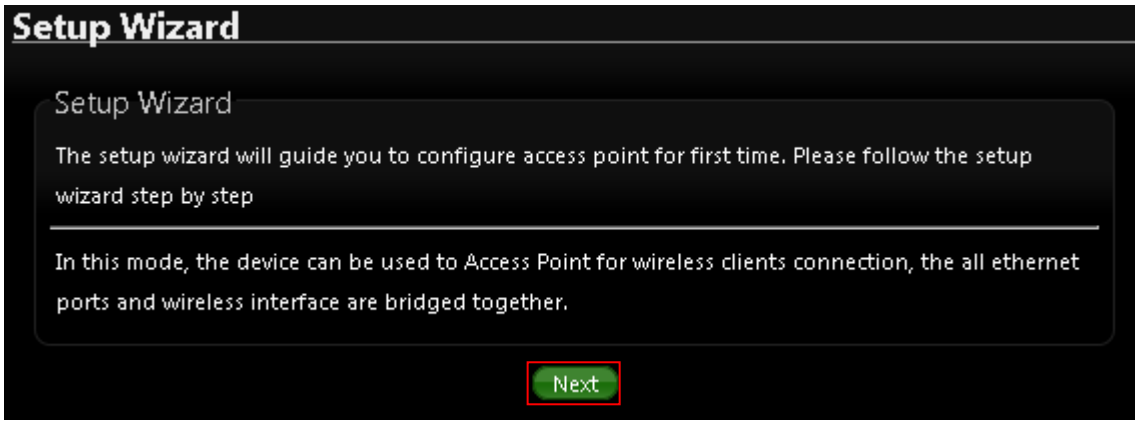
OW-215N2-X supports Multi operational modes, **AP and AP+WDS mode**, **WDS mode**, **Client Bridge + Repeater AP mode**, **CPE and CPE + Repeater AP mode etc.** respectively with built-in remote management features



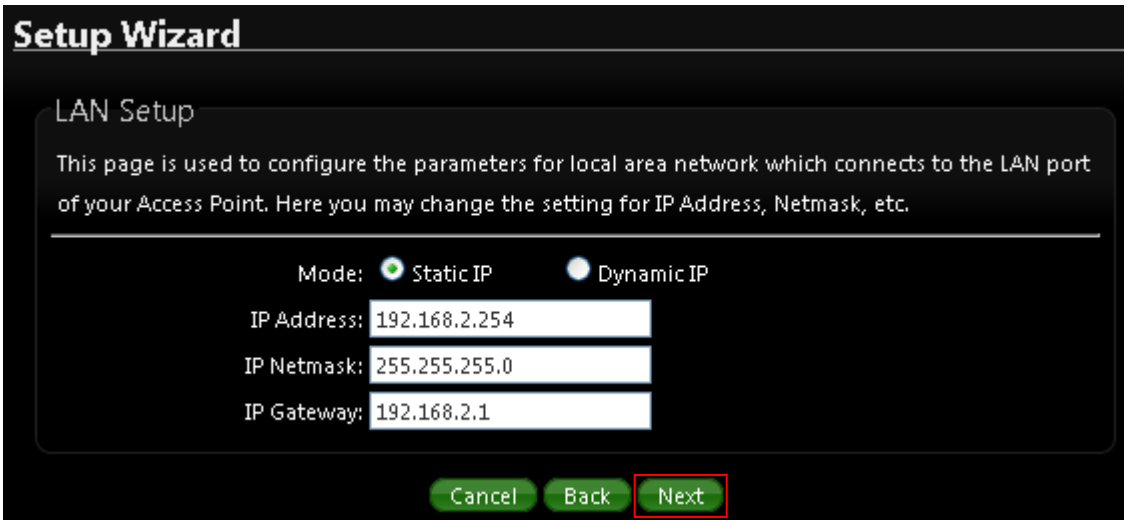
➢ **Wizard Guide**

Please click on **System → Setup Wizard** → Next and follow the below guide.

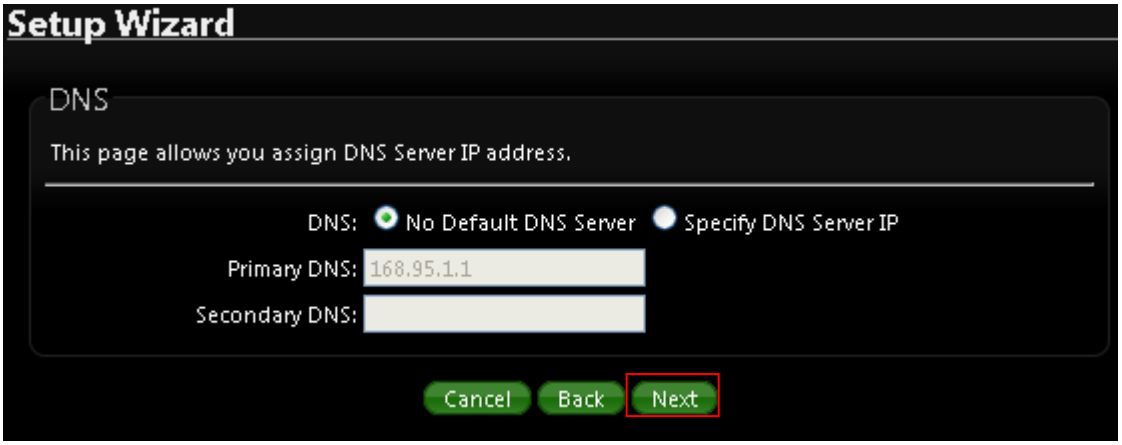
1) Follow And Guide Continuing Setting



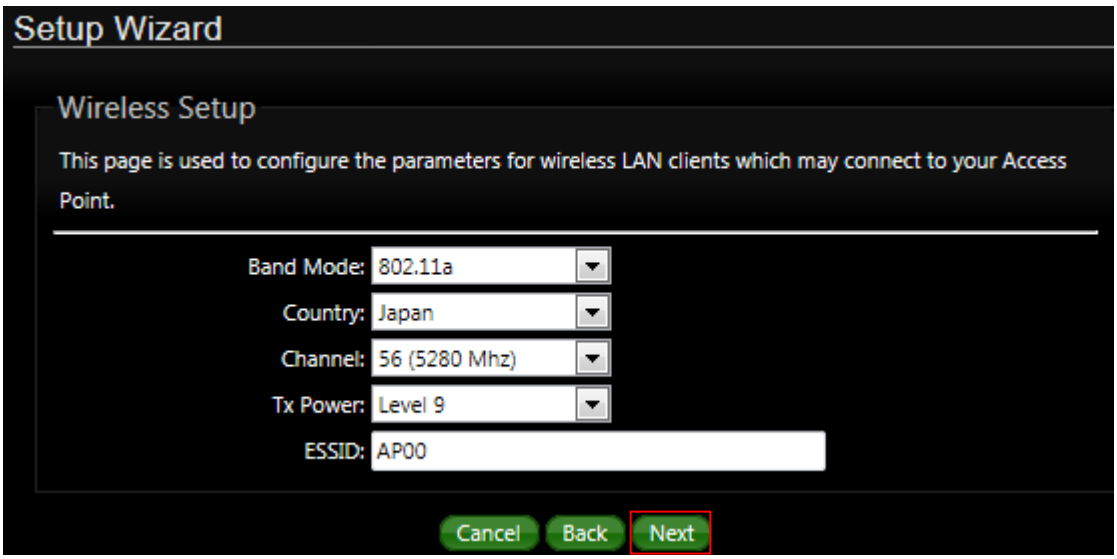
2) LAN setup → Here are the instructions for setup your OW-215N2-X local LAN IP address and netmask. If you don't want change the default OW-215N2-X IP 192.168.2.254 address, please keep the default and go next setup.



3) **DNS** → If you don't know for your ISP correct DNS IP address, Please click "No default DNS server" to follow your ISP DNS related IP address.



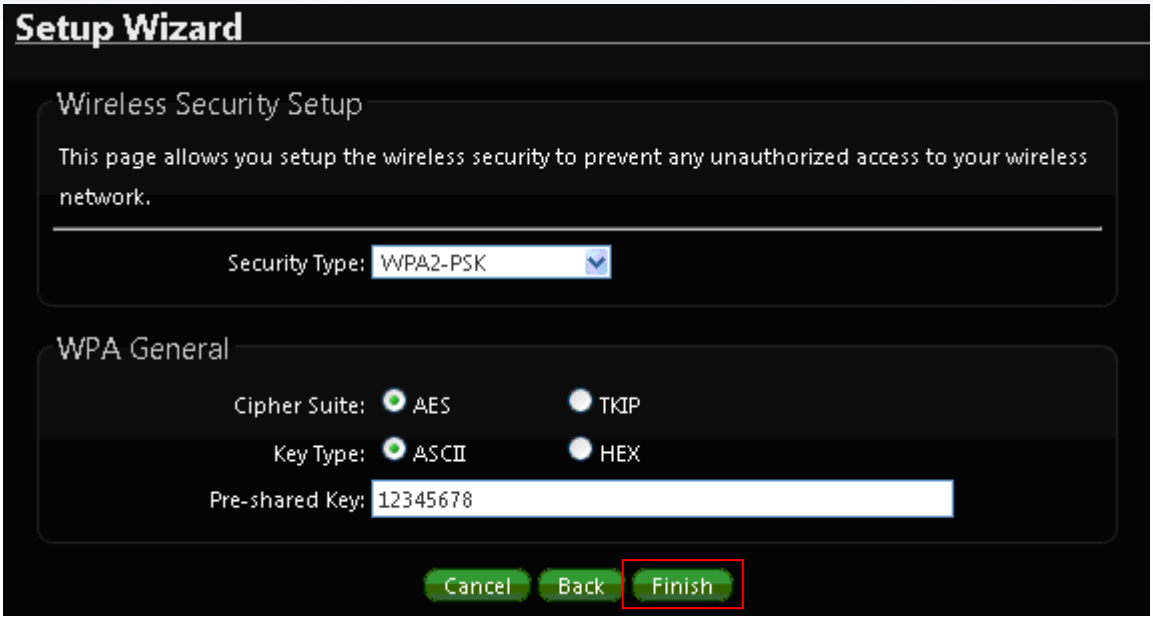
4) **Wireless Setup** → If you are not sure which setting to choose, Please then the default setting to best WiFi smart channel judgment for auto channel, and adjust the output power to level9 (100%) Extended service set ID indicated the SSID which the clients used to connect to the access point ESSID.



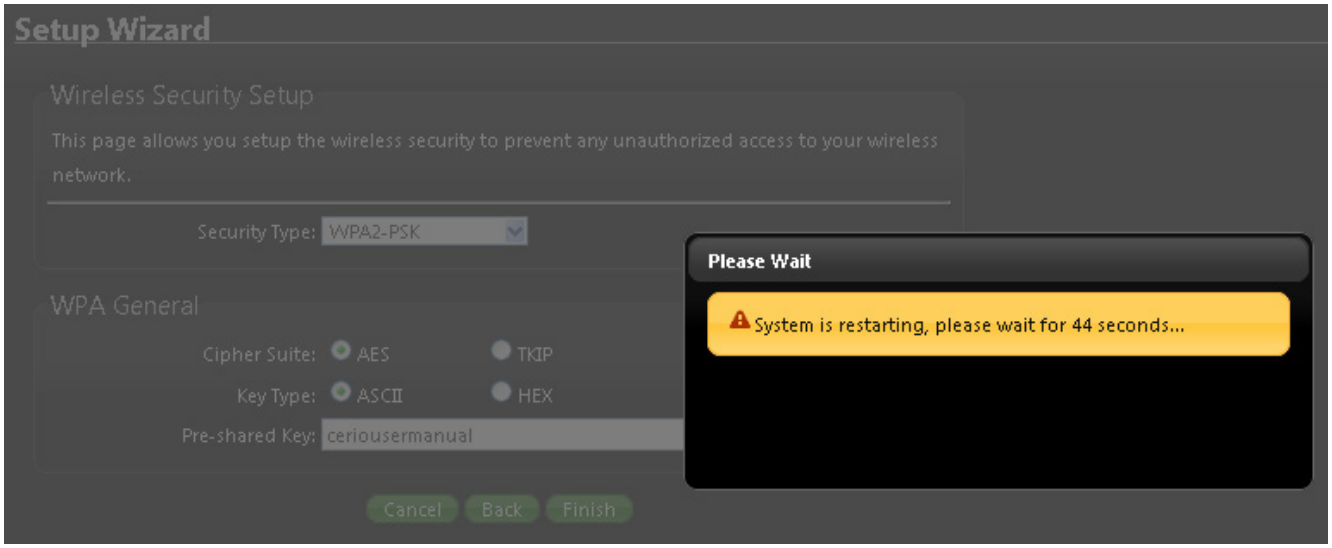
5) **Wireless Security setup** → Suggested setting that you use wireless encryption authentication type for **security Type :** to "WPA2-PSK" the **cipher suite :** to "AES", **Key Type :** to "ASCII" for 11n high speed mode.

Pre-shared Key : Enter the information for pre-shared key; Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format or 8 to 63 ASCII characters. The Pre-Shared key sample as "12345678" wireless encryption key for wireless access.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw



6) Finishing Wizard



Click ***Finish*** button to save your setting . please wait till completion of the reboot process.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

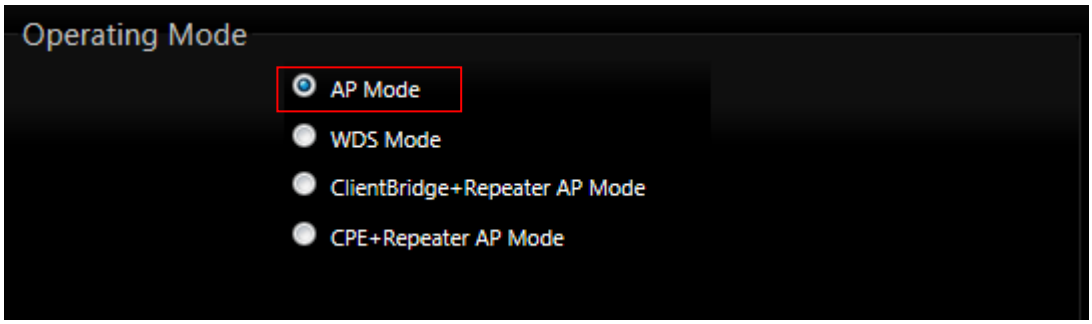
2. AP Mode Configuration

When AP mode is chosen, the system can be configured as an Access Point. This section provides detailed explanation for users to configure in the AP mode with help of illustrations. In the AP mode, functions listed in the table below are also available from the Web-based GUI interface.

2.1 Choose Your Operating Mode (AP Mode)

OW-215N2-X Operating mode support four operational modes, **AP mode**, the **WDS mode**, the **CPE mode** and the **Client Bridge + Repeater AP mode**, respectively with built-in remote management features.

The system administrator can set the desired mode via this page, and then configure the system according to their deployment needs, Please click on System -> Operating Mode and follow the below setting.



2.2 External Network Connection

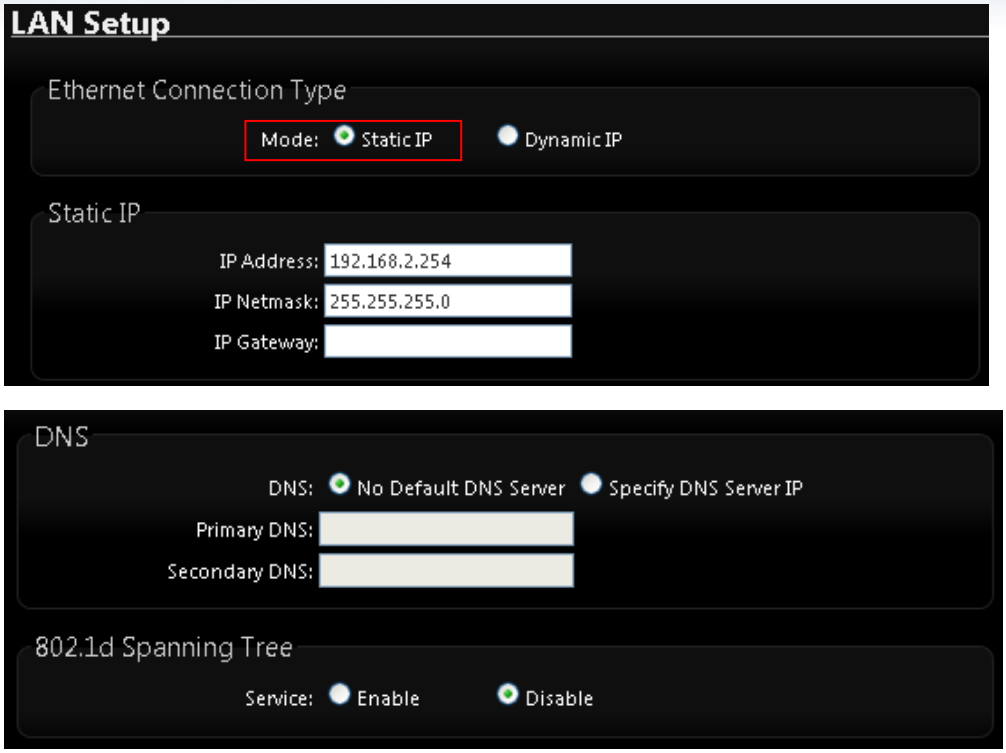
➢ **Network Requirement**

Normally, **OW-215N2-X** connects to a wired LAN and provides a wireless connection point to associate with wireless client. Then, Wireless clients could access to LAN or Internet by associating themselves with **OW-215N2-X** set in AP mode.

2.3 Configure OW-215N2-X LAN IP Address

Here are the instructions to setup the local IP Address and Netmask

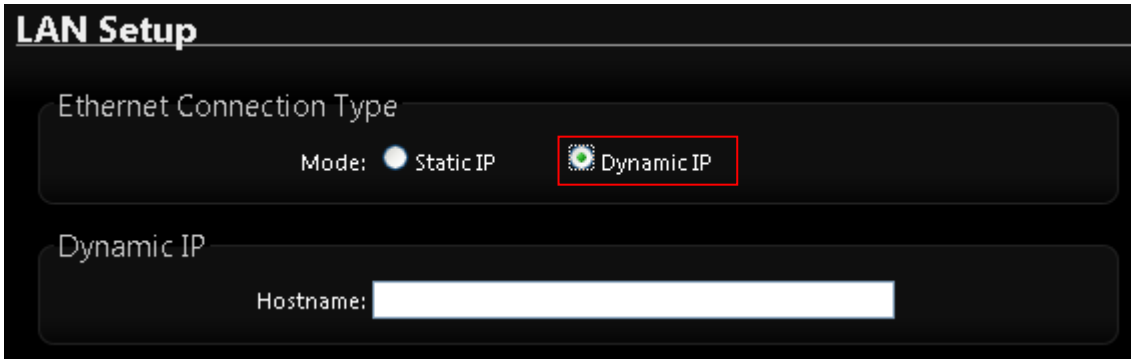
Please click on **System** -> **LAN** and follow the below setting.



- **Ethernet Connection Type**

  Check either "**Static IP**" or "**Dynamic IP**" button as desired to set up the system IP of LAN port.

- **Static IP**: The administrator can manually setup the LAN IP address when static IP is available/ preferred.
  - ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
  - ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
  - ✓ **IP Gateway** : The default gateway of the LAN port
- **Dynamic IP**: This configuration type is applicable when the **OW-215N2-X**is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

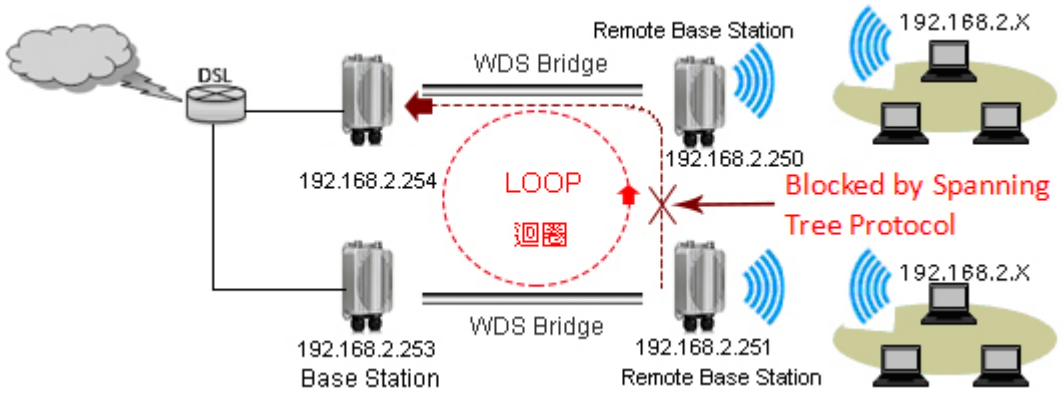


  - ✓ **Hostname** : The Hostname of the LAN port.
- **DNS**: Check either "**No Default DNS Server**" or "**Specify DNS Server IP**" button as desired to set up the system DNS.

- **Primary** : The IP address of the primary DNS server.
- **Secondary** : The IP address of the secondary DNS server.

➢ **802.1d Spanning Tree**

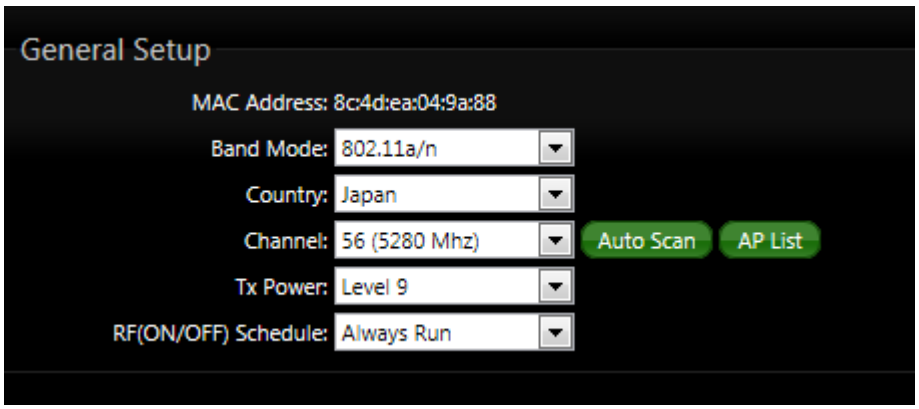
The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d

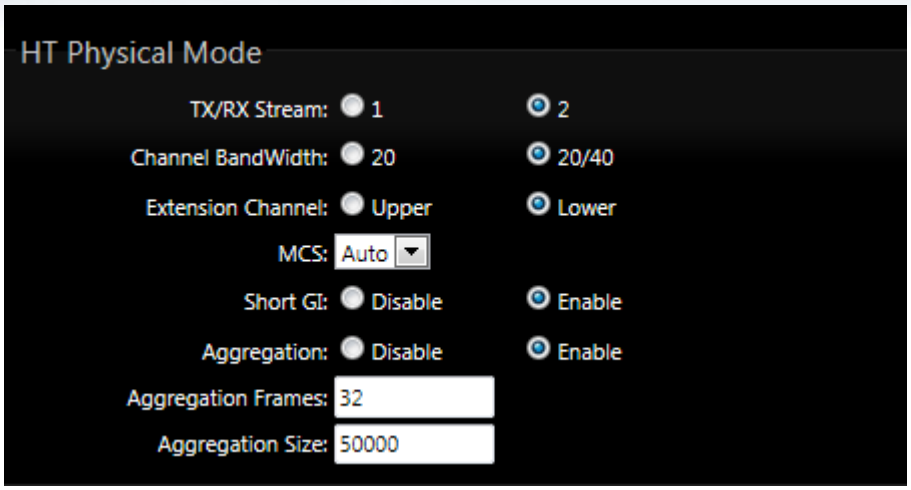


Click **Save** button to save your changes. Then click **Reboot** button to activate your changes.

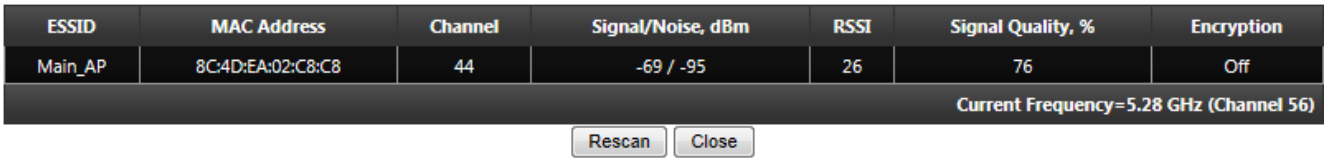
2.4 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.



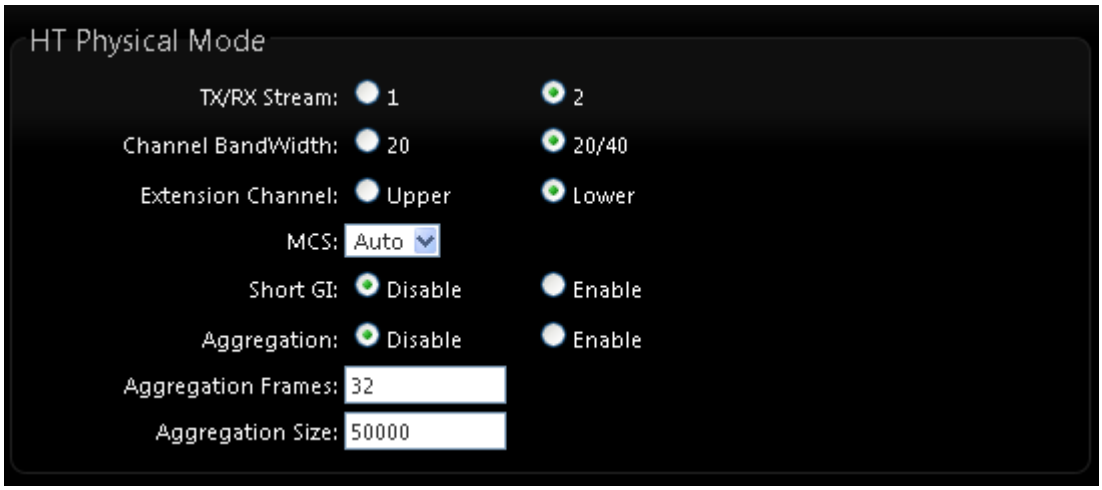


- **MAC Address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are **801.11 a/n mixed mode**
- **Country :** a region, the OW-215N2-X support region for US,ETSI and Japan
- **Channel :** Choosing the best 5G WiFi channel
  - ✧ Auto Scan : Smart channel judgment, the function can auto choose use best Channel
  - ✧ AP List : the function support search neighborhood AP and print site survey list



- **TX Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level ***1*** to level 9 (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level 9 (**100**%).
- **RF(On/Off) Schedule :** The AP **RF** Signal on/off by time Policy

➢ **HT Physical Mode**



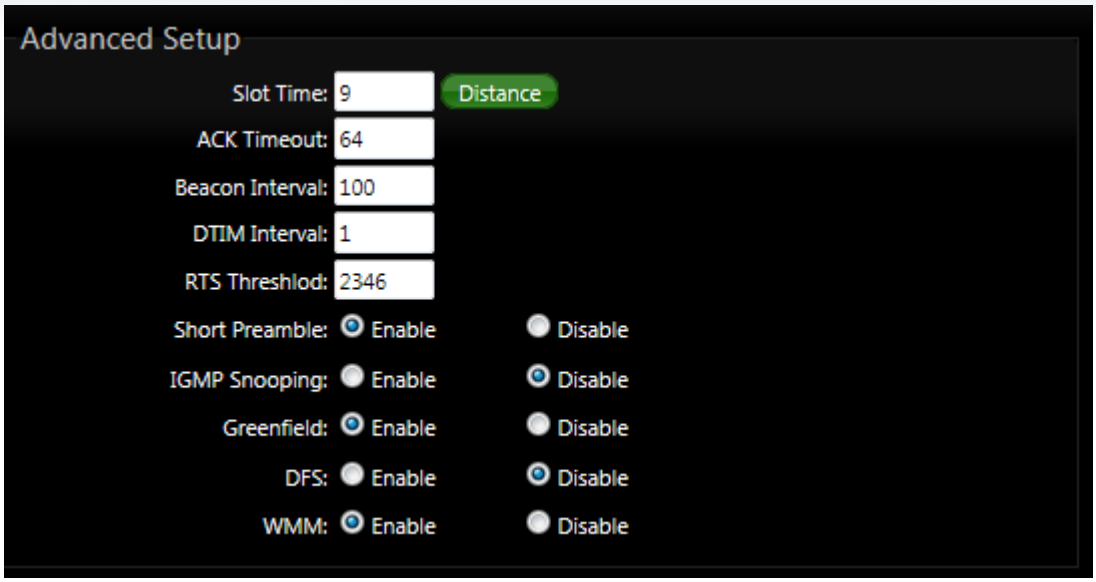
- **HT TxStream/RxStream :** By default, it's **2**

- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel :** Only for Channel Bandwidth "**40**" MHz. Select the desired channel bonding for control.
- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI :** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation :** By default, it's "**Enable**". To "Disable" to deactivated Aggregation.
  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.
- **Aggregation Frames :** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all VAPs and WDS Link**.

2.5 Configure Wireless Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.
  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.
  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".
  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Notice *Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.*

- **Beacon Interval :** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.
  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization. A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.
  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the

packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.
  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

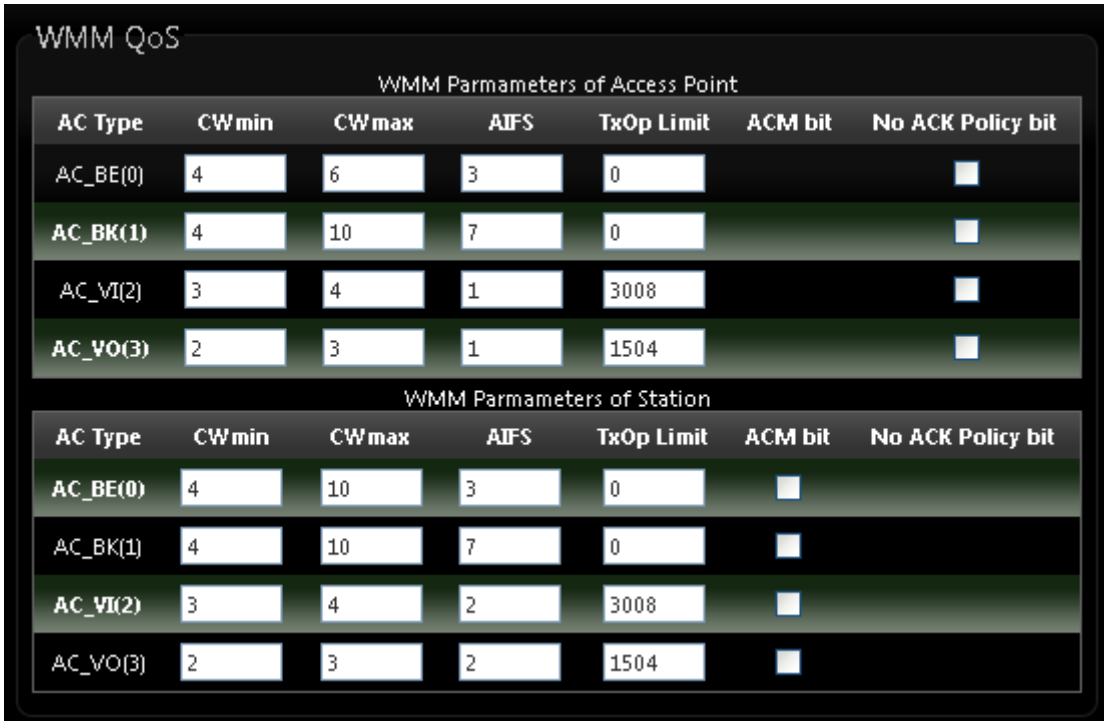
- **IGMP Snooping :** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

- **DFS :** Is IEEE802.11H With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary. The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

- **Greenfield :** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.

- **WMM QoS :** This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.
  As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications

and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.



