

CERIO Corporation

GS Software for CW-300N

**eXtreme Power 11n 2.4Ghz 2x2 Ceiling / Wall PoE with
CenOS3.0 Access Point (500mW)**

CenOS3.0

User's Manual

Table of Contents

1.	Introduction.....	4
1.1	Overview	4
1.2	CenOS 3.0 Software key Features	5
2.	CenOS 3.0 Operation Mode Applications	6
2.1	Pure AP Mode & AP/ AP+WDS Mode	6
2.2	Client Bridge + Universal Repeater Mode.....	7
3.	AP Mode Configuration.....	8
3.1	Choose Your Operating Mode (AP Mode)	8
3.2	External Network Connection	8
3.3	Configure CW-300N LAN IP Address	9
3.4	Wireless General Setup	10
3.5	Configure Wireless Advanced Setup	12
3.6	Create Virtual AP – Virtual AP Setup	17
3.8	WDS Setup - Expand your Wireless Network.....	27
3.9	WDS Status	28
3.10	Associated Clients	28
4.	Client Bridge + Repeater AP Mode Configuration	29
4.1	Choose Your Operating Mode(Client Bridge + Repeater AP).....	29
4.2	External Network Connection (Network Requirement)	29
4.3	Configure CW-300N LAN IP Address	30
4.4	Wireless General Setup	32
4.5	Configure Wireless Advanced Setup	33
4.6	Site Survey.....	39
4.7	Station Profile.....	40
4.8	Remote AP Status	42
4.9	Repeater AP Setup.....	42
4.10	Repeater AP MAC Filter Setup.....	46
5.	System Management.....	48
5.1	Configure Management	48
5.2	Configure System Time	52
5.3	Configure SNMP Setup.....	53
6.	Configure Advance Setup.....	54
6.1	Time Policy	54
7.	Configure Utilities Setup.....	56
7.1	Profile setting	56
7.2	Firmware Upgrade.....	57

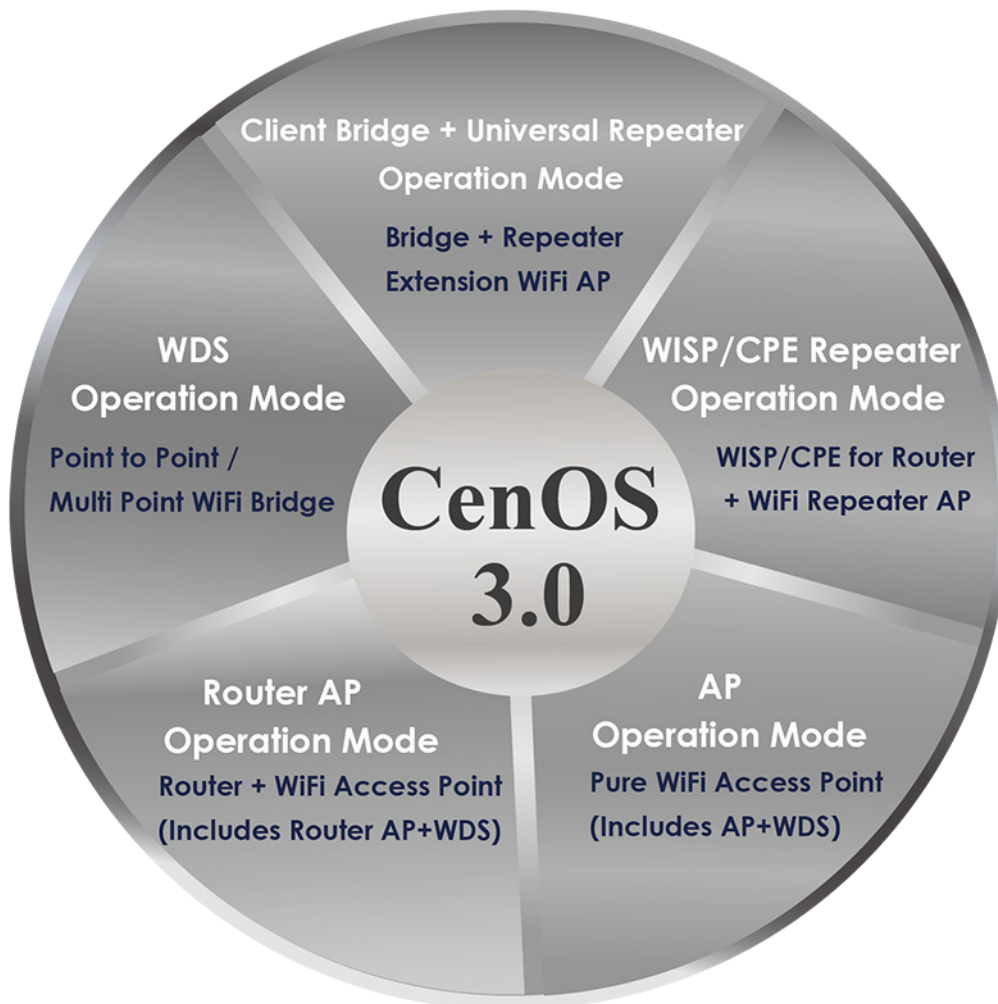
7.3	Network Utility	58
7.4	Reboot	59
8.	Configure Status	59
8.1	Overview	59
8.2	Extra Info	60
8.3	Event Log	63
Appendix A.	Windows TCP/IP Settings	64
Appendix B.	WEB GUI Valid Characters	66
Appendix C.	MCS Data Rate	68

1. Introduction

1.1 Overview

CERIO's GS Firmware utilizes the CenOS 3.0 core . The firmware's main functions are Wifi application for Pure WiFi Access Point, Point to Point / Multi Point WiFi Bridge and Bridge + Repeater Extension WiFi AP functions.

The CenOS 3.0 core's operational mode supports Pure AP with WDS Mode and Client Bridge + Universal Repeater + Universal Repeater Mode. These CenOS 3.0 features simplify deployment and reduce cost for continued maintenance of indoor Access Points. Cerio's CenOS is undoubtedly your best wifi application solution.



Only Cerio's special model supports Router AP mode

CERIO CW-300N 2.4Ghz 300Mbps 11nbg 500mW High Power AP/ Bridge supports two operational modes: **Pure AP mode / AP+WDS mode and Client Bridge + Universal Repeater Mode**. It utilizes built-in remote management features that simplify deployment and reduce costs for continued maintenance of the outdoor bridge.

1.2 CenOS 3.0 Software key Features

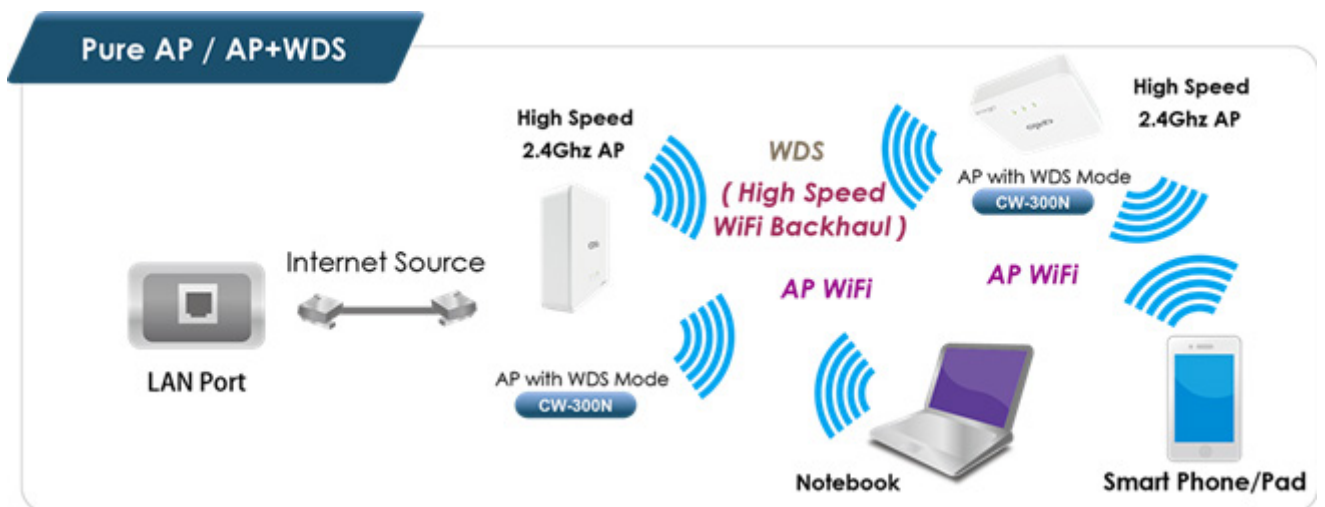
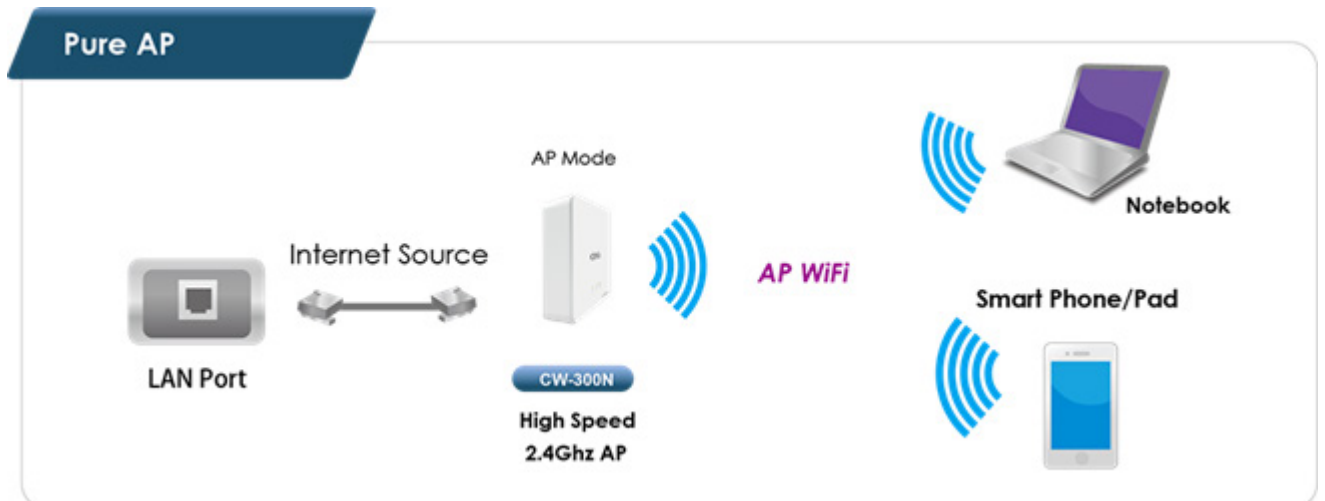
- Operation Modes : AP Mode, AP+WDS Mode, Client Bridge + Universal Repeater Mode
- Maximum Security with 802.1x, WAP, and WPA2
- Supports 8 Multiple-ESSID. And Support IEEE802.11f IAPP
- Built-in Wireless RF Signal Enable and Disable by time scheduling function
- Enable and Disable to control blinking of the devices LED lights
- Supports IEEE802.1d Spanning Tree
- Integrated IGMP v1/v2/v3 snooping functions and Supports Web management
- Ping Watchdog function support
- Supports Hardware chipset base Watch Time Dog , The OS will reboot automatically before crashing
- Software UI support Auto reboot setting function , Can by Hour/Daily/Weekly to setting software Auto reboot
- Auto Channel Scan and support Scan other AP site survey Single information
- Bundles Cerio CenOS3.0 software Core interface which allows for communication between Cerio Wireless Management Software (CWMS) and CERIO AM-Series AP Management WLAN Switch or Access Controller hardware device of network management servers
- Provides Traffic Monitor and Graphical GUI Status Interface

