Digital Wireless Bridge

User Guide

Revision 1.0.5

Revision History

Version	Date	Notes
1.0.5	Nov. 05, 2012	Initial Version

Introduction

ST58T8 SERIES outdoor high power WiFi-11a/n Bridge is the point of connection to Wireless Outdoor Network for service provider deploying last mile services to business or residential broadband subscribers. Network administrators can create multiple subscriber service tier using per-subscriber rate limiting features, and manage centrally. ST58T8 SERIES outdoor AP/CPE connects to the WiFi or WDS infrastructure and provides the subscriber with an Ethernet connection for a local access.

ST58T8 SERIES outdoor high power Bridge can be used for different purpose in three different modes. In the AP mode, it can be deployed either as traditional fixed wireless Access Point, or combination of AP and WDS(AP+WDS). In the WDS mode, it's only used to expand or bridge Ethernet networks and deployed as a main base, relay based or remote base station. In the Client Bridge + Repeater AP mode, it connects to Wireless Internet Service Provider's(WISP) outdoor network via wireless or wired bridge to access to Internet.

1 Access Point : It can be deployed as a traditional fixed wireless Access Point

2 WDS : It can be used to expand Ethernet network via wireless WDS Link Internet Service Provider's (WISP)

3 Client Bridge + Universal Repeater : It is a wireless repeater or bridge to connects to Wireless Internet Service Provider's (WISP)

Features & Benefits

Features	Benefits
High Speed Data Rate Up to 300Mbps	**Capable of handling heavy data payloads such as MPEG video streaming**
High Output Power and ACK timeout for Distance Control	**Extended excellent Range and Coverage (fewer APs)**
IEEE 802.11a Compliant	**Fully Interoperable with IEEE 802.11a compliant devices**
Multifunction application	**Access Point/WDS Bridge/Client Bridge + Repeater mode**
WDS (Wireless Distributed System)	**Make wireless AP and Bridge mode simultaneously as a wireless repeater up to 8 links**
WPA2/WPA/ IEEE 802.1x support	**Powerful data security**
MAC address filtering in AP mode(up to 50)	**Ensures secure network connection**

Client isolation through Layer 2 VLAN Technology	**Protect the private network between client users.**
Keep personal setting	**Keep the latest setting when firmware upgrade**
SNMP Remote Configuration Management	**Help administrators to remotely configure or manage the Access Point easily.**
QoS (WMM) support	**Enhance user performance and density**

System Requirements

The following are the minimum system requirements in order configure the device.

- PC/AT compatible computer with an Ethernet interface.
- Operating system that supports HTTP web-browser

Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) **The ability to access real-time information**
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) **Frequently changed environments**
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) **Small Office and Home Office (SOHO) networks**
SOHO users need a cost-effective, easy and quick installation of a small network.

f) **Wireless extensions to Ethernet networks**
Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) **Wired LAN backup**
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) **Training/Educational facilities**
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

FCC Notice

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed

and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacture is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user’s authority to operate the equipment.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only mobile configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

The Wireless Technology

Standard

The Wireless Access Point utilizes the 802.11a and the 802.11n standards. The IEEE 802.11n standard is an extension of the 802.11a standard. It increases the data rate up to 300 Mbps within the 5GHz band, utilizing OFDM technology. This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format you're your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing OFDM (Orthogonal Frequency Division Multiplexing) technology. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of cross talk (interference) in signal transmissions. The AP will automatically sense the best possible connection speed to ensure the greatest speed and range possible. 802.11a/n offers the most advanced network security features available today, including: WPA, WPA2, TKIP, AES and Pre-Shared Key mode.

Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with one another to form an ad-hoc network. The wireless adapters also provide users access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router. An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, providing that they both share the same channel and SSID. Before enabling you consider roaming, choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

Network Layout

The AP Access Point has been designed for use with 802.11a and 802.11n products. With 802.11n products communicating with the 802.11a standard, products using these standards can communicate with each other. The Access point is compatible with 802.11a and 802.11n adapters, such at the PC Cards for your laptop computers, PCI Card for your desktop PC, and USB Adapters for when you want to enjoy USB connectivity. These wireless products can also communicate with an 802.11a or 802.11n wireless Print Server. When you wish to connect your wired network with your wireless network, the Access Point's network port can be used to connect to any of switches or routers.

Installation Considerations

The AP lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
- Keep the number of walls and ceilings between the AP and other network devices to a minimum - each wall or ceiling can reduce your AP's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall that is 1.5 feet thick(.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or

ceiling (instead of at an angle) for better reception.

- Building materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

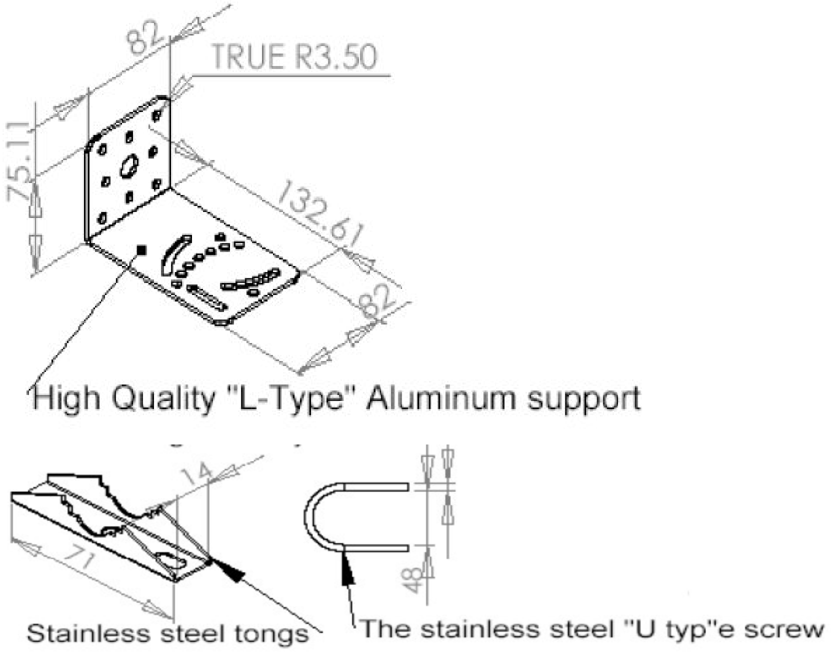
Applications

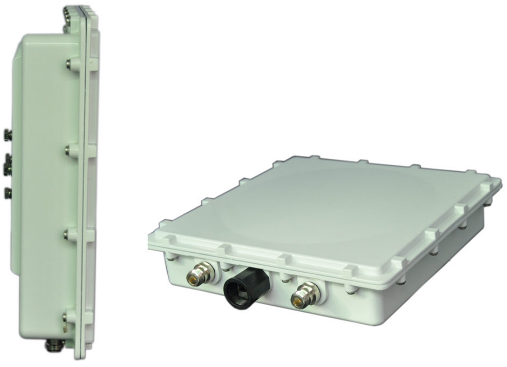
The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- **Difficult-to-wire environments**
  There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
- **Temporary workgroups**
  Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
- **The ability to access real-time information**
  Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
- **Frequently changed environments**
  Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
- **Small Office and Home Office (SOHO) networks**
  SOHO users need a cost-effective, easy and quick installation of a small network.
- **Wireless extensions to Ethernet networks**
  Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- **Wired LAN backup**
  Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

Installation Diagram

ST58T8G


82
TRUE R3.50
75.11
132.61
82
High Quality "L-Type" Aluminum support
14
71
Stainless steel tongs
48
The stainless steel "U typ"e screw



ST58T8G-N

ST58T8G

Attention:

- The cable distance between the Router and PC/hub/Switch should not exceed 100 meters.
- Make sure the wiring is correct. In 10Mbps operation, Category 3/4/5 cable can be used for connection. To reliably operate your network at 100Mbps, you must use Category 5 cable, or better Data Grade.

Configuration Using Device Discovery

While entering the Device Discovery utility, the Device Discovery will automatically search the AP available on the same network. Device Discovery will show the IP Address, Ethernet MAC Address, Host Name, Firmware Version, Firmware Date and Mode in first page. Before start using Device Discovery, make sure you disable personal firewall installed in you PC. (Ex. Windows XP personal firewall)

AP Configuration Using Web User Interface

Before Setup…

❖ Verify the IP address setting

You need to configure your PC's network settings to obtain an IP address. Computer use IP addresses to communicate with each other across a network, such as the Internet.

1. From the taskbar, click the **Start** button, select **Settings** > **Control Panel**. From there, double-click **the Network connections** icon.
2. Right click the **Local Area Connection** icon **Properties**; select the **TCP/IP** line for the applicable Ethernet adapter. Then, click the **Properties** button.
3. Click the **IP Address** tab page, select **USE the following IP address**, type **192.168.254.254** (but, **192.168.x.x** for the device use) in the **IP Address** field and **255.255.0.0** in the **Subnet Mask** field, then click **OK** button.

Start Setup by Browser...

1. After getting the correct connection, start the web browser (make sure you disable the proxy) and type 192.168.x.x (x is outdoor unit IP Address) in the **Address** field. Press **Enter**.

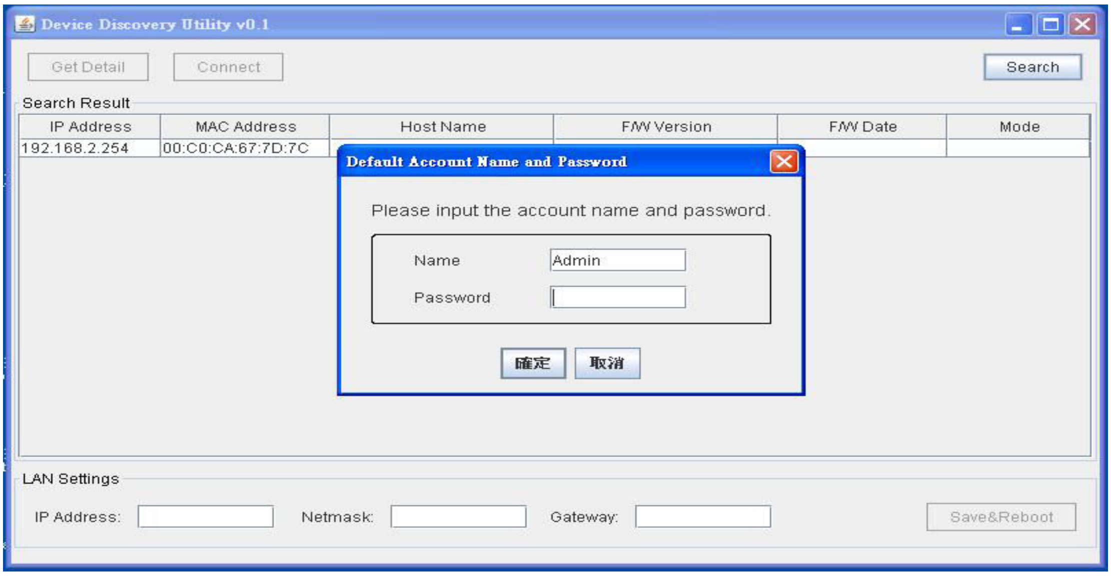
http://192.168.2.254/index.html

2. Enter the factory default ***User name*** and ***Password*** fields:
   User Name: **Admin**
   Password: **(blank)**
   then click **OK** button.

   You will enter the Utility homepage.

Start Setup by Device Discovery...

1. You just need to click on the “**Web**” icon in Device Discovery main page. The Device Discovery will launch a default browser for you and lead you into web UI directly



IP Address	MAC Address	Host Name	F/W Version	F/W Date	Mode
192.168.2.254	00:C0:CA:67:7D:7C				

Please input the account name and password.

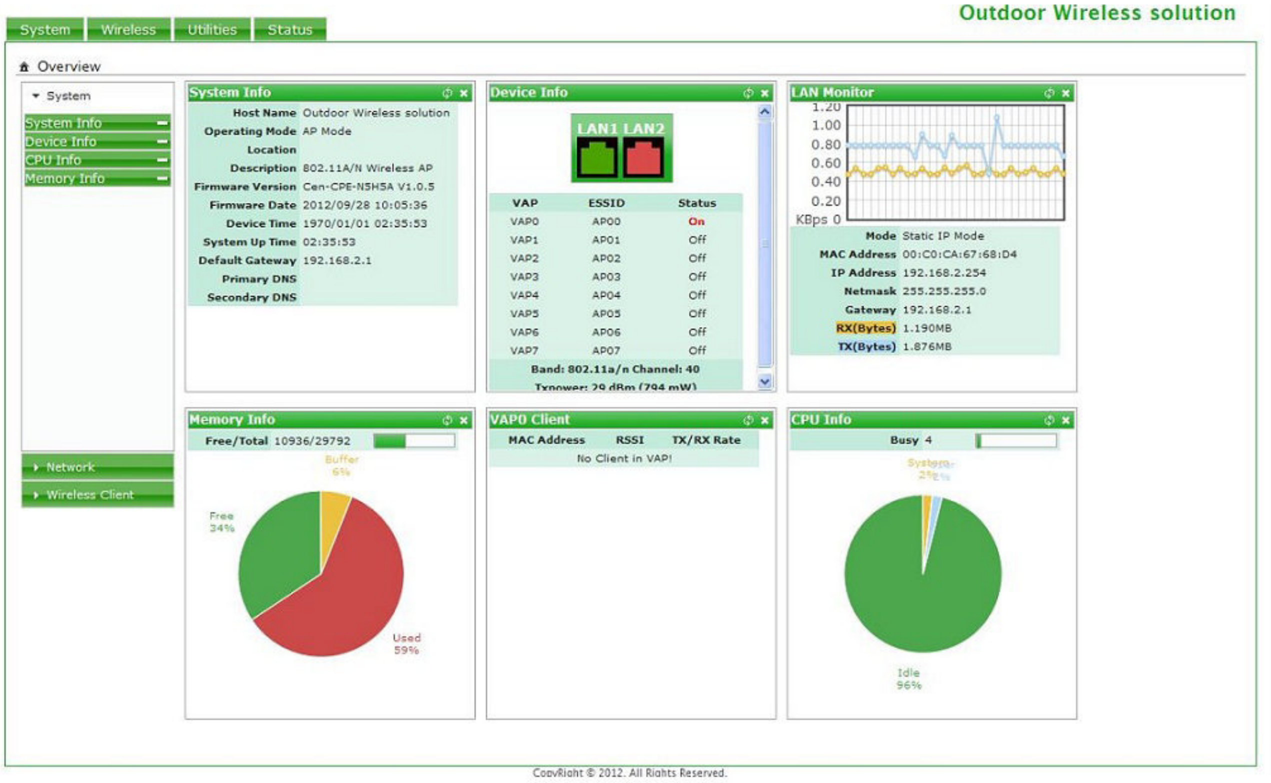
Name: Admin

Password:

System Status –

The first page appears in main page will show “**Overview**” automatically, you can find detail system configuration in this page including

- **System –** This will display System Info, Device Info, CPU info and Memory Info.
- **Network –** LAN Monitor and VAP0~VAP7 Monitor.
- **Wireless Client –** This will show VAP0~VAP7 Client and WDS status.