✓ **AC Type**：

Queue			
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

✓ **CWmin**：Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. ◦

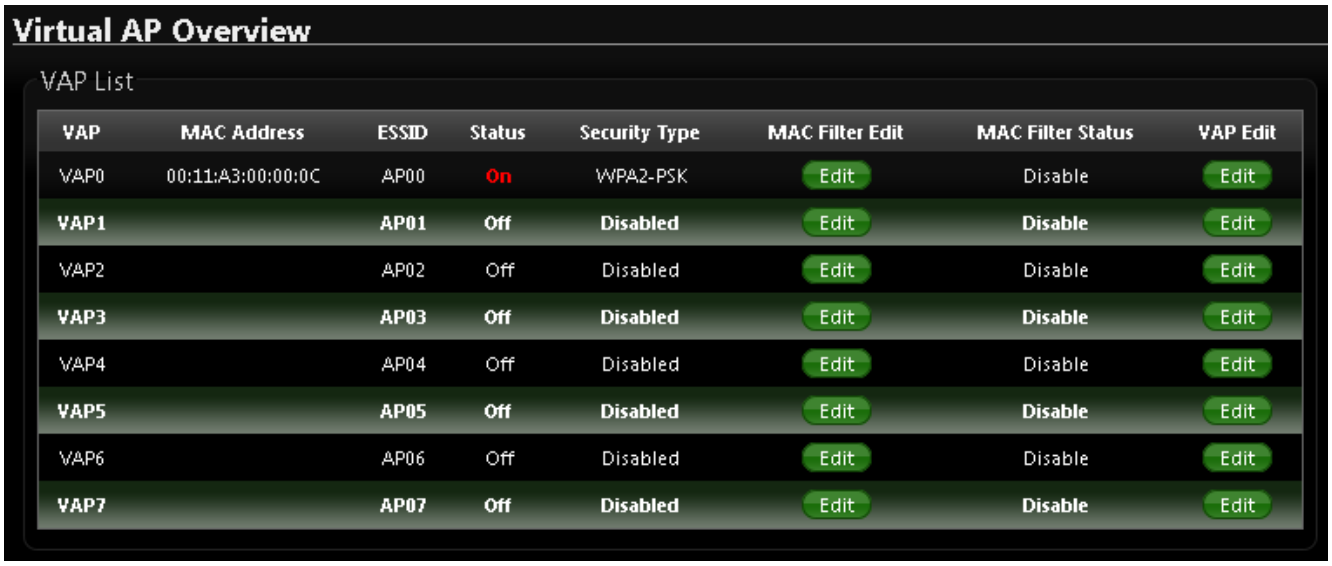
✓ **CWmax**：Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention

Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦

- ✓ **AIFS**：The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit**：Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit**：Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit**：Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click “**Checkbox**” indicates “**No ACK**”
  When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.
  When the Normal ACK policy is used, the recipient acknowledges each received uncast packet. ◦

2.6 Create Virtual AP – Virtual AP Setup

The administrator can create Virtual AP via this page. Please click on **Wireless** -> **Virtual AP Setup** and follow the below setting.

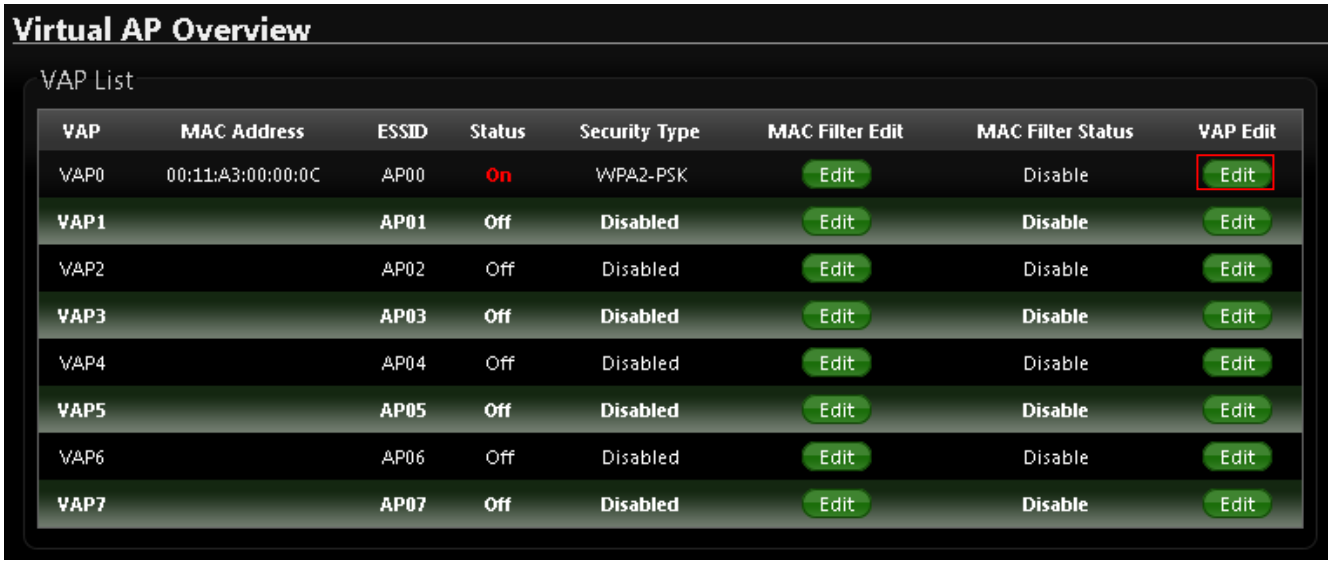


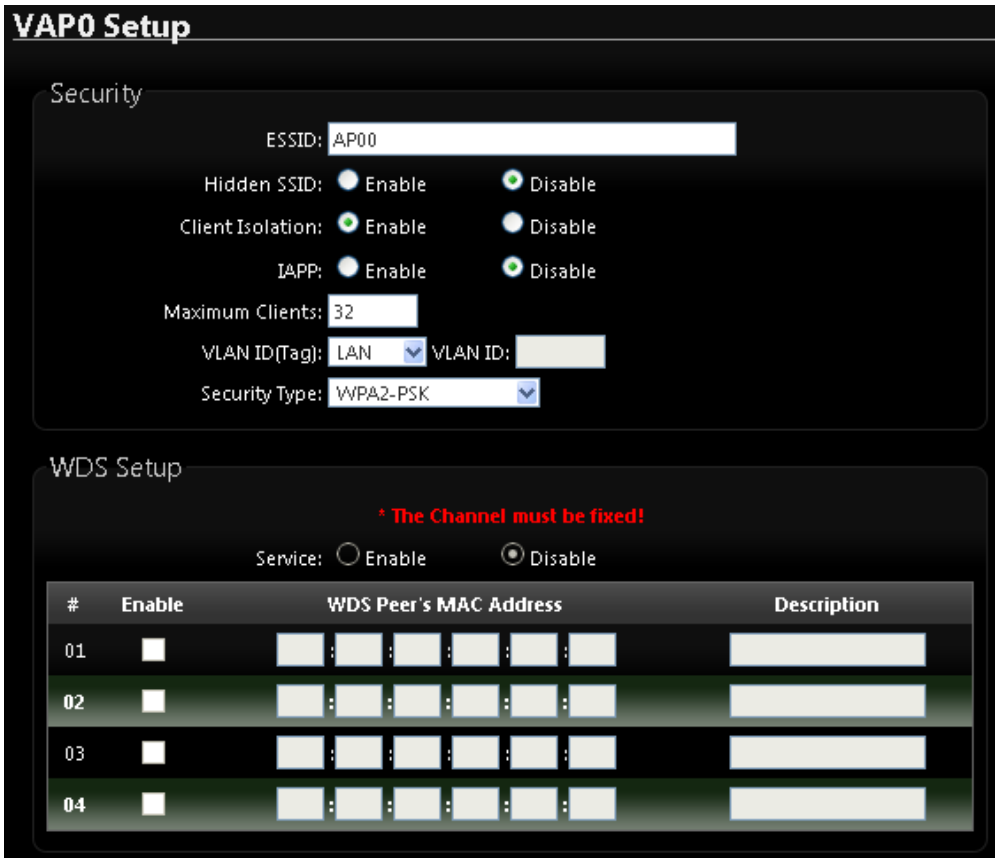
- **VAP**: Display number of system's Virtual AP.
- **MAC Address :** The MAC address of the VAP Interface is displayed here. When you enable AP and reboot system, the MAC address will display here
- **ESSID**: Display Virtual AP's ESSID; default is AP00~AP07.
- **Status**: Display VAP status; default VAP0 is always on and only VAP0 can support WPS function.
- **Security Type**: Display Virtual AP's Security Type; default is disabled.
- **MAC Filter Setup**: Click “Setup” button for configuring Virtual AP's Access Control List.
- **VAP Edit**: Click “Edit” button for configuring Virtual AP's settings and security type.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

2.7 Virtual AP General Configuration

For each Virtual AP, administrators can configure general settings and security type. Click **Wireless** -> **Virtual AP Setup,** click "**Edit**" of Virtual AP List and then Virtual AP Configuration page appears.





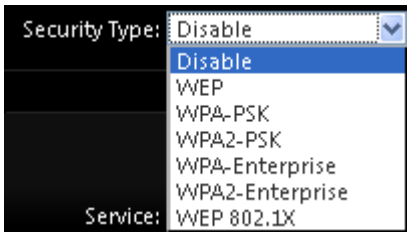
- **ESSID**: Extended Service Set ID indicates the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which is assigned to the specified VAP.

- **Hidden SSID**: Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from begin seen on networked.
- **Client Isolation**: Select Enable, all clients will be isolated from each other, that means all clients can not reach to other clients.
- **IAPP**: Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period.

Notice

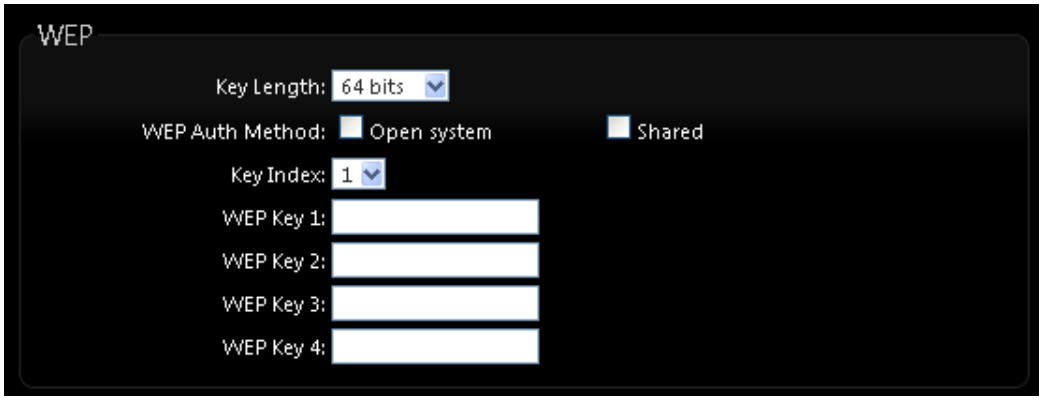
IAPP only used on WPA-PSK and WPA2-PSK security type. Only one of VAPs can be enabled.

- **Maximum Clients**: Enter maximum number of clients to a desired number. For example, while the number of client is set to 32, only 32 clients are allowed to connect with this VAP.
- **VLAN Tag(ID)**: Virtual LAN, the system supports tagged VLAN. To enable VLAN function; valid values are from 0 to 4094.
- **Security Type**: Select the desired security type from the drop-down list; the options are WEP, WPA-PSK, WPA2-PSK, WPA-Enterprise, WPA2-Enterprise and WEP 802.1X.



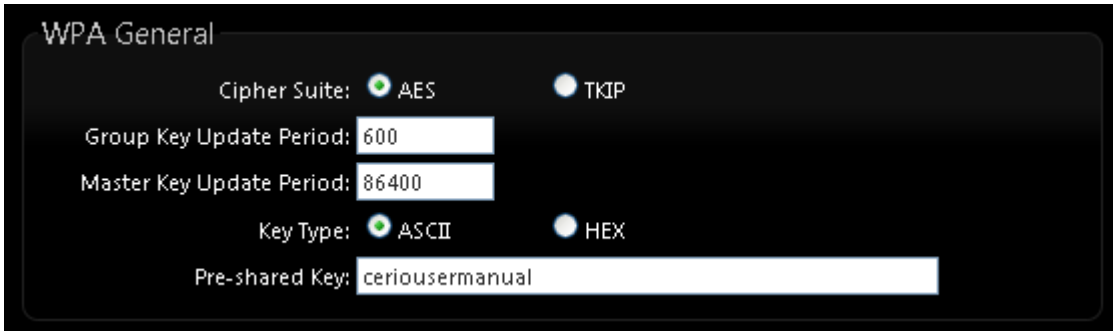
✓ **Disable**: Data are unencrypted during transmission when this option is selected.

✓ **WEP**: WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key. Select WEP as the security type from the drop down list as desired.



- ✧ **Key Length**: The key size of WEP encryption can be 64bit, 128bit or 152bit.
- ✧ **WEP auth method**: You can select the appropriate value: **Open system** (If enabling this mode, there is no need authentication to access AP or Wireless NIC) or **Shared** (Only those who are sharing the same key with the AP can connect with it).
- ✧ **Key Index**: You can select the Key which you want to use. Other wireless station must have the same key value to connect with OW-215N2-X, 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of WEP Key 1, 2, 3 or 4.
- ✧ **WEP Key #**: You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)

✓ **WPA-PSK (or WPA2-PSK)**: WPA-PSK is short for W-Fi Protected Access-Pre-Shared Key. WPA-SPK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user's certification.



- ✧ **Cipher Suite**: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

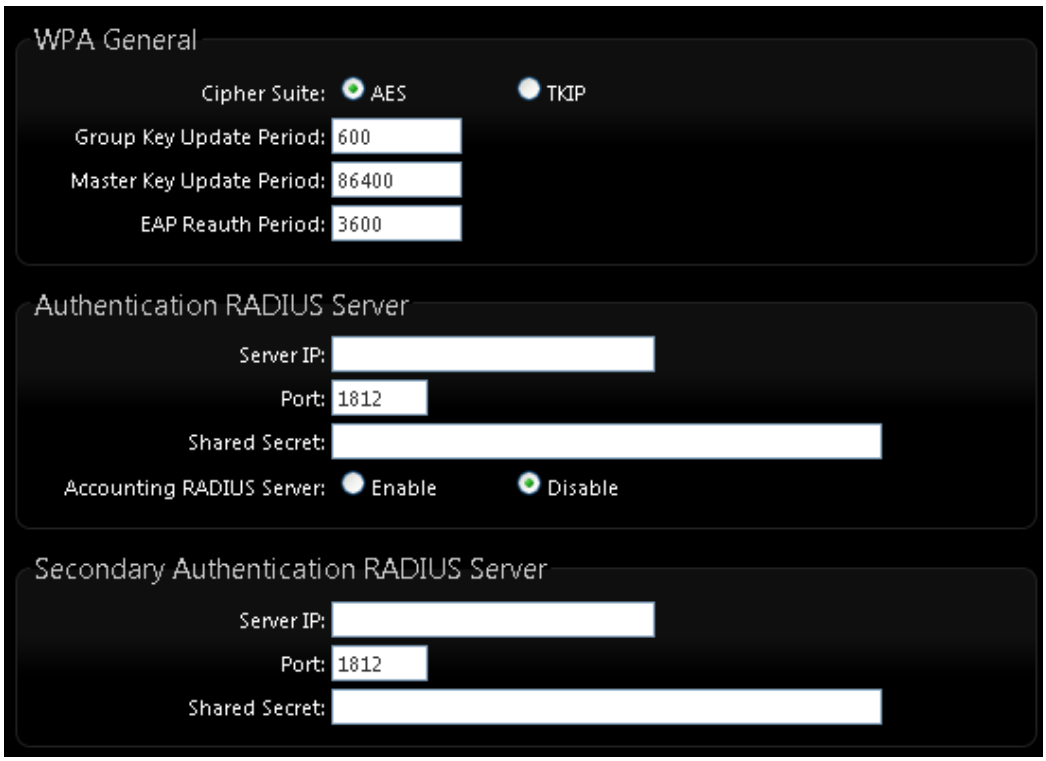
  AES is short for "**Advanced Encryption Standard**", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

  TKIP is short for "**Temporal Key Integrity Protocol**", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

- ✧ **Group Key Update Period**: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✧ **Master Key Update Period**: This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.
- ✧ **Key Type**: Check on the respected button to enable either **ASCII** or **HEX** format for the Pre-shared Key.
- ✧ **Pre-Shared Key**: Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

✓ **WPA-Enterprise (or WPA2-Enterprise) General Setting**

The RADIUS authentication and encryption will be both enabled if this selected.



General Setting :

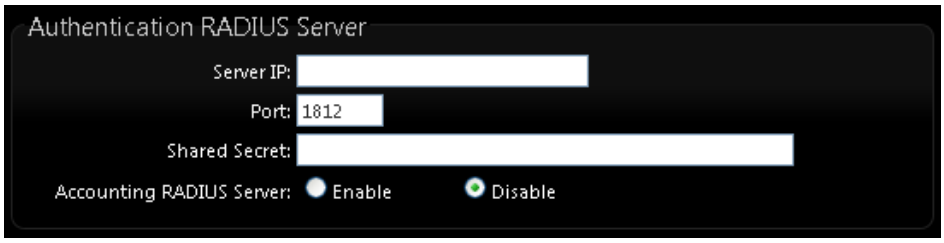
- ✧ **Cipher Suite**: You can chose use AES or TKIP with your WPA / WPA2 encryption method, **AES** is short for "**Advanced Encryption Standard**", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

TKIP is short for "**Temporal Key Integrity Protocol**", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

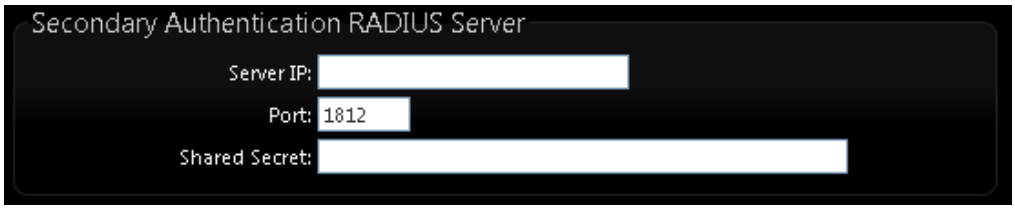
- ✧ **Group Key Update Period**: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✧ **Master Key Update Period**: This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.
- ✧ **EAP Reauth Period**: This time interval for re- authentication in seconds. Enter the time-length required; the default time is 3600 seconds; 0 = disable re-authentication.

Authentication RADIUS Server Settings



- ✧ **Authentication Server**: Enter the IP address of the Authentication RADIUS server.
- ✧ **Port**: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- ✧ **Shared secret**: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.
- ✧ **Accounting Server**: Check on the respected button to enable either Enable or Disable accounting RADIUS server.

Secondary Authentication RADIUS Server

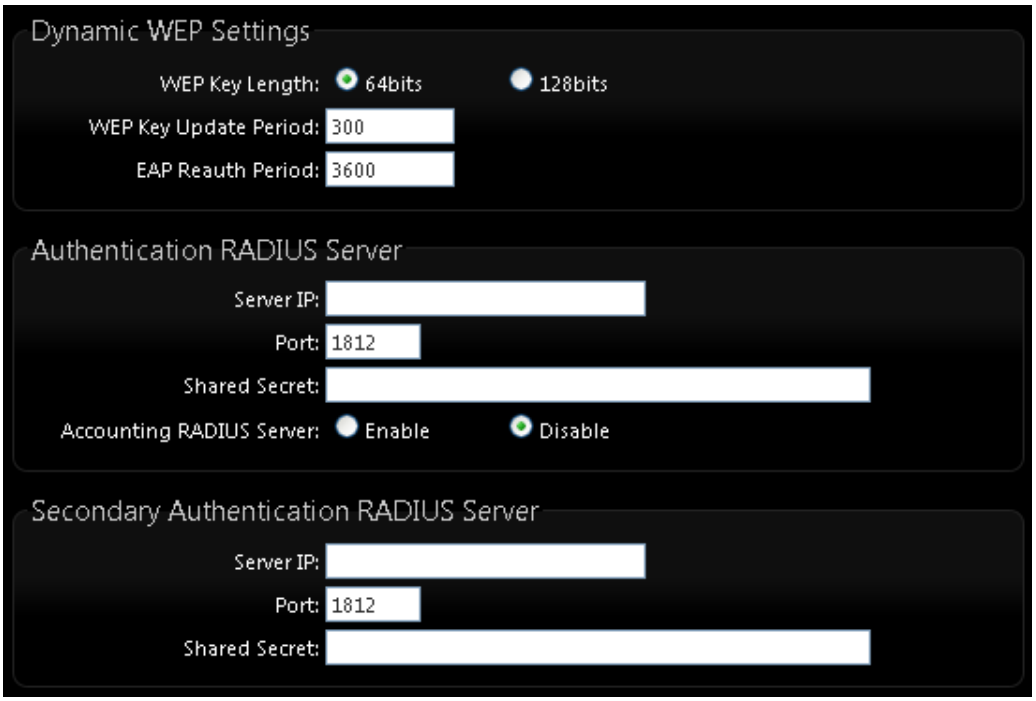


- ✧ **Authentication Server**: Enter the IP address of the Authentication RADIUS server.
- ✧ **Port**: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- ✧ **Shared secret**: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

✓ **WEP 802.1x :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.



Dynamic WEP Settings

- ✧ **WEP Key length**: Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- ✧ **WEP Key Update Period**: The time interval WEP will then be updated; the unit is in seconds; default is 300 seconds; 0 = do not rekey.
- ✧ **EAP Reauth Period**: EAP re-authentication period in seconds; default is 3600; 0 = disable re-authentication.

Authentication RADIUS Server Settings

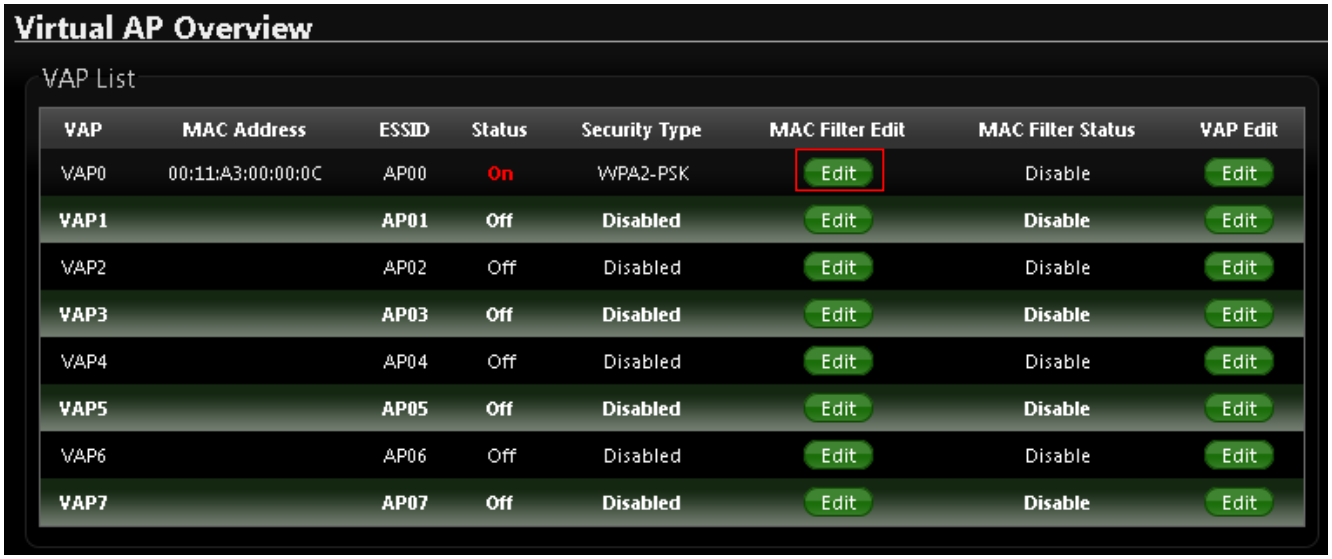
- ✧ **Authentication Server**: Enter the IP address of the Authentication RADIUS server.
- ✧ **Port**: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- ✧ **Shared secret**: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.
- ✧ **Accounting Server**: Check on the respected button to enable either Enable or Disable accounting RADIUS server.

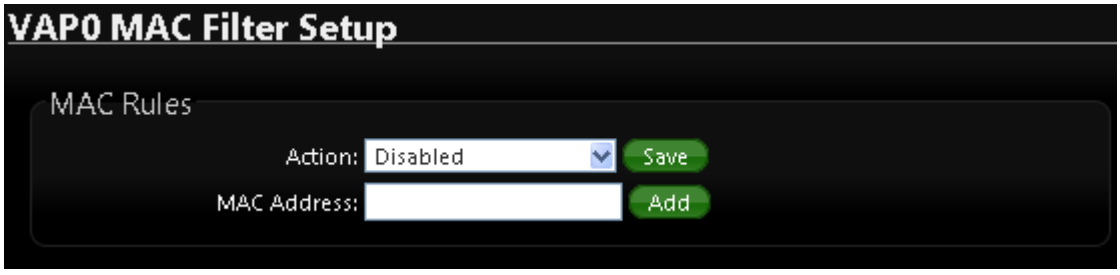
Secondary Authentication RADIUS Server

- ✧ **Authentication Server**: Enter the IP address of the Authentication RADIUS server.
- ✧ **Port**: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- ✧ **Shared secret**: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

➢ VAP MAC Filter Setup

In this function, the administrator can be allow or reject clients to access Virtual AP. Please click on **Wireless** -> **Virtual AP Setup** -> **MAC Filter Setup**, click "**Setup**" of Virtual AP List and then **MAC Filter Setup** page appears. Follow the below setting.





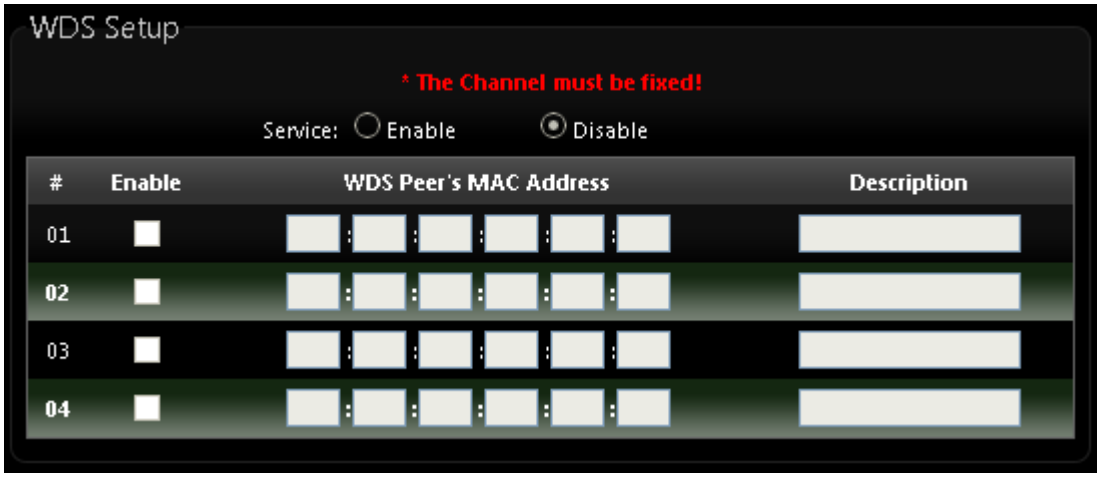
- **Action**: Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.
  - ✓ **Only Allow List MAC**: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "**Only Allow List MAC**".
  - ✓ **Only Deny List MAC**: Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to "**Only Deny List MAC**".

Notice

MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

2.8 WDS Setup - Expand your Wireless Network

The administrator can create WDS Links for expanding wireless network via this page. When you enable "**WDS**" function in AP Mode both Wireless and Ethernet user can connect your local network at the same time through **OW-215N2-X**. Please click on **Wireless** -> **Virtual AP Setup,** click "**Edit**" of Virtual AP List and follow the below setting.

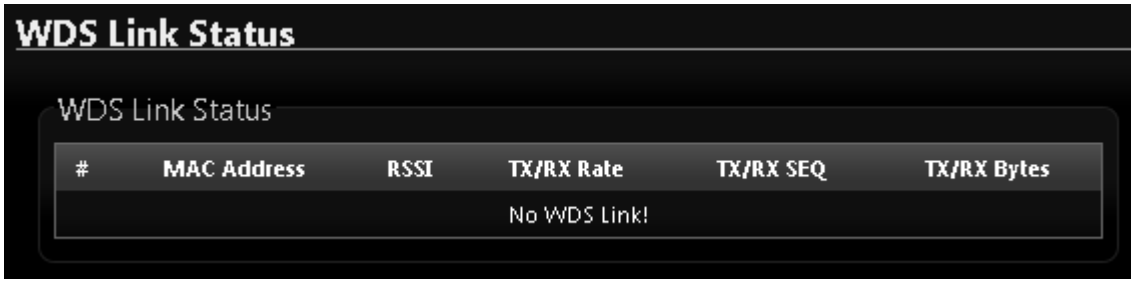


- **Service:** By default, it's "Disable". To "Enable" to activate WDS
- **Enable:** Click **Enable** checkbox to create WDS link.
- **WDS Peer's MAC Address**: Enter the MAC address of WDS peer.
- **Description**: Description of WDS link.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes.

2.9 WDS Status

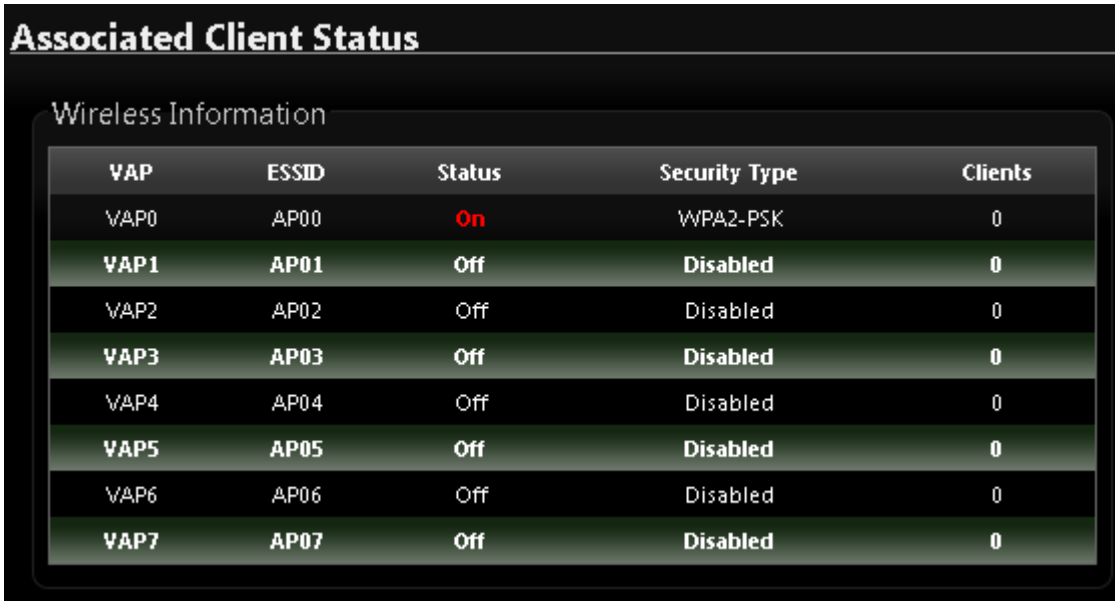
The Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.



- **MAC Address :** Display MAC address of WDS peer.
- **RSSI :** Indicate the RSSI of the respective WDS's link.
- **TX/RX Rate :** Indicate the TX/RX Rate of the respective WDS's link
- **TX/RX SEQ :** Indicate the TX/RX sequence of the respective WDS's link

2.10 Associated Clients

The administrator can obtain detailed wireless information and all associated clients status via this page. Please click on Wireless -> Associated Clients. The the Associated Clients Status appears.



Wireless Information : Display the Virtual AP configuration information of the system.

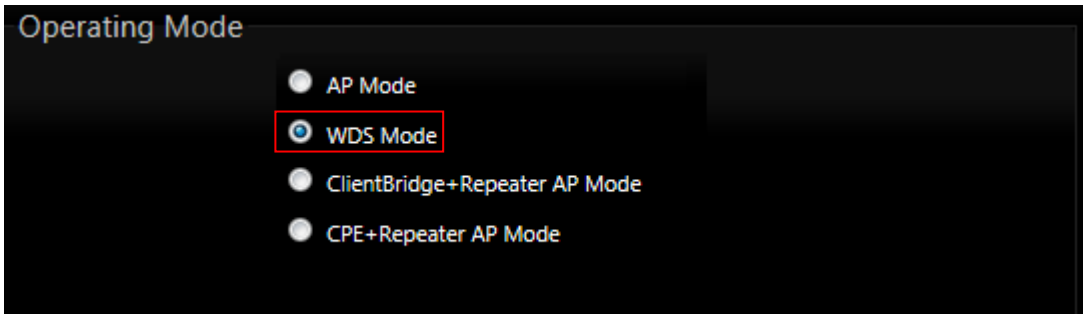
- **VAP** : Display number of system's Virtual AP.
- **ESSID** : Extended Service Set ID of the Virtual AP.
- **Status** : Display Virtual AP status currently.
- **Security Type :** Security type activated by the Virtual AP.
- **Clients :** Number of clients currently associated to the Virtual AP.

3. WDS Mode Configuration

When WDS mode is chosen, the system can be configured as an WDS mode. This section provides detailed explanation for users to configure in the WDS mode with help of illustrations. In the WDS mode, functions listed in the table below are also available from the Web-based GUI interface.