2. CenOS 3.0 Operation Mode Applications

CERIO CW-300N eXtreme Power 11n 2.4Ghz 2x2 Wireless Access Point with CenOS3.0 software supports two operational modes: **Pure AP mode / AP+WDS mode and Client Bridge + Universal Repeater Mode**. It utilizes built-in remote management features that simplify deployment and reduce costs of continued maintenance of the access point

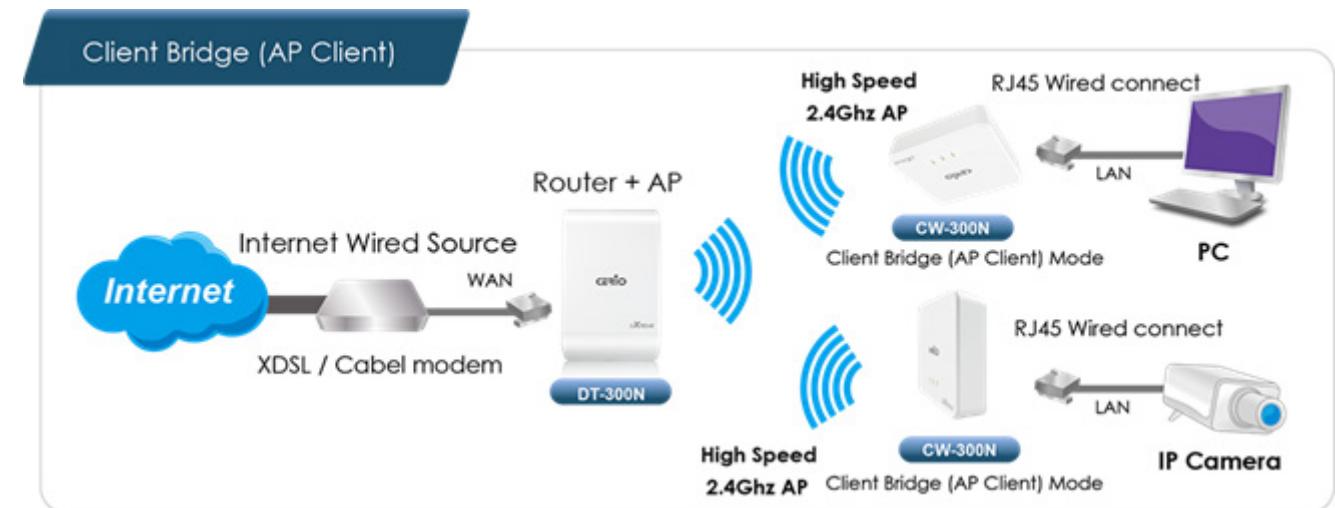
2.1 Pure AP Mode & AP/ AP+WDS Mode

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



2.2 Client Bridge + Universal Repeater Mode

- It can be used as a Client Bridge + Universal Repeater to receive wireless signals over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers
- In this mode, CW-300N is enabled with DHCP Server functions. The wired clients of CW-300N are in the same subnet from Main Base Station and it accepts wireless connections from client devices. You can disabled the repeater extending AP function, which will enable the “AP Client ” function



Notice

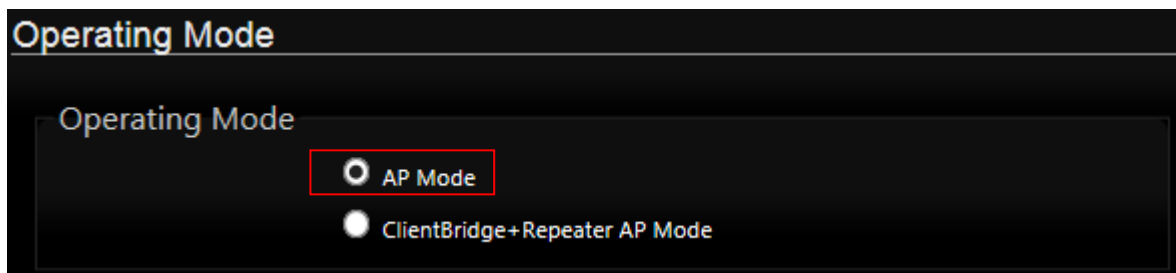
For Administrators using Client Bridge + Repeater AP mode, the Client Bridge must be connected to the Internet Source (AP) for the Universal Repeater Mode to properly function. If the Client Bridge AP is not properly connected to the Internet Source (AP), the option for Repeater Mode will not be visible.

3. 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.

3.1 Choose Your Operating Mode (AP Mode)

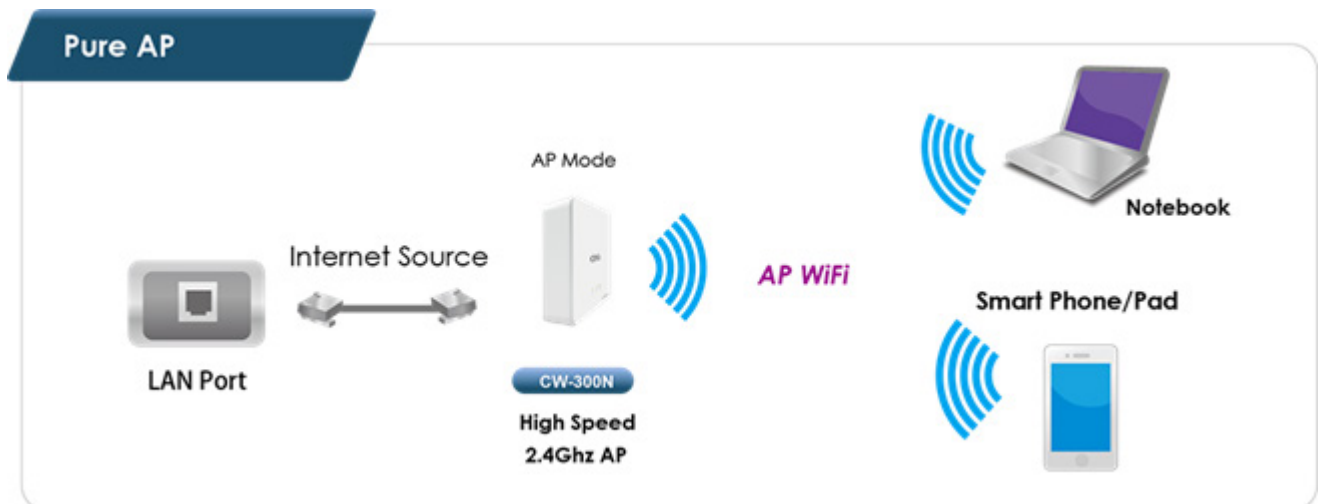
The system administrator can set the desired mode via this page, and then configure the system according to their deployment needs, Please click on **System -> Operating Mode** and follow the below setting.



3.2 External Network Connection

➤ **Network Requirement**

Normally, **CW-300N** connects to a wired LAN and provides a wireless connection point to associate with wireless client. Then, Wireless clients can access to LAN or Internet by associating themselves with **CW-300N** set in AP mode.



3.3 Configure CW-300N 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.

The screenshot shows the LAN Setup and DNS configuration interface. The LAN Setup section includes an Ethernet Connection Type section with radio buttons for Static IP (selected) and Dynamic IP. Below this is the Static IP section with input fields for IP Address (192.168.2.254), IP Netmask (255.255.255.0), and IP Gateway. The DNS section includes radio buttons for No Default DNS Server (selected) and Specify DNS Server IP, with input fields for Primary DNS and Secondary DNS. The 802.1d Spanning Tree section includes radio buttons for Enable (selected) and Disable.

➤ 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 **CW-300N** is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

LAN Setup

Ethernet Connection Type

Mode: Static IP Dynamic IP

Dynamic IP

Hostname:

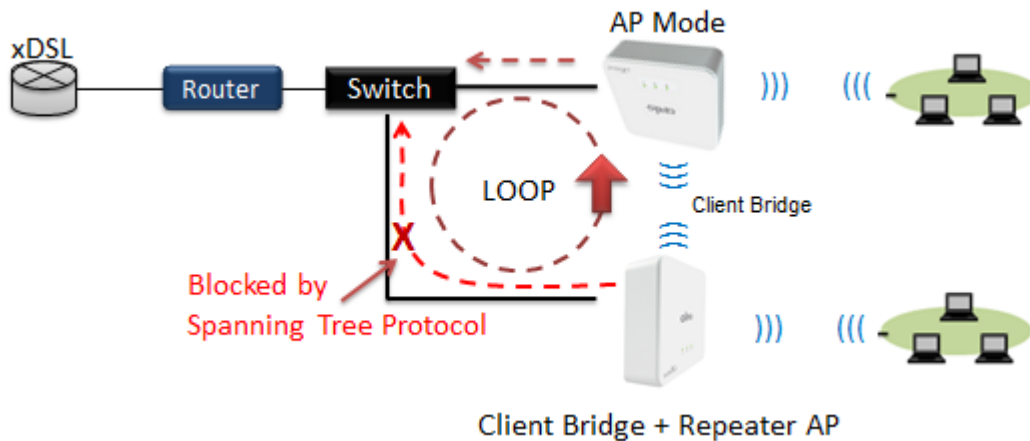
✓ **Hostname:** The Hostname of the LAN port.