System Info

Host Name	Outdoor Wireless solution
Operating Mode	AP Mode
Location	
Description	802.11A/N Wireless AP
Firmware Version	Cen-CPE-N5H5A V1.0.5
Firmware Date	2012/09/28 10:05:36
Device Time	1970/01/01 02:35:53
System Up Time	02:35:53
Default Gateway	192.168.2.1
Primary DNS	
Secondary DNS	

Device Info

VAP	ESSID	Status
VAP0	AP00	On
VAP1	AP01	Off
VAP2	AP02	Off
VAP3	AP03	Off
VAP4	AP04	Off
VAP5	AP05	Off
VAP6	AP06	Off
VAP7	AP07	Off

Band: 802.11a/n Channel: 40

Txpower: 29 dBm (794 mW)

LAN Monitor

Mode	Static IP Mode
MAC Address	00:C0:CA:67:68:D4
IP Address	192.168.2.254
Netmask	255.255.255.0
Gateway	192.168.2.1
RX(Bytes)	1.190MB
TX(Bytes)	1.876MB

Memory Info

Free/Total 10936/29792

VAP0 Client

MAC Address	RSSI	TX/RX Rate
No Client in VAP!		

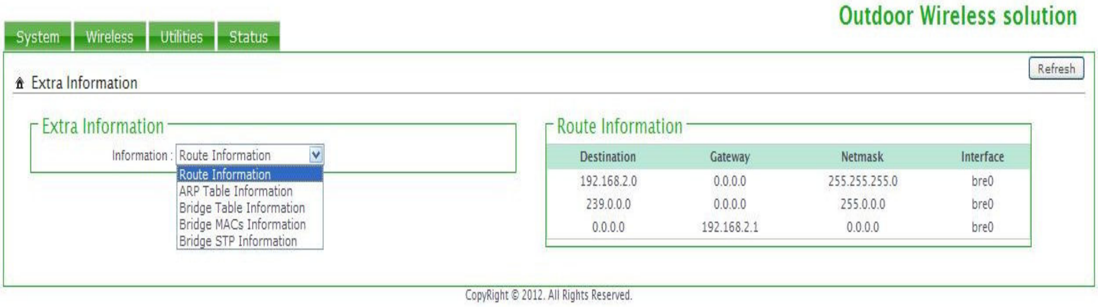
CPU Info

Busy 4

CopyRight © 2012. All Rights Reserved.

Extra Info –

This show Extra Information includes Route, ARP Table, Bridge Table, Bridge MACs and Bridge STP information.

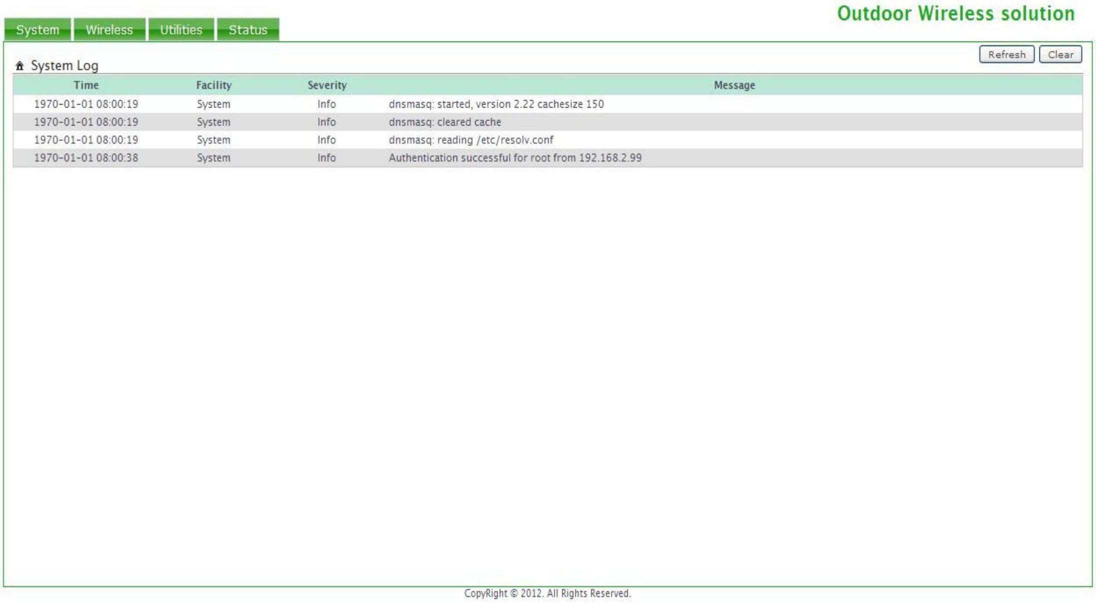


Route Information

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
0.0.0.0	192.168.2.1	0.0.0.0	bre0

Event (System) Log –

This show system log includes Time, Facility, Severity and Message.

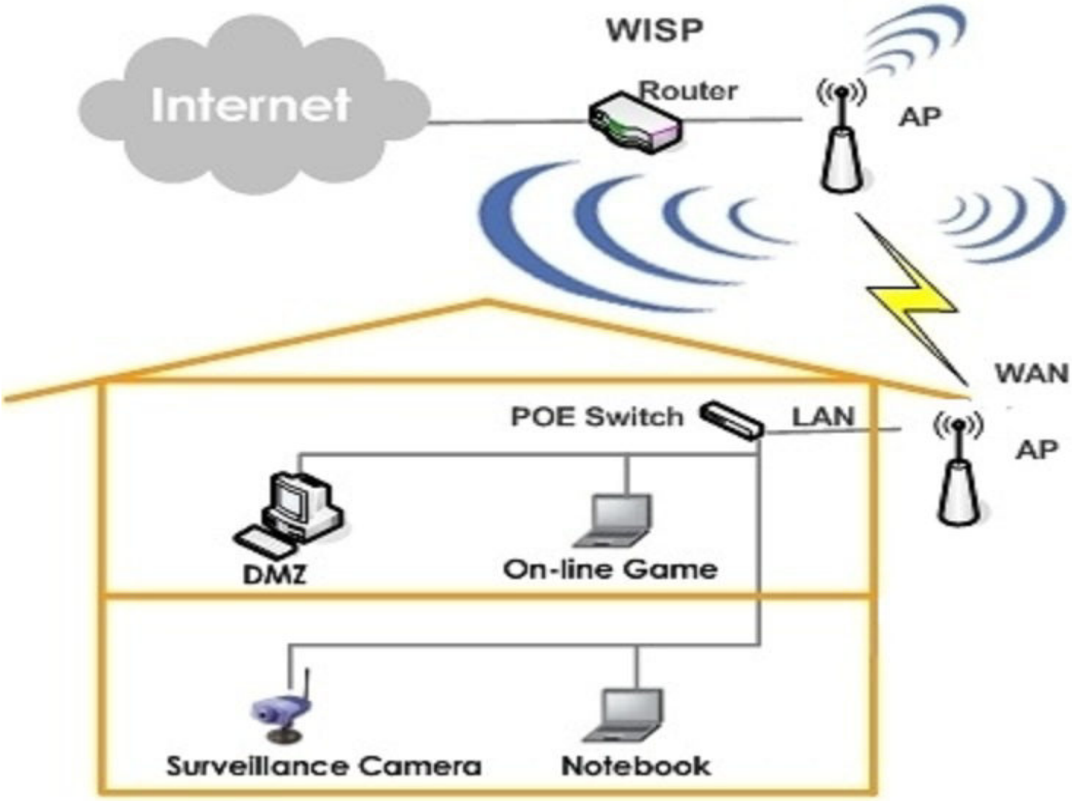

Outdoor Wireless solution
System
Wireless
Utilities
Status
Refresh
Clear
System Log
CopyRight © 2012. All Rights Reserved.

Time	Facility	Severity	Message
1970-01-01 08:00:19	System	Info	dnsmasq: started, version 2.22 cachesize 150
1970-01-01 08:00:19	System	Info	dnsmasq: cleared cache
1970-01-01 08:00:19	System	Info	dnsmasq: reading /etc/resolv.conf
1970-01-01 08:00:38	System	Info	Authentication successful for root from 192.168.2.99

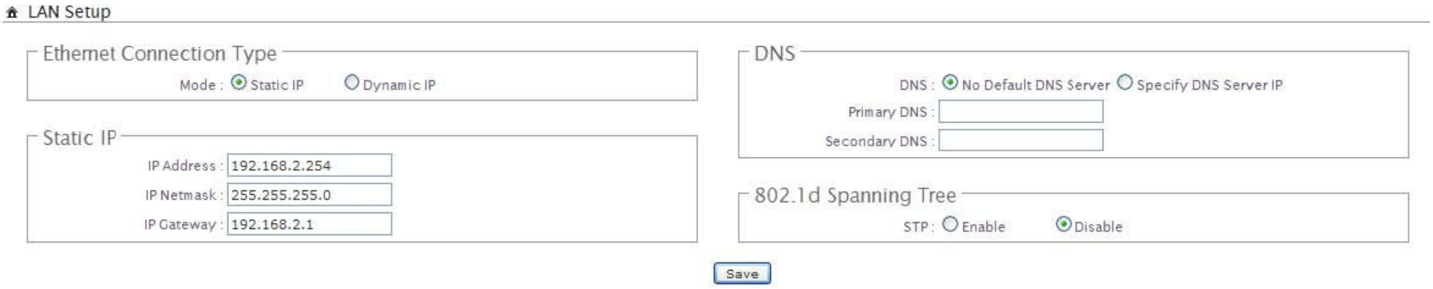
Option	**System**	**Wireless**	**Utilities**	**Status**
Functions	Operating Mode	General Setup	Profiles Settings	Overview
	Setup Wizard	Advance Setup	Firmware Upgrade	Extra Info
	LAN Setup	Virtual AP Setup	Network Utility	Event Info
	VLAN Setup	WDS Status	Reboot	
	Management	Associated Clients		
	Time Server			
	SNMP			

System Configuration –

Now you can start to configure the system. In **System** page, you can config



- **Operating Mode –**The default operation mode is Access Point, this connects your wireless PCs and devices to a wired network. In most cases, no change is necessary. You can switch operation mode to ClientBridge+RepeaterAP depends on your application. ClientBridge+RepeaterAP is able to talk with one remote access point within its range and retransmit its signal. Choose ClientBridge+RepeaterAP mode if you want to extend the range of your original AP. Wireless Bridge (WDS) can allow Bridge point to point or point to multi-point network architecture, In order to establish the wireless link between bridge radios, the MAC address of remotes bridge(s) need to be registered in the address table. Type the MAC address with format xx:xx:xx:xx:xx:xx (x is the hexadecimal digit) and use "Add" and "Delete" button to edit the address table. A Master Bridge Radio may accommodate up to **8** remote MAC addresses.
- **Setup Wizard** –



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 : 192.168.2.1

DNS

DNS : ● No Default DNS Server ○ Specify DNS Server IP

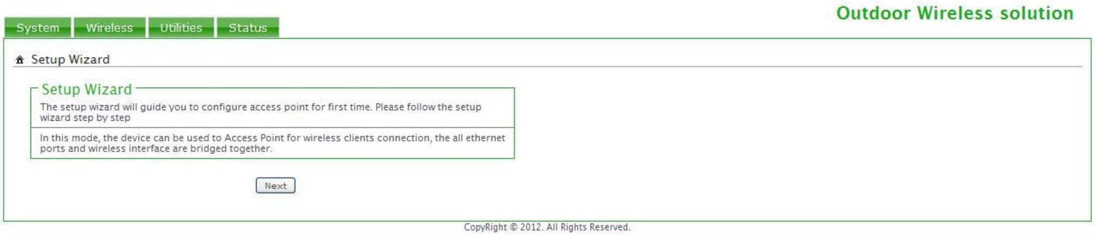
Primary DNS :

Secondary DNS :

802.1d Spanning Tree

STP : ○ Enable ● Disable

Save



System Wireless Utilities Status

Outdoor Wireless solution

Setup Wizard

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step

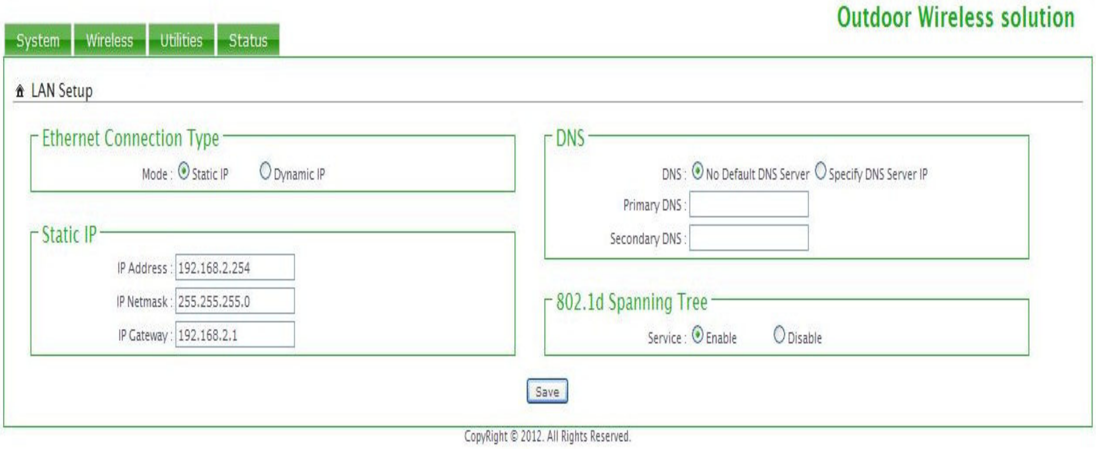
In this mode, the device can be used to Access Point for wireless clients connection, the all ethernet ports and wireless interface are bridged together.