3.1 Choose Your Operating Mode (WDS Mode)

The system administrator can set the desired mode via this page, and then configure the system according to their deployment needs, Please click on **System -> Operating** Mode and follow the below setting.

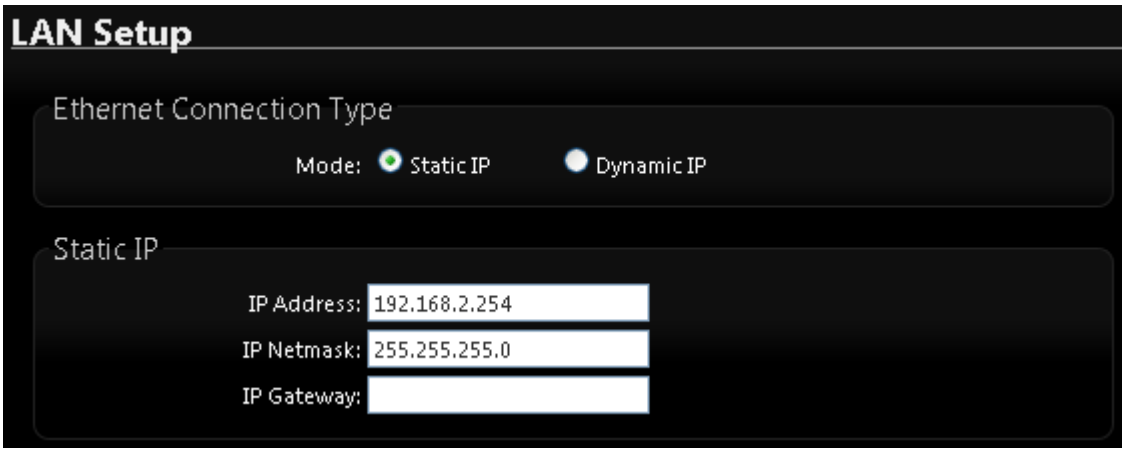


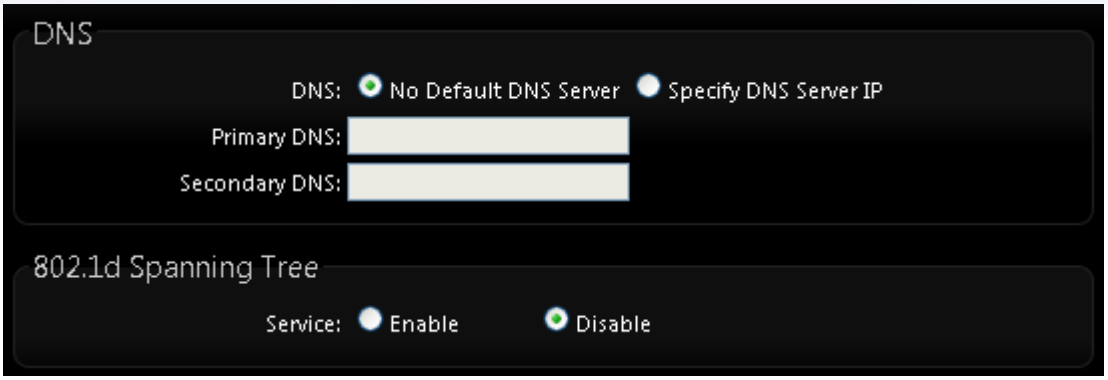
3.2 External Network Connection (Network Requirement)

You could expand your Ethernet network via WDS link. In this mode, the **OW-215N2-X** connects directly to a wired LAN, and wirelessly bridges to a remote access point via a WDS link as shown in picture. In the mode, it can't associate with any wireless clients.

3.3 Configure OW-215N2-X LAN IP Address

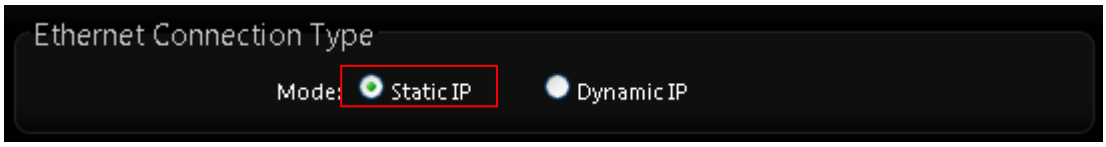
Here are the instructions to setup the local IP Address and Netmask.
Please click on **System** -> **LAN** and follow the below setting.



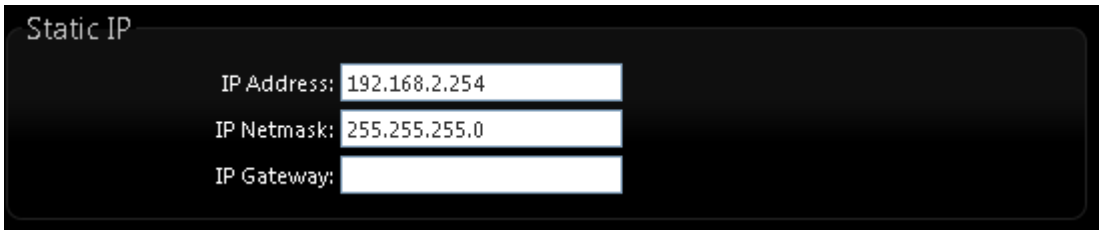


➢ **Ethernet Connection Type**:

Check either "**Static IP**" or "**Dynamic IP**" button as desired to set up the system IP of LAN port.



- **Static IP**: The administrator can manually setup the LAN IP address when static IP is available/ preferred.

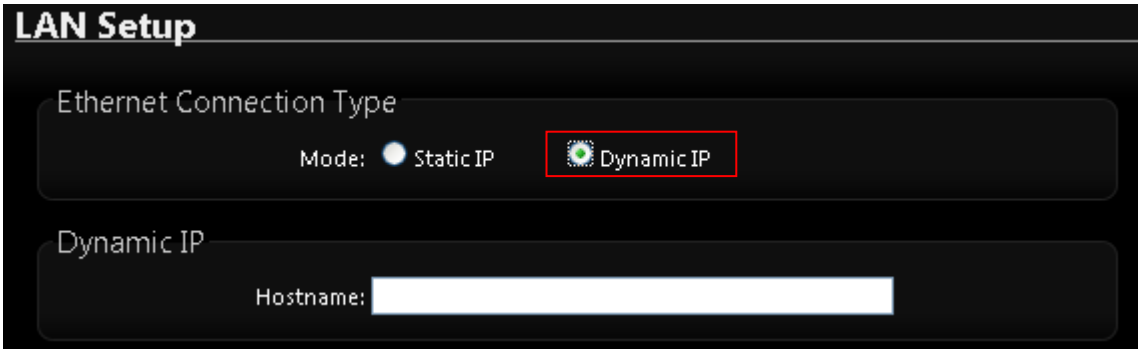


✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254

✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0

✓ **IP Gateway** : The default gateway of the LAN port

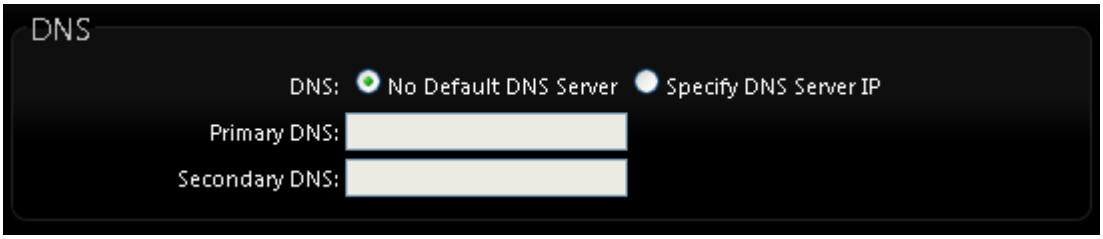
- **Dynamic IP**: This configuration type is applicable when the **OW-215N2-X** is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.



✓ **Hostname** : The Hostname of the LAN port.

➢ **DNS**:

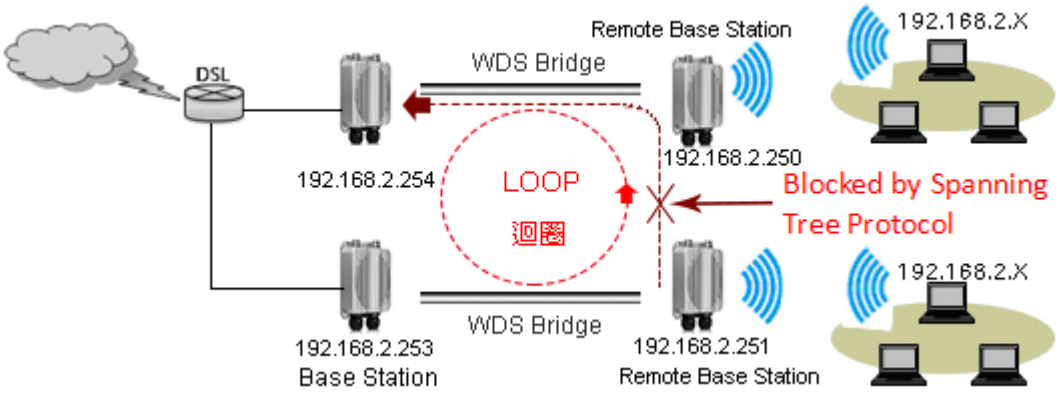
Check either "**No Default DNS Server**" or "**Specify DNS Server IP**" button as desired to set up the system DNS.

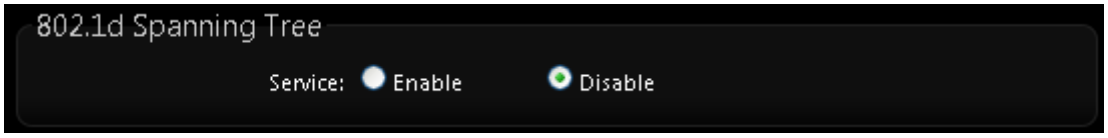


- **Primary** : The IP address of the primary DNS server.
- **Secondary** : The IP address of the secondary DNS server.

➢ **802.1d Spanning Tree**

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



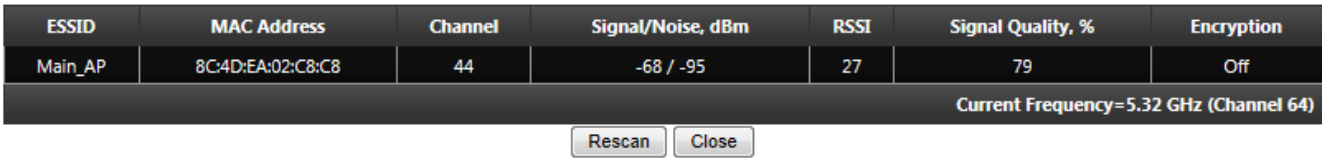


Click **Save** button to save your changes. Then click **Reboot** button to activate your changes.

3.4 Wireless General Settings

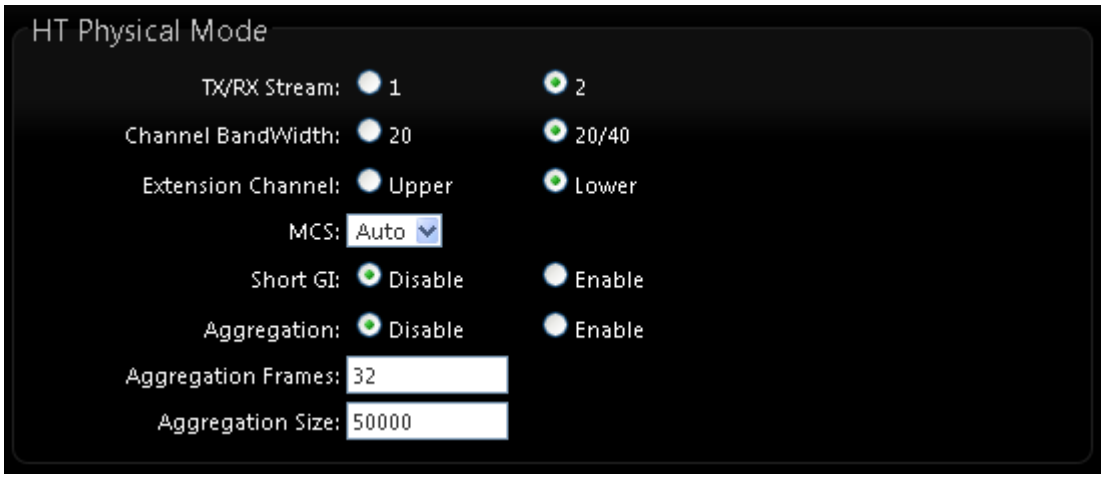
The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

- **Band Mode :** Select an appropriate wireless band; bands available are **801.11 a/n mixed mode or** Pure a mode or Pure n mode etc.
- **Country :** a region, the OW-215N2-Xsupport region for US,ETSI and Japan
- **Channel :** Choosing the best WiFi channel
  - ✧ Auto Scan : Smart channel judgment, the function can auto choose use best Channel
  - ✧ AP List : the function support search neighborhood AP and print site survey list



- **TX Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level ***1*** to level 9 (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level 9 (**100**%).
- **RF(On/Off) Schedule :** The AP **RF** Signal on/off by time Policy

➢ HT Physical Mode



- **HT TxStream/RxStream :** By default, it's **2**
- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- **Extension Channel :** Only for Channel Bandwidth "**40**" MHz. Select the desired channel bonding for control.
- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI :** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

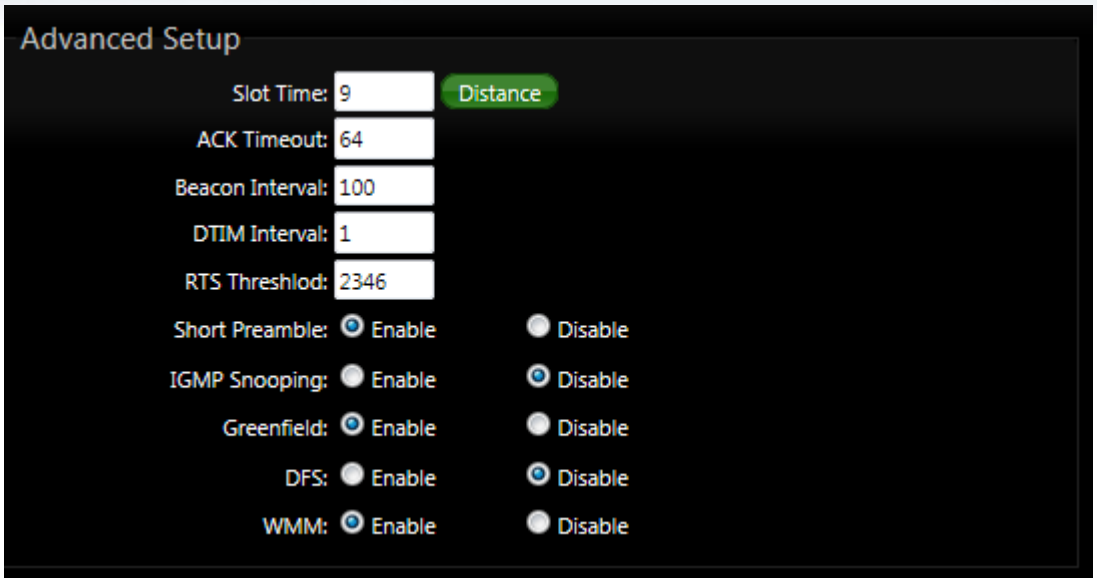
- **Aggregation :** By default, it's "**Enable**". To "Disable" to deactivated Aggregation.
  A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining 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.
- **Aggregation Frames :** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.

- **Aggregation Size :** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all VAPs and WDS Link**.

3.5 Configure Wireless Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.
  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.
  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".
  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Notice

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval :** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.
  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.
  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.
  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.
  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **IGMP Snooping :** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

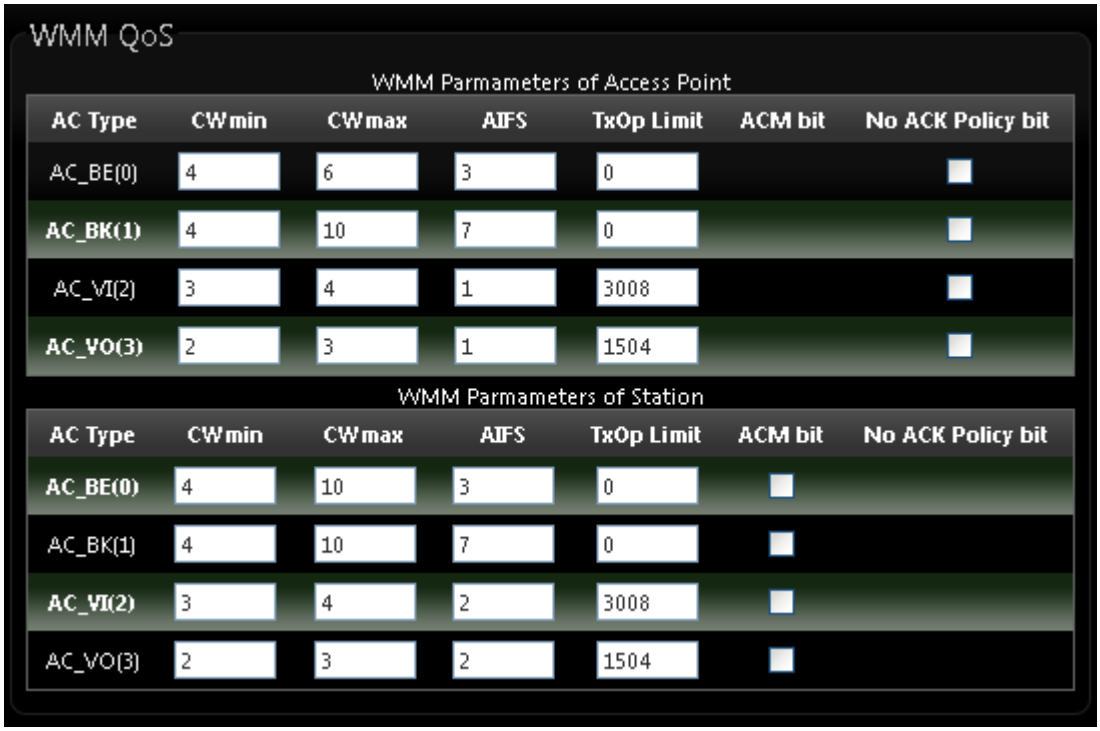
- **DFS :** Is IEEE802.11H With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary. The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

- **Greenfield :** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.

- **WMM QoS :** This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video,

multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.



✓ **AC Type** :

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

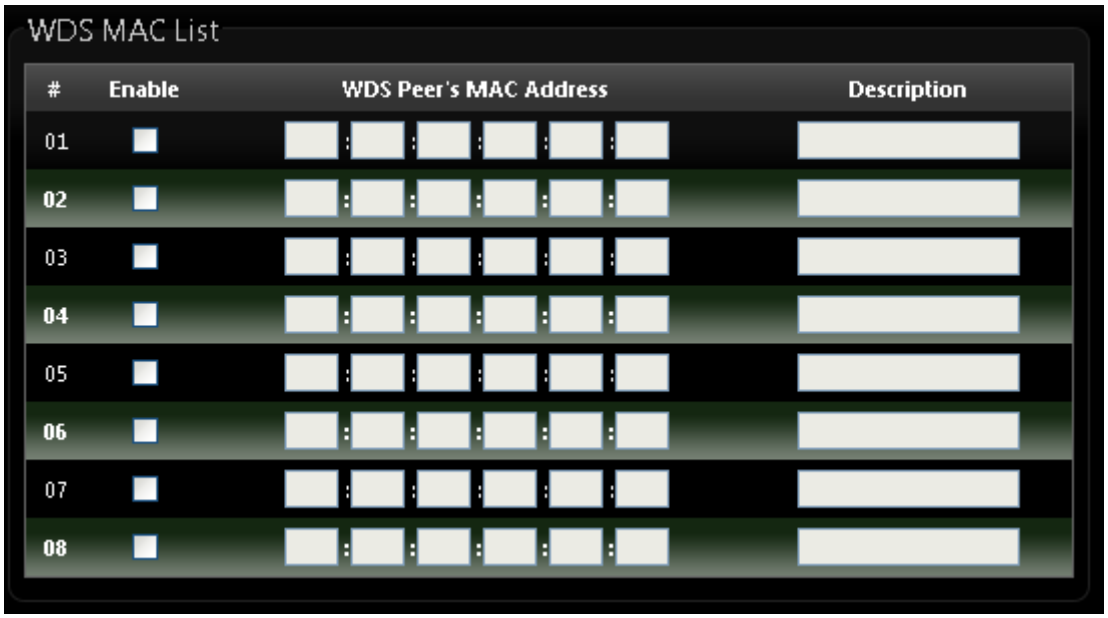
- ✓ **CWmin**：Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. ◦
- ✓ **CWmax**：Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦
- ✓ **AIFS**：The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit**：Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit**：Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit**：Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click “**Checkbox**” indicates “**No ACK**”
  When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.
  When the Normal ACK policy is used, the recipient acknowledges each received uncast packet. ◦

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

3.6 WDS Setup

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.

Please click on **Wireless** -> **WDS Setup** and follow the below setting.



- **Security Type** : Option is “Disable”, “WEP”, “TKIP”or “AES” from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
  - **WEP Key** : Enter 5 / 13 ASCII or 10 / 26 HEX format WEP key.
  - **AES Key** : Enter 8 to 63 ASCII or 64 HEX format AES key.

- **WDS MAC List**
  - **Enable** : Check “**Enable**” to create WDS link.
  - **WDS Peer's MAC Address** : Enter the MAC address of WDS peer.
  - **VLAN Tag(ID)**: Virtual LAN, the system supports tagged VLAN with WDS. To enable VLAN function; valid values are from 0 to 4094; space is disabled.

- **Description** : Description of WDS link.

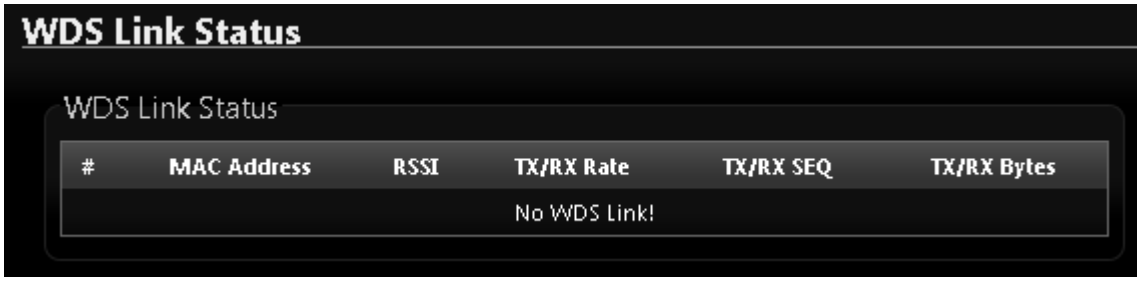
Notice

The WDS link needs to be set at same Channel and with same Security Type.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes.

3.7 WDS Status

The Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.



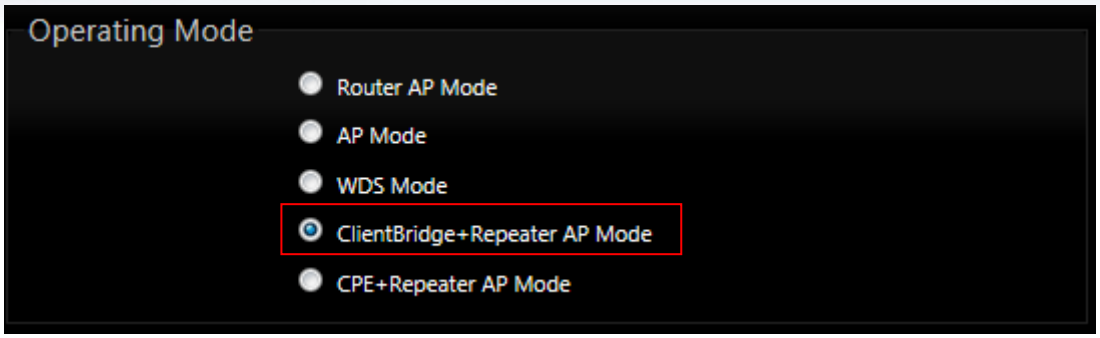
- **MAC Address :** Display MAC address of WDS peer.
- **RSSI :** Indicate the RSSI of the respective WDS's link.
- **TX/RX Rate :** Indicate the TX/RX Rate of the respective WDS's link
- **TX/RX SEQ :** Indicate the TX/RX sequence of the respective WDS's link

4. Client Bridge + Repeater AP Mode Configuration

When Client Bridge + Repeater AP Mode is chosen, the system can be configured as an Client Bridge + Repeater AP Model. This section provides detailed explanation for users to configure in the Client Bridge + Repeater AP Mode with help of illustrations. In the Client Bridge + Repeater AP Mode, functions listed in the table below are also available from the Web-based GUI interface.

4.1 Chose Your Operating Mode(Client Bridge + Repeater AP)

The system administrator can set the desired mode via this page, and then configure the system according to their deployment needs, Please click on System -> Operating Mode and follow the below setting.



4.2 External Network Connection (Network Requirement)

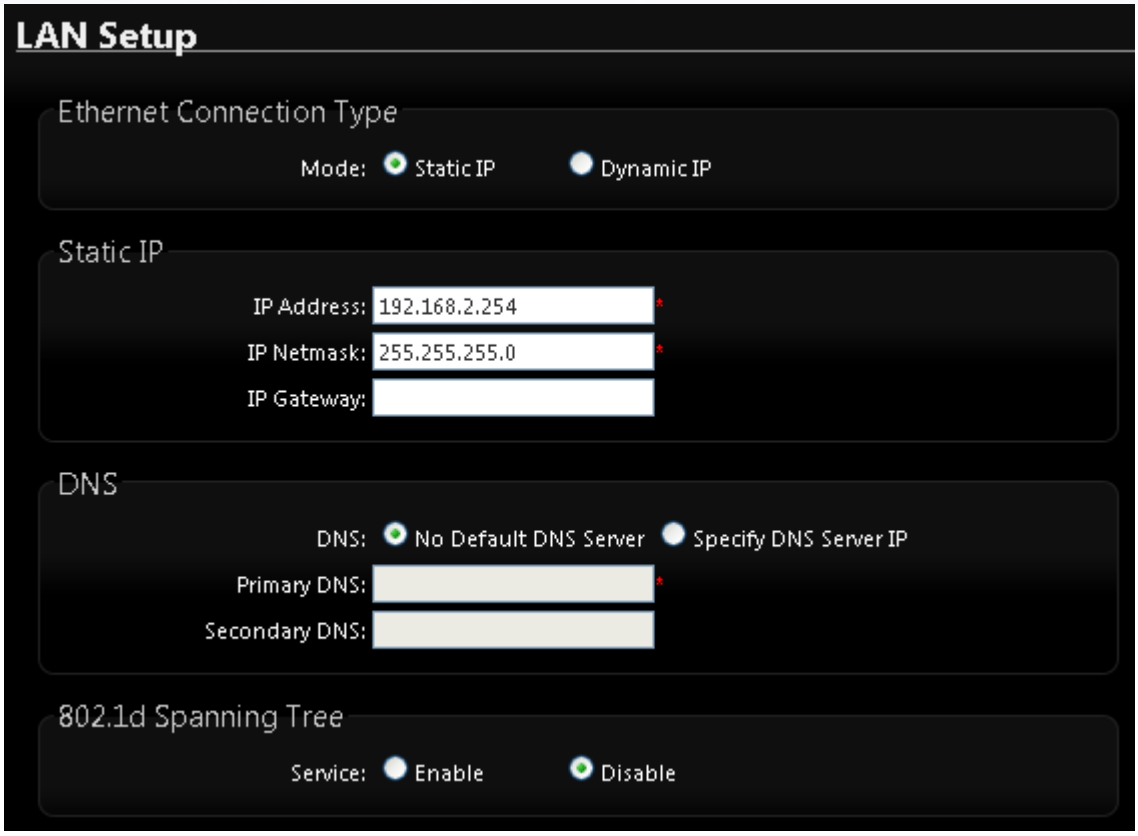
It can be used as an Client Bridge or Repeater AP to receive wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, **OW-215N2-X** is enabled with DHCP Server functions. The wired clients of **OW-215N2-X** are in the same subnet from Main Base Station and it accepts wireless connections from client devices.

Notice

*When the **OW-215N2-X** configured as an Access Point and Client Station simultaneously, the Wireless General and Advanced Setup also used simultaneously. But the Security Type can be different. In the other word, the channel or other settings will be the same between **OW-215N2-X** to Main Base Station and wireless client to **OW-215N2-X** , but security type can be different.*

4.3 Configure OW-215N2-X LAN IP Address

Here are the instructions for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.



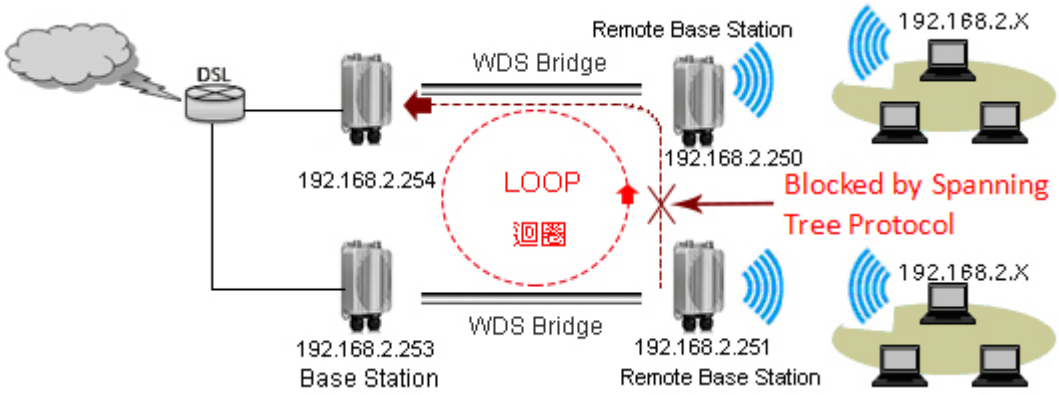
- **LAN IP Setup :** The administrator can manually setup the LAN IP address.
  - **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
  - **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0

- **DNS**: Check either "**No Default DNS Server**" or "**Specify DNS Server IP**" button as desired to set up the system DNS.
  - **Primary** : The IP address of the primary DNS server.
  - **Secondary** : The IP address of the secondary DNS server.

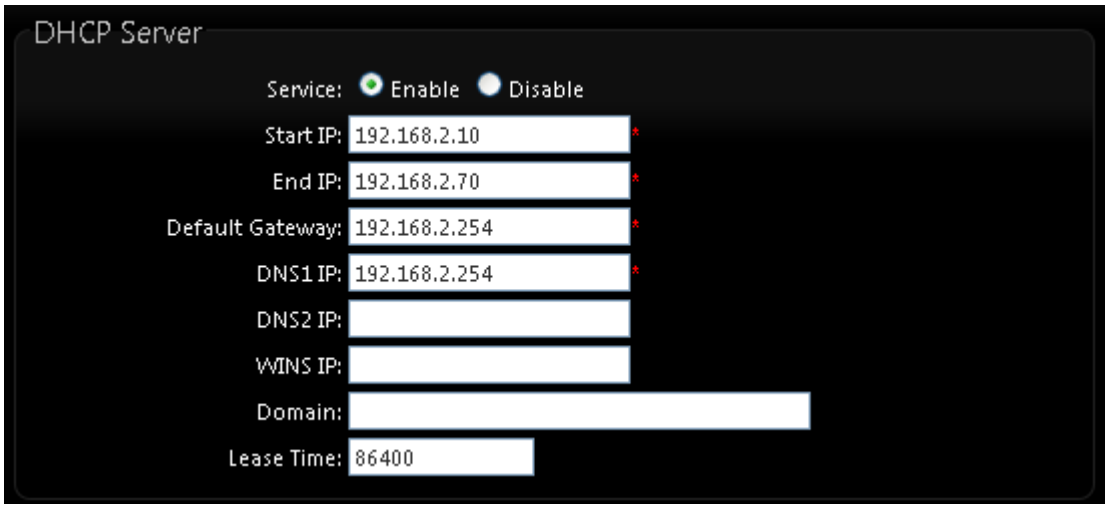
- **802.1d Spanning Tree :**

  The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw



➢ **DHCP Setup :** Devices connected to the system can obtain an IP address automatically when this service is enabled.