➤ **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**

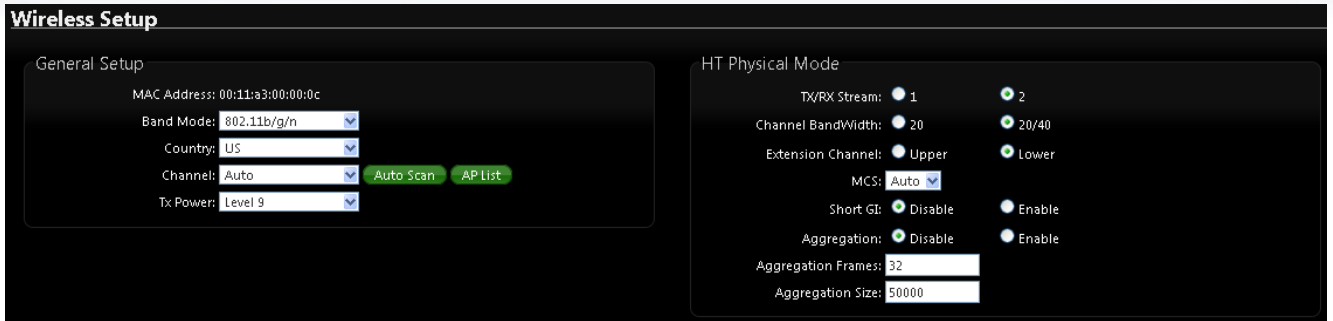
The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d



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

3.4 Wireless General 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.



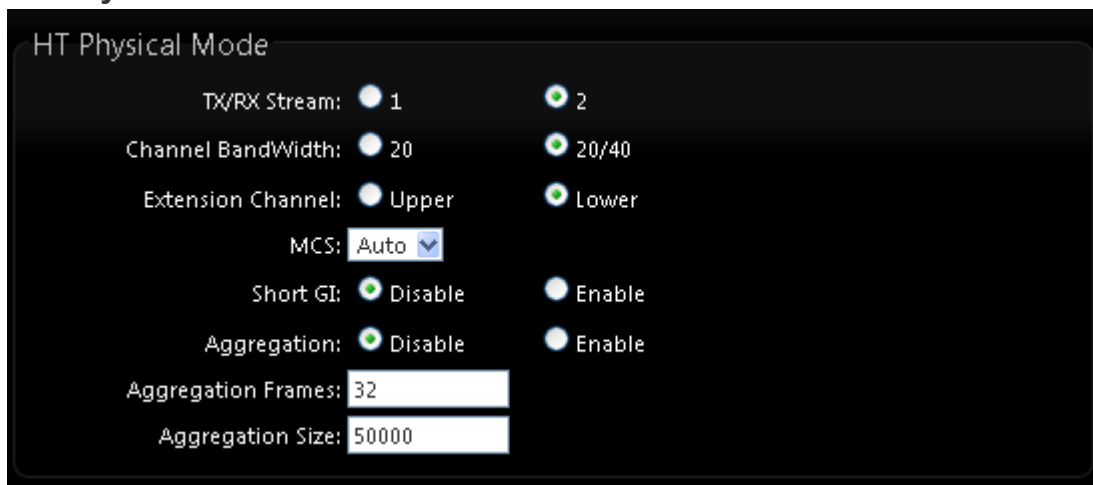
- **MAC Address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode**
- **Country** : a region, the CW-300N support region for US,ETSI and Japan
- **Channel** : Choosing the best WiFi channel
 - ✧ 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

ESSID	MAC Address	Channel	Signal/Noise, dBm	RSSI	Signal Quality, %	Encryption
Danny	00:23:F8:07:1F:10	6	-36 / -95	59	100	On
7904w	78:CD:8E:B4:00:89	6	-82 / -95	13	32	On

Current Frequency = 2.432 GHz (Channel 5)

- **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%**).

➤ **HT Physical Mode**



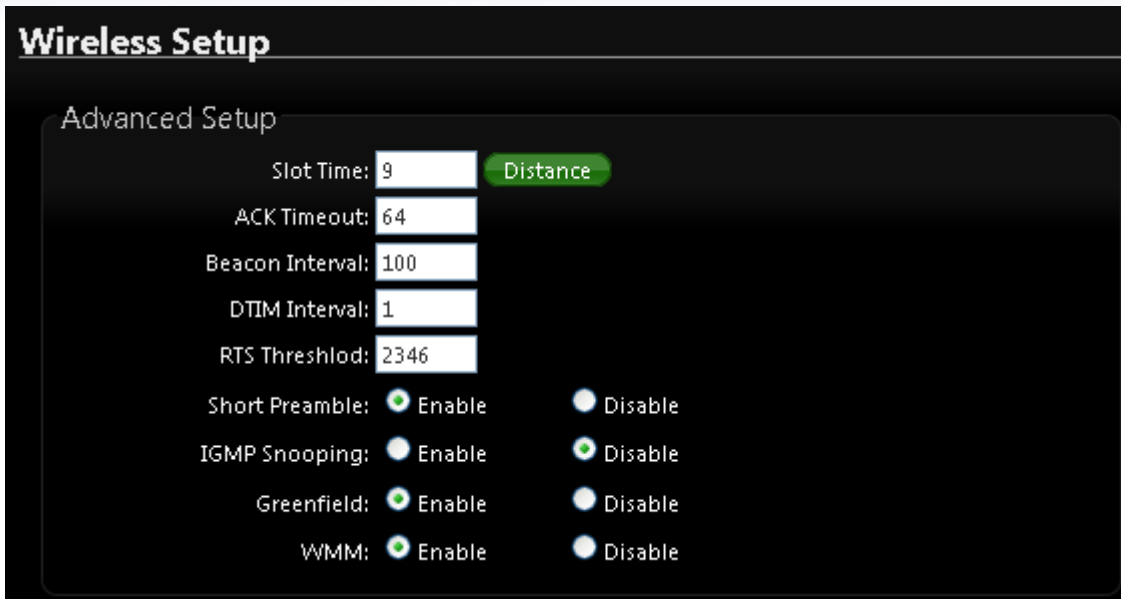
- **HT TxStream/RxStream** : By default, it's **2**
- **Channel Bandwidth** : The "20/40" MHz option is usually best. The other option is available for special circumstances.

- **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.
- **Short 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 item 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.

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.



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.
- **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.

WMM QoS

WMM Parameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	6	3	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI(2)	3	4	1	3008	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO(3)	2	3	1	1504	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	10	3	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI(2)	3	4	2	3008	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO(3)	2	3	2	1504	<input type="checkbox"/>	<input type="checkbox"/>

✓ **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 unicast packet. ◦

3.6 Create Virtual AP – Virtual AP Setup

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

Virtual AP Overview

VAP List

VAP	MAC Address	ESSID	Status	Security Type	MAC Filter Edit	MAC Filter Status	VAP Edit
VAP0	00:11:A3:00:00:0C	AP00	On	WPA2-PSK	Edit	Disable	Edit
VAP1		AP01	Off	Disabled	Edit	Disable	Edit
VAP2		AP02	Off	Disabled	Edit	Disable	Edit
VAP3		AP03	Off	Disabled	Edit	Disable	Edit
VAP4		AP04	Off	Disabled	Edit	Disable	Edit
VAP5		AP05	Off	Disabled	Edit	Disable	Edit
VAP6		AP06	Off	Disabled	Edit	Disable	Edit
VAP7		AP07	Off	Disabled	Edit	Disable	Edit

- **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

3.7 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.

Virtual AP Overview

VAP List

VAP	MAC Address	ESSID	Status	Security Type	MAC Filter Edit	MAC Filter Status	VAP Edit
VAP0	00:11:A3:00:00:0C	AP00	On	WPA2-PSK	Edit	Disable	Edit
VAP1		AP01	Off	Disabled	Edit	Disable	Edit
VAP2		AP02	Off	Disabled	Edit	Disable	Edit
VAP3		AP03	Off	Disabled	Edit	Disable	Edit
VAP4		AP04	Off	Disabled	Edit	Disable	Edit
VAP5		AP05	Off	Disabled	Edit	Disable	Edit
VAP6		AP06	Off	Disabled	Edit	Disable	Edit
VAP7		AP07	Off	Disabled	Edit	Disable	Edit

VAP0 Setup

Security

ESSID:

Hidden SSID: Enable Disable

Client Isolation: Enable Disable

IAPP: Enable Disable

Maximum Clients:

VLAN ID(Tag): VLAN ID:

Security Type:

WDS Setup

* The Channel must be fixed!

Service: Enable Disable

#	Enable	WDS Peer's MAC Address	Description
01	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
02	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
03	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
04	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

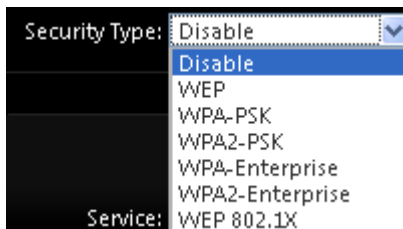
- **ESSID:** Extended Service Set ID indicates the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which is assigned to the specified VAP.

- **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 being seen on the network.
- **Client Isolation:** Select Enable, all clients will be isolated from each other, which means all clients cannot reach to other clients.
- **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association throughout an ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period.



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 clients 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 CW-300N, 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.

The screenshot displays the WPA General configuration interface. It is divided into three main sections: WPA General, Authentication RADIUS Server, and Secondary Authentication RADIUS Server. In the WPA General section, the Cipher Suite is set to AES (selected with a green dot) and TKIP (unselected with a grey dot). Below this, three input fields are shown: Group Key Update Period (600), Master Key Update Period (86400), and EAP Reauth Period (3600). The Authentication RADIUS Server section includes fields for Server IP, Port (1812), and Shared Secret, along with an Accounting RADIUS Server toggle set to Disable. The Secondary Authentication RADIUS Server section has similar fields for Server IP, Port (1812), and Shared Secret.