Next

CopyRight © 2012. All Rights Reserved.

- **LAN Setup** -

IP Setting page can configure system IP address. Default IP address is 192.168.2.254 and Subnet Mask is 255.255.255.0. You can manually input IP address setting or get an IP from a DHCP server.



System Wireless Utilities Status

Outdoor Wireless solution

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 : 192.168.2.1

DNS

DNS : ● No Default DNS Server ○ Specify DNS Server IP

Primary DNS :

Secondary DNS :

802.1d Spanning Tree

Service : ● Enable ○ Disable

Save

CopyRight © 2012. All Rights Reserved.

➢ **Ethernet Connection Type –** Here are the instructions to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting. **Mode**: Check either “Static IP” or “Dynamic IP” button

➢ **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

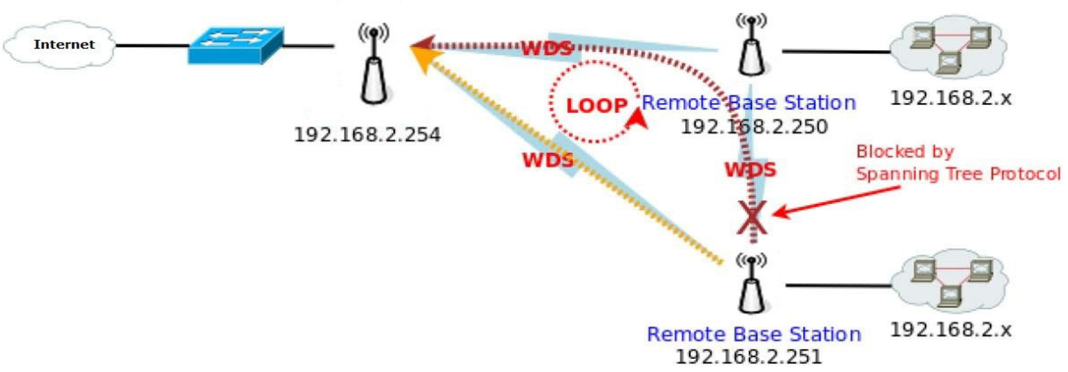
255.255.255.0

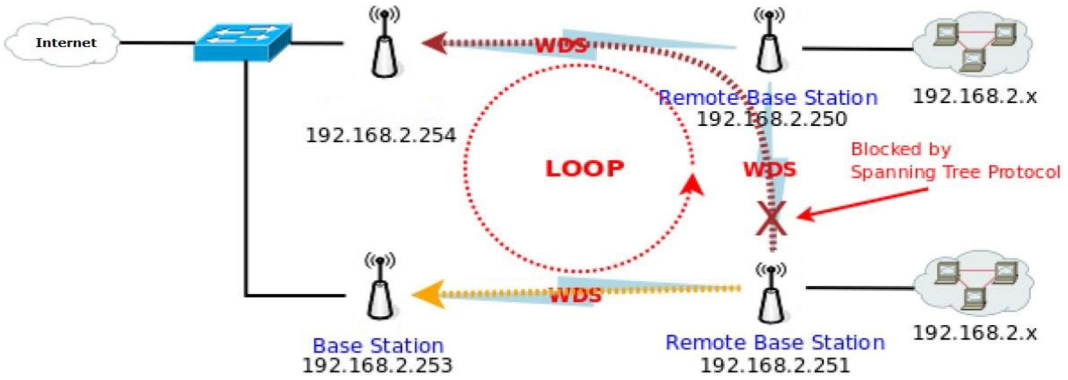
IP Gateway : The default gateway of the LAN port; default Gateway is 192.168.2.1

Dynamic IP : This configuration type is applicable when the ST58T8 SERIES is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

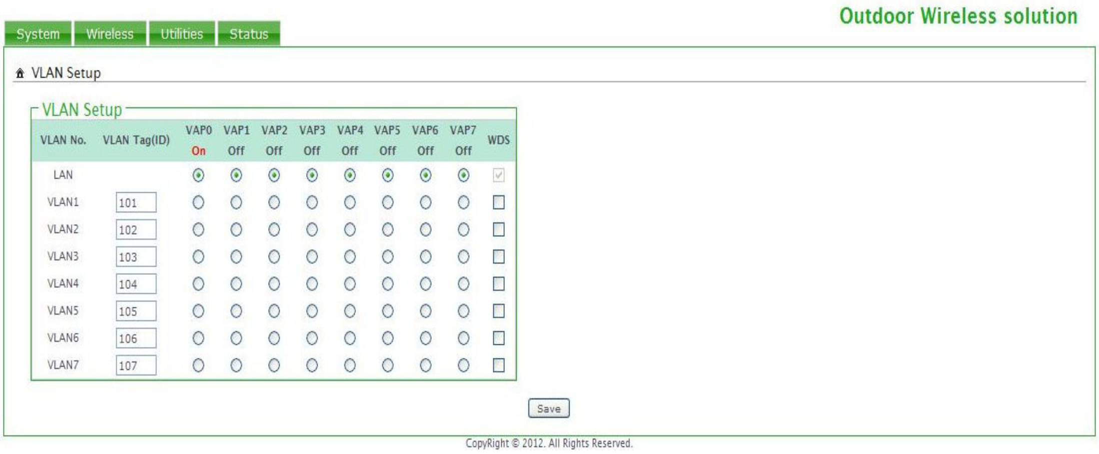
- **DNS –** Default is “No Default DNS Server”, or “Specify DNS Server IP” button as desired set up the system DNS.
  Primary DNS: The IP address of the primary server.
  Secondary DNS: The IP address of the secondary server.

- **802.1d Spanning Tree –**The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 4 WDS interfaces. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. The Spanning tree always enabled on ST58T8 SERIES. Below Figures depict a loop for a bridged LAN between LAN and WDS link Change these settings as described here and click “***Save***” button to save your changes. Click “***Reboot***” button to activate your changes.





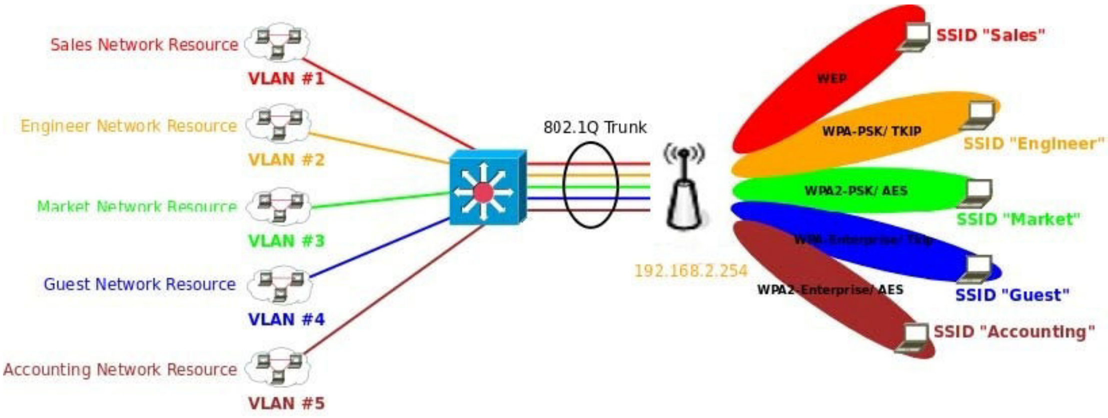
- **VLAN Setup -**



VLAN Setup

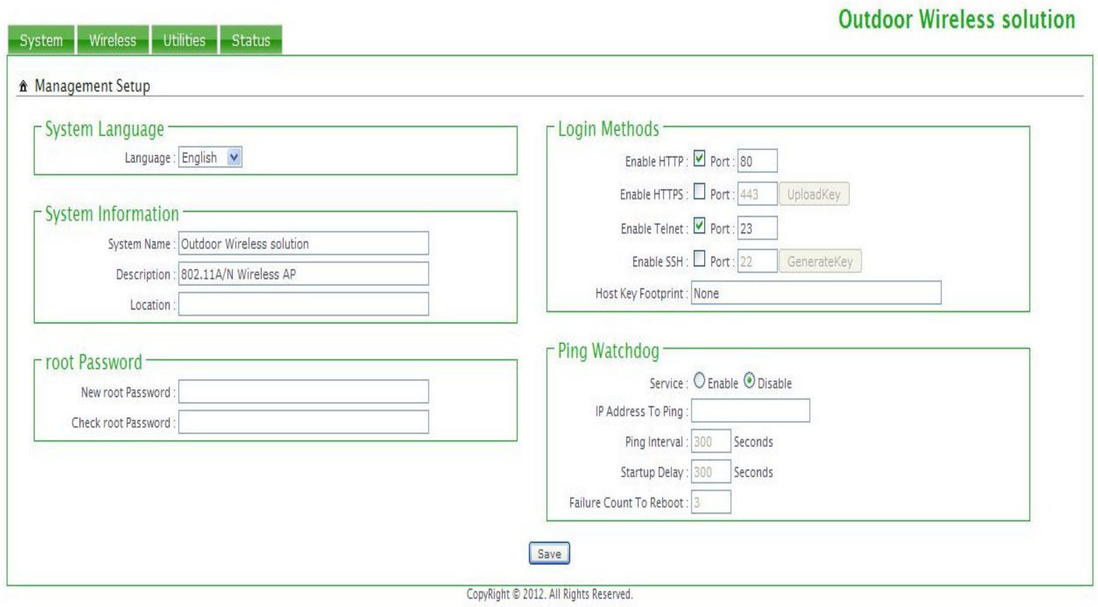
VLAN No.	VLAN Tag(ID)	VAP0	VAP1	VAP2	VAP3	VAP4	VAP5	VAP6	VAP7	WDS
		On	Off	Off	Off	Off	Off	Off	Off	
LAN		●	●	●	●	●	●	●	●	☑
VLAN1	101	○	○	○	○	○	○	○	○	□
VLAN2	102	○	○	○	○	○	○	○	○	□
VLAN3	103	○	○	○	○	○	○	○	○	□
VLAN4	104	○	○	○	○	○	○	○	○	□
VLAN5	105	○	○	○	○	○	○	○	○	□
VLAN6	106	○	○	○	○	○	○	○	○	□
VLAN7	107	○	○	○	○	○	○	○	○	□

CopyRight © 2012. All Rights Reserved.



The ST58T8 SERIES support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into **8** logical access points, each of which can have a different set of security, VLAN Tag(ID) and network settings.

- **Management Setup -**



Management Setup

System Language

Language : English

System Information

System Name : Outdoor Wireless solution

Description : 802.11A/N Wireless AP

Location :

root Password

New root Password :

Check root Password :

Login Methods

Enable HTTP : ☑ Port : 80

Enable HTTPS : □ Port : 443

Enable Telnet : ☑ Port : 23

Enable SSH : □ Port : 22

Host Key Footprint : None

Ping Watchdog

Service : ○ Enable ● Disable

IP Address To Ping :

Ping Interval : 300 Seconds

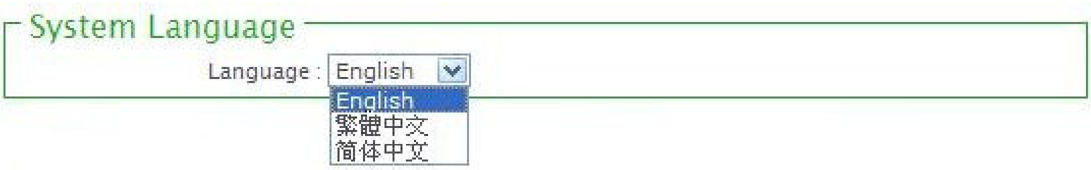
Startup Delay : 300 Seconds

Failure Count To Reboot : 3

CopyRight © 2012. All Rights Reserved.

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

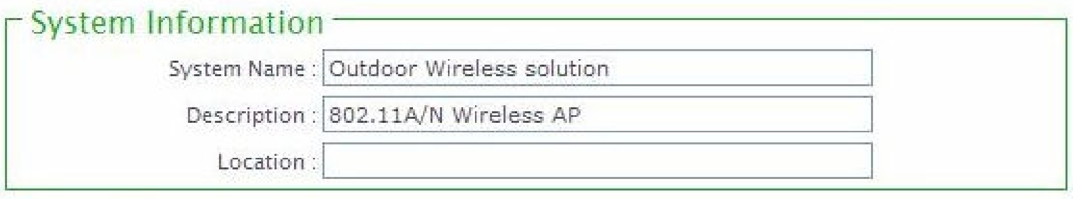
- **System Language**



System Language

Language : English

- **System Information**



System Information

System Name : Outdoor Wireless solution

Description : 802.11A/N Wireless AP

Location :

System Name: Enter a desired name or use the default one.

Description: Provide description of the system.

Location: Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance.

For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges.**

- **Root Password:** Log in as a root user and is allowed to change its own, plus admin user's password.

  New Password: Enter a new password if desired

  Check New Password: Enter the same new password again to check.

- **Login Methods:** Only **root** user can enable or disable system login methods and change services port.

  Enable HTTP: Check to select HTTP Service.

  HTTP Port: The default is **80** and the range is between 1 ~ 65535.

  Enable HTTPS: Check to select HTTPS Service

  HTTPS Port : The default is **443** and the range is between 1 ~ 65535.