- **DHCP :** Check ***Enable*** button to activate this function or ***Disable*** to deactivate this service.
- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- **DNS1 IP :** Enter IP address of the first DNS server; this field is required.
- **DNS2 IP :** Enter IP address of the second DNS server; this is optional.
- **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain :** Enter the domain name for this network.
- **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 interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.4 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

- **MAC Address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are **801.11 a/n mixed mode or pure a mode or pure n mode etc.**
- **Country :** a region, the OW-215N2-X support region for US,ETSI and Japan
- **TX Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level ***1*** to level 9 (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level 9 (**100**%).
- **RF(On/Off) Schedule :** The AP **RF** Signal on/off by time Policy

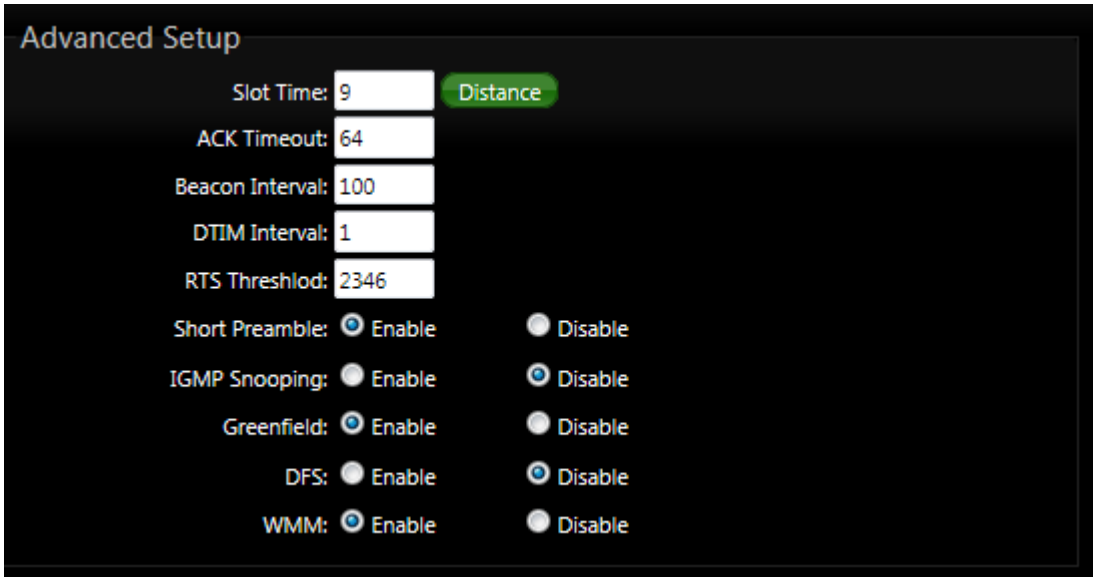
➢ **HT Physical Mode**

- **Tx/Rx Stream :** By default, it's **2**
- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.

- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI :** Short Guard Interval, by default, it's “Enable”. it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation :** By default, it's “**Enable**”. To “Disable” to deactivated Aggregation.
  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.
- **Aggregation Frames :** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

4.5 Configure Wireless Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.
  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

  Notice: Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval :** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec. Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.
  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.
  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.
  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

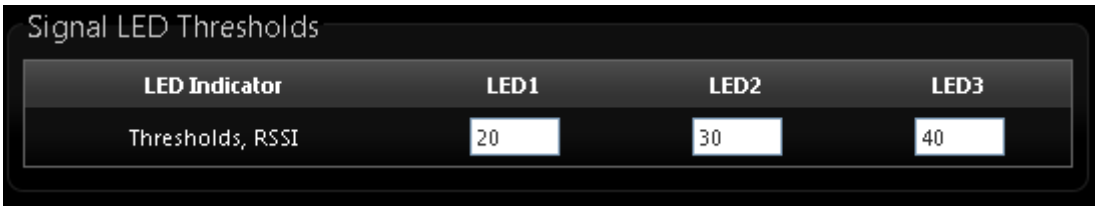
- **IGMP Snooping :** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

- **DFS :** Is IEEE802.11H With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary. The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

- **Greenfield :** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.

- **Signal LED Thresholds :** This function can setting RSSI number(1~99) to control signals LED's, The OW-215N2-X system will calculate for RSSI number and total of three LED's indicator, If LED's whole bright indicate signal is the strong.

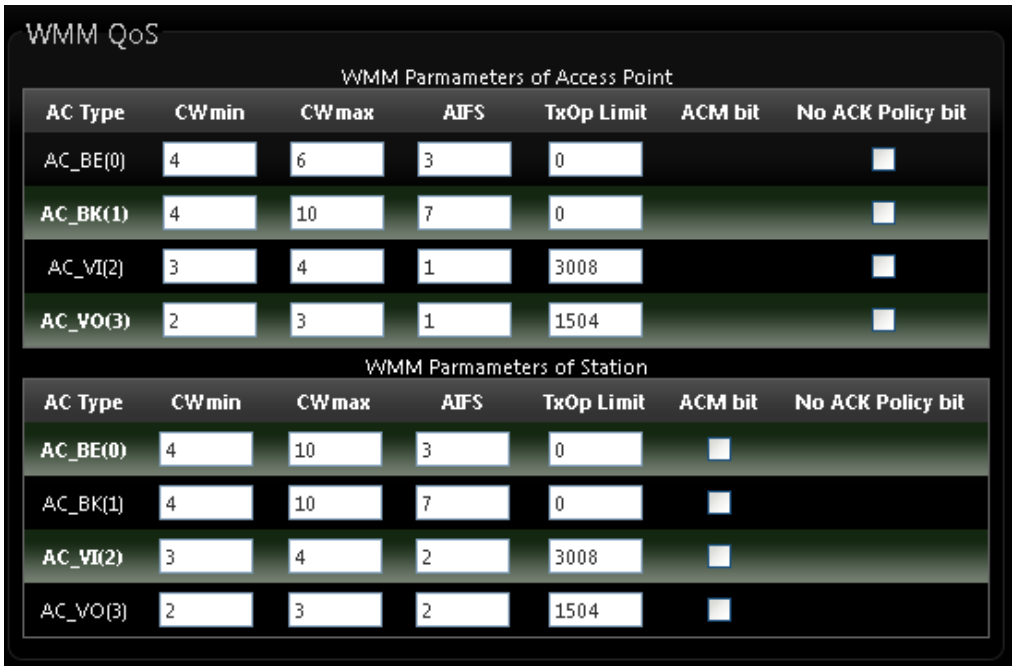
Notice The function only support Client Bridge and WISP modes



✓ LED Indicator : Total of three LED's, the LED1 RSSI number is Minimum

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- **WMM QoS :** This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.
  As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.



✓ **AC Type** :

Queue		Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

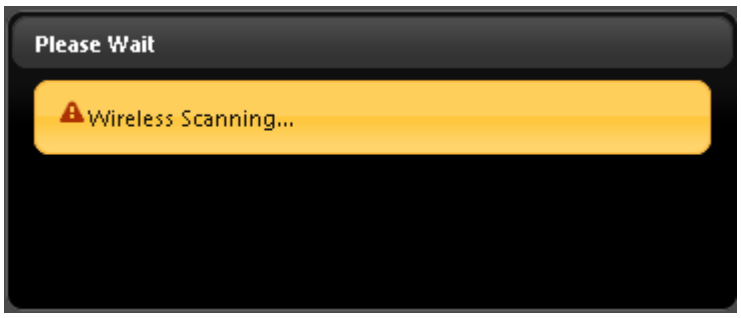
- ✓ **CWmin**：Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. ◦
- ✓ **CWmax**：Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦
- ✓ **AIFS**：The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit**：Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit**：Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit**：Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click “**Checkbox**” indicates “**No ACK**”
  When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange.

  This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received uncast packet. ◦

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

4.6 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with. Please click on **Wireless** -> **Site Survey**. Below depicts an example for site survey.



ESSID	MAC Address	Signal/Noise, dBm	RSSI	Signal Quality, %	Channel	Security	Select
Main_AP	8C:4D:EA:02:C8:C8	-69 / -95	26	76%	44	NONE	Select

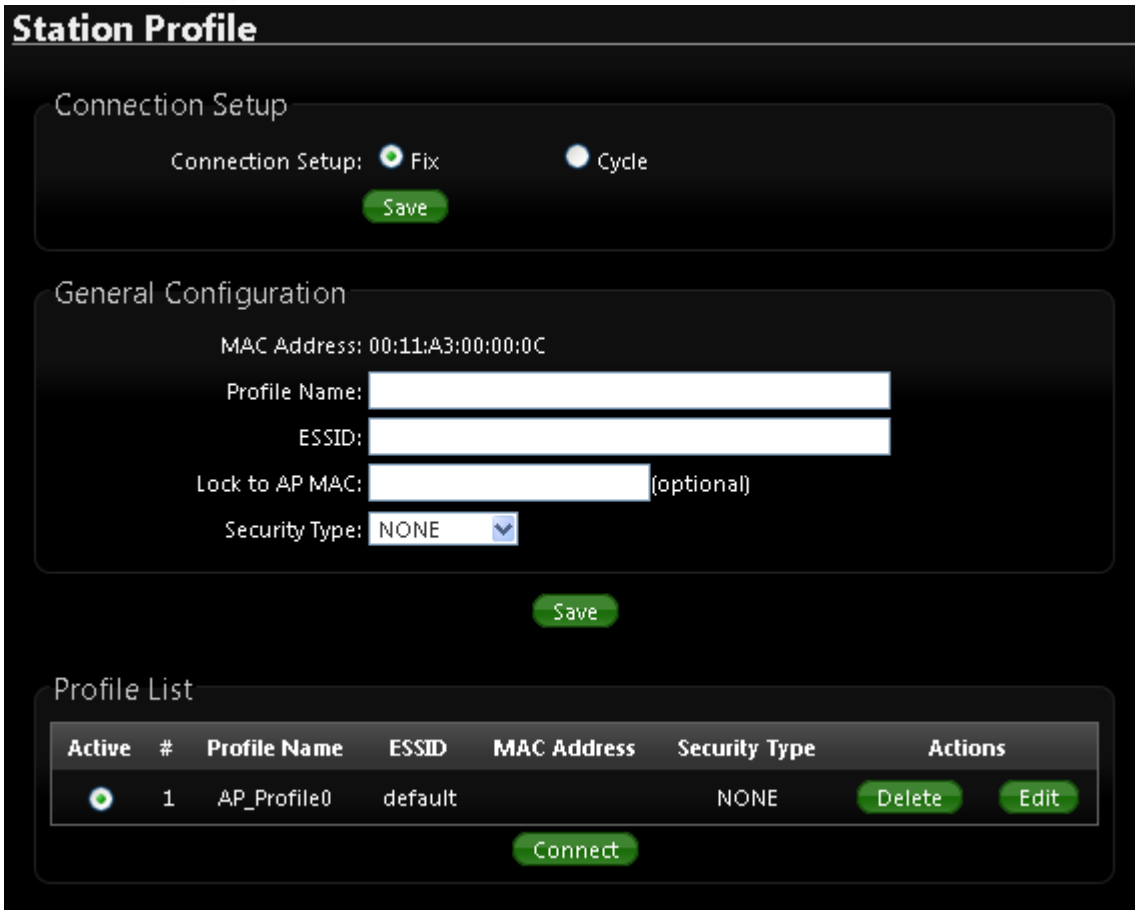
- **ESSID** : Available Extend Service Set ID of surrounding Access Points.
- **MAC Address** : MAC addresses of surrounding Access Points.
- **Signal/Noise dBm** : Received signal strength of all found Access Points.
- **RSSI :** Indicate the RSSI of the respective client's association.
- **Signal Quality (%) :** Received signal strength of all found Access Points.
- **Channel** : Channel numbers used by all found Access Points.
- **Security** : Security type by all found Access Points.
- **Select** : Click "**Select**" to configure settings and associate with chosen AP.

Notice

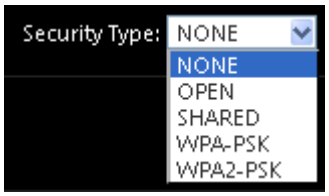
*While clicking "Select" button in the Site Survey Table, the "**ESSID**" and "**Security Type**" will apply in the Wireless General Setup. However, more settings are needed including Security Key.*

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

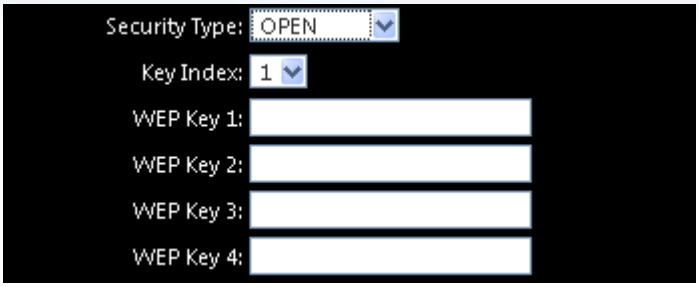
4.7 Station Profile



- **Connection Setup :** Can you choose Fix or cycle
- **General Configuration :**
  - **MAC address :** The remote AP MAC Address
  - **Profile Name** : Set different profiles for quick connection uses.
  - **ESSID** : Assign Service Set ID for the wireless system.
  - **Lock to AP MAC** : the function will lock remote AP MAC Address.
  - **Security Type :** Select an appropriate security type for association, the Security Type can be selected in "**NONE**", "**OPEN**", "**SHARED**", "**WPA-PSK**", or "**WPA2-PSK**" from drop-down list; the type needs to be the same as that associated access point.



  - **OPEN / SHARED** : OPEN and SHARED require the user to set a WEP key to exchange data.



✓ **Key Index** : key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.

✓ **WEP Key #** : Enter HEX or ASCII format WEP key value; the system supports up to 4 sets of WEP keys.

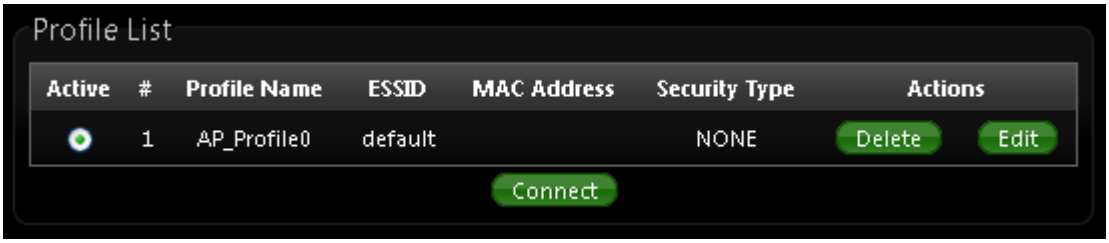
Key Length	Hex	ASCII
64-bit	10 Characters	5 Characters
128-bit	26 Characters	13 Characters

- **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

✓ **Cipher Suite** : Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**.

✓ **Pre-shared Key** : Enter the information for pre-shared key; the key can be either entered as a **256-bit** secret in **64** HEX digits format, or **8** to **63** ASCII characters.

➢ **Profile List :** The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List.



- Click “”**Edit**” an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “**Save**” button to save the profile.
- Click “**Delete**” to remove profile.
- Click and Select a profile from list, then click the “**Connect**” button to connecting to the wireless network with the profile setting.

Notice	*Before you click "**Connect**" button for connection, Please double check the "**Channel**" setting of "Wireless General Setup" page on OW-215N2-X as it must be the same with associated AP channel setting*

Notice	*If you only click "Connect" button and does not click "Save" button. The selected profile would not be saved on the Profile List*

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes.

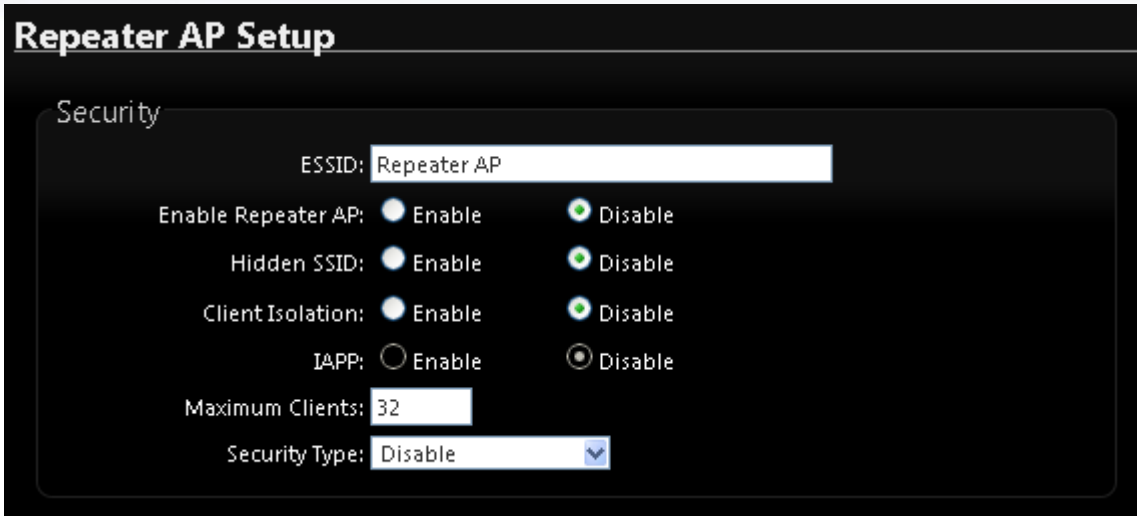
4.8 Remote AP Status

Show the remote bridge AP whether is link or unlinked

4.9 Repeater AP Setup

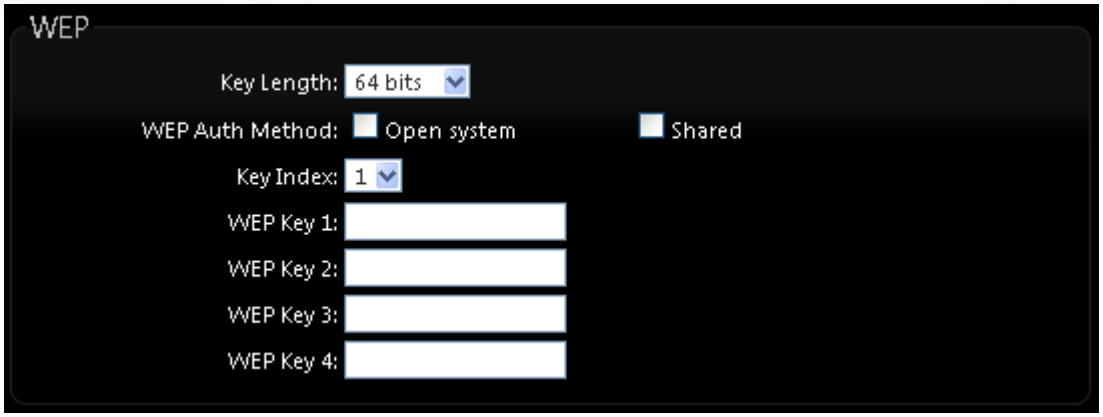
The network manager can configure related wireless settings, **AP Setup**, **Security Settings**, and **Access Control Settings**.

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings.



- **ESSID** : Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP clients associated with the specified VAP.
- **Enable Repeater AP :** choose Enable or Disable Repeater AP function, the default is Disable
- **Hidden SSID :** By default, it's "**Disable**". Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.
- **Client Isolation :** By default, it's "**Disable**". Select "Enable", all clients will be isolated from each other, which means they can't reach each other.
- **IAPP :** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period.
- **Maximum Clients** : The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.
- **Security Type** : Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
  - **Disable** : Data are unencrypted during transmission when this option is selected.
  - **WEP** : Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw



- ✓ **Key Index** : Skey index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **Key Auth Method :** Enable the desire option among OPEN or SHARED .
- ✓ **WEP Key #** : Enter HEX or ASCII format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

- **WPA-PSK (or WPA2-PSK) :**

WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

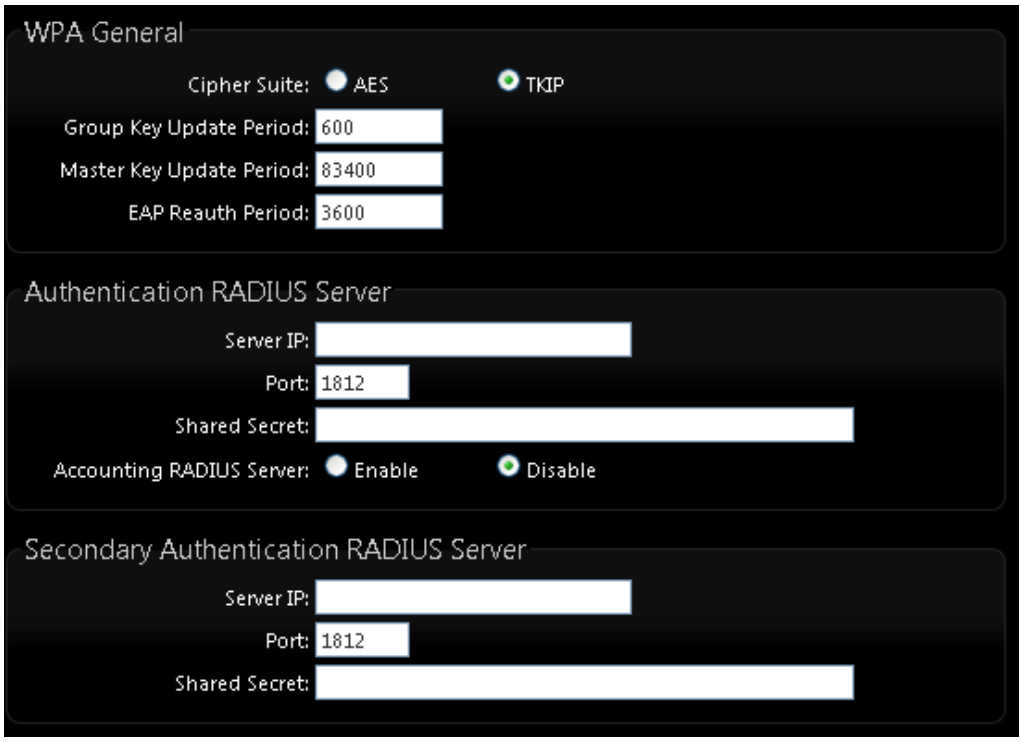
- ✓ **Cipher Suite** : By default, it is AES. Select either AES or TKIP cipher suites.
- ✓ **Pre-shared Key** : Enter the pre-shared key; the format shall go with the selected key type.

Notice

Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period** : By default, it is 3600 seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

- **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this is selected.



WPA General Settings :

- ✓ **Cipher Suite** : By default, it is AES. Select either AES or TKIP cipher suites.
- ✓ **Group Key Update Period** : By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- ✓ **PMK Cache Period** : By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- ✓ **Pre-Authentication** : By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.

Notice *PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise*

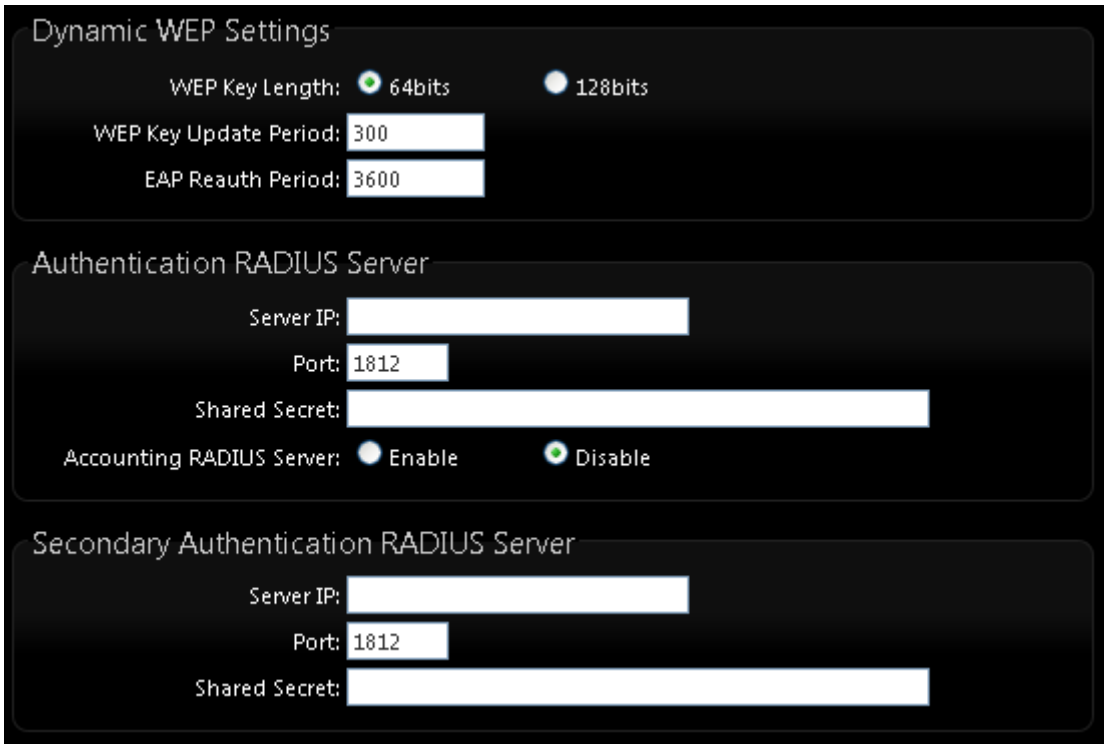
Authentication Radius Server Settings :

- ✓ **IP Address** : Enter the IP address of the Authentication RADIUS server.
- ✓ **Port** : By default, it's 1812. The port number used to communicate with RADIUS server.
- ✓ **Shared secret** : A secret key used between system and RADIUS server. Supports 8 to 64 characters.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- ✓ **Session Timeout** : The Session timeout is in the range of 0~60 seconds. The default is 0 to disable re-authenticate service. Amount of time before a client will be required to re-authenticate.

- **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

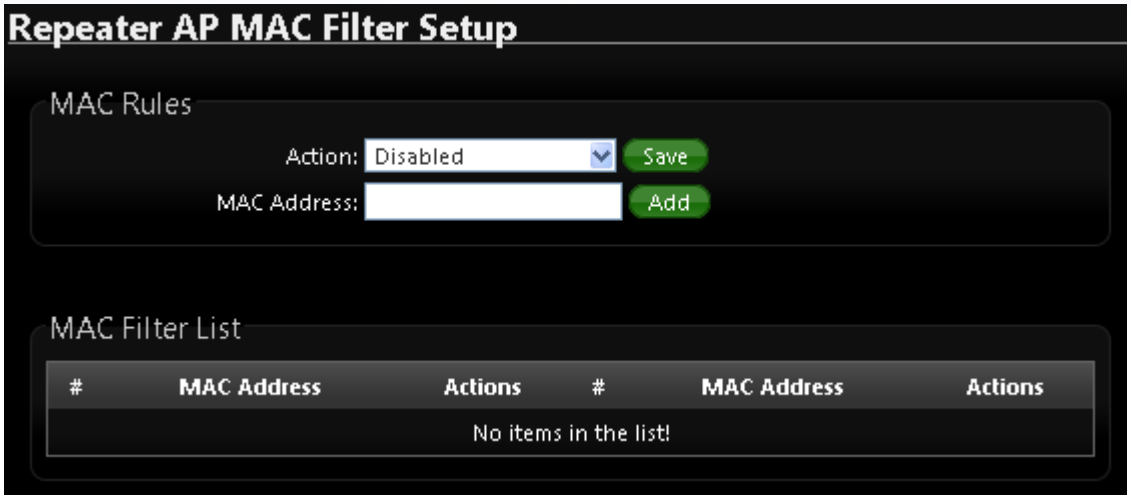


Authentication Radius Server Settings :

- ✓ **IP Address** : Enter the IP address of the Authentication RADIUS server.
- ✓ **Port** : By default, it's 1812. The port number used to communicate with RADIUS server.
- ✓ **Shared secret** : A secret key used between system and RADIUS server. Supports 8 to 64 characters.
- ✓ **Session Timeout** : The Session timeout is in the range of 0~60 seconds. The default is 0 to disable re-authenticate service. Amount of time before a client will be required to re-authenticate.

4.10 Repeater AP MAC Filter Setup

Continue **Virtual AP Setup** section. For each Virtual AP setting, the administrator can allow or reject clients to access each Virtual AP.



- **Action**: Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.
  - ✓ **Only Allow List MAC**: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "**Only Allow List MAC**".
  - ✓ **Only Deny List MAC**: Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to "**Only Deny List MAC**".

Notice

***Notice**: MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.*

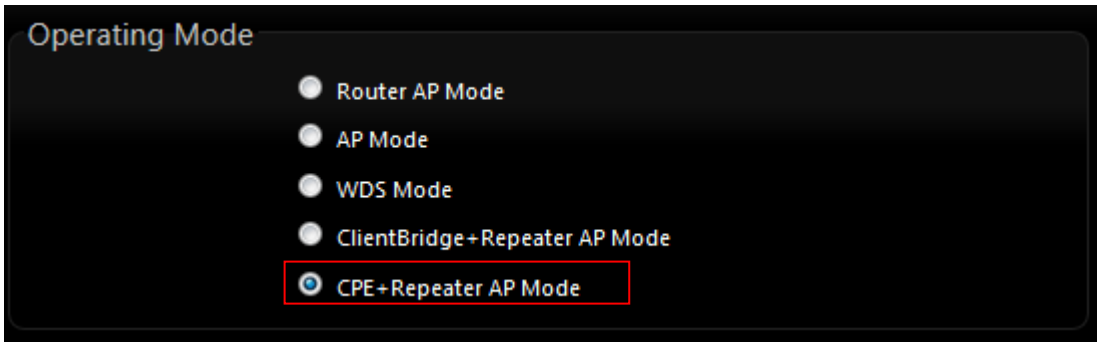
There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

5. CPE + AP Mode Configuration

When WISP + AP Mode is chosen, the system can be configured as an WISP + AP Mode. This section provides detailed explanation for users to configure in the WISP + AP Mode with help of illustrations. In the WISP + AP Mode, functions listed in the table below are also available from the Web-based GUI interface.

5.1 Choose Your Operating Mode (CPE + Repeater AP Mode)

The system administrator can set the desired mode via this page, and then configure the system according to their deployment needs, Please click on System -> Operating Mode and follow the below setting.



5.2 External Network Connection (Network Requirement)

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE mode, **OW-215N2-X** is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to **OW-215N2-X** are in **different** subnet from those connected to Main Base Station, and, in CPE mode, it **does not** accept wireless association from wireless clients.

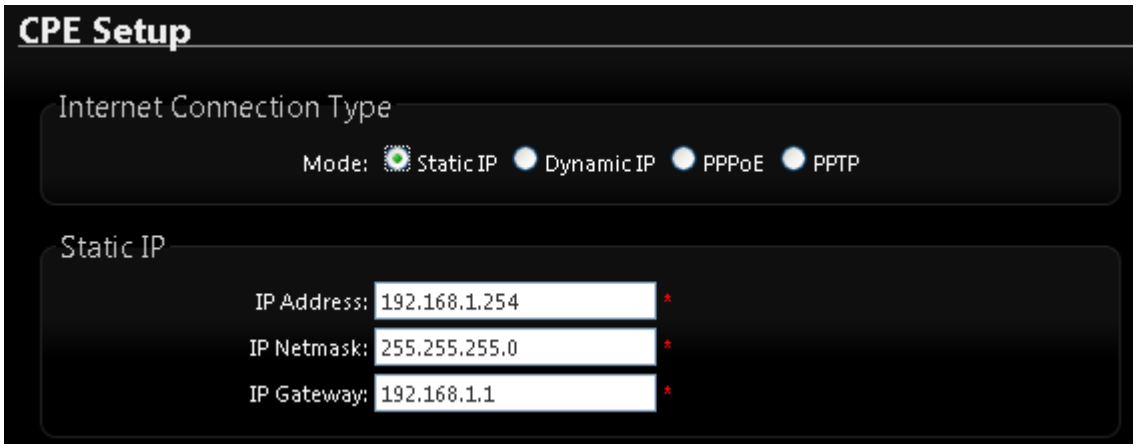
Notice *In CPE mode, the WAN port is the Wireless interface.*

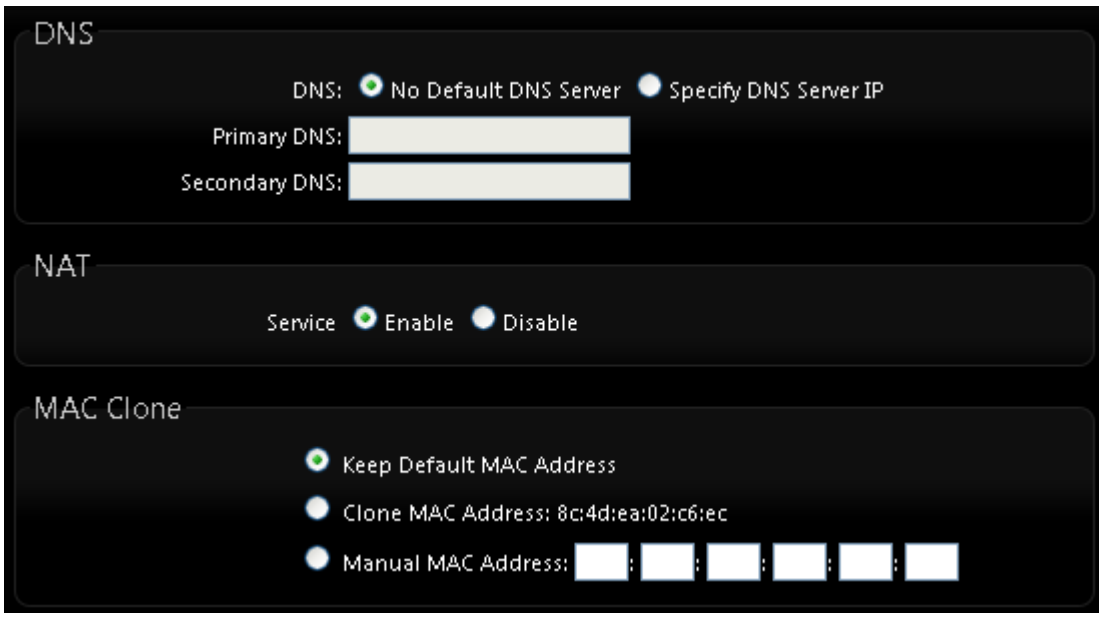
Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

5.3 Configure CPE(WAN) Setup

OW-215N2-X is a gateway enabled with NAT and DHCP Server functions. The wireless clients connected to Internet.