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.
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 RADIUS Server

Server IP:

Port:

Shared Secret:

Accounting RADIUS Server: Enable Disable

- ✧ **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

Secondary Authentication RADIUS Server

Server IP:

Port:

Shared Secret:

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

The screenshot shows a configuration interface with three main sections:

- Dynamic WEP Settings:** Includes radio buttons for '64bits' (selected) and '128bits'. Below are input fields for 'WEP Key Update Period' (300) and 'EAP Reauth Period' (3600).
- Authentication RADIUS Server:** Includes input fields for 'Server IP', 'Port' (1812), and 'Shared Secret'. At the bottom are radio buttons for 'Enable' and 'Disable' (selected).
- Secondary Authentication RADIUS Server:** Includes input fields for 'Server IP', 'Port' (1812), and 'Shared Secret'.

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 allow or reject clients to access Virtual AP. Please click on **Wireless -> Virtual AP Setup -> MAC Filter Setup**, then click “**Setup**” of Virtual AP List. The **MAC Filter Setup** page will then appears. Follow the below setting.

Virtual AP Overview

VAP List

VAP	MAC Address	ESSID	Status	Security Type	MAC Filter Edit	MAC Filter Status	VAP Edit
VAP0	00:11:A3:00:00:0C	AP00	On	WPA2-PSK	Edit	Disable	Edit
VAP1		AP01	Off	Disabled	Edit	Disable	Edit
VAP2		AP02	Off	Disabled	Edit	Disable	Edit
VAP3		AP03	Off	Disabled	Edit	Disable	Edit
VAP4		AP04	Off	Disabled	Edit	Disable	Edit
VAP5		AP05	Off	Disabled	Edit	Disable	Edit
VAP6		AP06	Off	Disabled	Edit	Disable	Edit
VAP7		AP07	Off	Disabled	Edit	Disable	Edit

VAP0 MAC Filter Setup

MAC Rules

Action: Save

MAC Address: Add

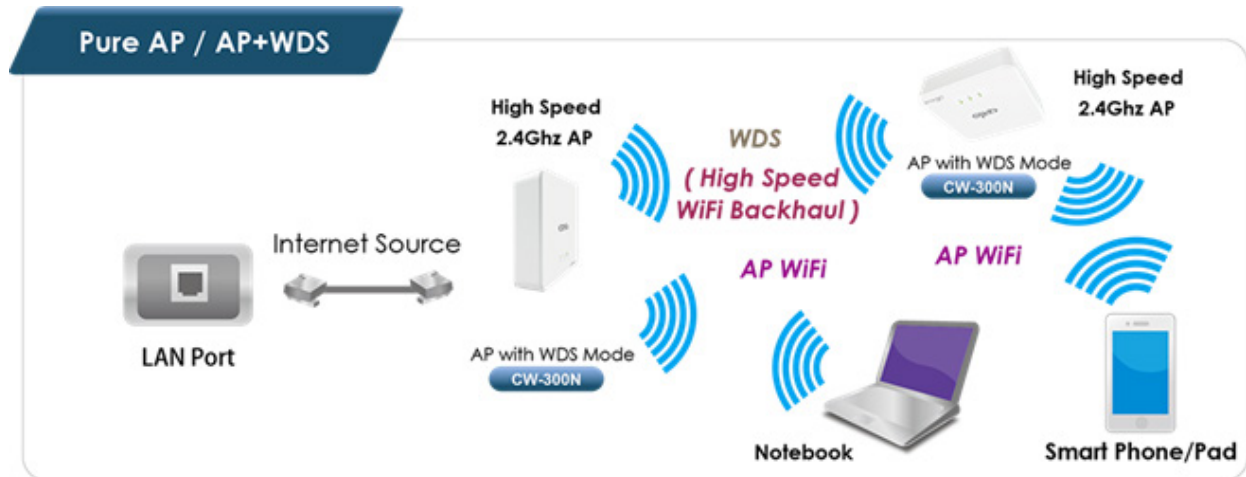
- **Action:** Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.
 - ✓ **Only Allow List MAC:** Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients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



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

3.8 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 CW-300N.



Please click on **Wireless** -> **Virtual AP Setup**, click “**Edit**” of Virtual AP List and follow the below setting.

WDS Setup

^ The Channel must be fixed!

Service: Enable Disable

#	Enable	WDS Peer's MAC Address	Description
01	<input type="checkbox"/>	: : : : : : :	
02	<input type="checkbox"/>	: : : : : : :	
03	<input type="checkbox"/>	: : : : : : :	
04	<input type="checkbox"/>	: : : : : : :	

- **Service:** By default, it's “Disable”. “Enable” to activate WDS
- **Enable:** Click the **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.

3.9 WDS Status

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

WDS Link Status					
WDS Link Status					
#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	TX/RX Bytes
No WDS Link!					

- **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

3.10 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.

Associated Client Status				
Wireless Information				
VAP	ESSID	Status	Security Type	Clients
VAP0	AP00	On	WPA2-PSK	0
VAP1	AP01	Off	Disabled	0
VAP2	AP02	Off	Disabled	0
VAP3	AP03	Off	Disabled	0
VAP4	AP04	Off	Disabled	0
VAP5	AP05	Off	Disabled	0
VAP6	AP06	Off	Disabled	0
VAP7	AP07	Off	Disabled	0

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

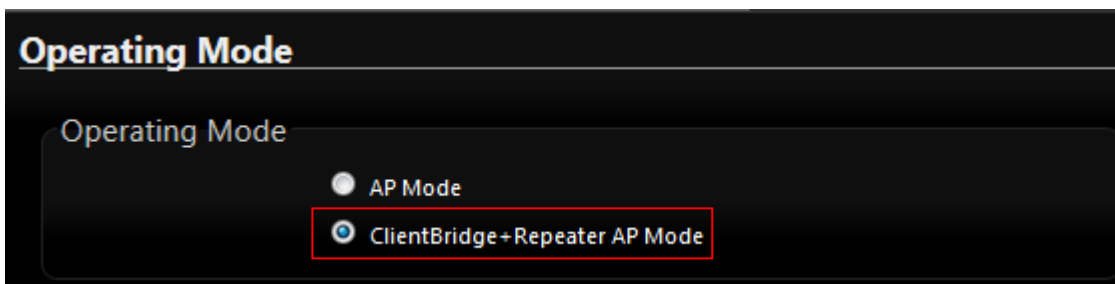
- **VAP:** Display number of system's Virtual AP.
- **ESSID:** Extended Service Set ID of the Virtual AP.
- **Status:** Display Virtual AP status currently.
- **Security Type:** Security type activated by the Virtual AP.
- **Clients:** Number of clients currently associated to the Virtual AP.

4. Client Bridge + Repeater AP Mode Configuration

When Client Bridge + Repeater AP Mode is chosen, the system can be configured as a Client Bridge + Repeater AP Mode. 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 Choose 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, **CW-300N** is enabled with DHCP Server functions. The wired clients of **CW-300N** are in the same subnet from Main Base Station and it accepts wireless connections from client devices.



When the **CW-300N** 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 **CW-300N** to Main Base Station and wireless client to **CW-300N** , but security type can be different.

4.3 Configure CW-300N 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 Setup

Ethernet Connection Type

Mode: Static IP Dynamic IP

Static IP

IP Address: 192.168.2.254 *

IP Netmask: 255.255.255.0 *

IP Gateway:

DNS

DNS: No Default DNS Server Specify DNS Server IP

Primary DNS: *

Secondary DNS:

802.1d Spanning Tree

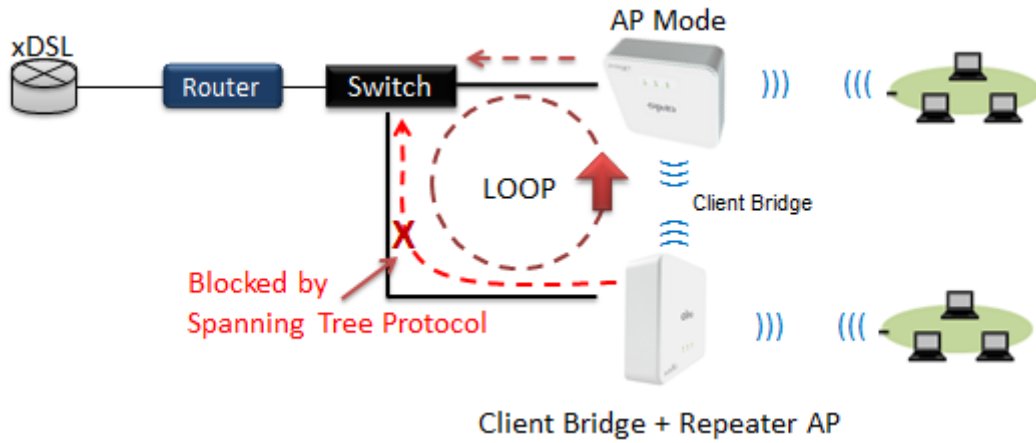
Service: Enable Disable

- **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.



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

DHCP Server

Service: Enable Disable

Start IP: *

End IP: *

Default Gateway: *

DNS1 IP: *

DNS2 IP:

WINS IP:

Domain:

Lease Time:

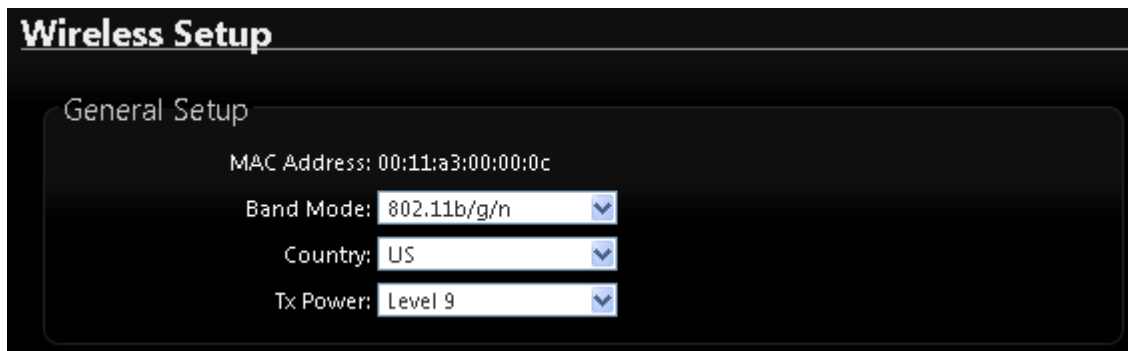
- **DHCP :** Check **Enable** button to activate this function or **Disable** to deactivate this service.
- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask 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.