If you already have an SSL Certificate, please click "**UploadKey**" 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.

Click "**GenerateKey**" 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 ST58T8 SERIES 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 ST58T8 SERIES device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

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

  Enable Ping Watchdog: control will enable Ping Watchdog Tool.

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

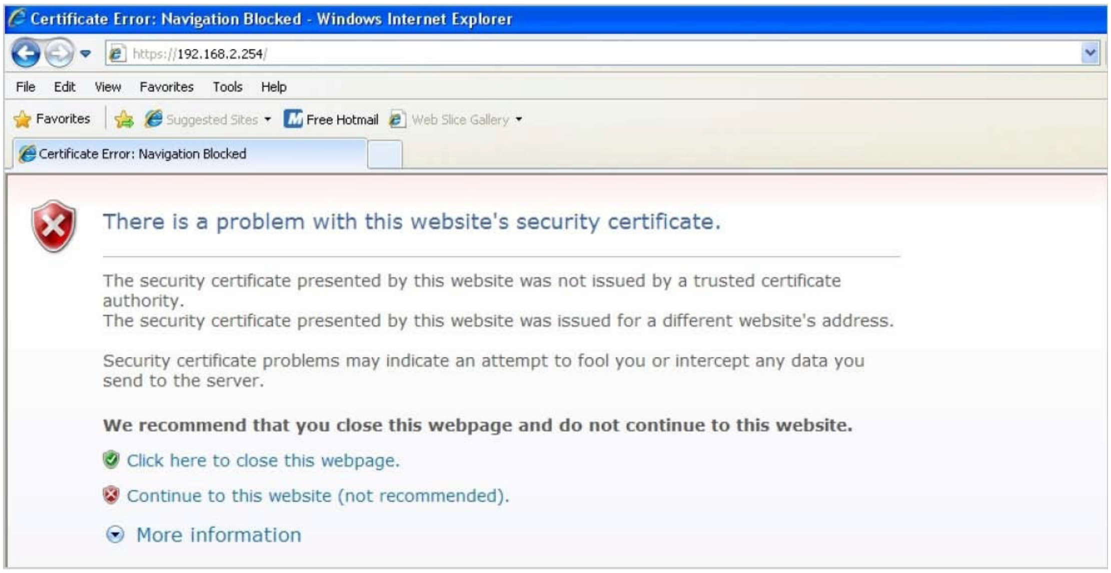
Ping Interval: specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. Default is **300** seconds.

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

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

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

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


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.2.254/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

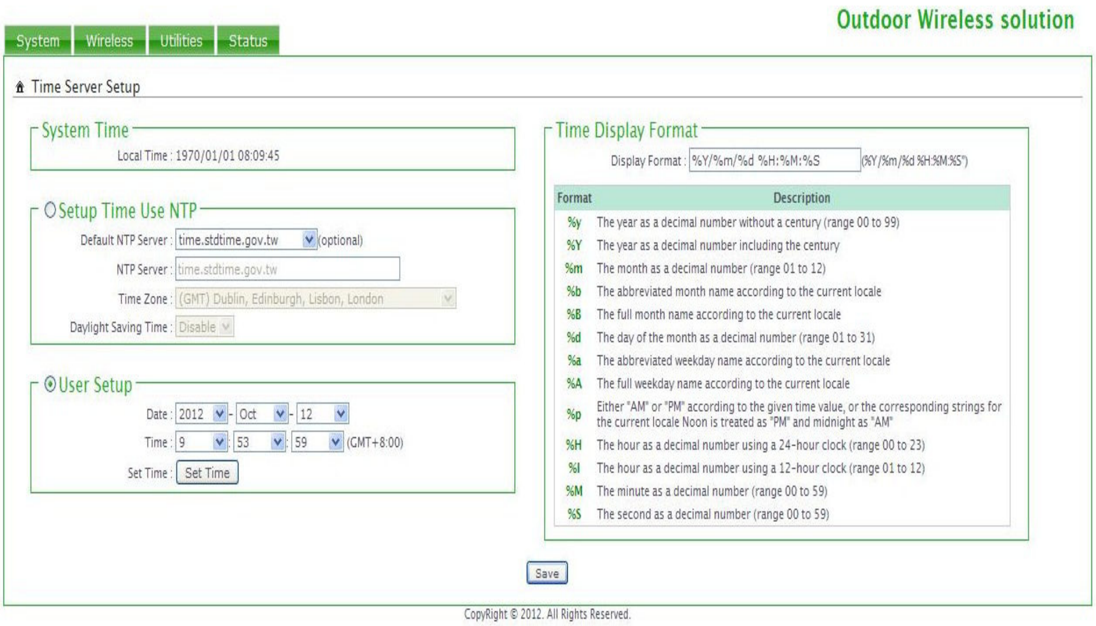
Click here to close this webpage.

Continue to this website (not recommended).

More information

Click “***Continue to this website***” to access the ST58T8 SERIES's GUI. The ST58T8 SERIES's Home page will be appear.

- **Time Server –**



Time Server Setup

System Time

Local Time : 1970/01/01 08:09:45

○ 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 - Oct - 12

Time : 9 : 53 : 59 (GMT+8:00)

Set Time : Set Time

Time Display Format

Display Format : %Y/%m/%d %H:%M:%S (%Y/%m/%d %H:%M:%S")

Format	Description
%y	The year as a decimal number without a century (range 00 to 99)
%Y	The year as a decimal number including the century
%m	The month as a decimal number (range 01 to 12)
%b	The abbreviated month name according to the current locale
%B	The full month name according to the current locale
%d	The day of the month as a decimal number (range 01 to 31)
%a	The abbreviated weekday name according to the current locale
%A	The full weekday name according to the current locale
%p	Either "AM" or "PM" according to the given time value, or the corresponding strings for the current locale Noon is treated as "PM" and midnight as "AM"
%H	The hour as a decimal number using a 24-hour clock (range 00 to 23)
%I	The hour as a decimal number using a 12-hour clock (range 01 to 12)
%M	The minute as a decimal number (range 00 to 59)
%S	The second as a decimal number (range 00 to 59)

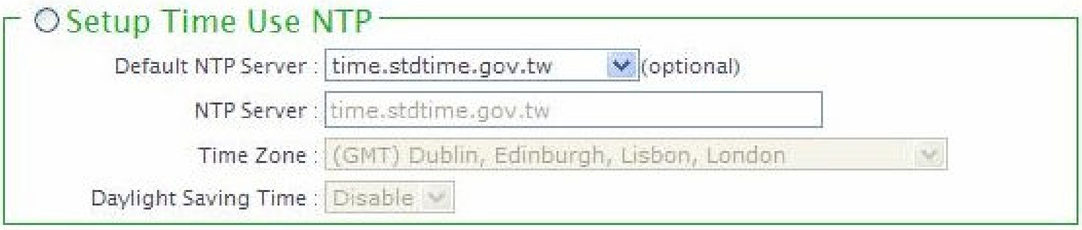
CopyRight © 2012. All Rights Reserved.

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

Local Time: Display the current system time.

- **Setup Time use NTP –**

To synchronize the system time with NTP server.



○ 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

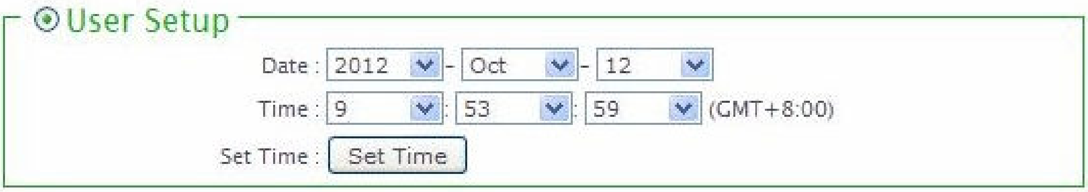
Daylight Saving Time : Disable

Default 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.

- **User Setup –**



● User Setup

Date : 2012 - Oct - 12

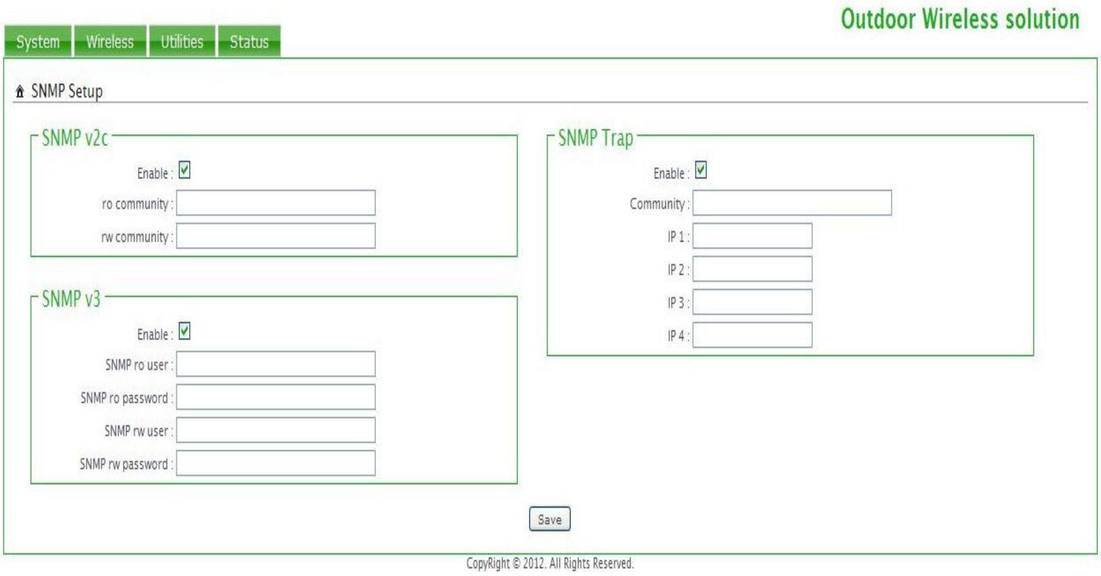
Time : 9 : 53 : 59 (GMT+8:00)

Set Time : Set Time

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

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

- **SNMP –**



SNMP Setup

SNMP v2c

Enable : ☑

ro community :

rw community :

SNMP v3

Enable : ☑

SNMP ro user :

SNMP ro password :

SNMP rw user :

SNMP rw password :

SNMP Trap

Enable : ☑

Community :

IP 1 :

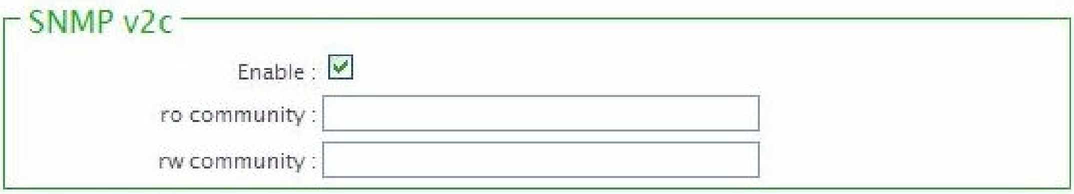
IP 2 :

IP 3 :

IP 4 :

CopyRight © 2012. All Rights Reserved.

SNMP is an application-layer protocol that provides a message format for communication between SNMP manager and agent. By enabling SNMP function, the administrator can obtain the system information remotely. Please click on **System -> SNMP Setup** and



SNMP v2c

Enable : ☑

ro community :

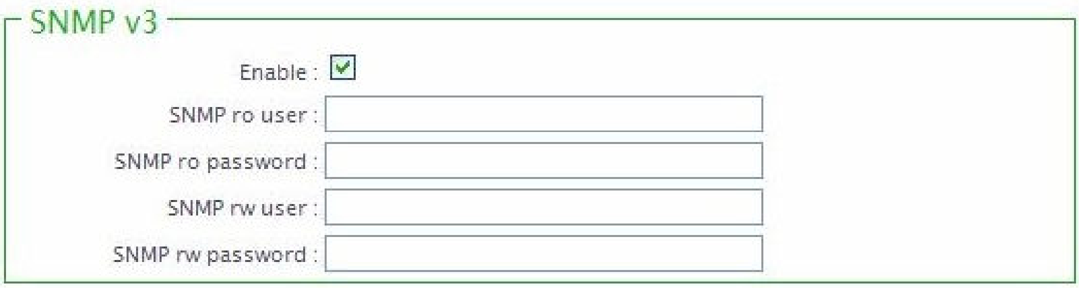
rw community :

follow the below setting.

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

ro community : Set a community string to authorize read-only access.

rw community : Set a community string to authorize read/write access.