There are three connection types for the WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**. Please click on **System -> CPE** and follow the below setting.

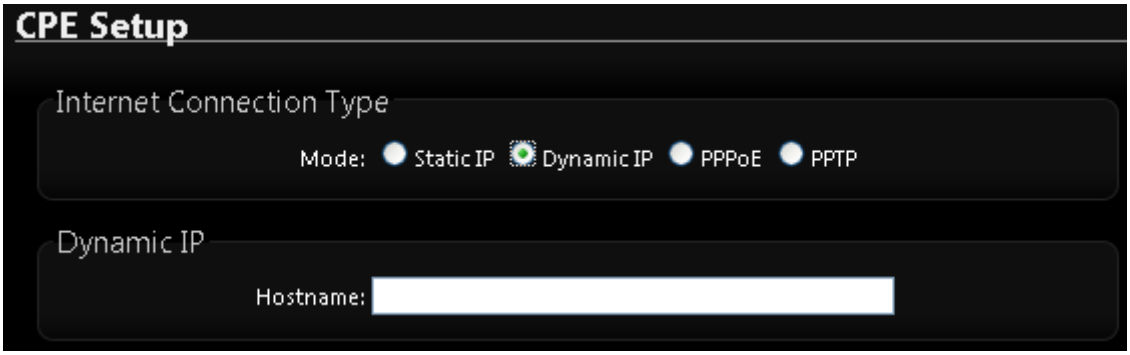




- **Mode :** By default, it's "***Static IP***". Check "Static IP", "Dynamic IP", "PPPoE" or "PPTP"to set up system WAN IP
  - ✓ **Static IP :** Users can manually setup the WAN IP address with a static IP provided by WISP.
    - ✧ **IP Address :** The IP address of the WAN port; default IP address is 192.168.1.254
    - ✧ **IP Netmask :** The Subnet mask of the WAN port; default Netmask is 255.255.255.0
    - ✧ **IP Gateway :** The default gateway of the WAN port; default Gateway is 192.168.1.1

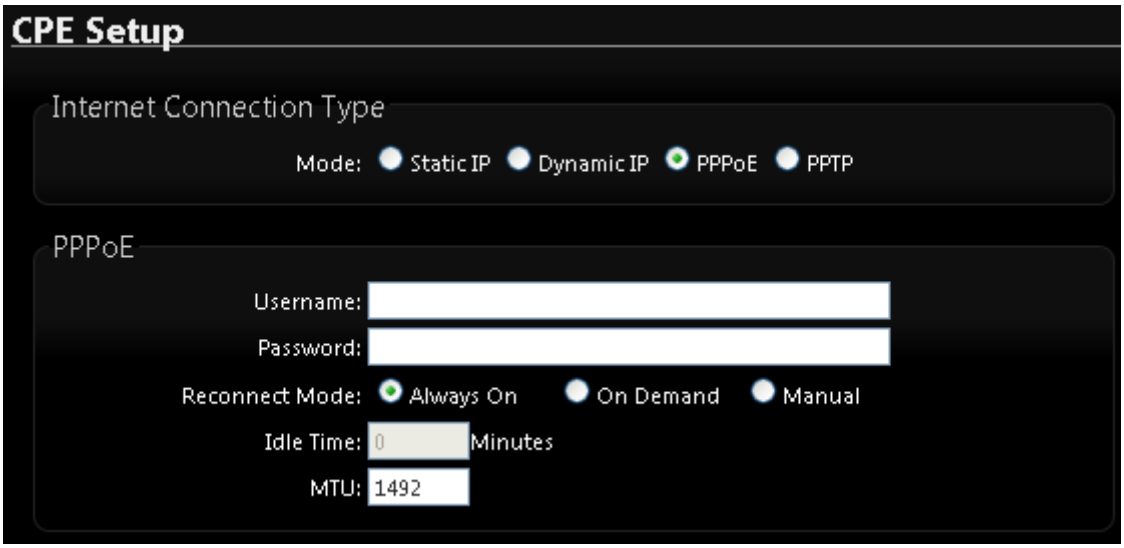
Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

✓ **Dynamic IP :** Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings including DNS can be available from DHCP server. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click ***Release*** button to release IP address and click ***Renew*** button to renew IP address again.



✧ **Hostname :** The Hostname of the WAN port

✓ **PPPoE :** To create wireless PPPoE WAN connection to a PPPoE server in network.



✧ **User Name :** Enter User Name for PPPoE connection

✧ **Password :** Enter Password for PPPoE connection

✧ **Reconnect Mode :**

Always on – A connection to Internet is always maintained.

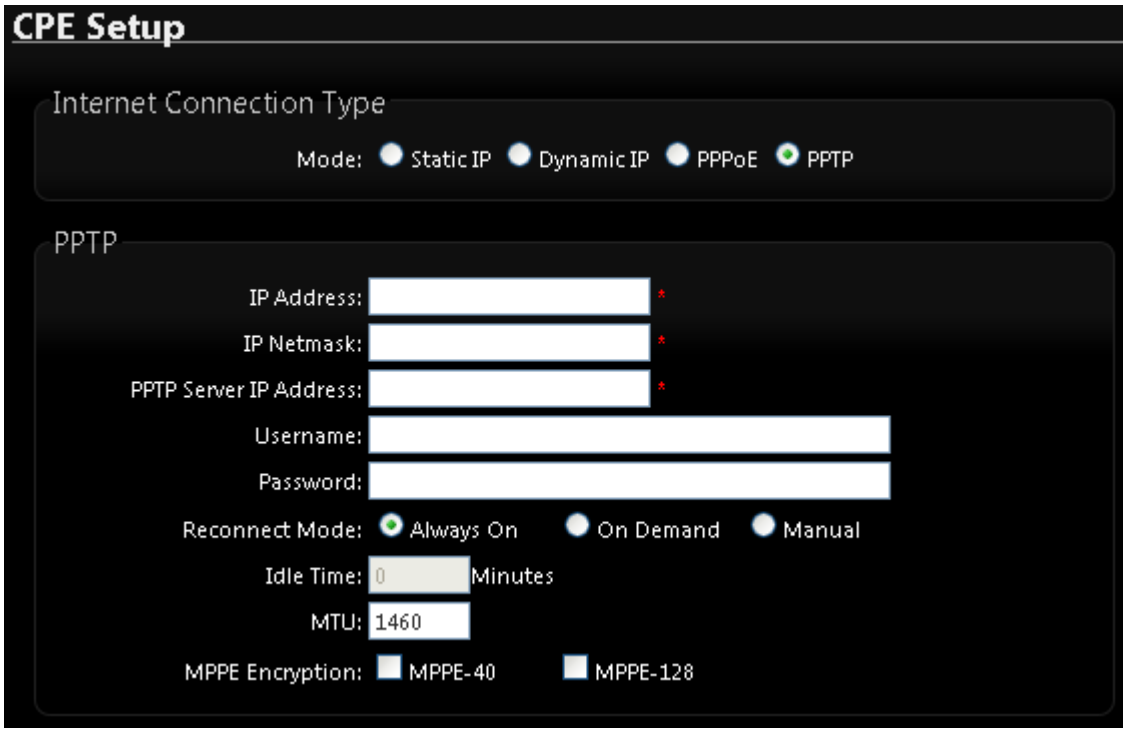
On Demand – A connection to Internet is made as needed.

Notice *When **Time Server** is enabled at the "On Demand" mode, the "Reconnect Mode" will turn out "Always on".*

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- ✧ **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.
- ✧ **Idle Time :** Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is "**0**", indicates disabled. When Idle time is disabled, the "**Reconnect Mode**" will turn out "**Always on**"
- ✧ **MTU :** By default, it's **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.

✓ **PPTP :** The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.



- ✧ **IP Address :** The IP address of the WAN port
- ✧ **IP Netmask :** The Subnet mask of the WAN port
- ✧ **PPTP Server IP Address :** The IP address of the PPTP server
- ✧ **User Name :** Enter User Name for PPTP connection
- ✧ **Password :** Enter Password for PPTP connection
- ✧ **Reconnect Mode :**

  Always on – A connection to Internet is always maintained.

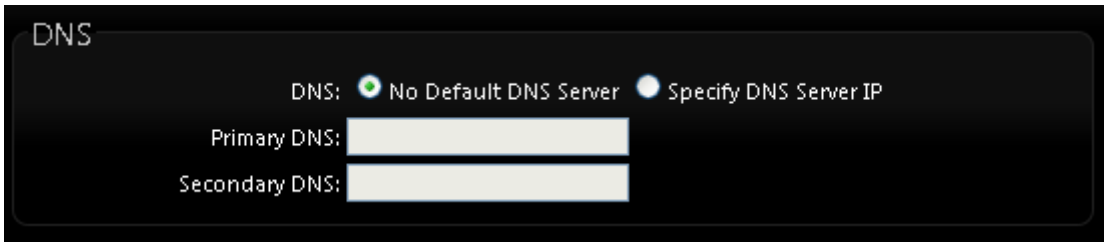
  On Demand – A connection to Internet is made as needed.

Notice *When **Time Server** is enabled at the "On Demand" mode, the "Reconnect Mode" will turn out "Always on"*

Manual – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.

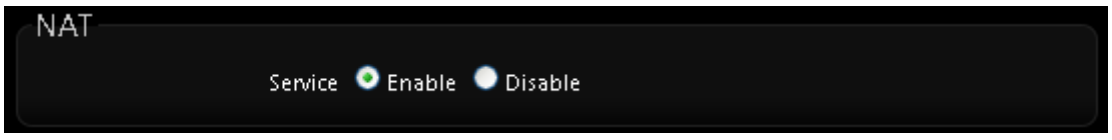
- ✧ **Idle Time :** Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is "**0**", indicates disabled. When Idle time is disabled, the "**Reconnect Mode**" will turn out "**Always on**"
- ✧ **MTU :** By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- ✧ **MPPE Encryption :** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.

- **DNS :** Check "No Default DNS Server" or "Specify DNS Server IP" radial button as desired to set up system DNS.

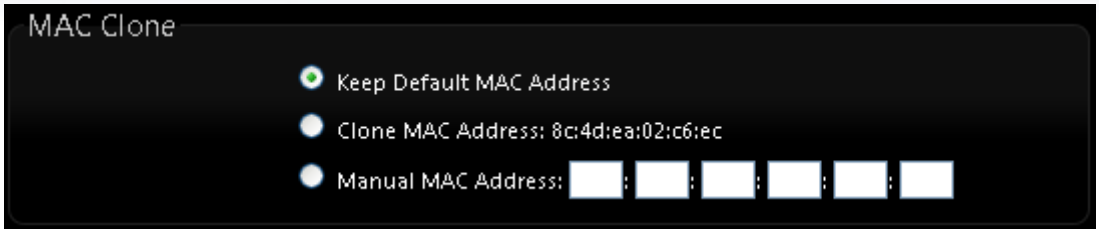


- ✓ **Primary :** The IP address of the primary DNS server.
- ✓ **Secondary :** The IP address of the secondary DNS server.

- **NAT :** The NAT support Enable and Disable Service



- **MAC Clone :** The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



- **Keep Default MAC Address :** Keep the default MAC address of WAN port on the system.
- **Clone MAC Address :** If you want to clone the MAC address of the PC, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.

Notice

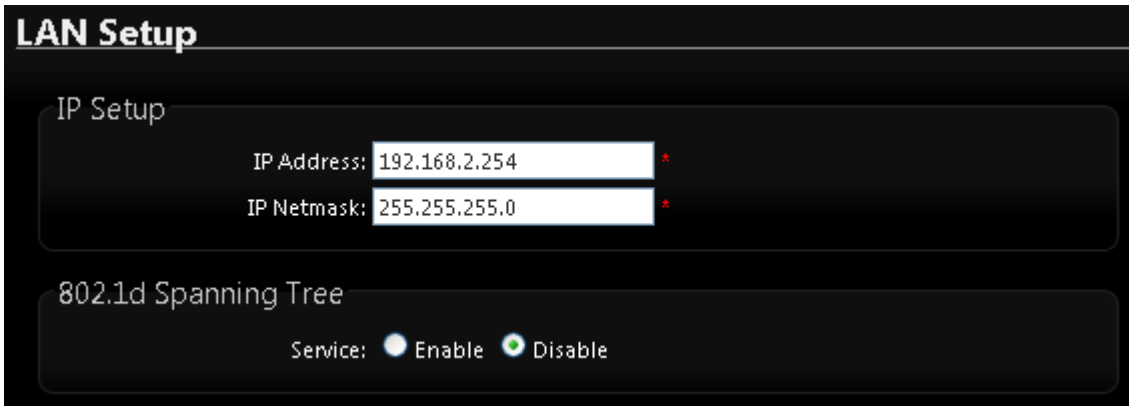
The Clone MAC Address field will display MAC address of the PC connected to system. Click "Save" button can make clone MAC effective.

- **Manual MAC Address :** Enter the MAC address registered with your ISP.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.4 Configure OW-215N2-X LAN IP Address

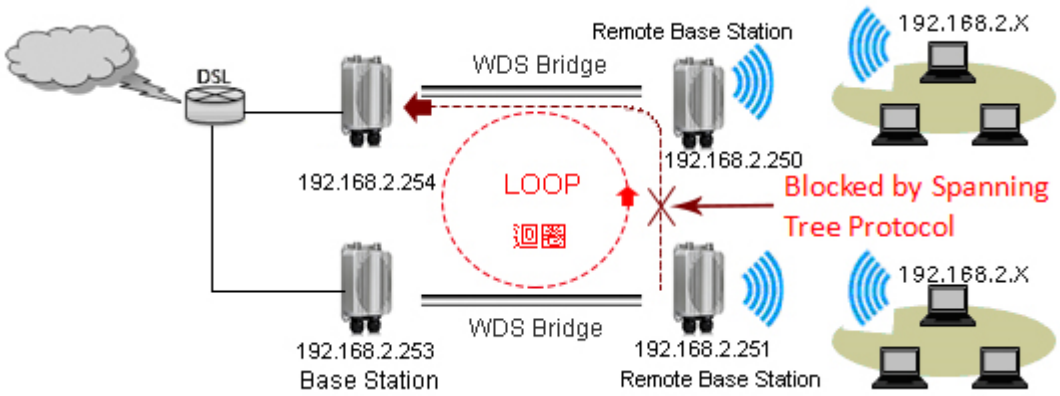
Here are the instructions for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.



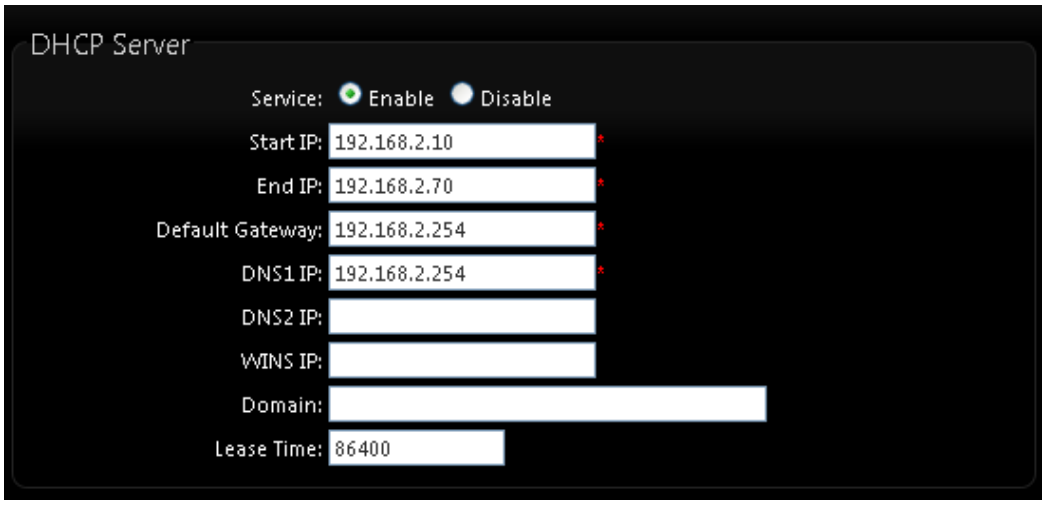
- **LAN IP Setup :** The administrator can manually setup the LAN IP address.
  - **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
  - **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0

- **802.1d Spanning Tree :**

  The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



- **DHCP Setup :** Devices connected to the system can obtain an IP address automatically when this service is enabled.



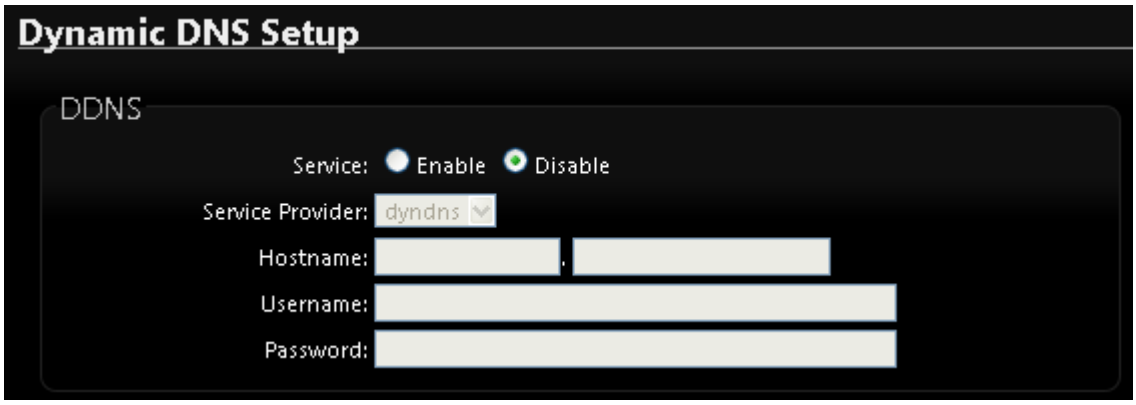
- **DHCP :** Check ***Enable*** button to activate this function or ***Disable*** to deactivate this service.
- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- **DNS1 IP :** Enter IP address of the first DNS server; this field is required.
- **DNS2 IP :** Enter IP address of the second DNS server; this is optional.
- **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain :** Enter the domain name for this network.

- **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 interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.5 Configure DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address. Please click on **System -> DDNS Setup** and follow the below setting.



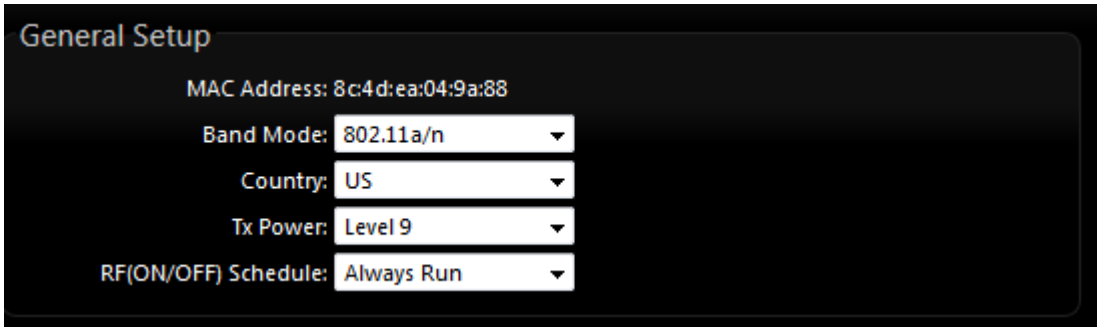
- **Enabled:** By default, it's "***Disable***". The mapping domain name won't change when dynamic IP changes. The beauty of it is no need to remember the dynamic WAP IP while accessing to it.
- **Service Provider:** Select the preferred Service Provider from the drop-down list including *dyndns*, *dhs*, *ods* and *tzo*
- **Hostname:** Host Name that you register to Dynamic-DNS service and export.
- **User Name & Password:** User Name and Password are used to login DDNS service.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

5.6 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.



- **MAC Address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are **801.11 a/n mixed mode or pure a mode or pure n mode**
- **Country :** a region, the OW-215N2-X support region for US,ETSI and Japan
- **TX Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level ***1*** to level 9 (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level 9 (**100**%).
- **RF(On/Off) Schedule :** The AP **RF** Signal on/off by time Policy

➢ HT Physical Mode

- **Tx/Rx Stream :** By default, it's **2**
- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

- **Shout GI :** Short Guard Interval, by default, it's “Enable”. it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

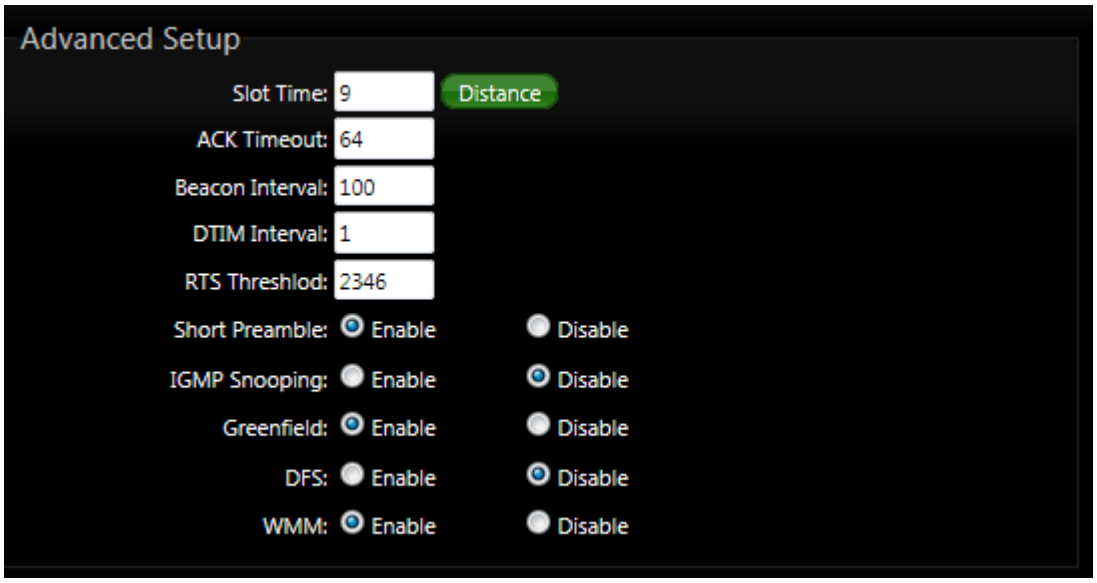
- **Aggregation :** By default, it's “**Enable**”. To “Disable” to deactivated Aggregation.
  A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining 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.

- **Aggregation Frames :** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.

- **Aggregation Size :** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

5.7 Configure Wireless Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.
  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Notice

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval :** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.
  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  a DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.
  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.
  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **IGMP Snooping :** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

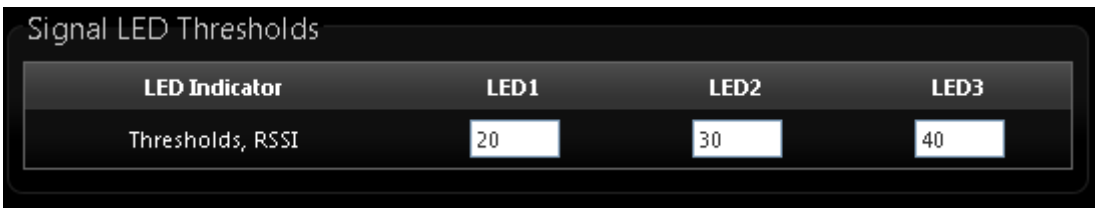
- **DFS :** Is IEEE802.11H With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary. The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

- **Greenfield :** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.

- **Signal LED Thresholds :** This function can setting RSSI number(1~99) to control signals LED's, The OW-215N2-X system will calculate for RSSI number and total of three LED's indicator, If LED's whole bright indicate signal is the strong.

Notice

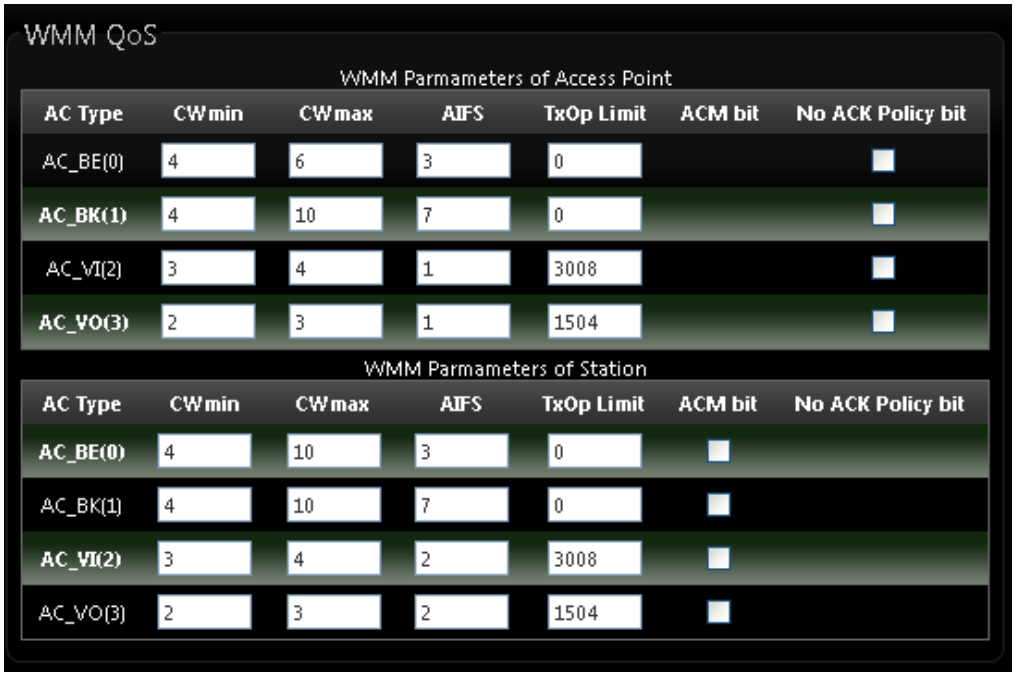
The function only support **Client Bridge + Repeater AP** and **WISP + Repeater AP** modes



✓ LED Indicator : Total of three LED's, the LED1 RSSI number is Minimum

- **WMM QoS :** This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.



✓ **AC Type** :

Queue	AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

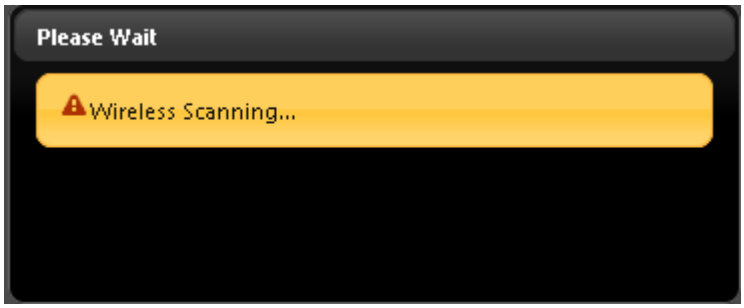
- ✓ **CWmin**：Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. ◦
- ✓ **CWmax**：Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦
- ✓ **AIFS**：The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit**：Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit**：Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit**：Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click “**Checkbox**” indicates “**No ACK**”

When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received uncast packet. ◦

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

5.8 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with. Please click on **Wireless** -> **Site Survey**. Below depicts an example for site survey.



ESSID	MAC Address	Signal/Noise, dBm	RSSI	Signal Quality, %	Channel	Security	Select
Main_AP	8C:4D:EA:02:C8:C8	-69 / -95	26	76%	44	NONE	Select

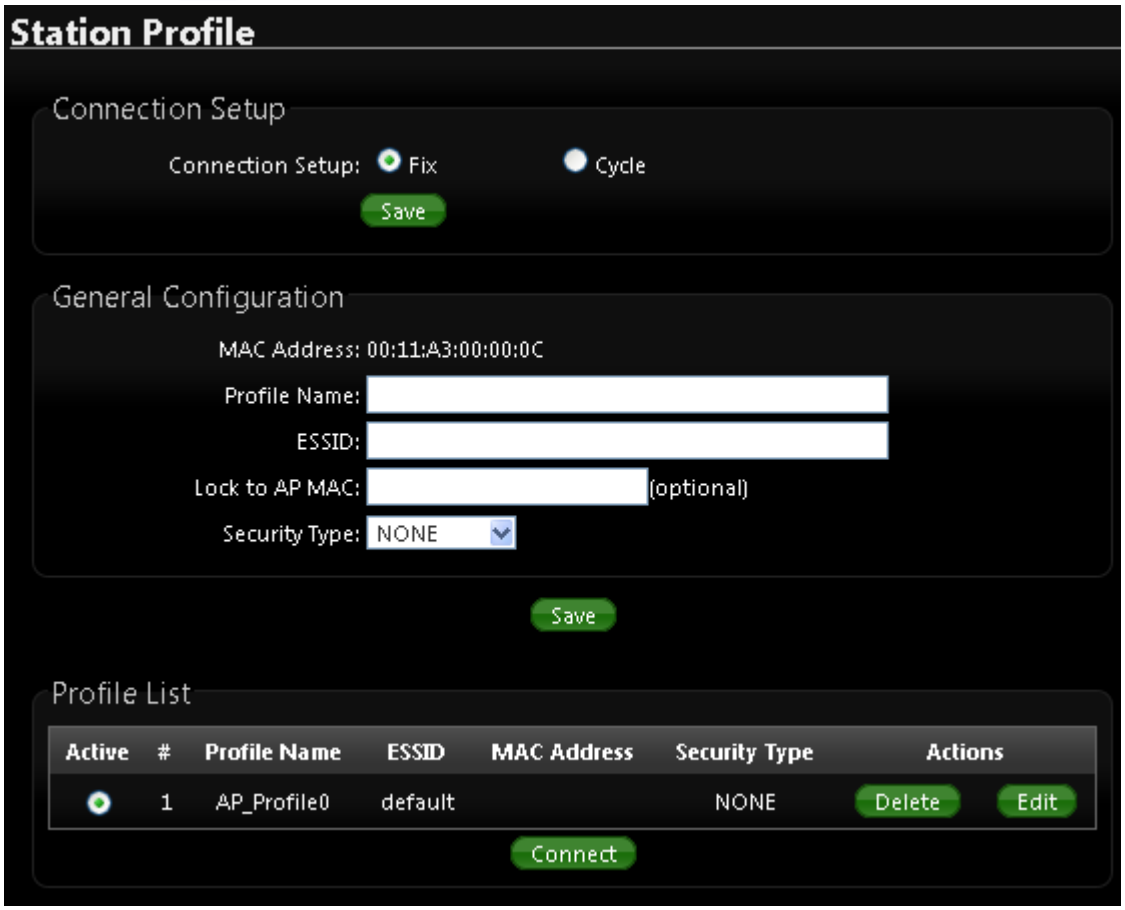
- **ESSID** : Available Extend Service Set ID of surrounding Access Points.
- **MAC Address** : MAC addresses of surrounding Access Points.
- **Signal/Noise dBm** : Received signal strength of all found Access Points.
- **RSSI :** Indicate the RSSI of the respective client's association.
- **Signal Quality (%) :** Received signal strength of all found Access Points.
- **Channel** : Channel numbers used by all found Access Points.
- **Security** : Security type by all found Access Points.
- **Select** : Click "**Select**" to configure settings and associate with chosen AP.

Notice

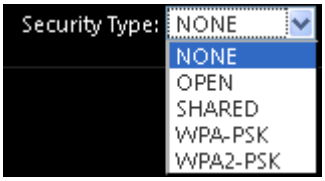
*While clicking "Select" button in the Site Survey Table, the "**ESSID**" and "**Security Type**" will apply in the Wireless General Setup. However, more settings are needed including Security Key.*

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

5.9 Station Profile



- **Connection Setup :** Can you choose Fix or cycle
- **General Configuration :**
  - **MAC address :** The remote AP MAC Address
  - **Profile Name** : Set different profiles for quick connection uses.
  - **ESSID** : Assign Service Set ID for the wireless system.
  - **Lock to AP MAC** : the function will lock remote AP MAC Address.
  - **Security Type :** Select an appropriate security type for association, the Security Type can be selected in "**NONE**", "**OPEN**", "**SHARED**", "**WPA-PSK**", or "**WPA2-PSK**" from drop-down list; the type needs to be the same as that associated access point.
  - **OPEN / SHARED** : OPEN and SHARED require the user to set a WEP key to exchange data.