Wireless Setup

General Setup

MAC Address: 00:11:a3:00:00:0c

Band Mode: 802.11b/g/n

Country: US

Tx Power: Level 9

- **MAC Address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode**
- **Country** : a region, the CW-300N 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%**).

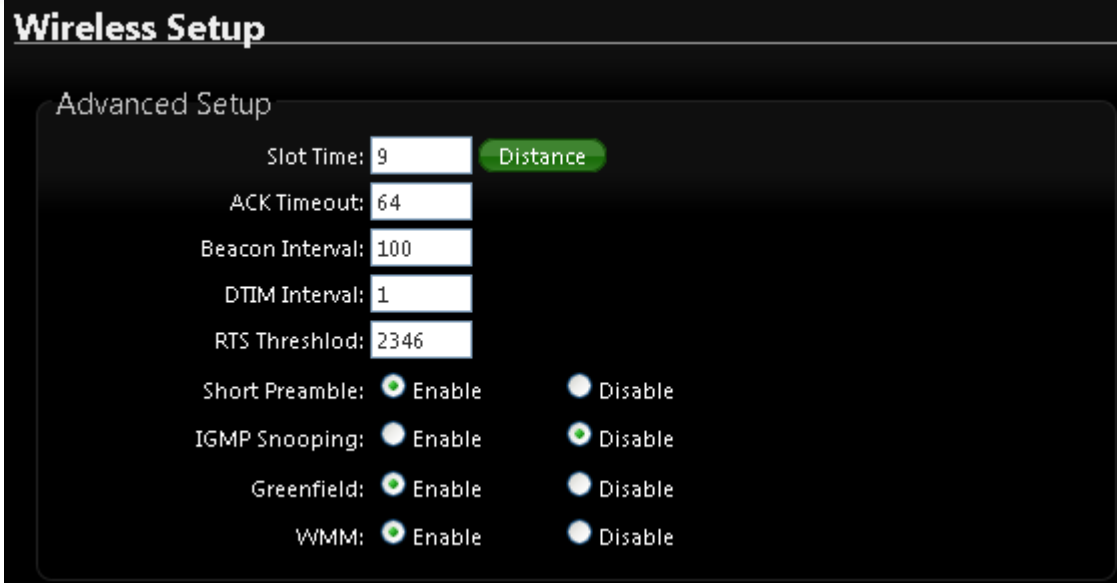


➤ HT Physical Mode

- **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.
- **Short GI** : Short Guard Interval, by default, it's "Enable". It 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 deactivate 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.



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.
- **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 CW-300N system will calculate for RSSI number and total of three LED's indicator, If LED's whole bright indicate signal is the strong.



The function only support Client Bridge and WISP modes

Signal LED Thresholds

LED Indicator	LED1	LED2	LED3
Thresholds, RSSI	20	30	40

✓ 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.

WMM QoS

WMM Parameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	6	3	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI(2)	3	4	1	3008	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO(3)	2	3	1	1504	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	10	3	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI(2)	3	4	2	3008	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO(3)	2	3	2	1504	<input type="checkbox"/>	<input type="checkbox"/>

✓ **AC Type :**

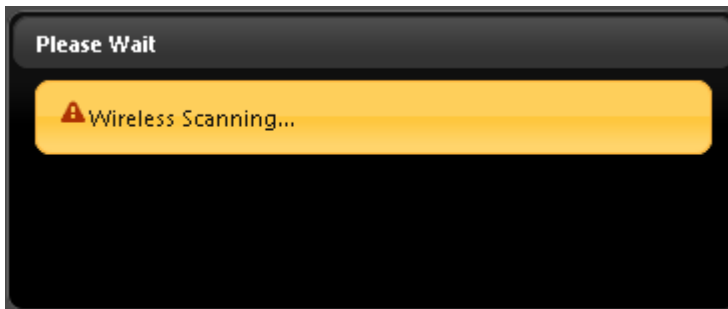
Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to 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 unicast packet. ◦

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.



AP Site Survey List							
ESSID	MAC Address	Signal/Noise, dBm	RSSI	Signal Quality, %	Channel	Security	Select
Danny	00:23:F8:07:1F:10	-40 / -95	55	100%	6	WPA-PSK/AES	Select
7904w	78:CD:8E:B4:00:89	-88 / -95	7	11%	6	WPA-PSK/AES	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.



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.

4.7 Station Profile

Station Profile

Connection Setup

Connection Setup: Fix Cycle

General Configuration

MAC Address: 00:11:A3:00:00:0C

Profile Name:

ESSID:

Lock to AP MAC: (optional)

Security Type:

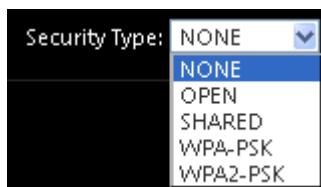
Profile List

Active	#	Profile Name	ESSID	MAC Address	Security Type	Actions
<input checked="" type="radio"/>	1	AP_Profile0	default		NONE	<input type="button" value="Delete"/> <input type="button" value="Edit"/>

➤ **Connection Setup** : You can choose to 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.

Security Type: OPEN
 Key Index: 1
 WEP Key 1:
 WEP Key 2:
 WEP Key 3:
 WEP Key 4:

- ✓ **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.

Security Type: WPA-PSK
 Cipher Suite: AES
 Pre-shared Key:

- ✓ **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.

Profile List

Active	#	Profile Name	ESSID	MAC Address	Security Type	Actions
<input checked="" type="checkbox"/>	1	AP_Profile0	default		NONE	Delete Edit

Connect

- Click **“Edit”** on an existing 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.



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



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

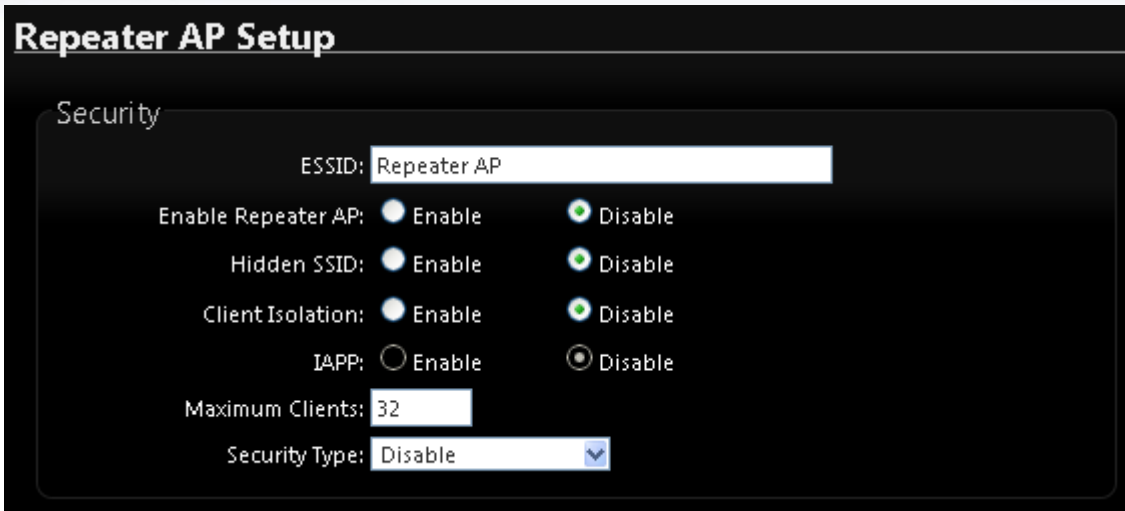
Shows the remote bridge AP whether it is linked or unlinked

Remote AP Status							Refresh
ESSID	MAC Address	Signal/Noise, dbm	RSSI	Signal Quality, %	TX/RX Rate	Status	
default		0 / 0	0	0%	0M /0M	Unlinked	

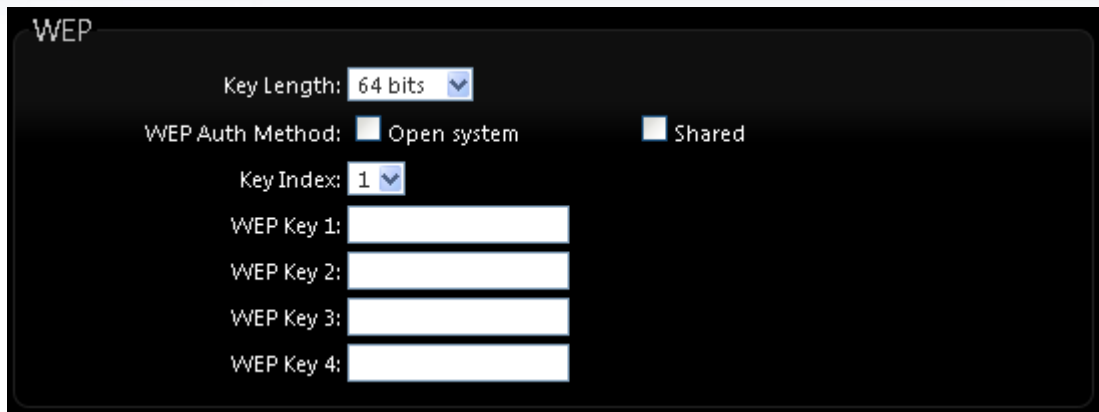
4.9 Repeater AP Setup

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.



The screenshot shows the WEP configuration interface with the following settings:

- Key Length: 64 bits (dropdown menu)
- WEP Auth Method: Open system, Shared
- Key Index: 1 (dropdown menu)
- WEP Key 1: [Empty text box]
- WEP Key 2: [Empty text box]
- WEP Key 3: [Empty text box]
- WEP Key 4: [Empty text box]

- ✓ **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.