SNMP v3

Enable : ☑

SNMP ro user :

SNMP ro password :

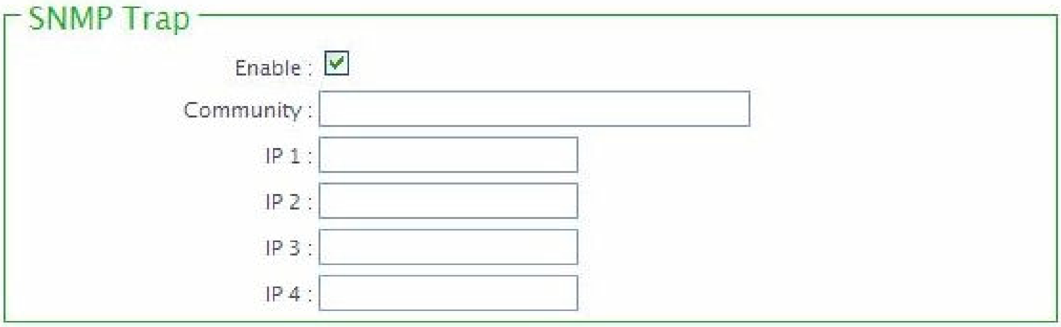
SNMP rw user :

SNMP rw password :

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

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

- **SNMP Trap Enable:** Check to enable SNMP Trap supports



SNMP Trap

Enable : ☑

Community :

IP 1 :

IP 2 :

IP 3 :

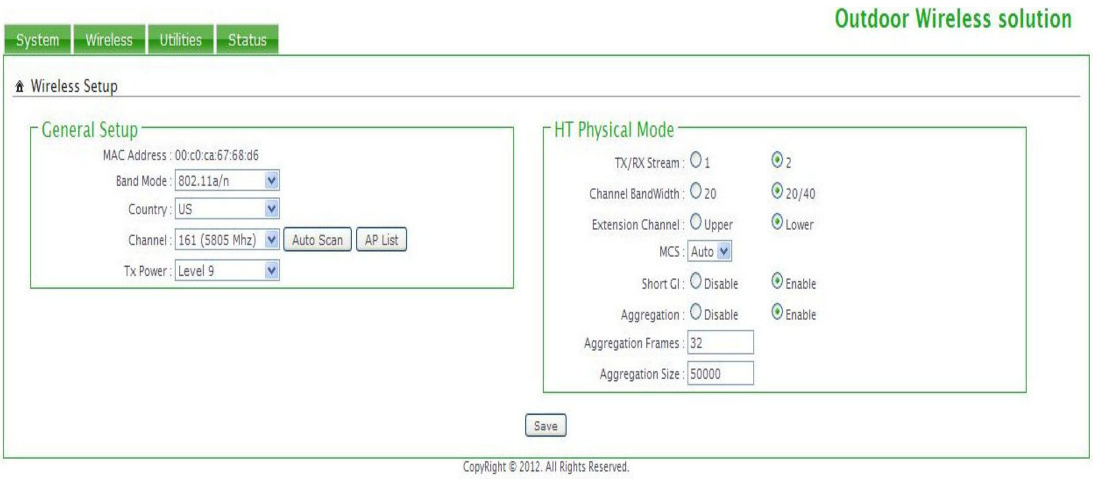
IP 4 :

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: Enter the IP addresses of the remote hosts to receive trap messages.

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

Wireless –

- Access Point Association



Wireless Setup

General Setup

MAC Address : 00:c0:ca:67:68:d6
Band Mode : 802.11a/n
Country : US
Channel : 161 (5805 Mhz) Auto Scan AP List
Tx Power : Level 9

HT Physical Mode

TX/RX Stream : ○ 1 ● 2
Channel BandWidth : ○ 20 ● 20/40
Extension Channel : ○ Upper ● Lower
MCS : Auto
Short GI : ○ Disable ● Enable
Aggregation : ○ Disable ● Enable
Aggregation Frames : 32
Aggregation Size : 50000

CopyRight © 2012. All Rights Reserved.

- Configured 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 **801.11a** or **802.11a/n mixed** or **802.11n** mode.

Transmit Rate Control: Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54Mbps** only for **802.11a** mode.

Country: Select the desired country code from the drop-down list; the options are ***US***, ***ETSI***, ***JP*** and ***NONE***.

Channel/Frequency: The channel range will be changed by selecting different country code. Below depicts the channel range for different ***Country***. When "**Band Mode**" selected in "**802.11a**", the Channel **140** and **165** does not shown-up on list.

Tx Power: You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify level between ***Level 1*** to ***Level 9*** for your environment. If you are not sure which setting to choose, then keep the default setting, **Level 9**

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput) Physical Mode** settings should be hidden immediately.

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 : It indicates the use of channel bonding that allows the wireless network to use two channels at once. Using two channels improves the performance of the Wi-Fi connection. Below depicts the **Upper** and **Lower**

Channel range for different ***Country***.

Lower Channel
40, 48, 56, 64, 104, 112, 120, 128, 136, 153, 161 40, 48, 56, 64, 104, 112, 120, 128, 136 40, 48, 56, 64, 104, 112, 120, 128, 136

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.

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.

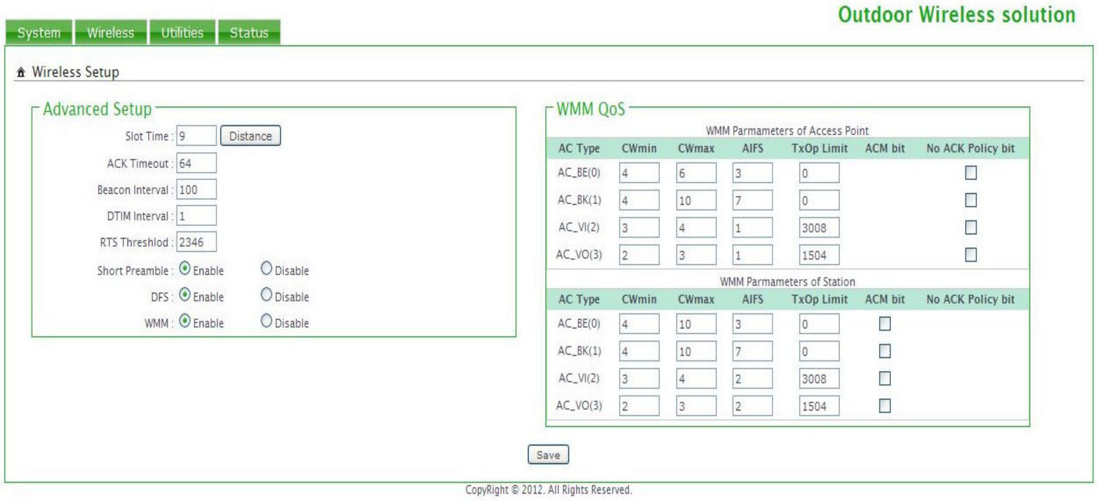
Aggregation Frames: The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.

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.
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **Repeater AP**

➢ **Wireless Advanced Setup –**

To achieve optimal wireless performance, it is necessary advance setting per requirements properly, not necessary higher the better or lower.

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



Advanced Setup

Slot Time : 9

ACK Timeout : 64

Beacon Interval : 100

DTIM Interval : 1

RTS Threshlod : 2346

Short Preamble : ● Enable ○ Disable

DFS : ● Enable ○ Disable

WMM : ● Enable ○ Disable

WMM QoS

WMM Parmameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	6	3	0		□
AC_BK(1)	4	10	7	0		□
AC_VI(2)	3	4	1	3008		□
AC_VO(3)	2	3	1	1504		□

WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	10	3	0	□	
AC_BK(1)	4	10	7	0	□	
AC_VI(2)	3	4	2	3008	□	
AC_VO(3)	2	3	2	1504	□	

CopyRight © 2012. All Rights Reserved.

Short Slot: Slot time is in the range of **9~1498** 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.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set *timeout* it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the *timeout* is set too short or too long, it will result in poor connection and throughput performance.

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 4**0~3500** 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:

Greenfield:

DFS : By default, it's “***Disable***”. ***DFS*** is the part of the IEEE 802.11h wireless standard. With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

DFS Channels
52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140(not used)

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain. The Channel **52-140** is DFS channel. If turn on DFS, AP Will have **60** sec to do channel available check, and will not send beacon and cannot be connect. When ST58T8 SERIES detect radar(5GHz) signal, the AP will switch channel and stop beacon transmit between **15** sec.

WMM QoS:

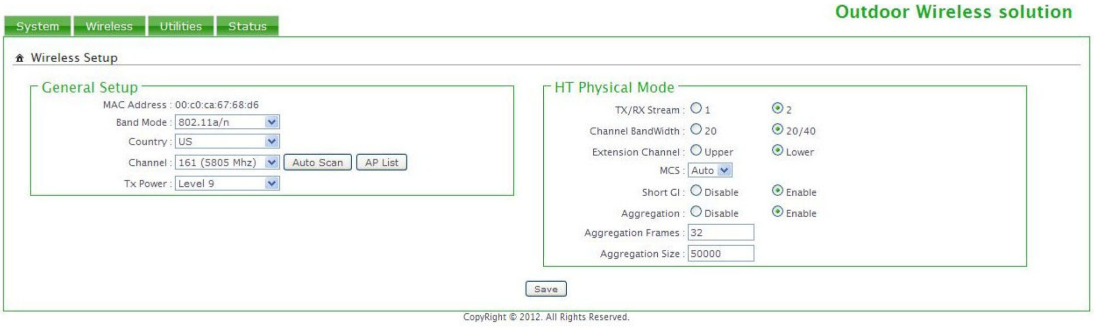
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.
The items in this page are for AP's RF advanced settings and will be applied to

all VAPs and **WDS Links**.

Configuration in AP Mode (including Access Point + WDS)

An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly.

same as Wireless Setup --->General Setup



Wireless Setup

General Setup

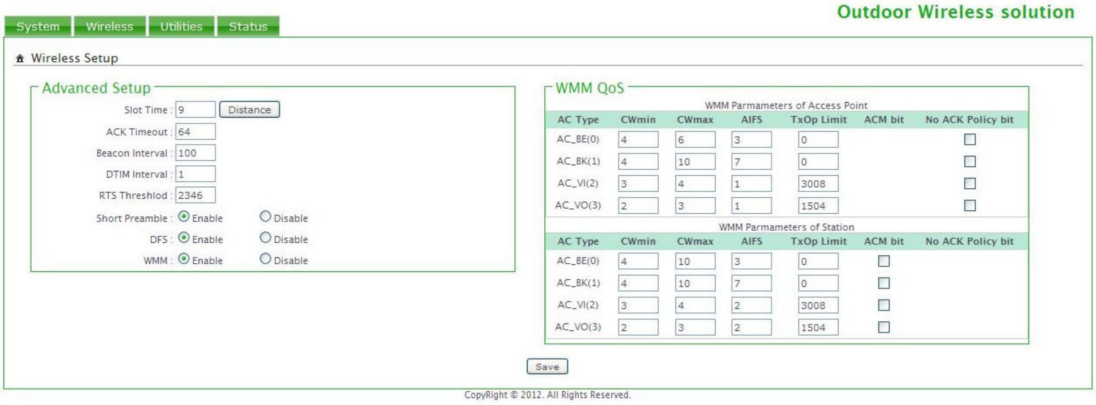
MAC Address : 00:c0:ca:67:68:d6
Band Mode : 802.11a/n
Country : US
Channel : 161 (5805 Mhz)
Tx Power : Level 9

HT Physical Mode

TX/RX Stream : ○ 1 ● 2
Channel BandWidth : ○ 20 ● 20/40
Extension Channel : ○ Upper ● Lower
MCS : Auto
Short GI : ○ Disable ● Enable
Aggregation : ○ Disable ● Enable
Aggregation Frames : 32
Aggregation Size : 50000

CopyRight © 2012. All Rights Reserved.

same as Wireless Setup --->Advanced Setup



Wireless Setup

Advanced Setup

Slot Time : 9
ACK Timeout : 64
Beacon Interval : 100
DTIM Interval : 1
RTS Threshlod : 2346
Short Preamble : ● Enable ○ Disable
DFS : ● Enable ○ Disable
WMM : ● Enable ○ Disable

WMM QoS

WMM Parmameters of Access Point

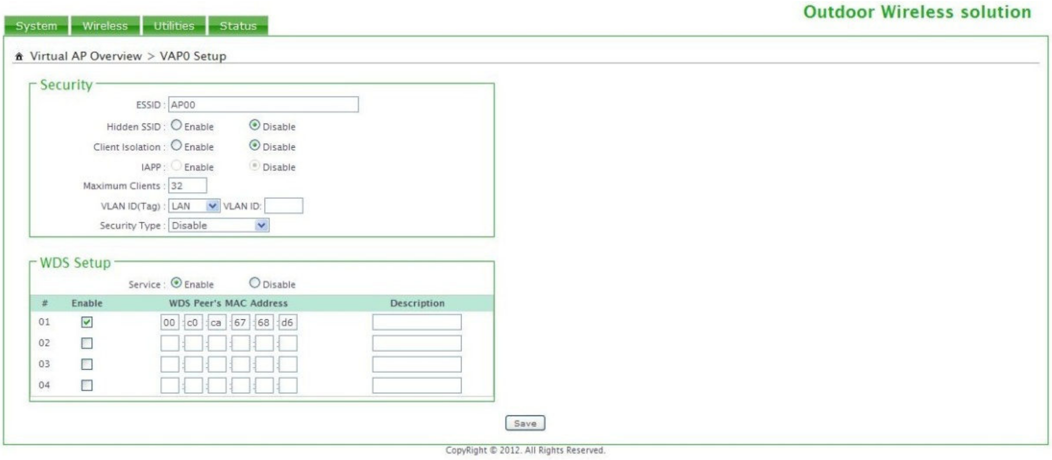
AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	6	3	0		□
AC_BK(1)	4	10	7	0		□
AC_VI(2)	3	4	1	3008		□
AC_VO(3)	2	3	1	1504		□

WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	10	3	0	□	
AC_BK(1)	4	10	7	0	□	
AC_VI(2)	3	4	2	3008	□	
AC_VO(3)	2	3	2	1504	□	

CopyRight © 2012. All Rights Reserved.

same as Wireless Setup ---> Virtual Overview --->VAP0 Setup



Virtual AP Overview > VAP0 Setup

Security

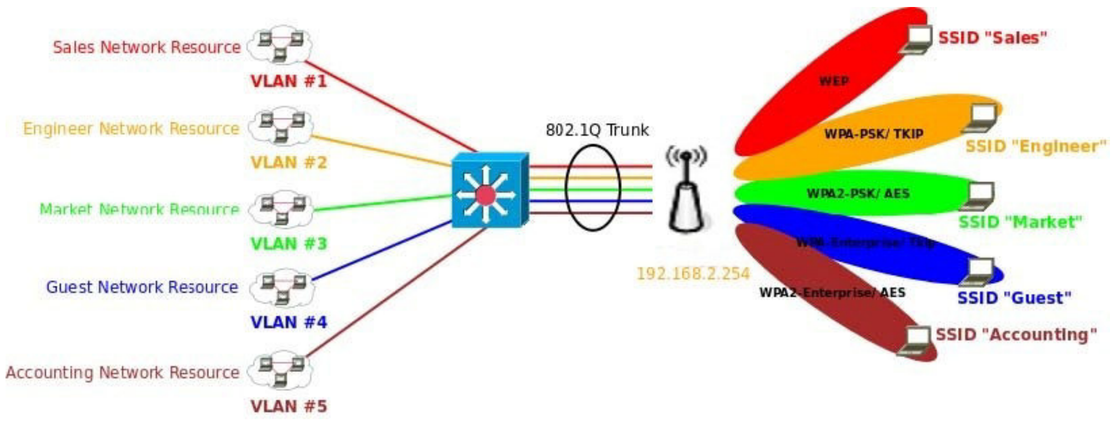
ESSID : AP00
Hidden SSID : ○ Enable ● Disable
Client Isolation : ○ Enable ● Disable
IAPP : ○ Enable ● Disable
Maximum Clients : 32
VLAN ID(Tag) : LAN VLAN ID:
Security Type : Disable