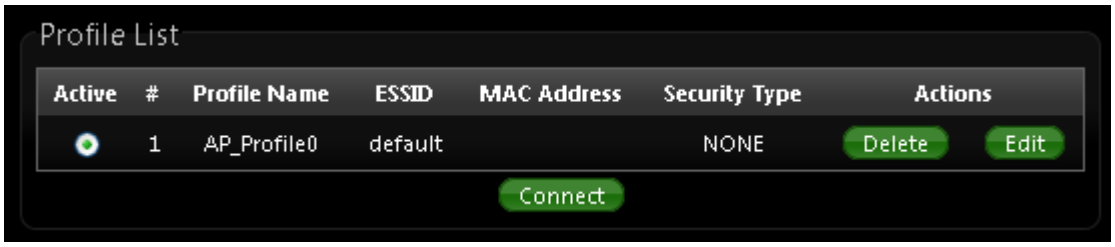
- ✓ **Key Index** : key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key #** : Enter HEX or ASCII format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 Characters	5 Characters
128-bit	26 Characters	13 Characters

- **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

- ✓ **Cipher Suite** : Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**.
- ✓ **Pre-shared Key** : Enter the information for pre-shared key; the key can be either entered as a **256-bit** secret in **64** HEX digits format, or **8** to **63** ASCII characters.

➢ **Profile List :** The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List.



- Click “”**Edit**” an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “**Save**” button to save the profile.
- Click “**Delete**” to remove profile.
- Click and Select a profile from list, then click the “**Connect**” button to connecting to the wireless network with the profile setting.

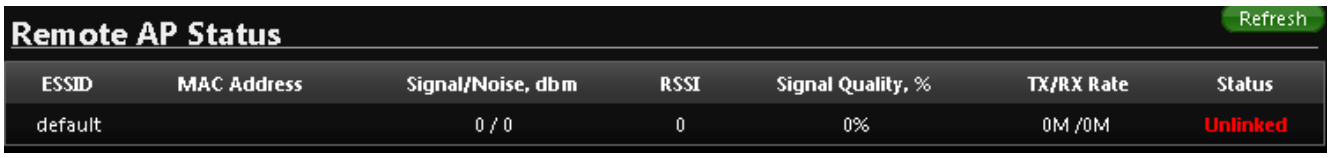
Notice

If you only click "Connect" button and does not click "Save" button. The selected profile would not be saved on the Profile List

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes.

5.10 Remote AP Status

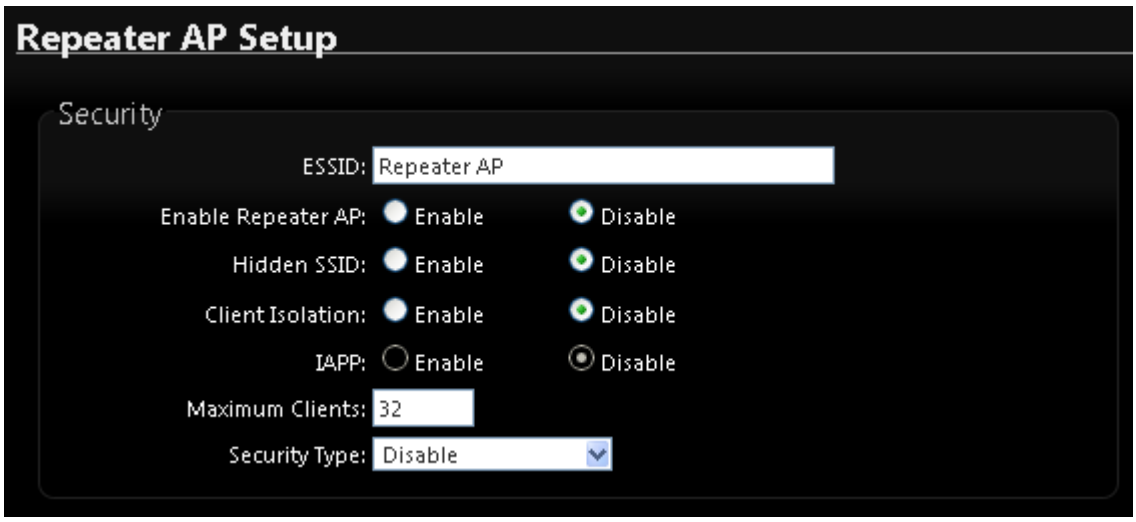
Show the remote bridge AP whether is link or unlinked



5.11 Repeater AP Setup

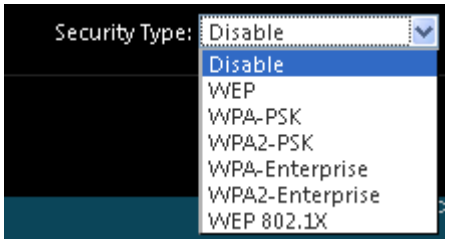
The network manager can configure related wireless settings, **AP Setup**, **Security Settings**, and **Access Control Settings**.

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings.

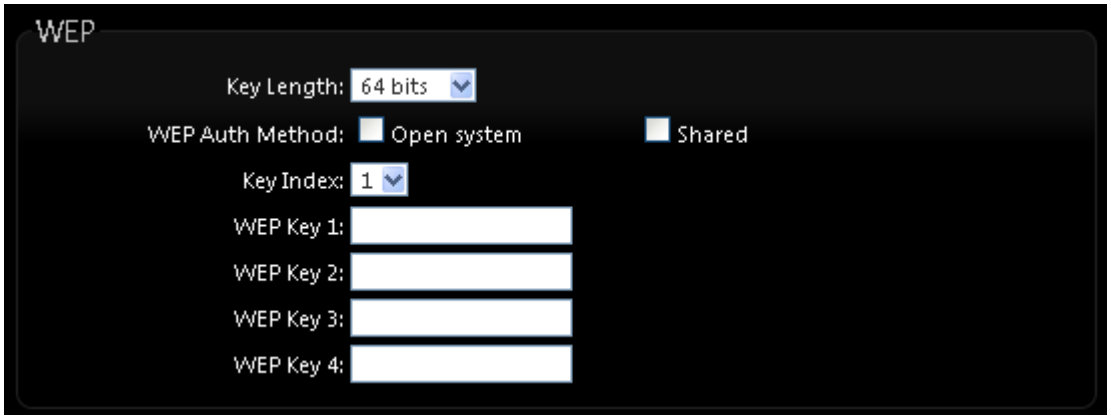


- **ESSID** : Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP clients associated with the specified VAP.
- **Enable Repeater AP :** choose Enable or Disable Repeater AP function, the default is Disable

- **Hidden SSID :** By default, it's "**Disable**". Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.
- **Client Isolation :** By default, it's "**Disable**". Select "Enable", all clients will be isolated from each other, which means they can't reach each other.
- **IAPP :** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period.
- **Maximum Clients** : The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.
- **Security Type** : Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.



- **Disable** : Data are unencrypted during transmission when this option is selected.
- **WEP** : Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.



- ✓ **Key Index** : Skey index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Auth Method :** Enable the desire option among OPEN or SHARED.

✓ **WEP Key #** : Enter HEX or ASCII format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

- **WPA-PSK (or WPA2-PSK) :**

WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

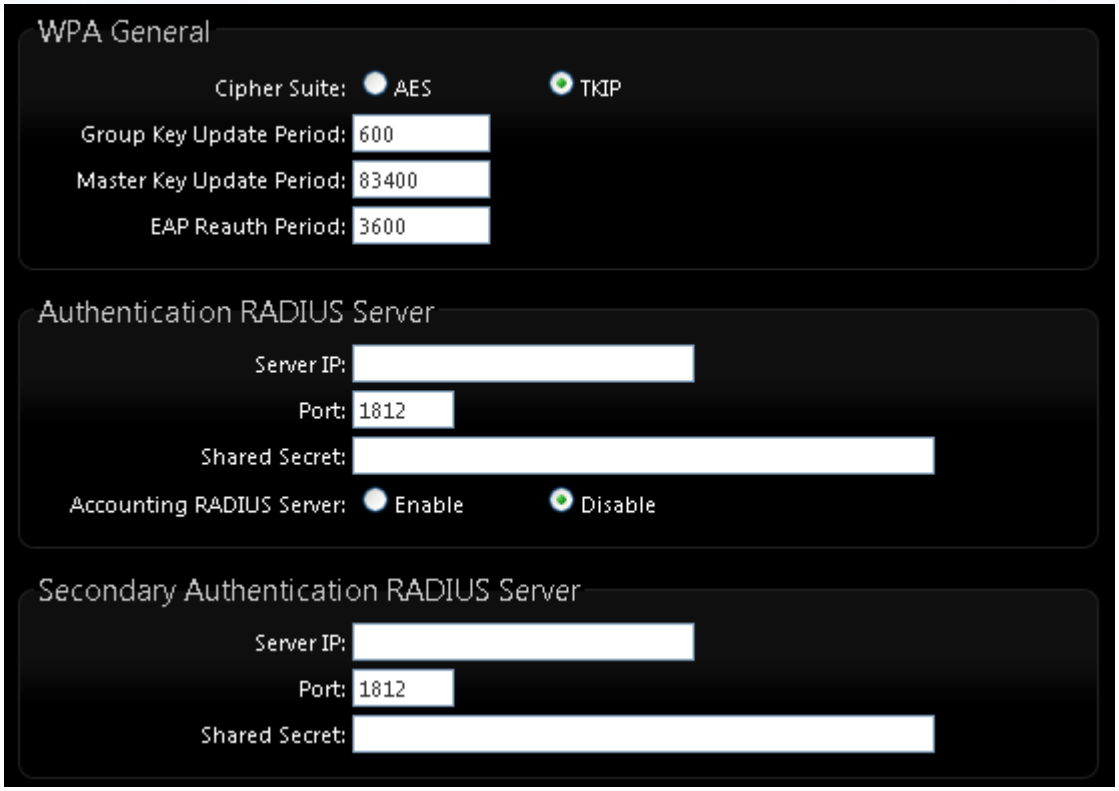
✓ **Cipher Suite** : By default, it is AES. Select either AES or TKIP cipher suites.

✓ **Pre-shared Key** : Enter the pre-shared key; the format shall go with the selected key type.

Notice *Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.*

✓ **Group Key Update Period** : By default, it is 3600 seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

- **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this is selected.



WPA General Settings :

- ✓ **Cipher Suite** : By default, it is AES. Select either AES or TKIP cipher suites.
- ✓ **Group Key Update Period** : By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- ✓ **PMK Cache Period** : By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- ✓ **Pre-Authentication** : By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.

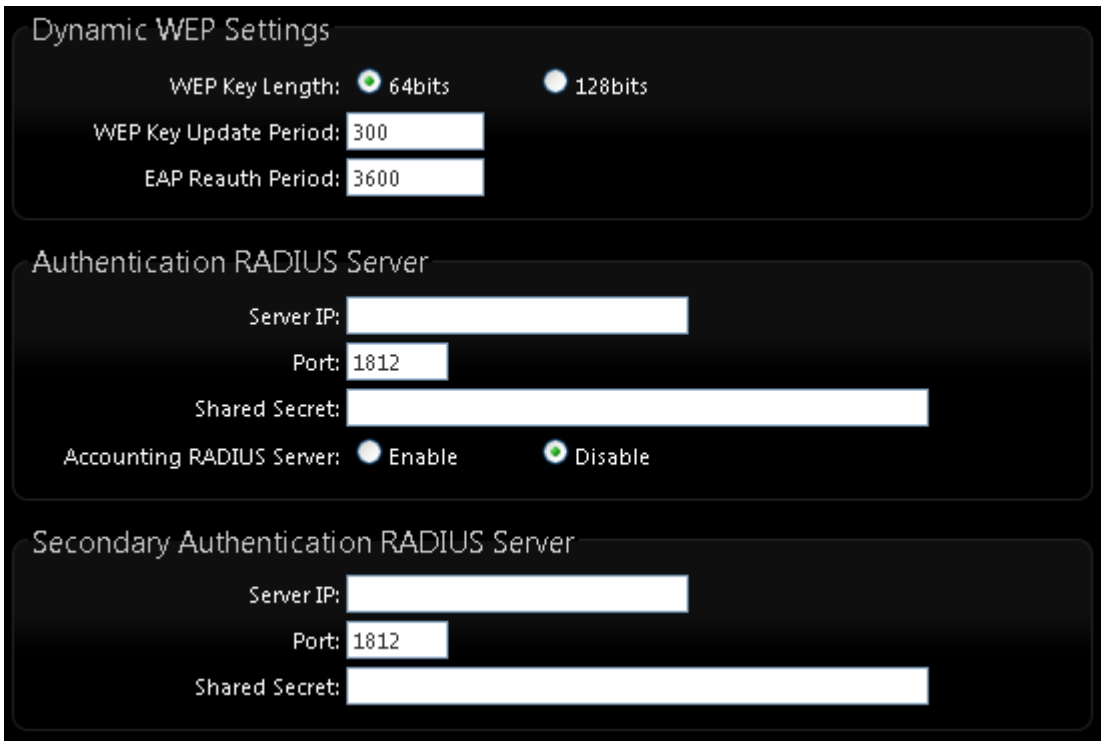
Notice *PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise*

Authentication Radius Server Settings :

- ✓ **IP Address** : Enter the IP address of the Authentication RADIUS server.
- ✓ **Port** : By default, it's 1812. The port number used to communicate with RADIUS server.
- ✓ **Shared secret** : A secret key used between system and RADIUS server. Supports 8 to 64 characters.

- ✓ **Session Timeout** : The Session timeout is in the range of 0~60 seconds. The default is 0 to disable re-authenticate service. Amount of time before a client will be required to re-authenticate.

- **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

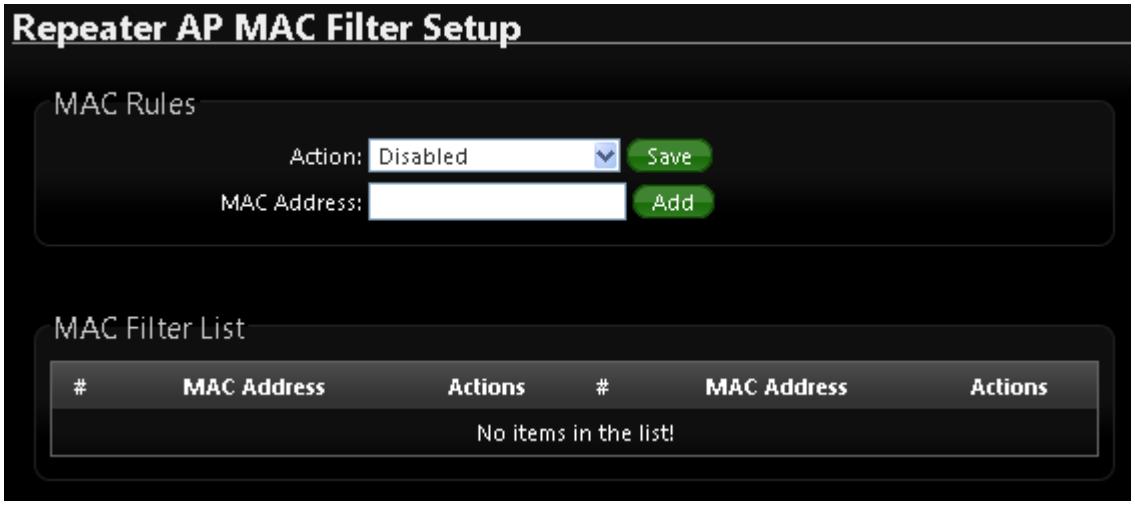


Authentication Radius Server Settings :

- ✓ **IP Address** : Enter the IP address of the Authentication RADIUS server.
- ✓ **Port** : By default, it's 1812. The port number used to communicate with RADIUS server.
- ✓ **Shared secret** : A secret key used between system and RADIUS server. Supports 8 to 64 characters.
- ✓ **Session Timeout** : The Session timeout is in the range of 0~60 seconds. The default is 0 to disable re-authenticate service. Amount of time before a client will be required to re-authenticate.

5.12 Repeater AP MAC Filter Setup

Continue **Virtual AP Setup** section. For each Virtual AP setting, the administrator can allow or reject clients to access each Virtual AP.



- **Action**: Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.
  - ✓ **Only Allow List MAC**: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "**Only Allow List MAC**".
  - ✓ **Only Deny List MAC**: Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to "**Only Deny List MAC**".

Notice

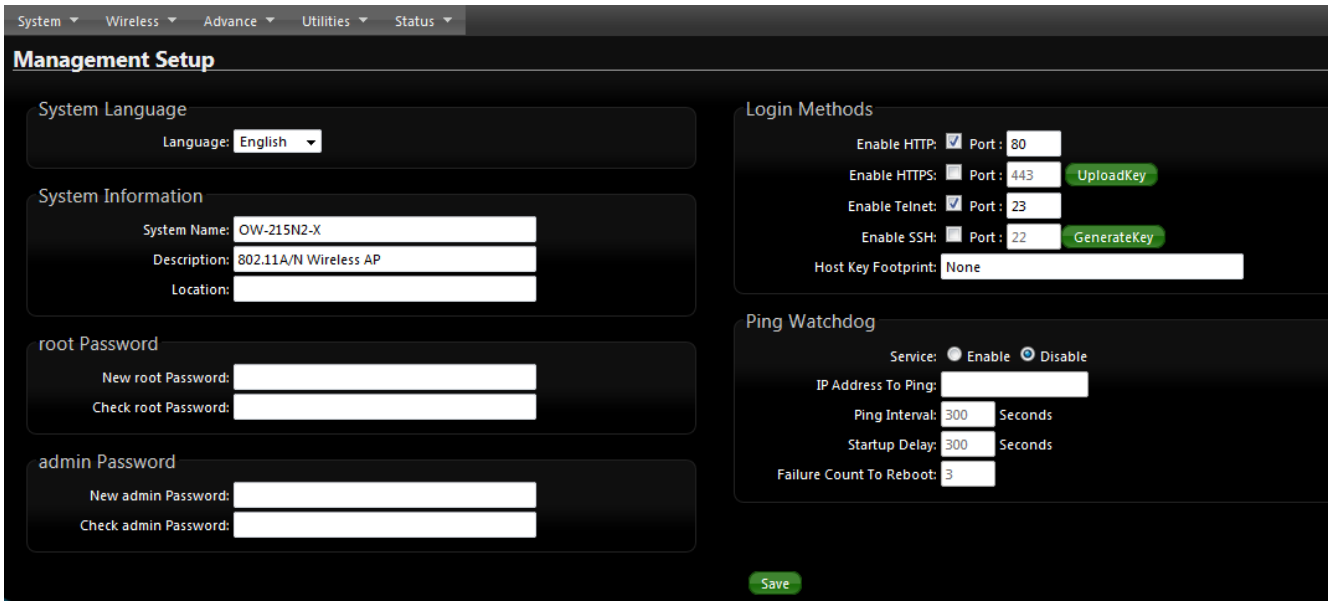
MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

6. System Management

6.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods. Please click **System -> Management** and follow the below settings



- **System Information**
  - **System Name :** Enter a desired name or use the default one.
  - **Description :** Provide description of the system.
  - **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

  The system supports two management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as root user, to manage the system in all aspects. While logging in as an admin user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to *Appendix D. Network manager Privileges*.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ✓ **New Password :** Enter a new password if desired
  - ✓ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ✓ **New Password :** Enter a new password if desired
  - ✓ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only root user can enable or disable system login methods and change services port.
  - ✓ **Enable HTTP :** Check to select HTTP Service.
  - ✓ **Enable HTTPS :** Check to select HTTPS Service
  - ✓ **HTTPS Port :** The default is 443 and the range is between 1 ~ 65535.

Notice *If you already have an SSL Certificate, please click "**Upload Key**" button to select the file and upload it.*

  - ✓ **Enable Telnet :** Check to select Telnet Service
  - ✓ **Telnet Port :** The default is 23 and the range is between 1 ~ 65535.
  - ✓ **Enable SSH :** Check to select SSH Service
  - ✓ **SSH Port :** Please The default is 22 and the range is between 1 ~ 65535**.**

Notice *Click "**Generate Key**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

- **Ping Watchdog :** The ping watchdog sets the **OW-215N2-X** 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 **OW-215N2-X** device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

  Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

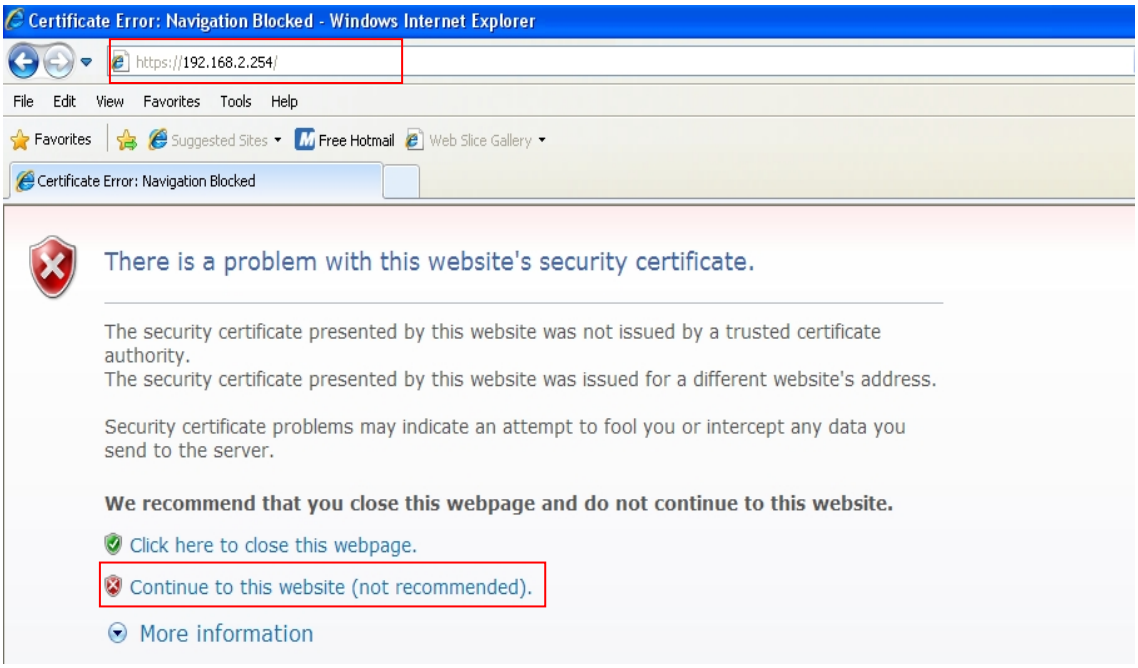
  - ✓ **Enable Ping Watchdog :** control will enable Ping Watchdog Tool.
  - ✓ **IP Address To Ping :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
  - ✓ **Ping Interval :** specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is 300 seconds.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

- ✓ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. 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. Default is 300 seconds.
- ✓ **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.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (https://192.168.2.254). There will be a “Certificate Error”, because the browser treats system as an illegal website.

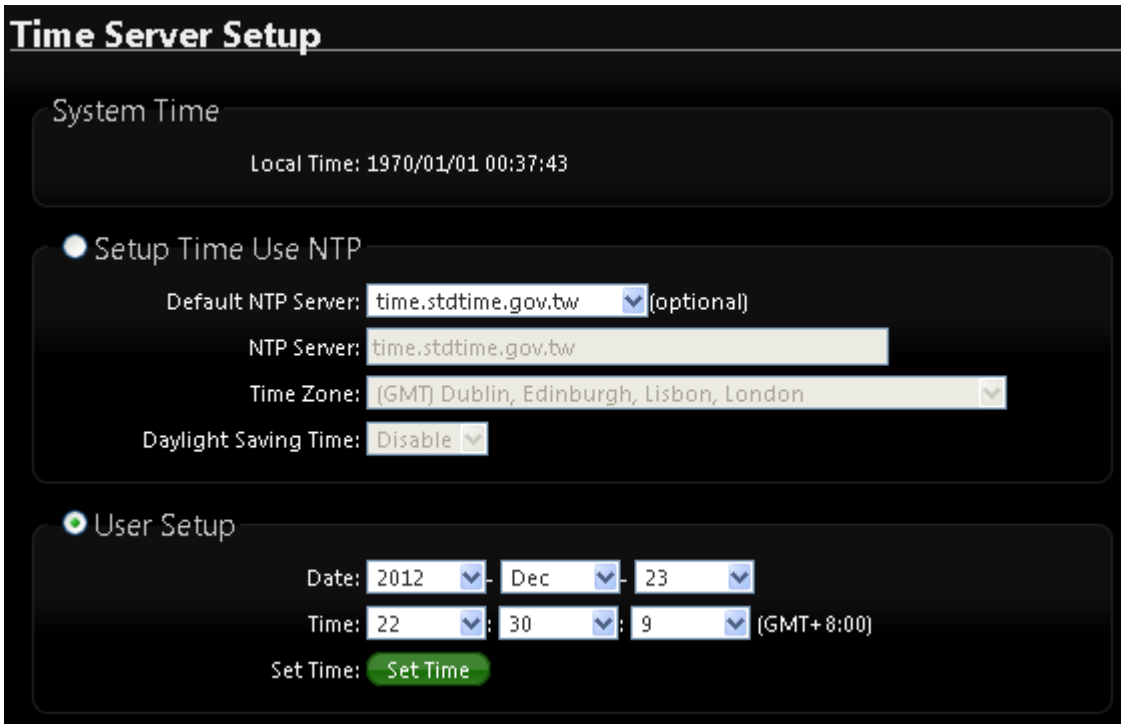


Click **“*Continue to this website*”** to access the system's WMI. The system's Overview page will appear.

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

6.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported. Please click on **System -> Time Server** and follow the below setting.



- **Local Time :** Display the current system time.
- **Setup Time Use NTP :** To synchronize the system time with NTP server.
- **Default NTP Server / NTP Server :** Select the NTP Server from the drop-down list.
- **Time Zone :** Select a desired time zone from the drop-down list.
- **Daylight saving time :** Enable or disable Daylight saving.

Notice *If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings*

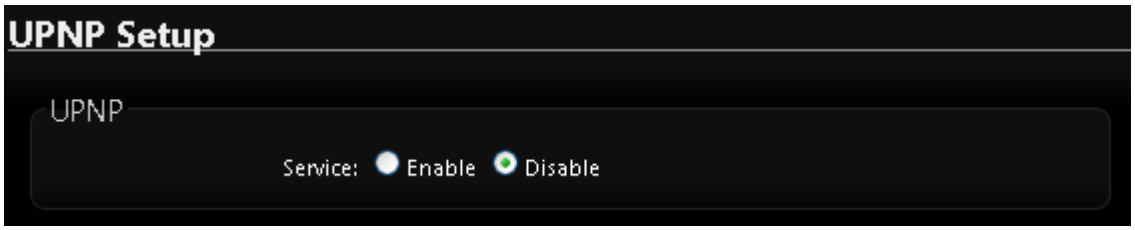
- **User Setup :** The management can set time by system time
  - **Date:** Setting the date for system.
  - **Time :** Setting the time for system.

Click *Save* button to save your changes. Click *Reboot* button to activate your changes

6.3 Configure UPnP Setup by CPE mode

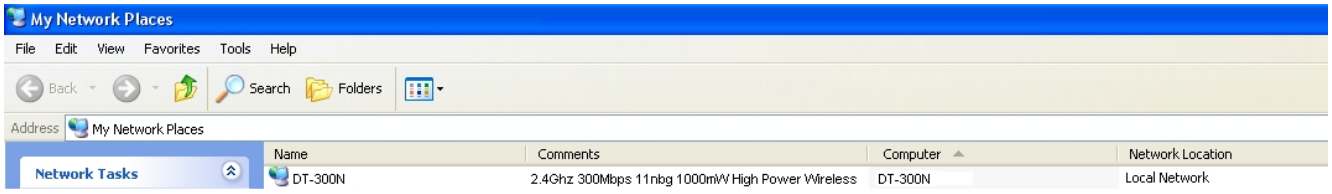
Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

Please click **System -> UPnP** and follow the below settings



- **UPnP :** By default, it's "**Disable**". Select "**Disable**" or "**Enable"** of UPnP Service.

For UPnP to work in Windows XP, the **"OW-215N2-X"** must be available in "***My Network Places***", as shown here: (your specific model may vary)



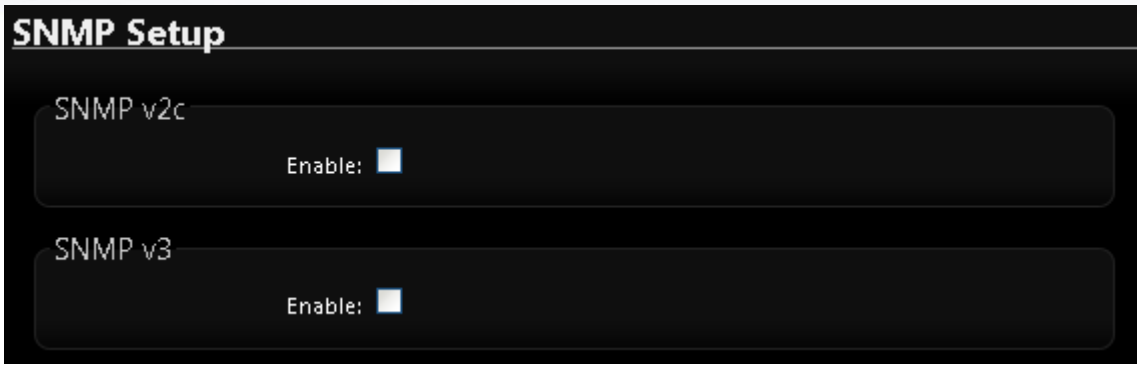
If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to ***Appendix D. Using UPnP on Windows XP***

Click ***Save*** button to save changes and click ***Reboot*** button to activate changes

6.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

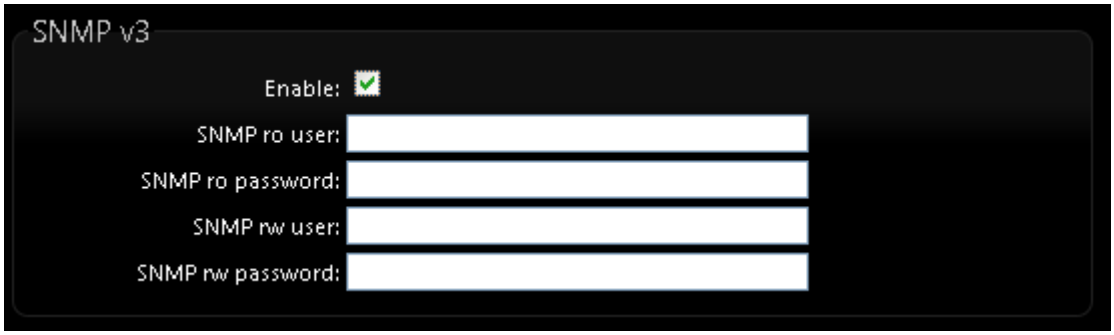
Please click on **System -> SNMP** and follow the below setting.



➢ **SNMP v2c Enable:** Check to enable SNMP v2c.

- **ro community :** Set a community string to authorize read-only access.
- **rw community :** Set a community string to authorize read/write access.

➢ **SNMP v3 Enable:** Check to enable SNMP v3.
SNMPv3 supports the highest level SNMP security.



- **SNMP ro user :** Set a community string to authorize read-only access.
- **SNMP ro password :** Set a password to authorize read-only access.
- **SNMP rw user :** Set a community string to authorize read/write access.
- **SNMP rw password :** Set a password to authorize read/write access.

➢ **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

- **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- **IP(1~4) :** Enter the IP addresses of the remote hosts to receive trap messages.

Click ***Save*** button to save changes and click ***Reboot*** button to activate.

7. Configure Advance Setup

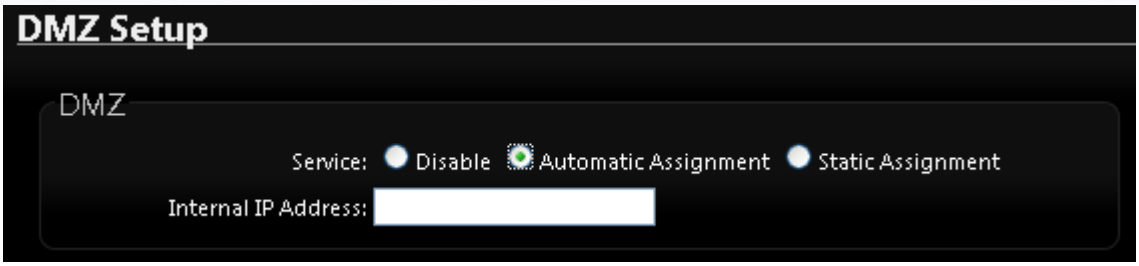
7.1 DMZ by CPE mode

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding*)* while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.