The screenshot shows the WPA General configuration interface with the following settings:

- Cipher Suite: AES, TKIP
- Group Key Update Period: 600
- Master Key Update Period: 83400
- Key Type: ASCII, HEX
- Pre-shared Key: [Empty text box]

- ✓ **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.



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.

The screenshot displays the WPA General settings interface. It is divided into three main sections: WPA General, Authentication RADIUS Server, and Secondary Authentication RADIUS Server. In the WPA General section, the Cipher Suite is set to AES (selected with a radio button), and TKIP is unselected. Below this, there are three input fields: Group Key Update Period (600), Master Key Update Period (83400), and EAP Reauth Period (3600). The Authentication RADIUS Server section includes fields for Server IP, Port (1812), and Shared Secret, along with an Accounting RADIUS Server toggle set to Disable. The Secondary Authentication RADIUS Server section has fields for Server IP, Port (1812), and Shared Secret.

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.



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.

The screenshot shows a configuration interface with three sections:

- Dynamic WEP Settings**:
 - WEP Key Length: 64bits 128bits
 - WEP Key Update Period:
 - EAP Reauth Period:
- Authentication RADIUS Server**:
 - Server IP:
 - Port:
 - Shared Secret:
 - Accounting RADIUS Server: Enable Disable
- Secondary Authentication RADIUS Server**:
 - Server IP:
 - Port:
 - Shared Secret:

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.

Repeater AP MAC Filter Setup

MAC Rules

Action:

MAC Address:

MAC Filter List

#	MAC Address	Actions	#	MAC Address	Actions
No items in the list!					

- **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**”.



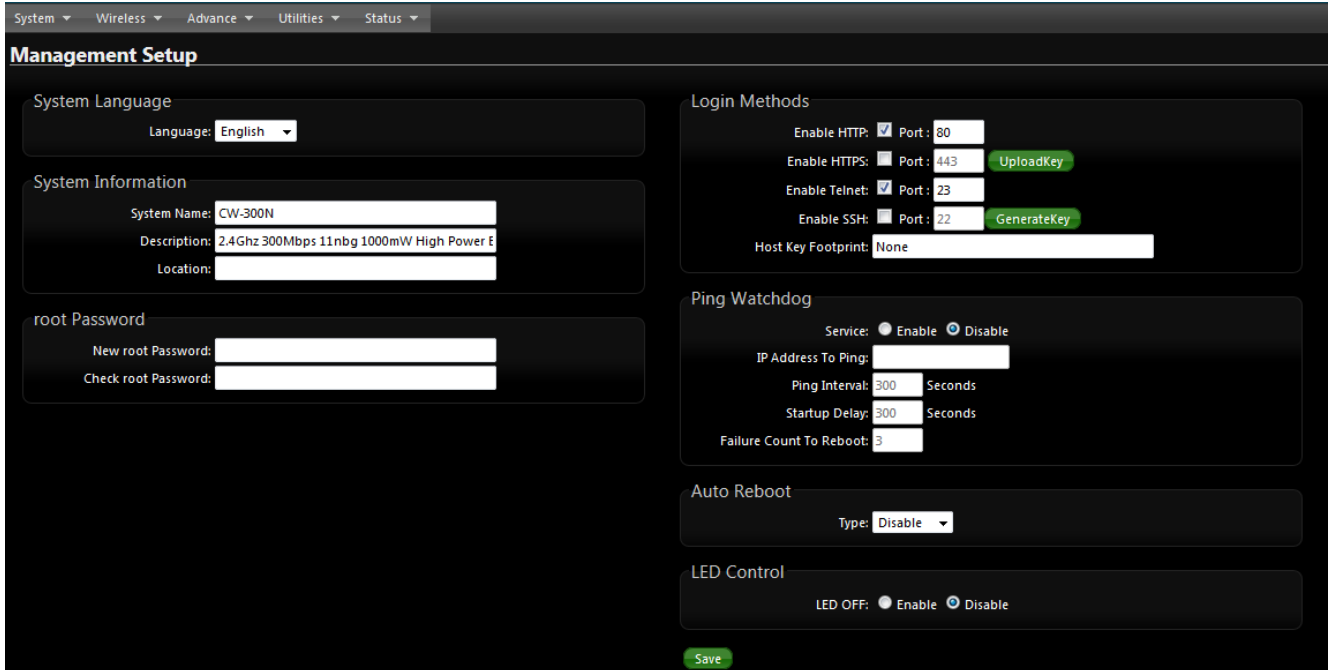
Notice: MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

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.

5. System Management

5.1 Configure Management

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



The screenshot shows the 'Management Setup' page with the following sections:

- System Language:** Language: English
- System Information:** System Name: CW-300N, Description: 2.4Ghz 300Mbps 11nbg 1000mW High Power E, Location: [empty]
- root Password:** New root Password: [empty], Check root Password: [empty]
- Login Methods:**
 - Enable HTTP: Port: 80
 - Enable HTTPS: Port: 443 [UploadKey]
 - Enable Telnet: Port: 23
 - Enable SSH: Port: 22 [GenerateKey]
 - Host Key Footprint: None
- Ping Watchdog:**
 - Service: Enable Disable
 - IP Address To Ping: [empty]
 - Ping Interval: 300 Seconds
 - Startup Delay: 300 Seconds
 - Failure Count To Reboot: 3
- Auto Reboot:** Type: Disable
- LED Control:** LED OFF: Enable Disable

A green 'Save' button is located at the bottom center of the form.

➤ System Information

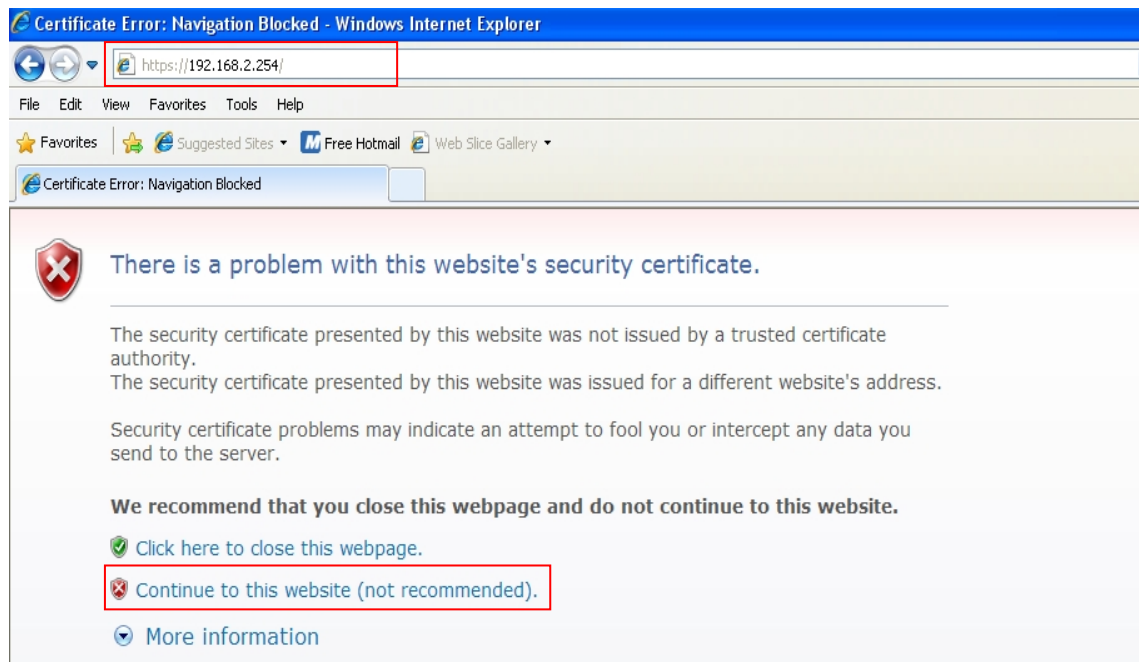
- **System Name** : Enter a desired name or use the default one.
- **Description** : Provide description of the system.
- **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports two management accounts, root and admin. The network manager is assigned with full administrative privileges when logging in as a root user to manage the system in all aspects. While logging in as an admin user, only subset of privileges are granted such as basic maintenance. For example, root users 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** : Users logging in as a root user are allowed to change their own password, as well as the 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** : Users logging in as an admin user are allowed to only change their own password.
 - ✓ **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, The default is 443 and the range is between 1 ~ 65535.

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.



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

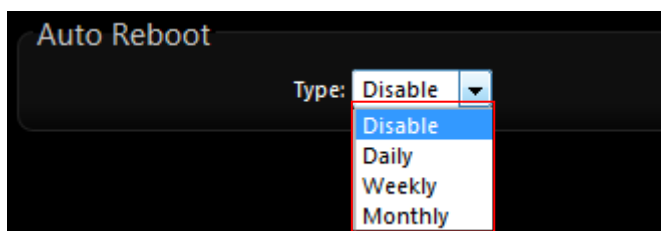
- ✓ **Enable Telnet** : Check to select Telnet Service
- ✓ **Telnet Port** : The default is 23 and the range is between 1 ~ 65535.
- ✓ **Enable SSH** : Check to select SSH Service
- ✓ **SSH Port** : Please The default is 22 and the range is between 1 ~ 65535.

 **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 **CW-300N** 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 **CW-300N** device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated to 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.
 - ✓ **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.
- **Auto Reboot:**
The functions can Auto-reboot the system by Date/time management



- ✓ **Daily** : Setting time to system reboot

Auto Reboot

Type: **Daily** ▼

Time: 0 ▼ : 0 ▼

- ✓ **Weekly** : Setting frequency (ex. Weekly) and time of system reboot

Auto Reboot

Type: **Weekly** ▼ **Sunday** ▼

Time: 0 ▼ : 0 ▼

- ✓ **Monthly** : Setting Every month, fixed date and time to system reboot

Auto Reboot

Type: **Monthly** ▼ **1** ▼

Time: 0 ▼ : 0 ▼

- **LED Control**: Administrator can turn the LED on/off by CW-300N

LED Control

LED OFF: Enable Disable

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

5.2 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.

Time Server Setup

System Time
Local Time: 1970/01/01 00:37:43

Setup Time Use NTP

Default NTP Server: time.stdtime.gov.tw (optional)
NTP Server: time.stdtime.gov.tw
Time Zone: [GMT] Dublin, Edinburgh, Lisbon, London
Daylight Saving Time: Disable

User Setup

Date: 2012 Dec 23
Time: 22:30:09 (GMT+8:00)
Set Time: **Set Time**

- **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.