WDS Setup

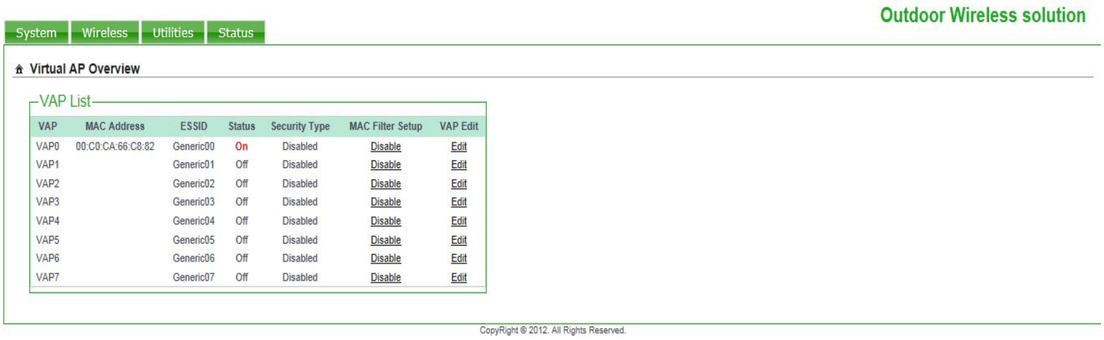
Service : ● Enable ○ Disable

#	Enable	WDS Peer's MAC Address	Description
01	☑	00 : c0 : ca : 67 : 68 : d6	
02	□		
03	□		
04	□		

CopyRight © 2012. All Rights Reserved.



Multiple SSIDs with different Security Type and VLAN Tag



Virtual AP Overview

VAP List

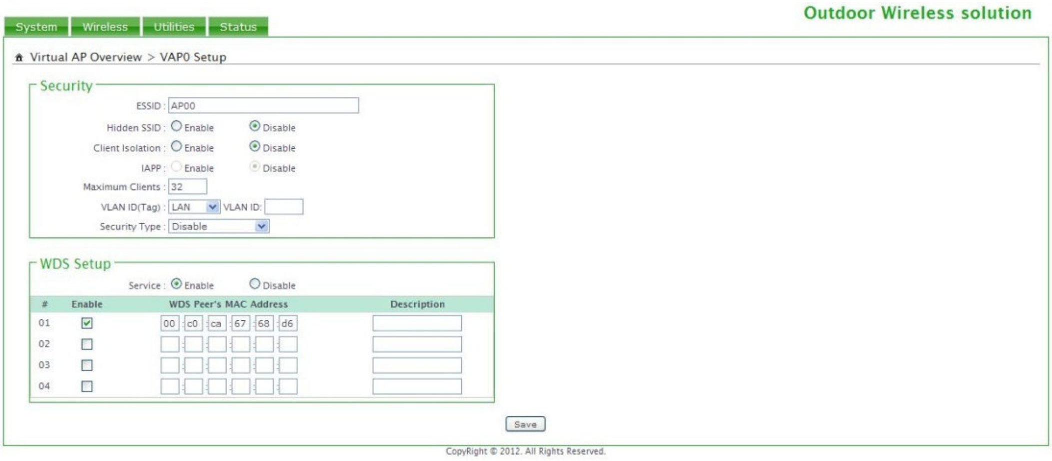
VAP	MAC Address	ESSID	Status	Security Type	MAC Filter Setup	VAP Edit
VAP0	00:C0:CA:66:C8:82	Generic00	On	Disabled	Disable	Edit
VAP1		Generic01	Off	Disabled	Disable	Edit
VAP2		Generic02	Off	Disabled	Disable	Edit
VAP3		Generic03	Off	Disabled	Disable	Edit
VAP4		Generic04	Off	Disabled	Disable	Edit
VAP5		Generic05	Off	Disabled	Disable	Edit
VAP6		Generic06	Off	Disabled	Disable	Edit
VAP7		Generic07	Off	Disabled	Disable	Edit

CopyRight © 2012. All Rights Reserved.

Edit : Click **Edit** button to configure Virtual AP's settings.
For each Virtual AP, administrators can configure SSID, VLAN tag(ID), SSID broadcasting, Maximum number of client associations, security type settings. Click **Edit** button on the Edit column, and then a Virtual AP setup page appears.

The ST58T8 SERIES support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into 8 logical access points, each of which can have a different set of security, VLAN Tag(ID) and network settings.

VAP : Indicate the 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 : Indicate the ESSID of the respective Virtual AP
Status : Indicate the Status of the respective Virtual AP. The VAP0 always on.



Virtual AP Overview > VAP0 Setup

Security

ESSID : AP00

Hidden SSID : ○ Enable ● Disable

Client Isolation : ○ Enable ● Disable

IAPP : ○ Enable ● Disable

Maximum Clients : 32

VLAN ID(Tag) : LAN VLAN ID:

Security Type : Disable

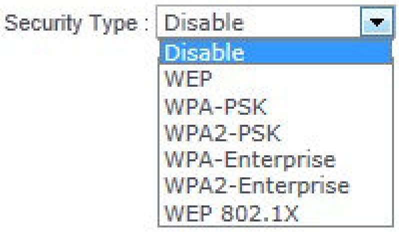
WDS Setup

Service : ● Enable ○ Disable

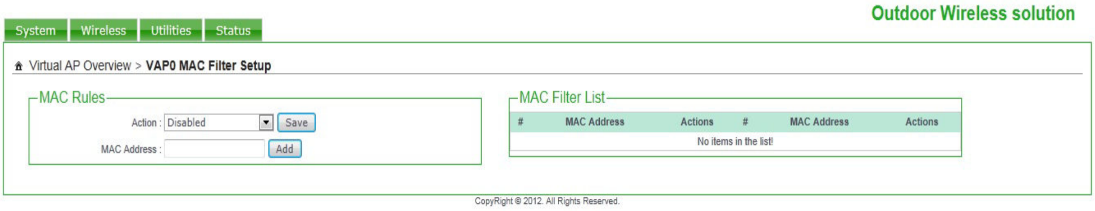
#	Enable	WDS Peer's MAC Address	Description
01	☑	00 : c0 : ca : 67 : 68 : d6	
02	□		
03	□		
04	□		

CopyRight © 2012. All Rights Reserved.

Security Type : Indicate an used security type of the respective Virtual AP.


Security Type : Disable

MAC Filter : Indicate an used MAC filter of the respective Virtual AP. Click button to configure MAC Filter of the respective Virtual AP.



Virtual AP Overview > **VAP0 MAC Filter Setup**

MAC Rules

Action : Disabled

MAC Address :

MAC Filter List

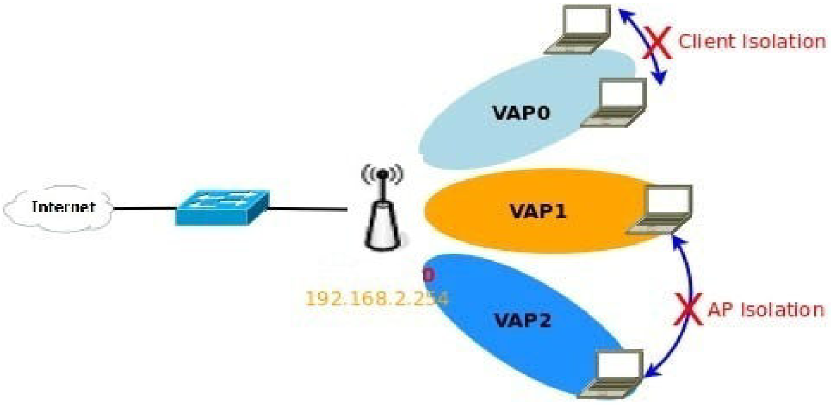
#	MAC Address	Actions	#	MAC Address	Actions
No items in the list!					

CopyRight © 2012. All Rights Reserved.

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. **Enable AP :** By default, it's "***Disable***" for VAP1 ~ VAP7. **The VAP0 always enabled**. Select "***Enable***" to activate VAP or click "***Disable***" to deactivate this function

Hidden SSID : Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from begin seen on networked.

Client Isolation : Select **Enable**, all clients will be isolated from each other, that means all clients cannot reach to other clients. Below Figures depict Client Isolation and AP Isolation



WMM : Select Enable, the packets with QoS WMM will has higher priority.

IAPP Support : 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.

VLAN Tag(ID) : By default, it's selected "***Disable***". This system supports tagged Virtual LAN(VLAN). A valid number of **0** to **4094** can be entered after it's enabled. If your network utilize VLANs you could tie a VLAN Tag to a specific SSID, and packets from/to wireless clients belonging to that SSID will be tagged with that VLAN Tag. This enables security of wireless applications by applying VLAN Tag.

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**.

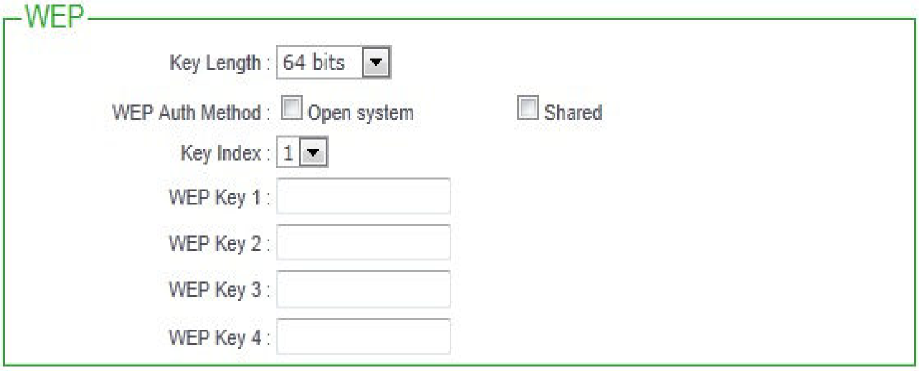
Disable : Data are unencrypted during transmission when this option is selected.

WEP : 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 : Select the desire option are ***64 bits***, ***128 bits*** or ***152 bits*** from drop-down list.

WEP auth Method : Enable the desire option among ***Open system*** or ***Shared***.

Key Index : Select key index used to designate the WEP key during data transmission. 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 Length : 64 bits

WEP Auth Method : □ Open system □ Shared

Key Index : 1

WEP Key 1 :

WEP Key 2 :

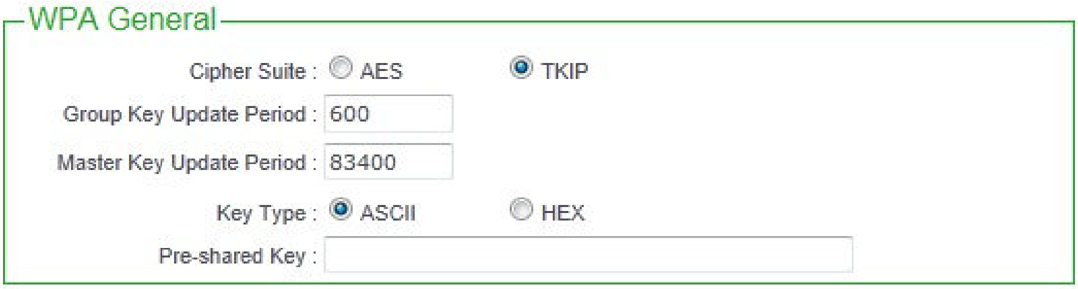
WEP Key 3 :

WEP Key 4 :

WEP Key : Enter HEX format WEP key value; the system support up to 4 sets of WEP keys.

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

Cipher Suite : Check on the respected button to enable either **AES** or **TKIP** cipher suites; default is **TKIP**.



WPA General

Cipher Suite : ○ AES ● TKIP

Group Key Update Period : 600

Master Key Update Period : 83400

Key Type : ● ASCII ○ HEX

Pre-shared Key :

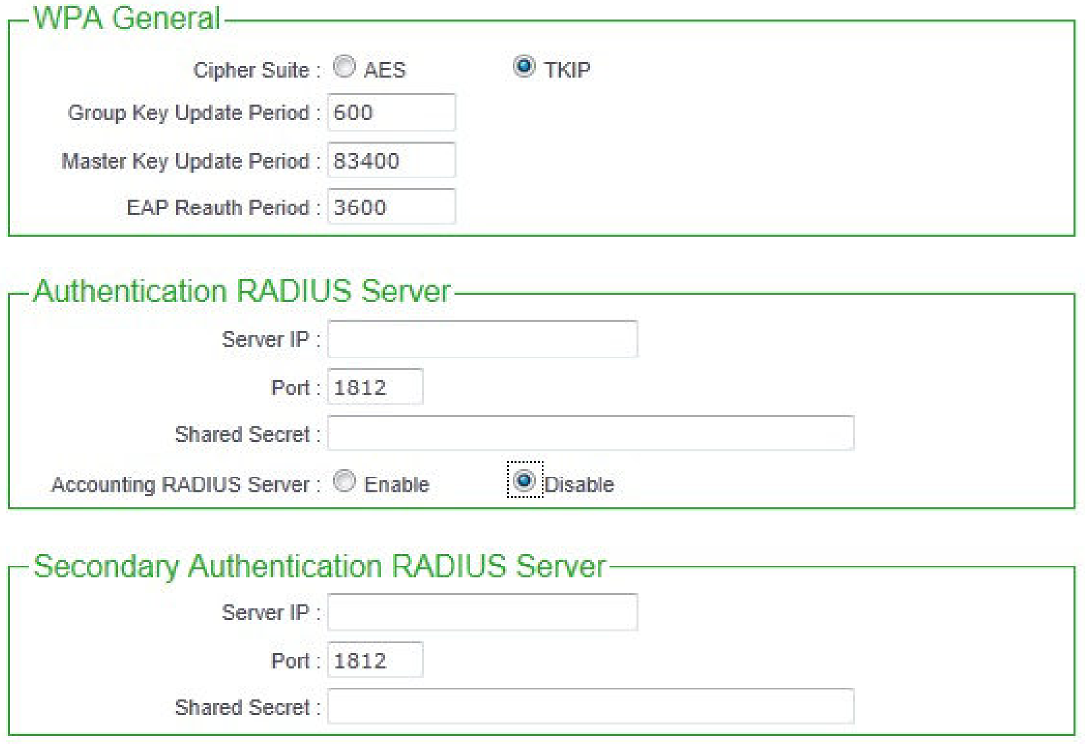
Group Key Update Period : This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is **600** seconds.