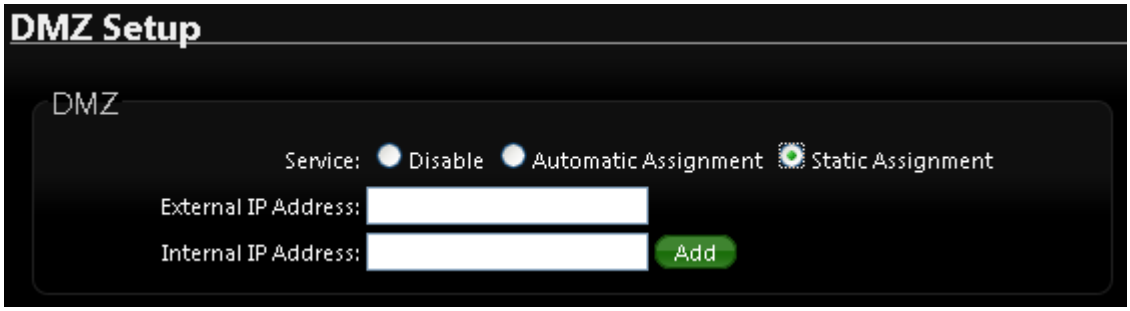
Please click on **Advance -> DMZ** and follow the below setting.

➢ **Service :** The DMZ default by *"**Disable**"*. Check ***Enable*** radial button to enable DMZ.

- **Automatic Assignment :** Enter Internal IP address of DMZ host and only one DMZ host is supported.



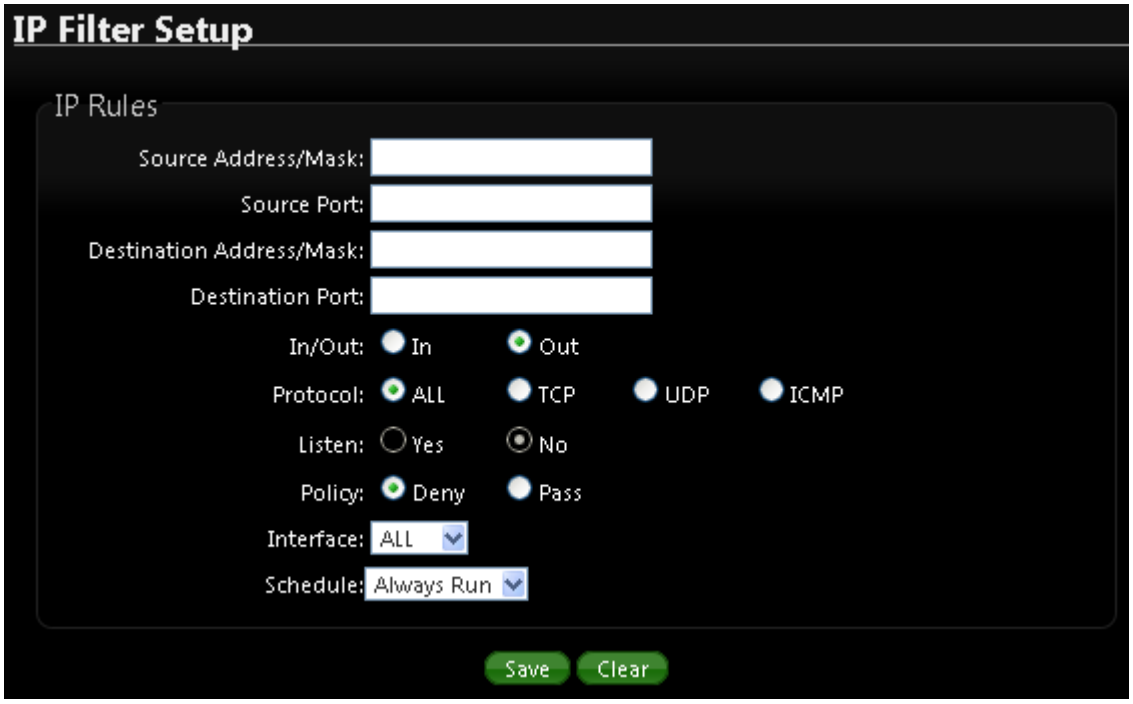
- **Static Assignment :** Enter external and internal IP address of DMZ host. The function only external IP to Internal IP address



Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

7.2 IP Filter by CPE mode

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.



- **Source Address/Mask :** Enter desired source IP address and netmask. *i.e. 192.168.2.10/32.*
- **Source Port :** Enter a port or a range of ports as ***start:end***. *i.e. port 20:80*
- **Destination Address/Mask :** Enter desired destination IP address and netmask. *i.e. 192.168.1.10/32*
- **Destination Port :** Enter a port or a range of ports as ***start:end.*** *i.e. port 20:80*
- **In/Out :** Applies to Ingress or egress packets.
- **Protocol :** Supports ***TCP***, ***UDP*** or ***ICMP***.
- **Listen :** Click ***Yes*** radial button to match TCP packets only with the SYN flag.
- **Policy :** ***Deny*** to drop and ***Pass*** to allow per filter rules
- **Interface :** The interface that a filter rule applies
- **Schedule :** Can choose to use rule by "Time Policy"

Notice

All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

Example 1 :

Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN

Example 2 :

All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

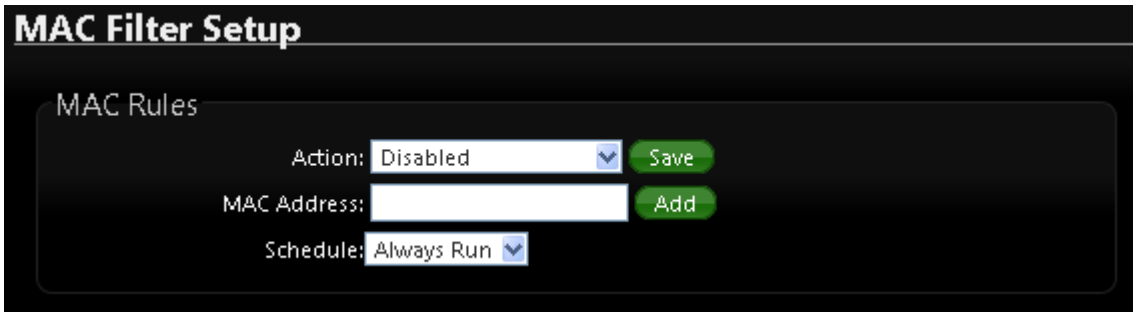
Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Deny	LAN

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

7.3 MAC Filter by CPE mode

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important and must note. That MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.



Click ***Save*** button to save your change. Two ways to set the MAC Filter List

MAC Filter Rule : By default, it's "***Disable***". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**.

- **Action :**
  - **Only Allow List MAC**:
    The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.
  - **Only Deny List MAC**
    The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.
- **MAC Address :**
  Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

  There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons.

- **Schedule :** Can choose to use rule by "Time Policy"

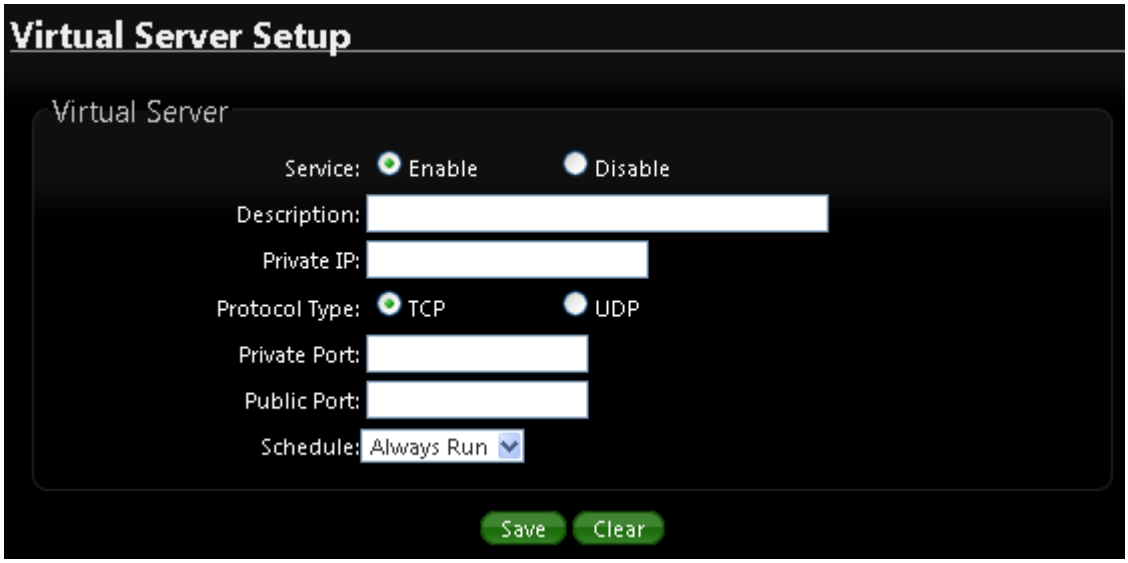
  Click ***Reboot*** button to activate your changes

7.4 Virtual Server by CPE mode

The **"Virtual Server"** can also referred to as "Port Forward" as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Please click on **Advance -> Virtual Server** and follow the below setting.



- **Service :** By Default, It's "***Disable***"**.** Check ***Enable*** radial button to enable Virtual Server.
- **Description :** Enter appropriate message for resource sharing via Virtual Server.
- **Private IP :** Enter corresponding IP address of internal resource to share.
- **Protocol Type :** Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80
- **Public Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80

Notice

The Private Port and Public Port can be different. However, total number of ports need to be the same.

Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.

Click "**Add**" button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List.

Click ***Reboot*** button to activate your changes.

➢ **Schedule :** Can choose to use rule by “Time Policy”

While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

Example 1 :

All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP ***20~80*** will be redirected to port TCP ***20~80*** of ***192.168.2.11***

Ex.

DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.10	22	22
2	TCP	192.168.2.11	20:80	20:80

Example 2 :

All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port ***20~80*** will be redirected to port ***20~80*** of ***192.168.2.11***. The rule 2 won’t take effect.

Ex.

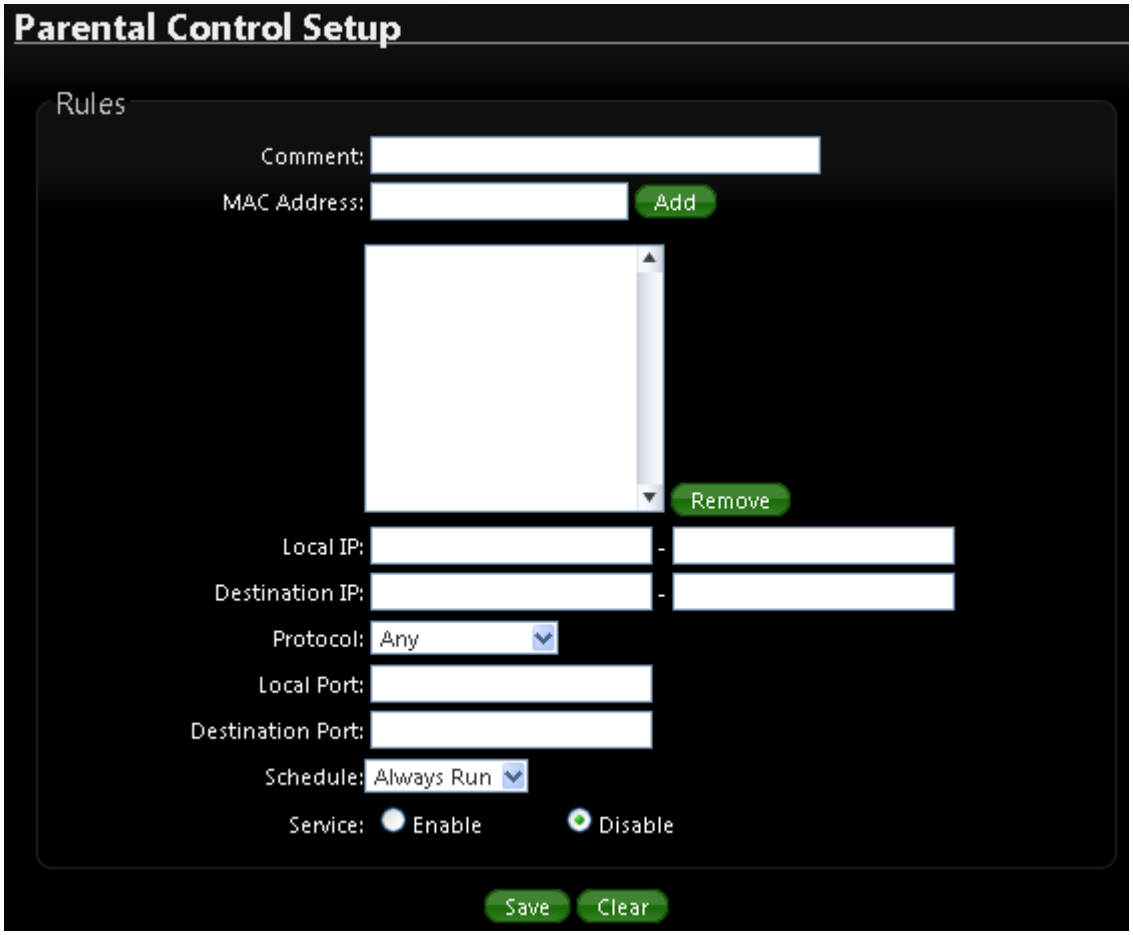
DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.11	20:80	20:80
2	TCP	192.168.2.10	22	22

7.5 Parental Control by CPE mode

Parental Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites.

Please click on **Advance -> Parental Control** and follow the below setting.

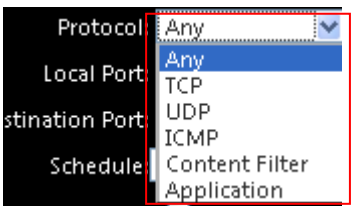


Rules :

Control can be managed by a rule. Use the settings on this screen to establish an access policy.

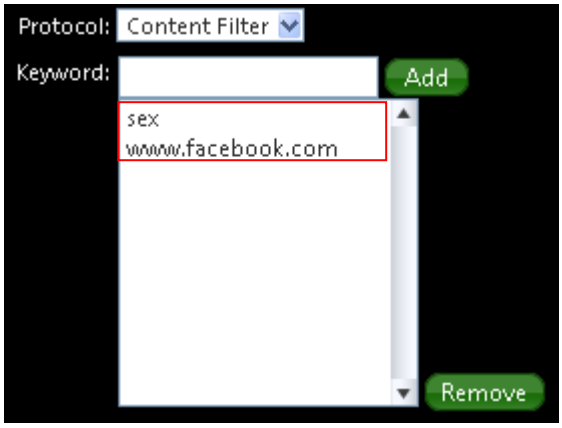
- **Comment :** Enter a descriptive name for this rule for identifying purposes.
- **MAC Address :** Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**" button to add in the MAC group of each rule. Click "**Remove**" button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.

- **Local / Destination IP :** Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
- **Protocol :** Select **Any** or specify protocol(**TCP**, **UDP**, **ICMP**, **Content Filter** and **Application**) from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Local(LAN)/ Destination Port can not used.



Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

If you want to block websites with specific URL address or using specific keywords, enter each URL or keyworks in the "**Content Filter**" field and click "**Add**" button to add in the Content Filter list of each rule. Click "**Remove**" button can remove URL or keywords.



- **Local Port :** Specify local port(LAN port) range required for this rule
- **Destination Port :** Specify destination port range required for this rule
- **Schedule :** Can choose to use rule by "Time Policy"
- **Service :** Check ***Enable*** button to activate this rule, and ***Disable*** to deactivate.

Click "**Add**" button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the List.

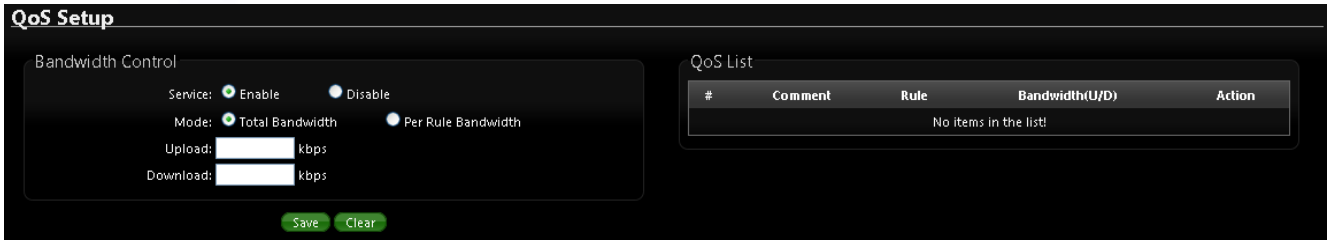
Click ***Reboot*** button to activate your changes.

7.6 QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as FTP) to form a flow.

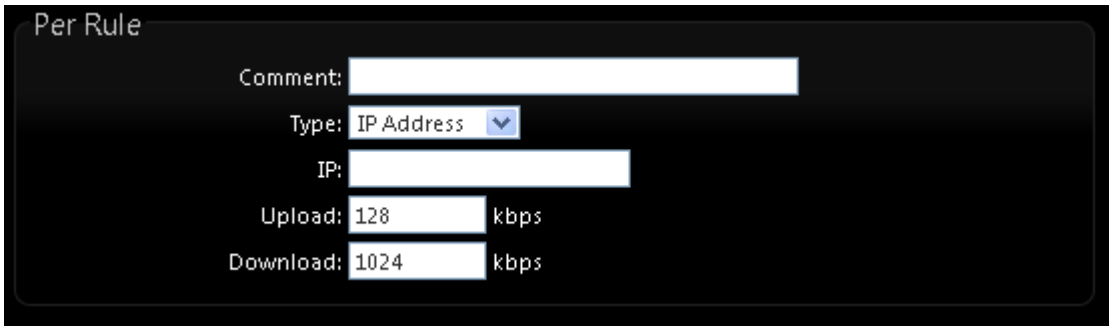
Please click on **"Advance"** → **"QoS"**



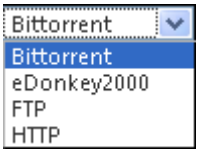
※ Bandwidth Control

- **Service :** The default is Disable, Select "**Disable**" or "**Enable"** of QoS Service.
- **Mode :** Can choose a **total Bandwidth control** or **Per Rule Bandwidth control**.
  - ✓ **Total Bandwidth :** the function is all customers use a total bandwidth.
    - **Upload :** Setting use upload control by total bandwidth
    - **Download :** Setting use download control by total bandwidth
  - ✓ **Per Rule Bandwidth :** Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules.

※ Per Rule



- **Comment :** Enter a descriptive name for this rule for identifying purposes.
- **IP Address / IP segment :** Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.1.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.1.254.
- **Port :** Specify local port(LAN port) range required for this rule.
- **MAC :** Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**"
- **Application : the Layer 7 application control support "Bittorrent" , "eDonkey2000" , "FTP" and "HTTP"** 。

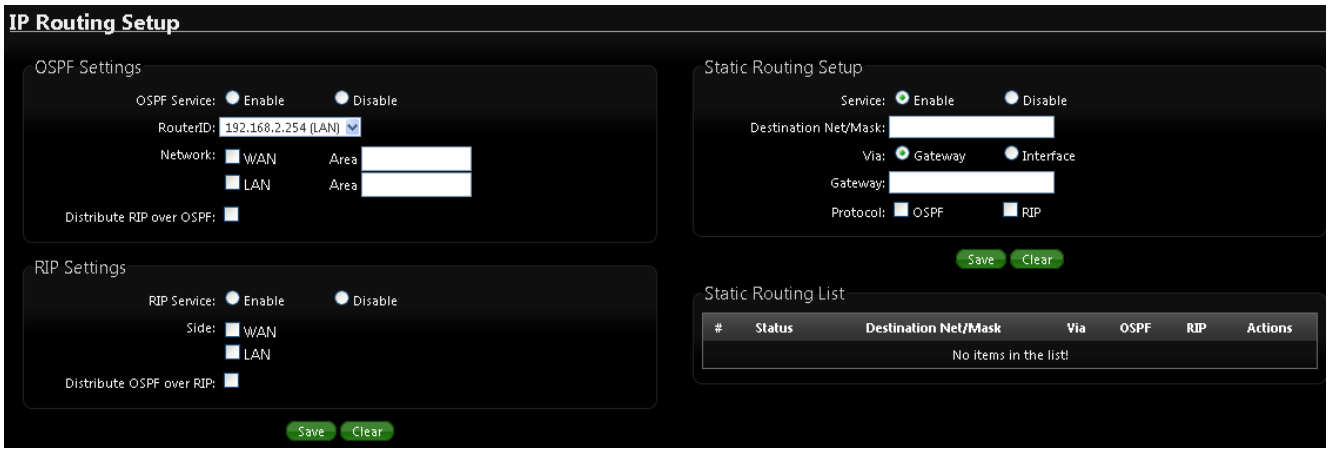


Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

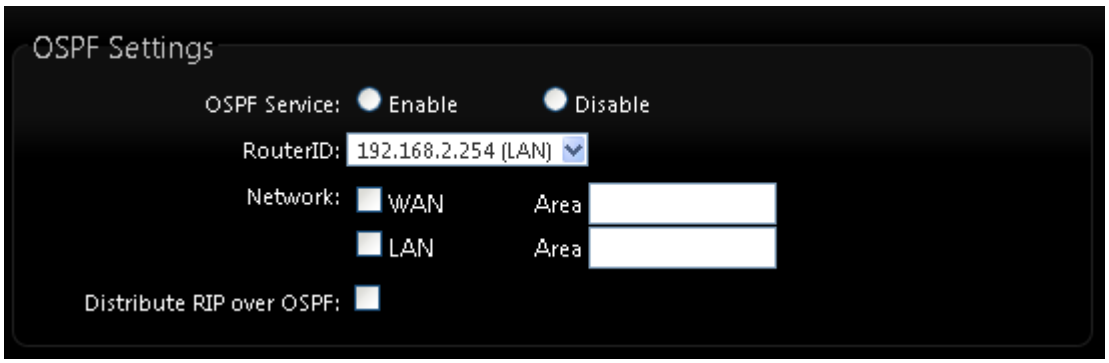
7.7 IP Routing by CPE mode

The IP Routing Settings allows you to configure routing feature in the gateway. The system supports RIP(Routing Information Protocol) and OSPF(Open Shortest Path First) dynamic routing and allows you to manually configure static network routes.

Please click on **Advance -> IP Routing** and follow the below setting.



OSPF Settings :



- **OSPF Service :** By default, it's Disable. To Enable to activated OSPF routing service.
- **Route ID :** The router ID is typically derived by each router from its interface IP address.
- **Distribute RIP over OSPF :** Allow RIP routes will redistributed into OSPF.

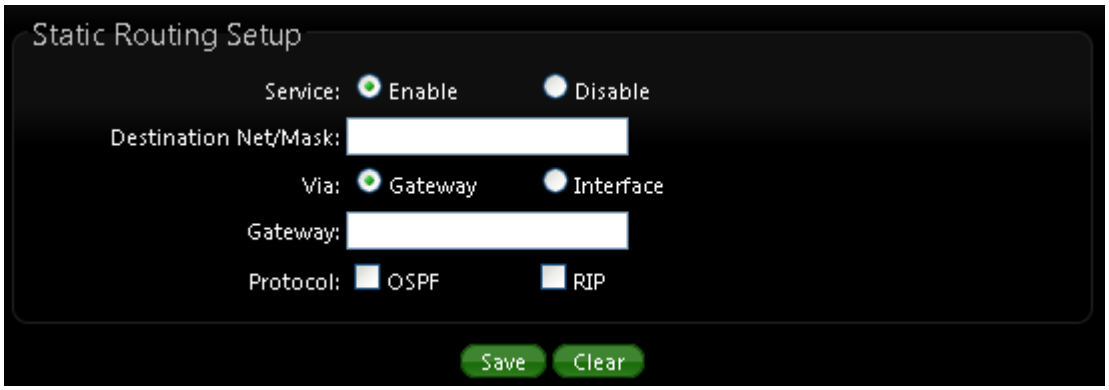
RIP Settings :

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

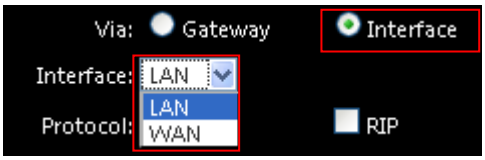
- **RIP Service :** By default, it's Disable. To Enable to activated RIP routing service.
- **Side :** Specify desired interface WAN, LAN for sending and receiving of RIP packets.
- **Distribute OSPF over RIP :** Allow OSPF routes redistributed into RIP.

Change these settings as described here and click Save button to save your changes. Click Reboot button to activate your changes

Static Routing Setup :



- **Service :** Click Enable to activated static routing.
- **Destination Net/Mask :** Specify desired destination IP network address with format of A.B.C.D/M
- **Via :** Select a next hop of Gateway or Interface to the destination IP network.
  - **Gateway :** Enter gateway IP address
  - **Interface :** Choose the interface via LAN or WAN



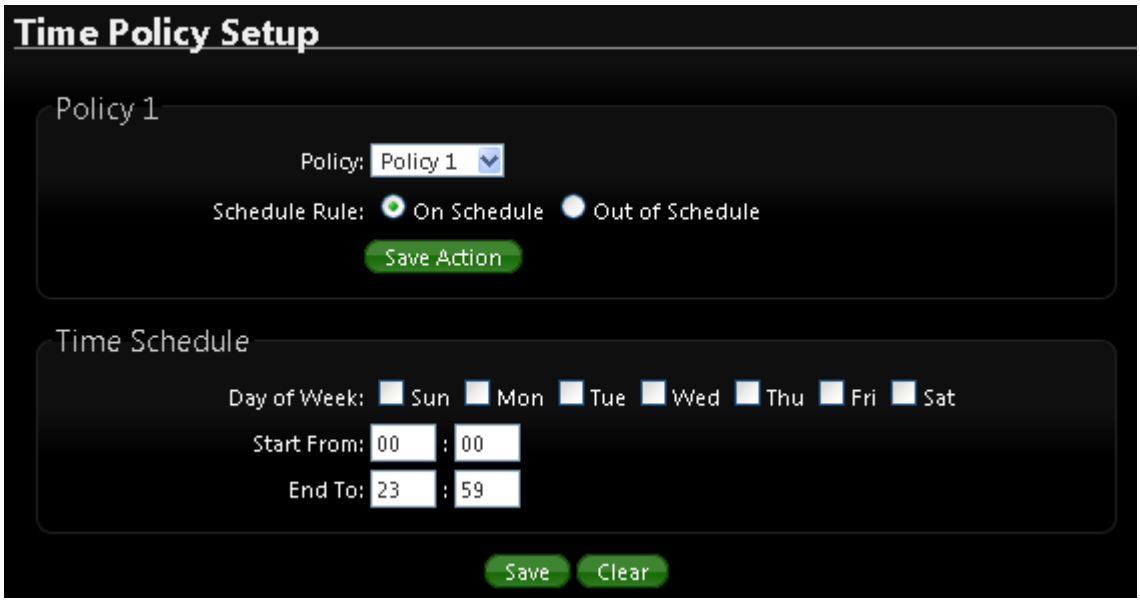
- **Protocol :** Set static routing rule to RIP or OSPF network. Select RIP to associate specific network on RIP routing process. Select OSPF to associate specific network with the specified area on OSPF routing process

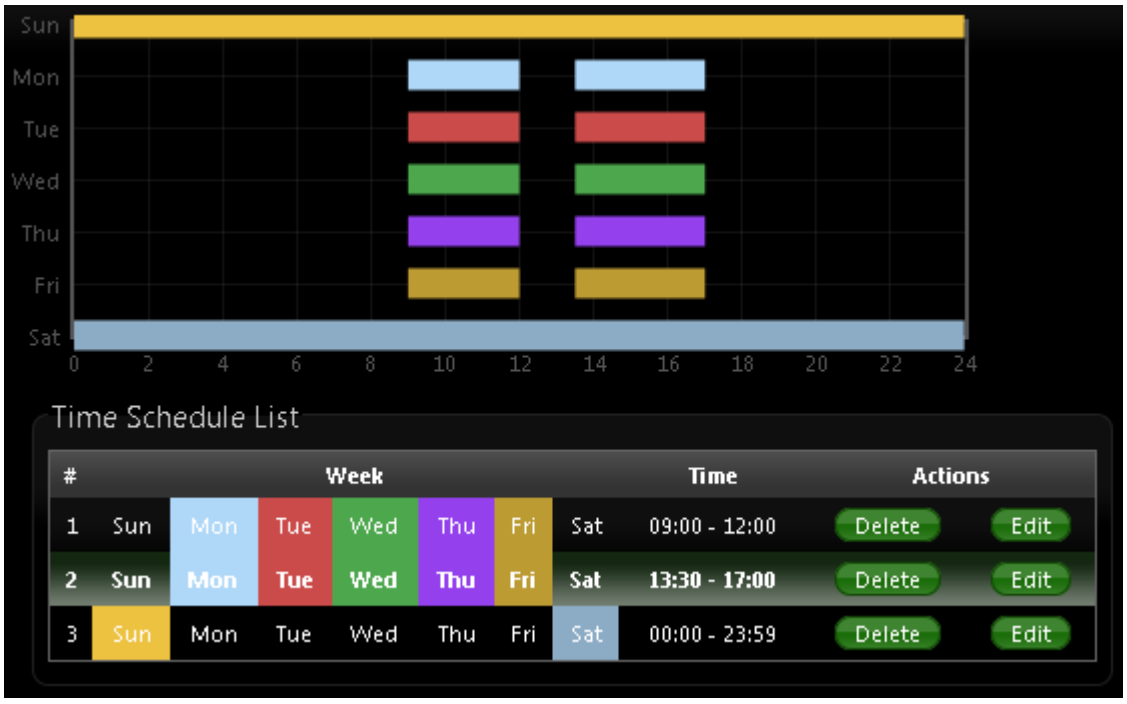
Click “Save” button to add Routing rule to List. There are maximum 20 rules allowed in this List. All rules can be edited or removed on the List. Click **Reboot** button to activate your changes.

7.8 Time Policy

Administrator can define time policy for Service Domain, IP Filtering, MAC Filtering and Virtual Server. There are 10 policy can be defined.

Please click on **Advance →Time Policy** to enter Time Policy Setup page.





- **Policy** : There are 10 Policy can be selected.
- **Schedule Rule** : Select desired schedule for this policy.

Time Schedule :

Select desired day of week and time period for this policy. Below depicts an example for "**On Schedule**" and "**Out of Schedule**"

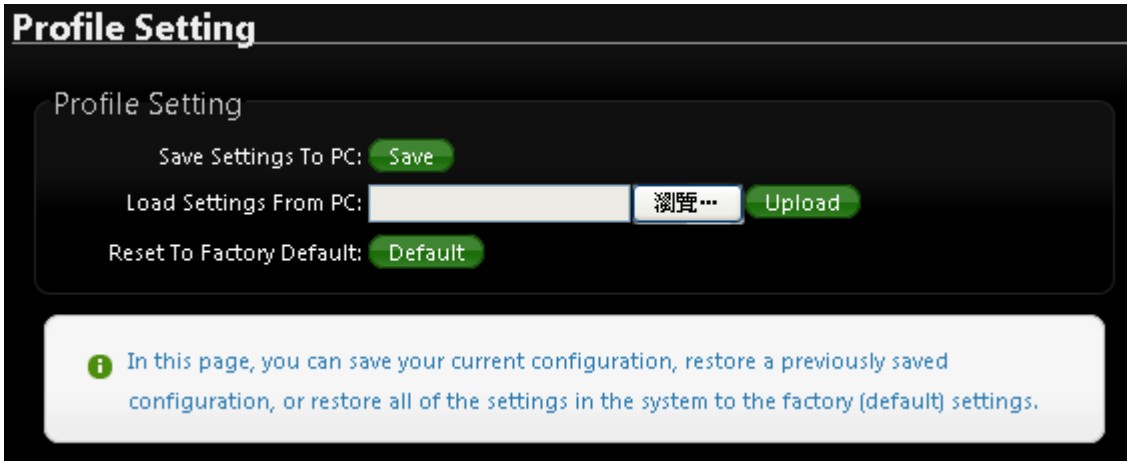
Click **"Save"** button to add schedule to policy. There are 10 schedule maximum allowed in the each time policy. All schedule can be edited or removed in the each time policy. Click **Reboot** button to activate your changes.