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

5.3 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 Setup

SNMP v2c

Enable:

SNMP v3

Enable:

SNMP Trap

Enable:

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

SNMP v2c

Enable:

ro community:

rw community:

- **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 v3

Enable:

SNMP ro user:

SNMP ro password:

SNMP rw user:

SNMP rw password:

- **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.

6. Configure Advance Setup

6.1 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.

Time Policy Setup

Policy 1

Policy: Policy 1

Schedule Rule: On Schedule Out of Schedule

Save Action

Time Schedule

Day of Week: Sun Mon Tue Wed Thu Fri Sat

Start From: 00 : 00

End To: 23 : 59

Save Clear

Time Schedule List

#	Week	Time	Actions
1	Sun Mon Tue Wed Thu Fri Sat	09:00 - 12:00	Delete Edit
2	Sun Mon Tue Wed Thu Fri Sat	13:30 - 17:00	Delete Edit
3	Sun Mon Tue Wed Thu Fri Sat	00:00 - 23:59	Delete Edit

- **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**”

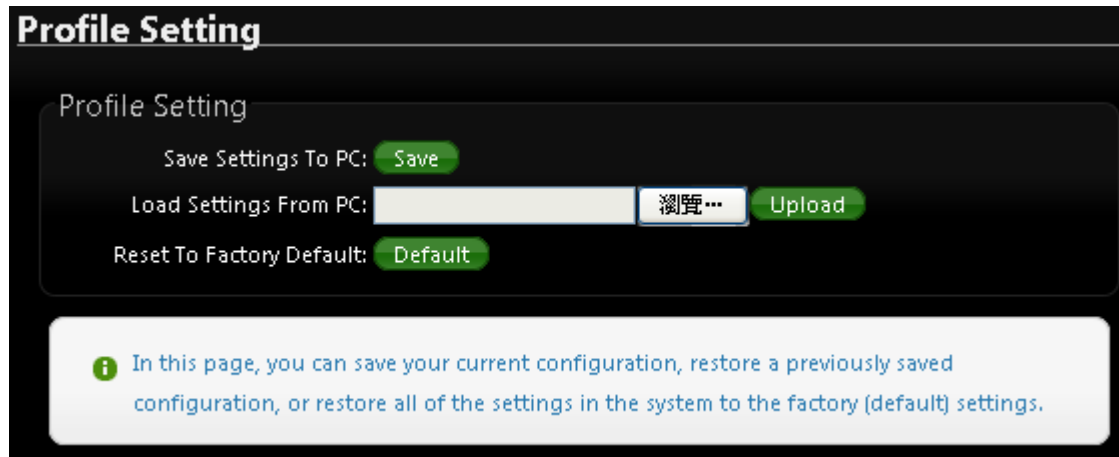
Click “Save” button to add schedule to policy. There are 10 schedule maximum allowed in the each time policy. All schedule can be edited or removed in the each time policy. Click **Reboot** button to activate your changes.

7. Configure Utilities Setup

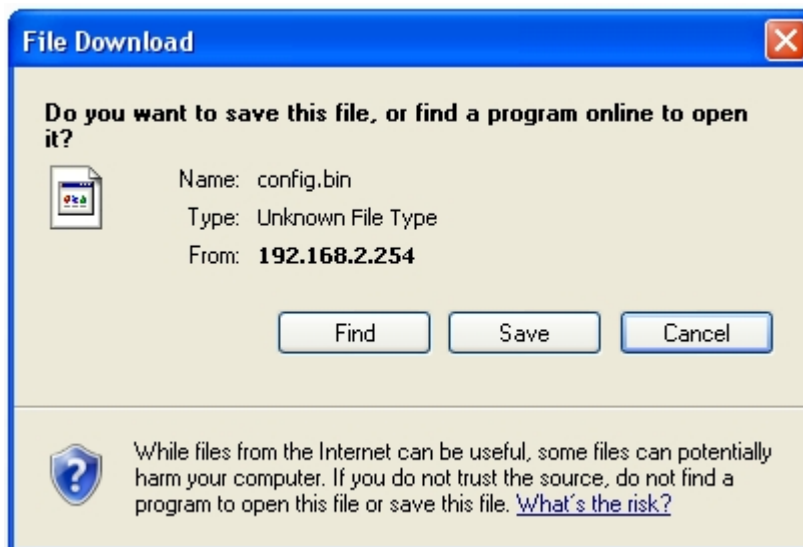
7.1 Profile setting

This function includes actions such as: 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.

7.2 Firmware Upgrade

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

Firmware Upgrade

Firmware Information

Firmware Version: Cen-OS V3.0.1 BETA02
Firmware Date: 2015/02/04 16:38:30

Upgrade Via Local PC

Select File: 未選擇檔案

Upgrade Via TFTP Server

TFTP Server IP:
File Name:

Upgrade Via HTTP URL

URL:



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

Below currently shows the **CW-300N** of system software version and software date

Firmware Information

Firmware Version: Cen-OS V3.0.1 BETA02
Firmware Date: 2015/02/04 16:38:30

From time to time, the product may release new versions of the system's firmware. You can download up-to-date firmware to upgrade system.

➤ Upgrade firmware

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

The screenshot shows a dark-themed interface with three upgrade options:

- Upgrade Via Local PC:** Includes a 'Select File:' label, a text input field, a '瀏覽...' (Browse) button, and a green 'Upgrade' button.
- Upgrade Via TFTP Server:** Includes 'TFTP Server IP:' and 'File Name:' labels, two text input fields, and a green 'Upgrade' button.
- Upgrade Via HTTP URL:** Includes a 'URL:' label, a text input field, and a green 'Upgrade' button.

7.3 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.

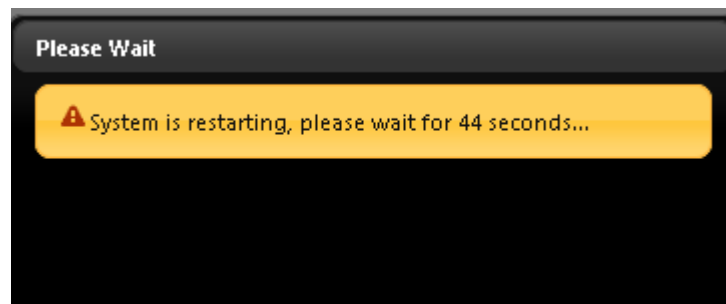
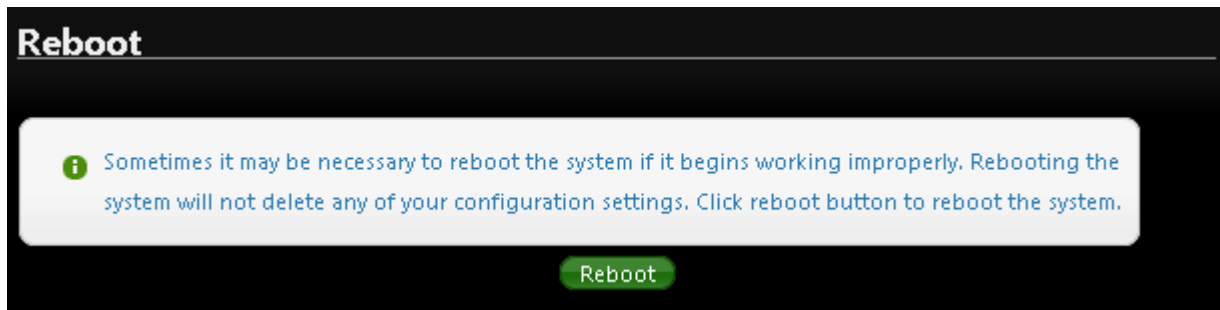
The screenshot shows the 'Network Utility' section with two sub-sections:

- Ping:** Features an 'IP/Domain:' label, a text input field, a 'Times' label with a value of '5', and a green 'Start' button.
- Traceroute:** Features a 'Destination Host:' label, a text input field, a 'Max. Hops' label with a value of '6', and green 'Start' and 'Stop' buttons.

- **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 CW-300N 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.

7.4 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.

8. Configure Status

8.1 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.

8.2 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. CW-300N 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.

Extra Information

Information:

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.

Extra Information

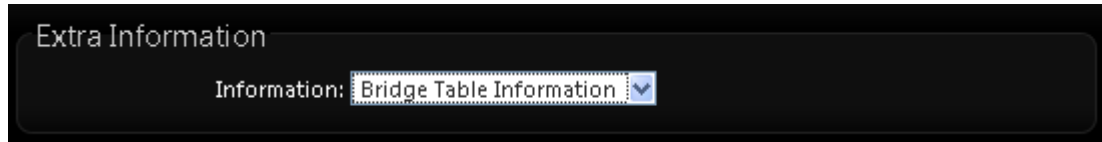
Information:

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).

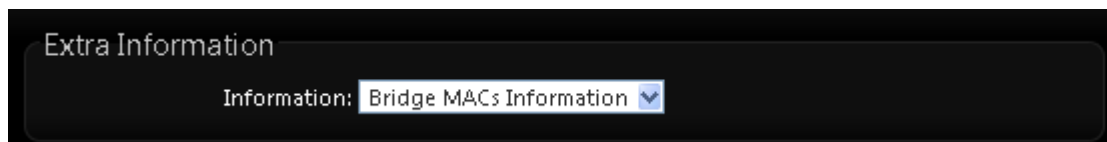


Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
LAN	8000.0011a300000a	no	eth1
			eth0

- **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.

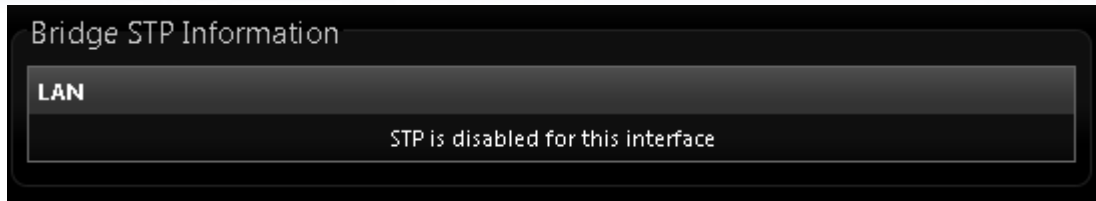


Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:11:a3:00:00:0a	yes	0.00
WAN	00:11:a3:00:00:0b	yes	0.00
LAN	8c:4d:ea:02:c6:ec	no	0.04

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





8.3 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.