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

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



WPA General

Cipher Suite : ○ AES ● TKIP

Group Key Update Period : 600

Master Key Update Period : 83400

EAP Reauth Period : 3600

Authentication RADIUS Server

Server IP :

Port : 1812

Shared Secret :

Accounting RADIUS Server : ○ Enable ● Disable

Secondary Authentication RADIUS Server

Server IP :

Port : 1812

Shared Secret :

WPA General Setup

Cipher Suite : Check on the respected button to enable either **AES** or **TKIP** cipher suites; default is **TKIP**.

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 : EAP re-authentication period in seconds; default is **3600**; **0** indicates **disable** re-authentication.

Authentication RADIUS Server Settings :

Authentication Server : 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 **1** to **64** characters.

Accounting RADIUS Server : Check on the respected button to enable either Enable or Disable accounting RADIUS server.

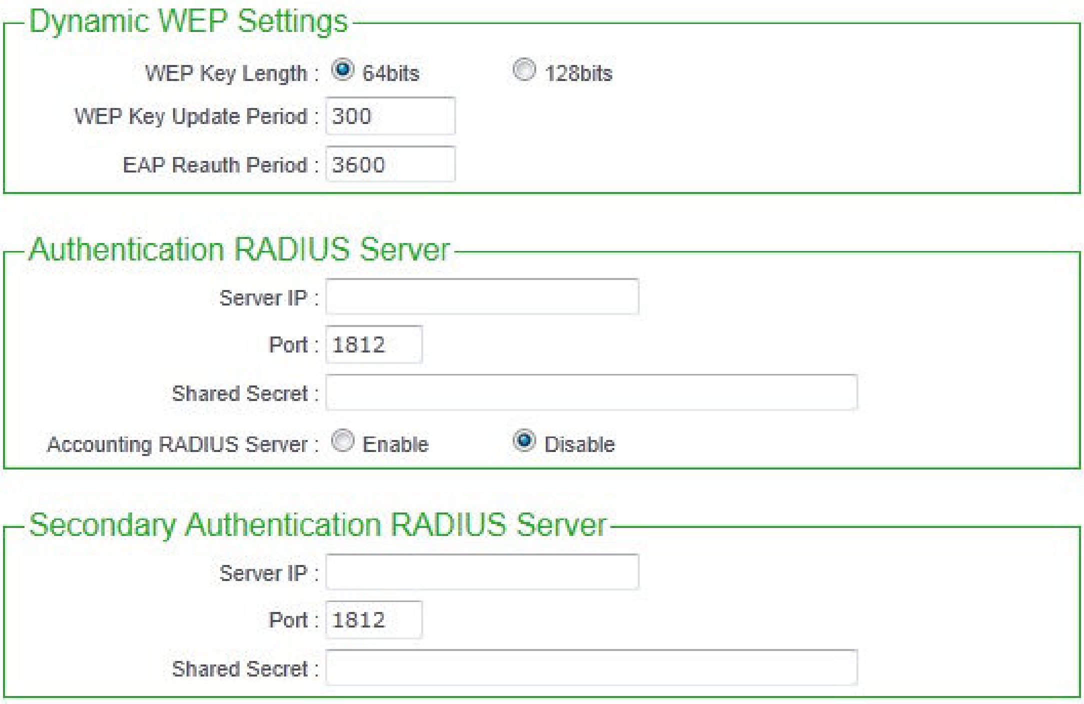
Accounting Server Settings :

Accounting Server : Enter the IP address of the Accounting RADIUS server.

Port : The port number used by Accounting RADIUS server. Use the default 1813 or enter port number specified.

Shared Secret : The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.

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



Dynamic WEP Settings

WEP Key Length : ● 64bits ○ 128bits

WEP Key Update Period : 300

EAP Reauth Period : 3600

Authentication RADIUS Server

Server IP :

Port : 1812

Shared Secret :

Accounting RADIUS Server : ○ Enable ● Disable

Secondary Authentication RADIUS Server

Server IP :

Port : 1812

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** indicates no re-key.

EAP Reauth Period : EAP re-authentication period in seconds; default is **3600**; **0** indicates **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 Accounting RADIUS server. Support **1** to **64** characters.

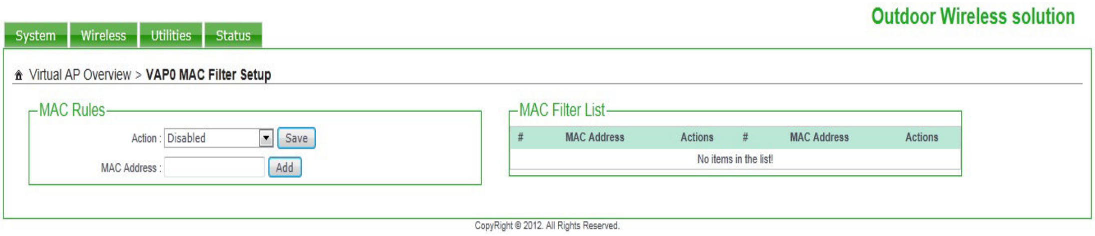
Accounting RADIUS Server : Check on the respected button to enable either Enable or Disable accounting RADIUS server.

Secondary **Accounting Server Settings :**
Accounting Server : Enter the IP address of the Accounting RADIUS server.

Port : The port number used by Accounting RADIUS server. Use the default **1813** or enter port number specified.

Shared Secret : The secret key for system to communicate with Accounting RADIUS server. Support **1** to **64** characters.

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



Virtual AP Overview > **VAP0 MAC Filter Setup**

MAC Rules

Action : Disabled

MAC Address :

MAC Filter List

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

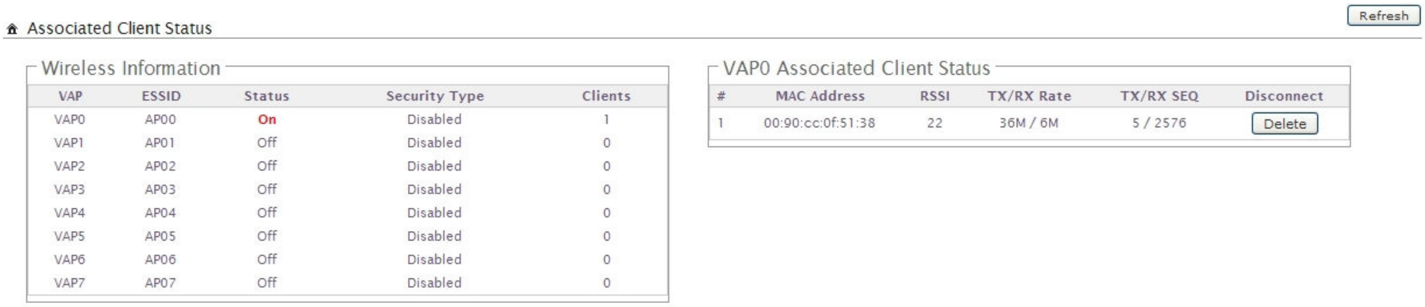
CopyRight © 2012. All Rights Reserved.

Action : Select the desired access control type from the drop-down list; the options are “**Disabled**”, “**Only Deny List MAC**” or “**Only Allow 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** is set to **Only Deny 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** is set to **Only Allow List MAC**.

MAC Address : Enter MAC address in this field. There are maximum **20** clients users allowed in this MAC address list.



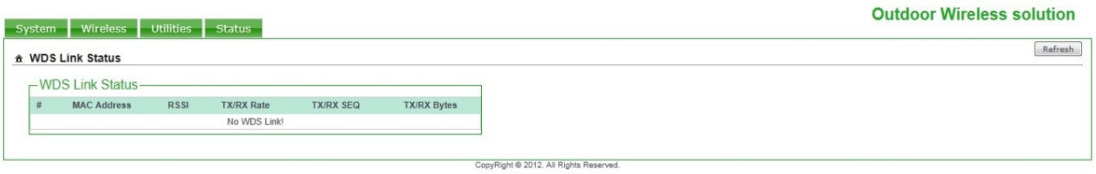
Associated Client Status

Wireless Information

VAP	ESSID	Status	Security Type	Clients
VAP0	AP00	On	Disabled	1
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

VAP0 Associated Client Status

#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	Disconnect
1	00:90:cc:0f:51:38	22	36M / 6M	5 / 2576	Delete

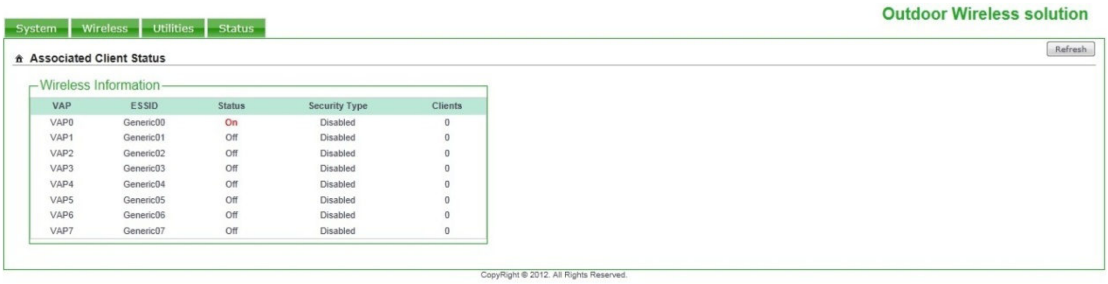


WDS Link Status

WDS Link Status

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

CopyRight © 2012. All Rights Reserved.



Associated Client Status

Wireless Information

VAP	ESSID	Status	Security Type	Clients
VAP0	Generic00	On	Disabled	0
VAP1	Generic01	Off	Disabled	0
VAP2	Generic02	Off	Disabled	0
VAP3	Generic03	Off	Disabled	0
VAP4	Generic04	Off	Disabled	0
VAP5	Generic05	Off	Disabled	0
VAP6	Generic06	Off	Disabled	0
VAP7	Generic07	Off	Disabled	0

CopyRight © 2012. All Rights Reserved.

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

The Associated Clients Status appears.

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

VAP : Display number of system's Virtual AP.

ESSID : Extended Service Set ID of the Virtual AP.

Status : Display Virtual AP status currently.

Security Type : Security type activated by the Virtual AP.

Clients : Number of clients currently associated to the Virtual AP.

Associated Client Status : Display the each Virtual AP associated clients status.

MAC Address : Indicate the MAC address of the respective client's association.

RSSI : Indicate the RSSI of the respective client's association.

TX/RX Rate : Indicate the TX/RX Rate of the respective client's association.

TX/RX SEQ : Indicate the TX/RX sequence of the respective client's association.

Disconnect : Administrator can kick out a specific client, click

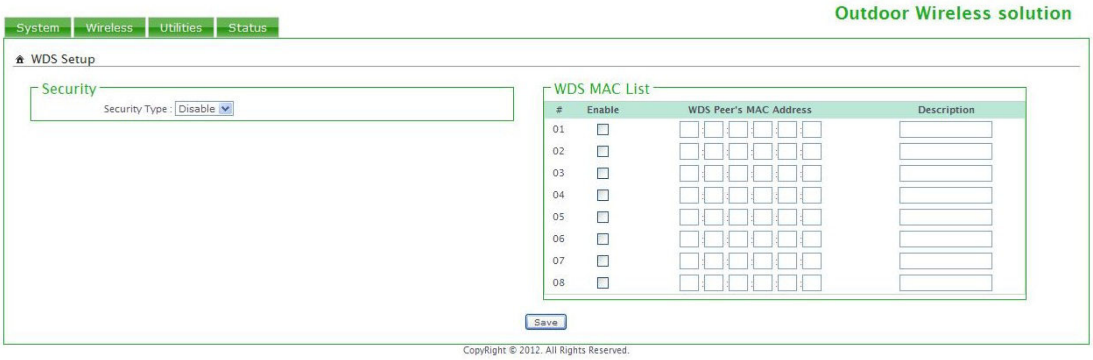
■ Configuration in WDS Mode (Pure WDS)

An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly. In this mode, it can support single or multiple WDS links and no wireless clients **can** associate with it.

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

Create WDS Link

The administrator can create WDS Links for expanding wireless network via this page. Please click on **Wireless -> WDS Setup** and follow the below setting.


Outdoor Wireless solution
System
Wireless
Utilities
Status
WDS Setup
Security
WDS MAC List
Save
CopyRight © 2012. All Rights Reserved.

Security Type : Disable

#	Enable	WDS Peer's MAC Address	Description
01	□	□:□:□:□:□:□	
02	□	□:□:□:□:□:□	
03	□	□:□:□:□:□:□	
04	□	□:□:□:□:□:□	
05	□	□:□:□:□:□:□	
06	□	□:□:□:□:□:□	
07	□	□:□:□:□:□:□	
08	□	□:□:□:□:□:□	

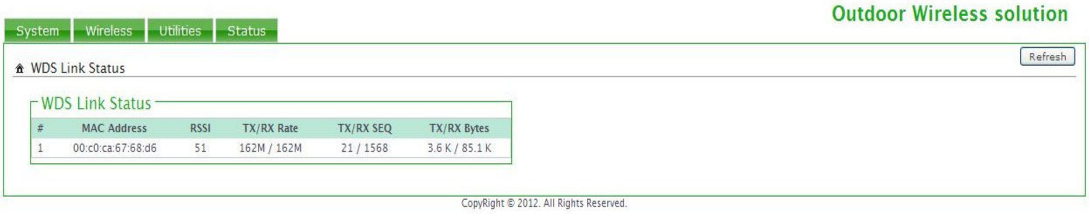
Security Type : Option is “**Disable**”, “**WEP**” or “**AES**” from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.