8. Configure Utilities Setup

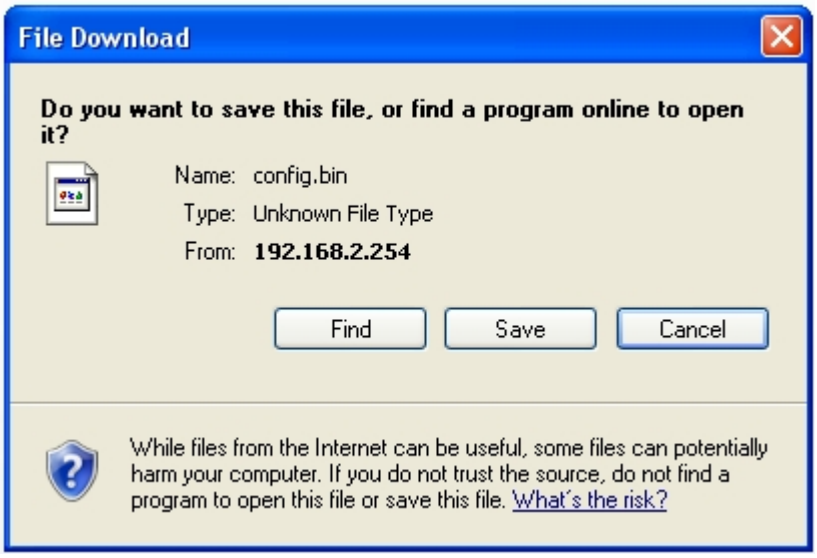
8.1 Profile setting

The Function is backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting



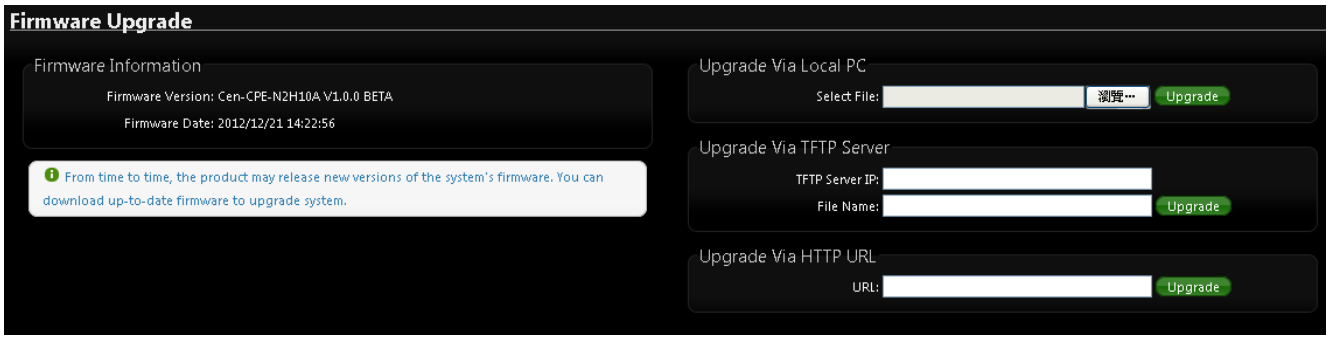
- **Save Settings to PC :** Click ***Save*** button to save the current configuration to a local disk.



- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.
- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

8.2 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around 2 minutes to upgrade due to complexity of firmware. To upgrade system firmware, click Browse button to locate the new firmware, and then click Upgrade button to upgrade.

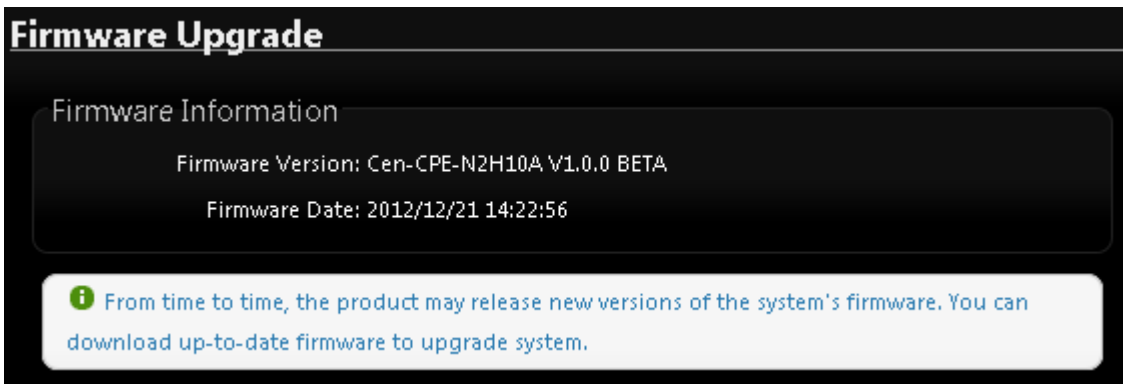


Notice

1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*

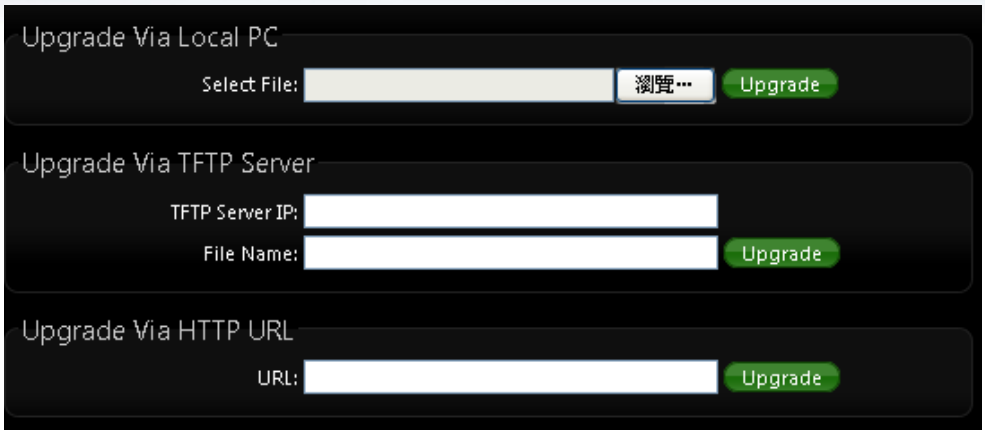
➢ **Firmware Information**

Show currently the **OW-215N2-X** of system software version and software date



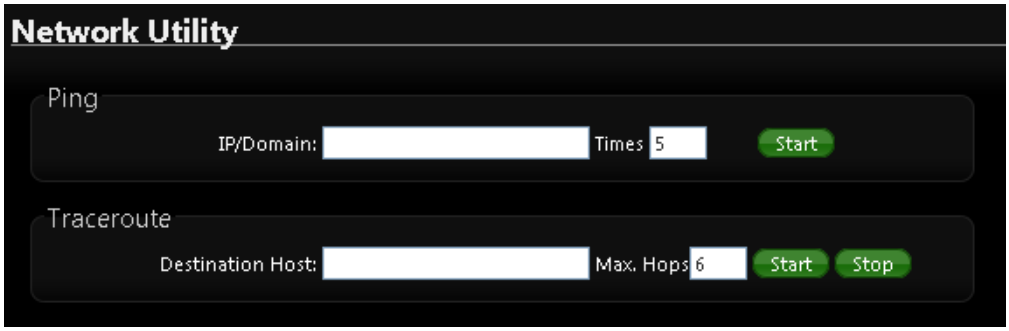
➢ **Upgrade firmware**

The upgrade firmware will support via local PC and TFTP Server and HTTP URL to upgrade system



8.3 Network Utility

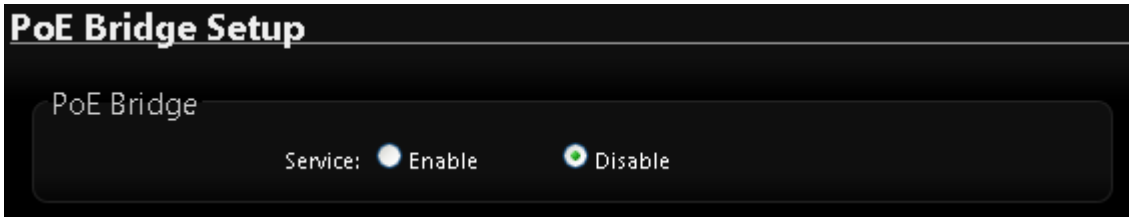
The administrator can diagnose network connectivity via the PING or TRACEROUTE utility. Please click on **Utilities** -> **Network Utility** and follow the below setting.



- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
  - **IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ping button to proceed. The ping result will be shown in the Result field.
  - **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.
- **Traceroute** : Allows tracing the hops from the OW-215N2-X device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test.
  - **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
  - **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) trace route will probe.

8.4 PoE Bridge

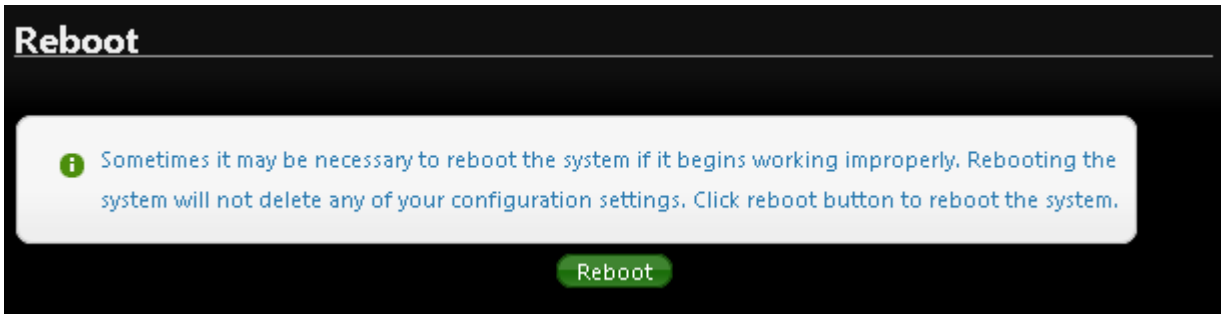
CERIO OW-215N2-X Design smart PoE Bridge function, the PoE Bridge function support provide next AP power. Can will be structure become very convenience. And the PoE bridge support CERIO WM-series AP or OW-series to be dual band budle wireless soultion.(The hardware Install can reference to “1.6 Hardware Installation Steps”)

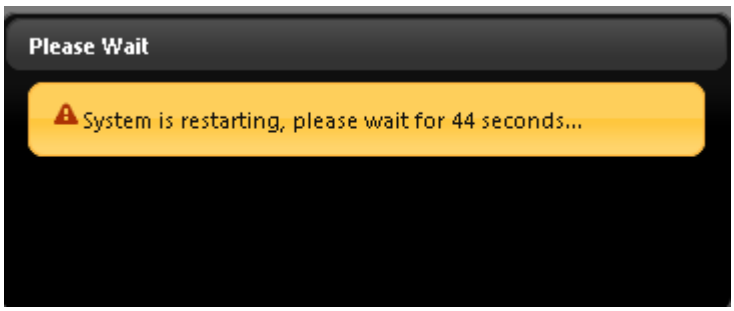


Service : The default is Disable, the function can Enable or Disable PoE Power

8.5 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



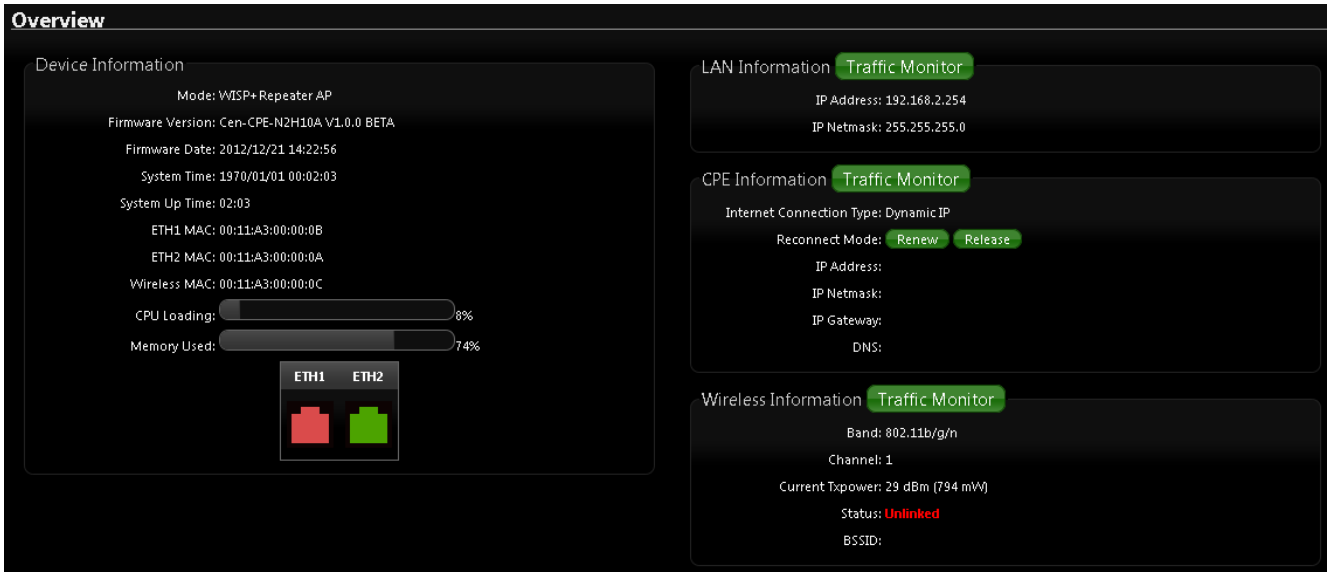


The System Overview page appears upon the completion of reboot.

9. Configure Status

9.1 Overview

Detailed information on System, Network can be reviewed via this page.

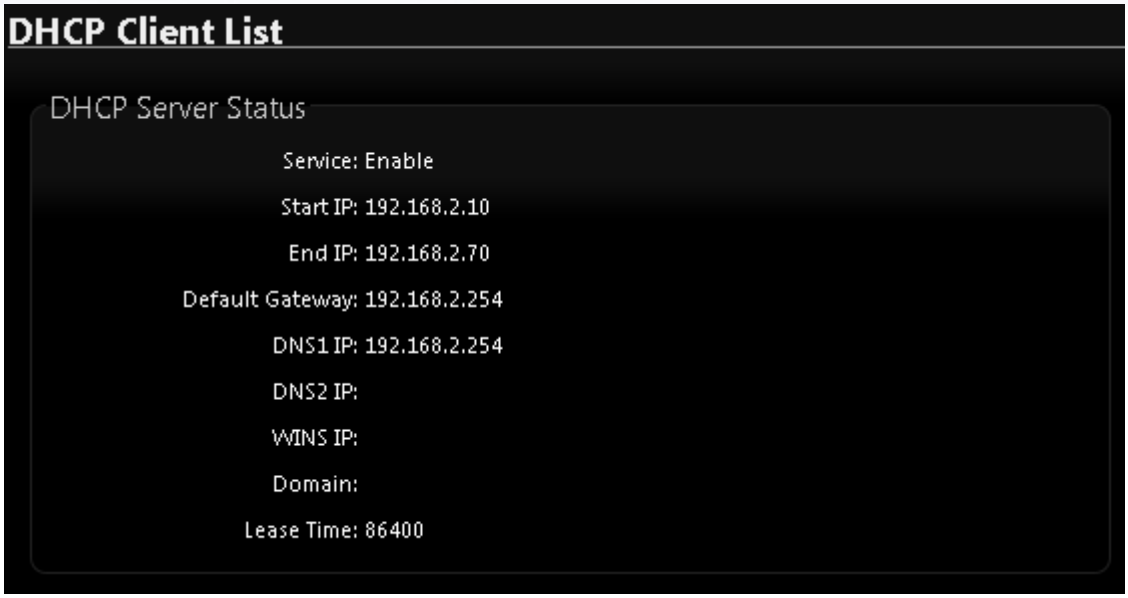


- **System Information :** Display the information of the system.
- **Device Information :** Display the information of the Port link.
- **CPU Information :** Display the information of the system CPU
- **Memory information :** Display the information of the system Memory.
- **Networking Information :** Display the information of the network.
- **Wireless Clients :** Display the information of the wireless user link.

9.2 DHCP Client

The administrator can view status of all DHCP Client Users on each DHCP Server.

Please click on **Status → DHCP Client** to look DHCP information.



- **DHCP Server Status :** Display the information of the DHCP Server.
- **DHCP Client List :** Display the information of the DHCP Client users.

9.3 Extra Info

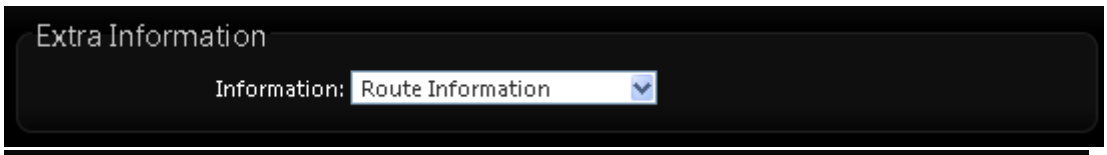
Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The **"Refresh"** button is used to retrieve latest table information.

- **Netstat Information :** Select "NetStatus Information" on the drop-down list, the connection track list should show-up. NetStatus will show all connection track on the system, the information include Protocol, Live Time, Status, Source/Destination IP address and Port.

Netstat Information

Protocol	LiveTime	Status	SrcIP	SrcPort	DstIP	DstPort
tcp	31	TIME_WAIT	192.168.2.22	2506	192.168.2.254	80
tcp	29	TIME_WAIT	192.168.2.22	2505	192.168.2.254	80
tcp	599	ESTABLISHED	192.168.2.22	2511	192.168.2.254	80
tcp	119	TIME_WAIT	192.168.2.22	2510	192.168.2.254	80
tcp	18	TIME_WAIT	192.168.2.22	2503	192.168.2.254	80
tcp	7	TIME_WAIT	192.168.2.22	2502	192.168.2.254	80
unknown	327		192.168.2.254	2502	224.0.0.22	80

- **Route Information :** Select "**Route Information**" on the drop-down list to display route table. OW-215N2-X could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

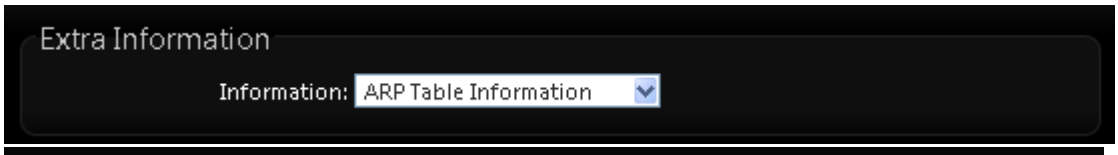


Route Information

Destination	Gateway	Netmask	Interface
192.168.2.0	0.0.0.0	255.255.255.0	bre0
239.0.0.0	0.0.0.0	255.0.0.0	bre0
224.0.0.0	0.0.0.0	224.0.0.0	bre0

- **ARP Table Information** : Select "ARP Table Information" on the drop-down list to display ARP table.

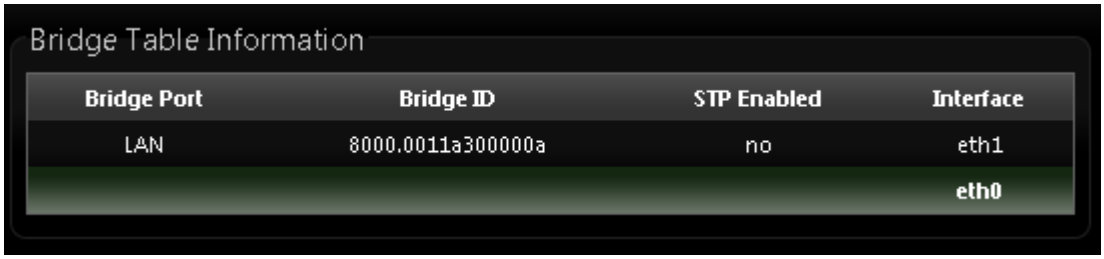
  ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.



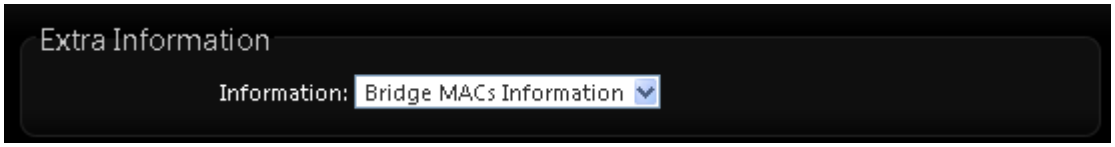
ARP Table Information

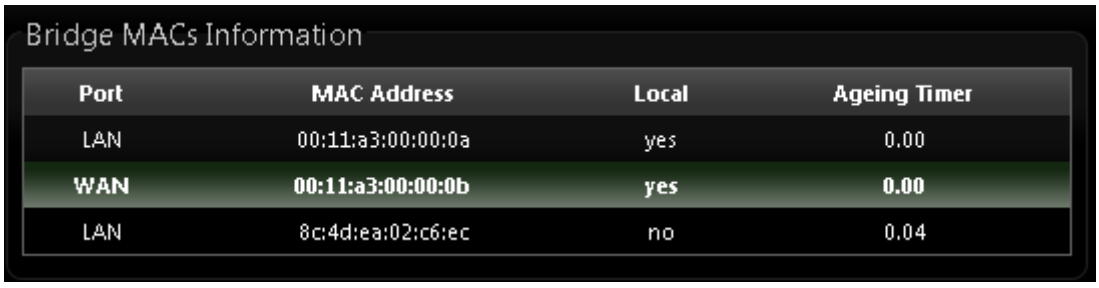
IP Address	MAC Address	Interface
192.168.2.22	8c:4d:ea:02:c6:ec	bre0

- **Bridge table information** : Select “Bridge Table information” on the drop-down list to display bridge table.
  Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth2, ra0~ra7 and wds0~wds3).



- **Bridge MACs Information :** Select “Bridge MACs Information” on the drop-down list to display MAC table.
  This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces. Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.

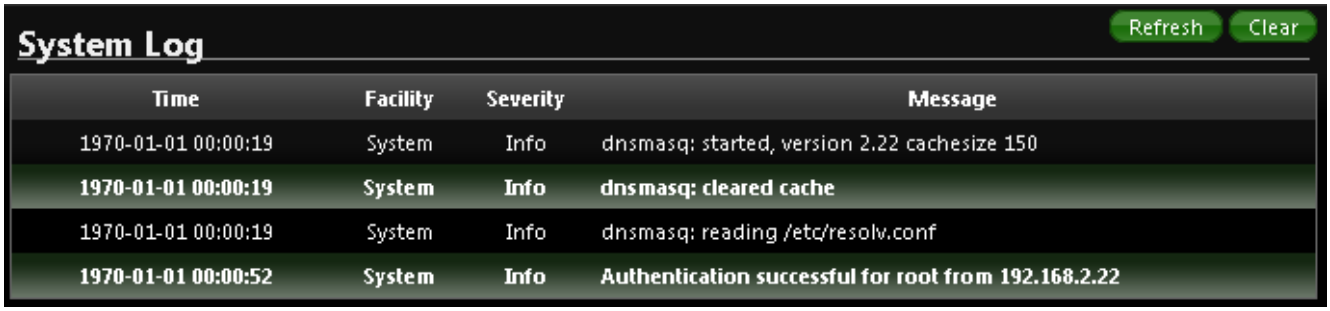




- **Bridge STP Information :** Select “Bridge STP Information” on the drop-down list to display a list of bridge STP information.

9.4 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.



- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.
- Click **“Refresh”** button to renew the log
- Click “**Clear”** button to clear all the record.

Appendix A. MCS Data Rate

The table below shows the relationships between the variables that allow for the maximum data rate

Table C MCS Data Rate

MCS Index	Modulation	Data Rate (Mb/s)			
		Channel Bandwidth = 20		Channel Bandwidth = 40	
		Long Guard Interval	Short Guard Interval	Long Guard Interval	Short Guard Interval
0	BPSK	6.5	7.2	13.5	15.0
1	QPSK	13.0	14.4	27.0	30.0
2	QPSK	19.5	21.7	40.5	45.0
3	16-QAM	26.0	28.9	54.0	60.0
4	16-QAM	39.0	43.3	81.0	90.0
5	64-QAM	52.0	57.8	108.0	120.0
6	64-QAM	58.5	65.0	121.5	135.0
7	64-QAM	65.0	72.2	135.0	157.5
8	BPSK	13.0	14.4	27.0	30.0
9	QPSK	26.0	28.9	54.0	60.0
10	QPSK	39.0	43.3	81.0	90.0
11	16-QAM	52.0	57.8	108.0	120.0
12	16-QAM	78.0	86.7	162.0	180.0
13	64-QAM	104.0	115.6	216.0	240.0
14	64-QAM	117.0	130.0	243.0	270.0
15	64-QAM	130.0	114.4	270.0	300.0

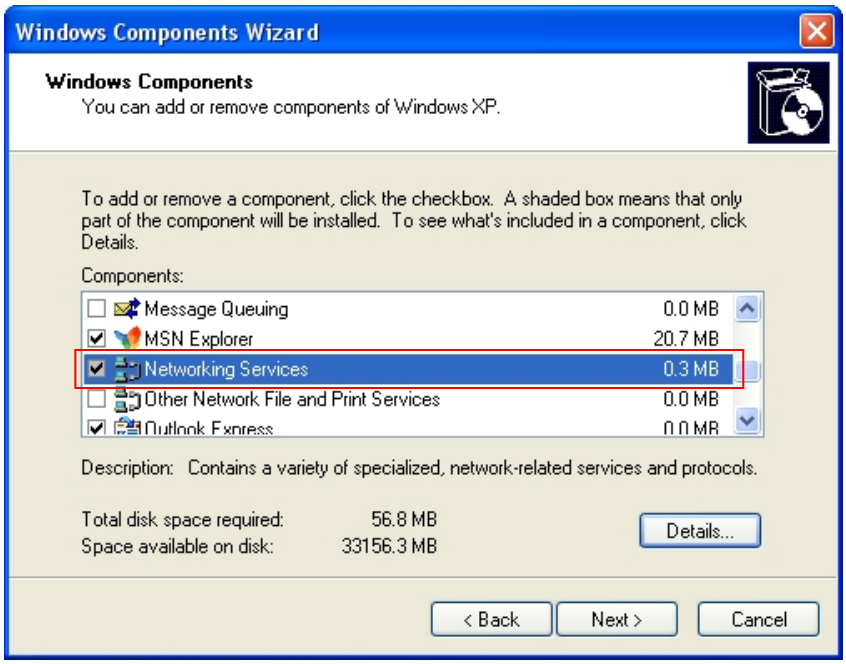
Note :

- When MCS=32, only Short Guard Interval option is supported, Channel Bandwidth=20 is not supported. If Channel Bandwidth=40, the HT duplicate 6Mbps.
- When MCS=0~7(One Tx Stream), Guard Interval and Channel Bandwidth are supported
- When MCS=8~15(Two Tx Stream), Guard Interval and Channel Bandwidth are supported

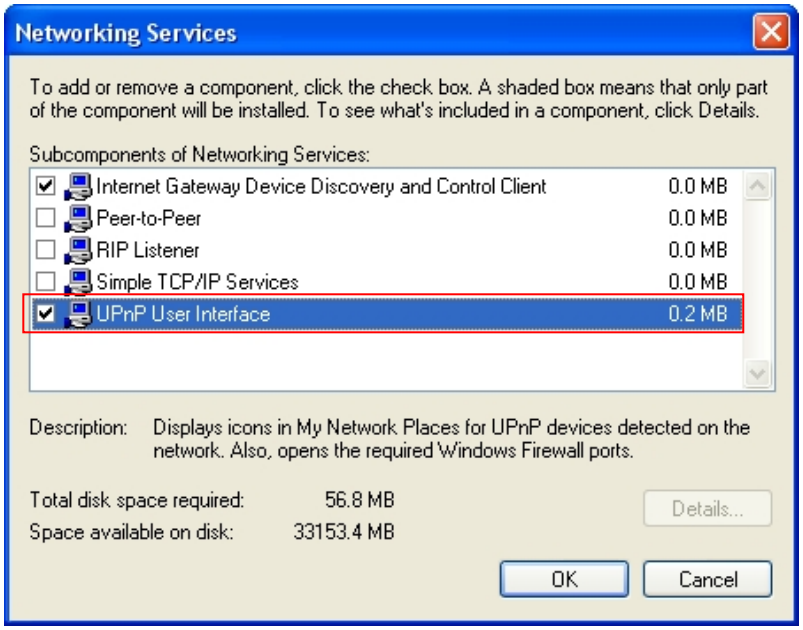
Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

Appendix B. Enabling UPnP in Windows XP

i. Open the "***Add/Remove Programs***" control panel, and then click on "***Add/Remove Windows Components***" in the sidebar. Scroll down and find "***Networking Services***", highlight it, and then click ***Details***.



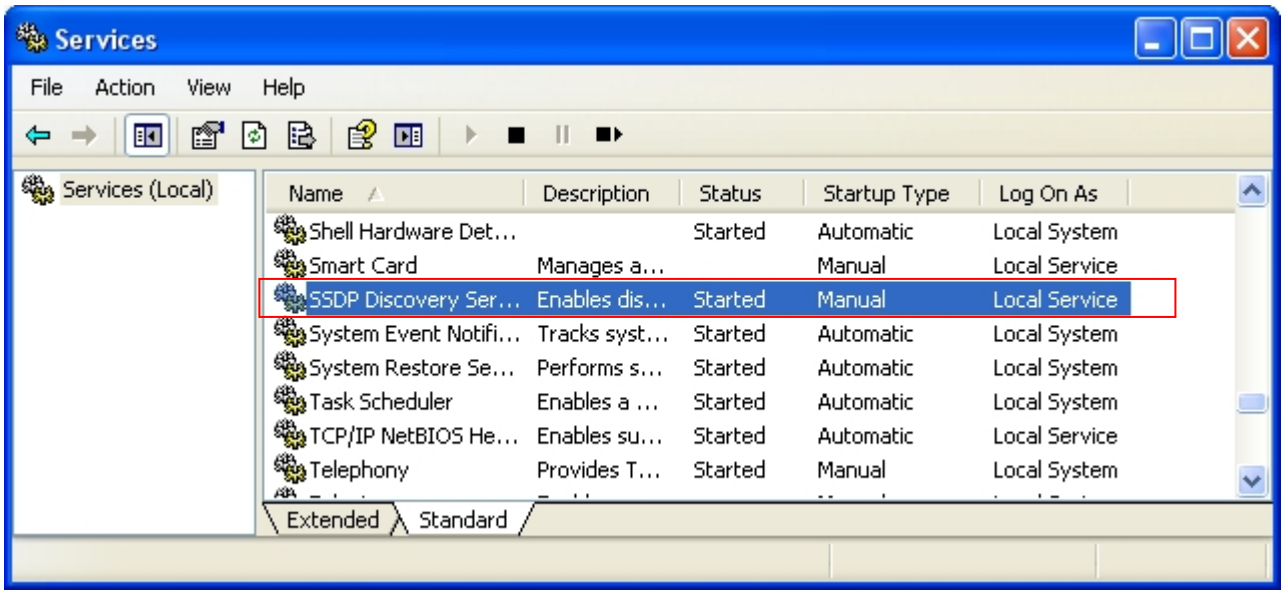
ii. In the "**Networking Services**" window, ensure that the "***Internet Gateway Device***" and "***UPnP User Interface***" options are checked. If they are not, check it to enable them, as shown below, and click OK to continue.



iii. Next, in the "**Control panel**", open the "***Administrative Tools***" and then open "***Services***". Scroll down until you find the "***SSDP Discovery Interface***". If the Status is not ***Started***, double-click on

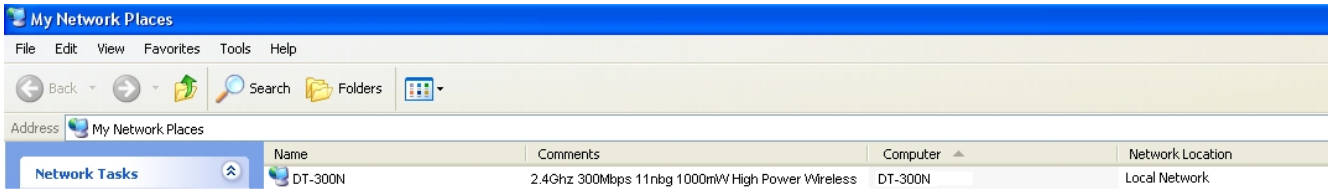
Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

SSDP Discovery Interface to open the service properties. Change the startup type to ***Automatic***, then close the properties. Now, right-click on *SSDP Discovery Services*, and choose ***Start*** from the pop-up menu. The SSDP Discovery Service will then be running and start each time you boot.



PnP and starting the SSDP Discovery Service, it may take few minutes for the “Air Force One

iv. To be discovered and appear in your “***My Network Places***”.



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 FCC Rules. These limits are designed to provide reasonable protection against

Sales-Mail : issales@cerio.com.tw
Support : support@cerio.com.tw

harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
Reorient or relocate the receiving antenna.
Increase the separation between the equipment and receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio technician for help.

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 5 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.
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.
Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.
Federal Communication Commission (FCC) Radiation Exposure Statement
This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Cerio Corporation technique support
E-mail: support@cerio.com.tw
TEL: +886-2-8667-6160 #222
Web Site: www.cerio.com.tw