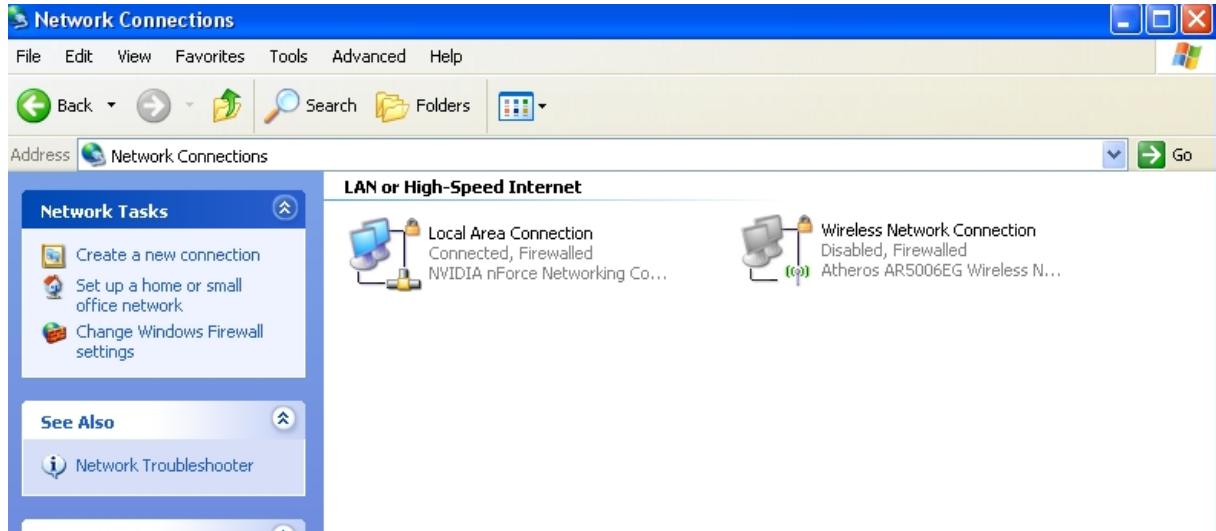
System Log				Refresh	Clear
Time	Facility	Severity	Message		
1970-01-01 00:00:19	System	Info	dnsmasq: started, version 2.22 cachesize 150		
1970-01-01 00:00:19	System	Info	dnsmasq: cleared cache		
1970-01-01 00:00:19	System	Info	dnsmasq: reading /etc/resolv.conf		
1970-01-01 00:00:52	System	Info	Authentication successful for root from 192.168.2.22		

- **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.

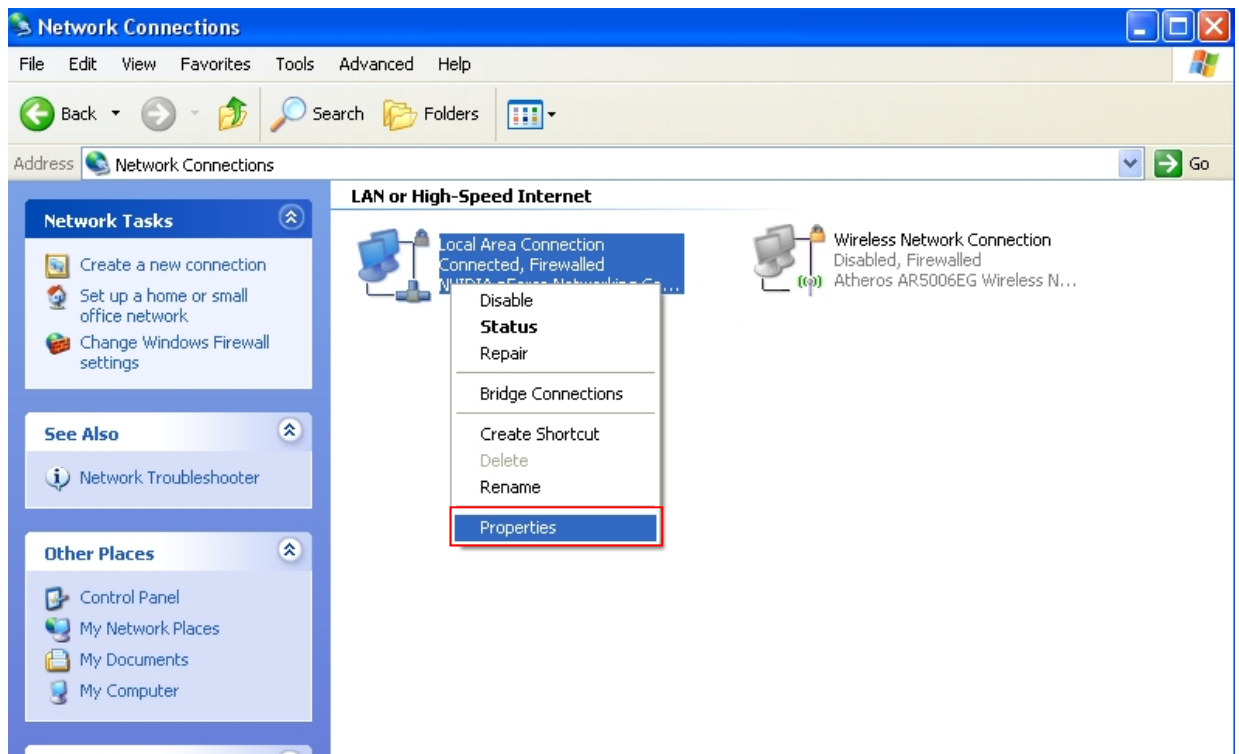
Appendix A. Windows TCP/IP Settings

➤ Windows XP

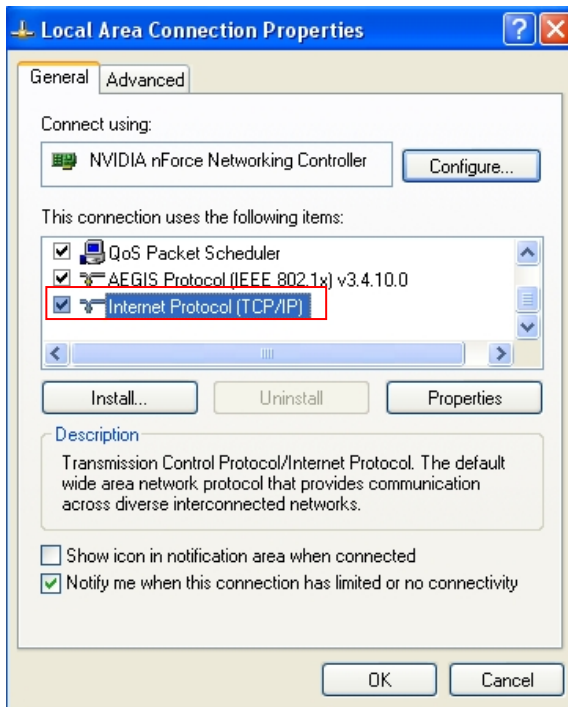
- i. Click **Start -> Settings -> Control Panel**, and then “Control Panel” window appears. Click on “**Network Connections**”, and then “Network Connections” window appears.



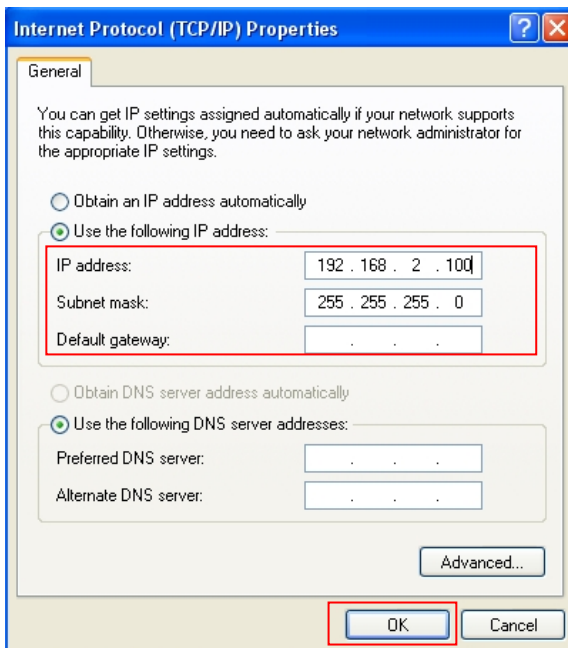
- ii. Click right on “**Local Area Connection**”, and select **Properties**.



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



- iv. Select “**Use the following IP address**”, and type in
IP address : 192.168.2.100
Subnet mask : 255.255.255.0



Click “**OK**” completion set up IP address

Appendix B. WEB GUI Valid Characters

Table B WEB GUI Valid Characters

Block	Field	Valid Characters
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Primary DNS	IP Format; 1-254
	Secondary DNS	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Management	System Name/ Location	Length : 32 0-9, A-Z, a-z Space ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =
	Description	32 chars
	Password	Length : 4 ~ 30 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =
	HTTP/ HTTPS Port	1 ~ 65535
	Telnet/ SSH Port	1 ~ 65535
SNMP	RO/RW community	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =
	RO/RW user	Length : 31 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =
	RO/RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =
	Community	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =
General Setup Wireless Profile	IP	IP Format; 1-254
	Tx Power	1-100 %
	Profile Name	32 chars
	ESSID	Length : 31 Space 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ : <> ? [] / ; ` , . =

Block	Field	Valid Characters
Advanced Setup	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Pre-shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Beacon Interval	20 ~ 1024
	Date Beacon Rate	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
WDS Setup	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	TKIP Key	8 ~ 63 ASCII chars; 64 HEX chars
	AES Key	8 ~ 63 ASCII chars; 64 HEX chars
	Peer's MAC Address	12 HEX chars
	Description	32 chars

Appendix C. 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

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 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: +886-2-8911-6160 #222

Web Site: www.cerio.com.tw