WEP Key : Enter **5 / 13 ASCII** or **10 / 26 HEX** format WEP key.
AES Key : Enter **32 HEX** format AES key.
WDS MAC List **Enable :** Click ***Enable*** to create WDS link.
WDS Peer's MAC Address : Enter the MAC address of WDS peer.
Description : Description of WDS link.

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

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

“**Delete**” button to kick out specific client



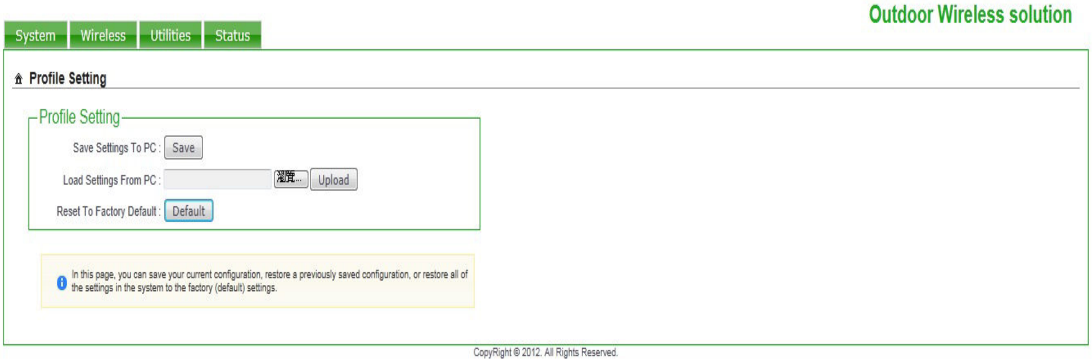
WDS Link Status

WDS Link Status

#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	TX/RX Bytes
1	00:c0:ca:67:68:d6	51	162M / 162M	21 / 1568	3.6 K / 85.1 K

CopyRight © 2012. All Rights Reserved.

Utilities



Profile Setting

Profile Setting

Save Settings To PC :

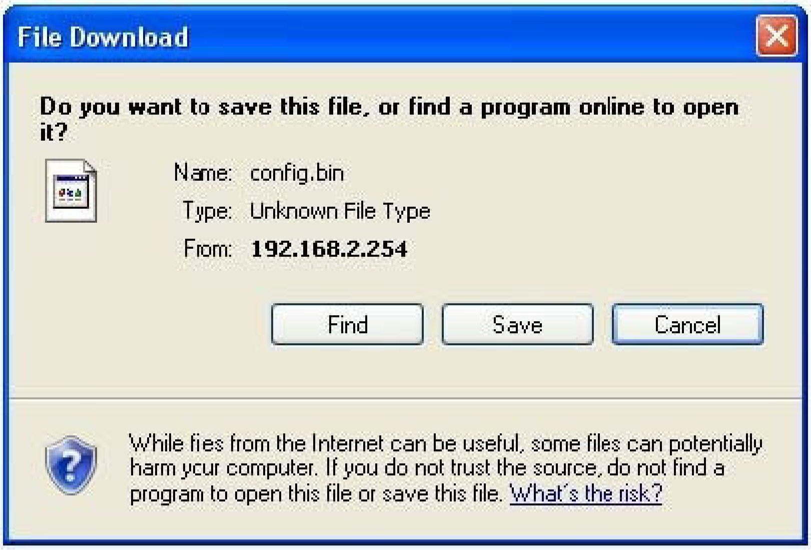
Load Settings From PC :

Reset To Factory Default :

In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

CopyRight © 2012. All Rights Reserved.

Backup / Restore and Reset to Factory



Do you want to save this file, or find a program online to open it?

Name: config.bin
Type: Unknown File Type
From: 192.168.2.254

While fies from the Internet can be useful, some files can potentially harm ycur computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

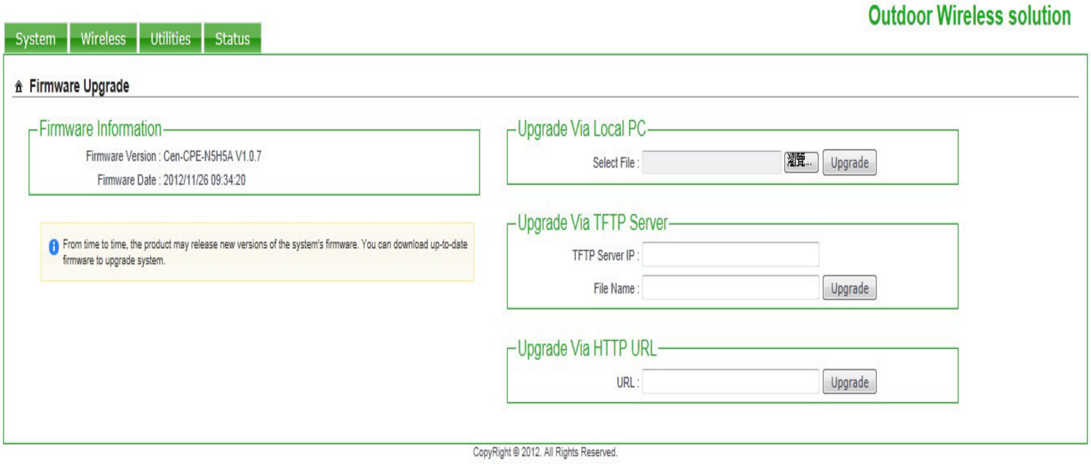
Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page. Please click on **Utilities -> Profile Setting** and follow the below setting.

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. The system will **restart** after uploading configuration and database.

Firmware Upgrade



Firmware Version : Cen-CPE-N5H5A V1.0.7

Firmware Date : 2012/11/26 09:34:20

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.

CopyRight © 2012. All Rights Reserved.

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **80 seconds** to upgrade due to complexity of firmware. The system support three methods to upgrade system firmware : via Local PC, TFTP Server or HTTP Server.

Update Via Local PC : Click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.

Update Via TFTP Server : Enter TFTP Server IP address and firmware file, and then click Upgrade button to upgrade.

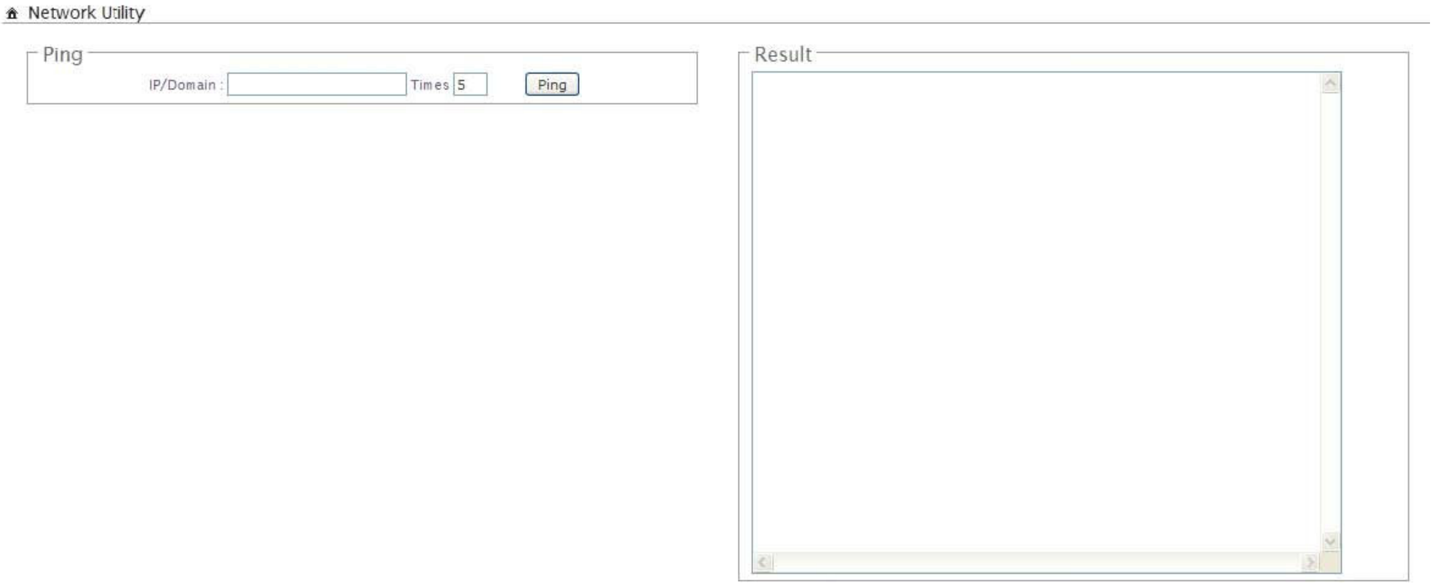
Update Via HTTP URL : Enter URL address(example : http://192.168.2.10/xxx.bin), and then click Upgrade button to upgrade.

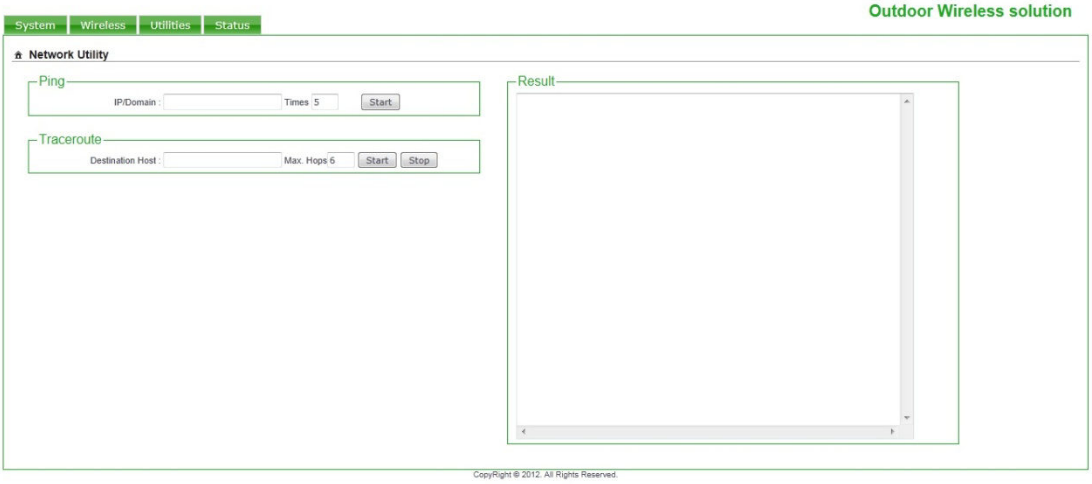
1 To prevent data loss during firmware upgrade, please back up current settings before proceeding.

2 Do not interrupt during firmware upgrade including power on/off as this may damage system.

3 Never perform firmware upgrade over wireless connection or via remote access connection.

Network Utility





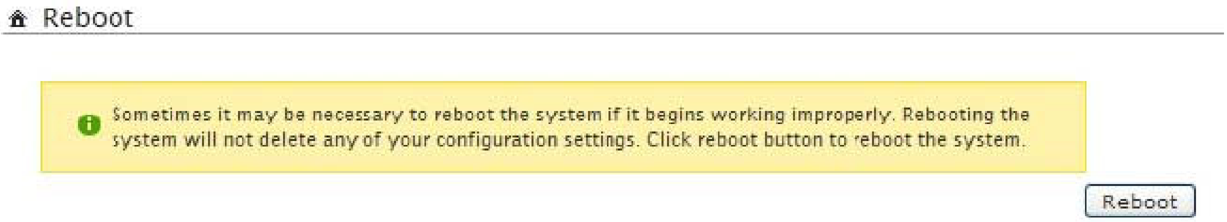
The administrator can diagnose network connectivity via the PING or TRACEROUTE utility. Please click on **Utilities -> Network Utility** and follow the below setting.

Ping : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.

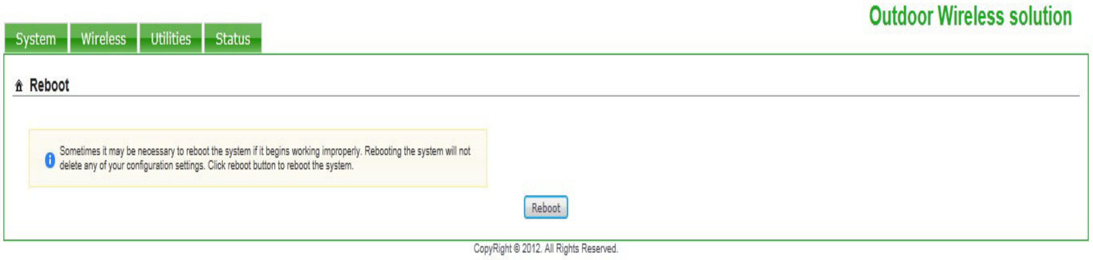
Destination IP/Domain : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.

Count : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

Reboot

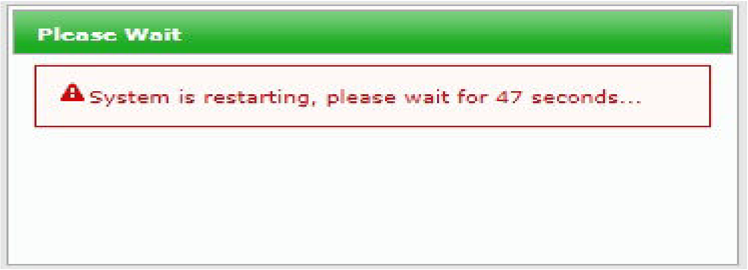


Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.



Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

CopyRight © 2012. All Rights Reserved.



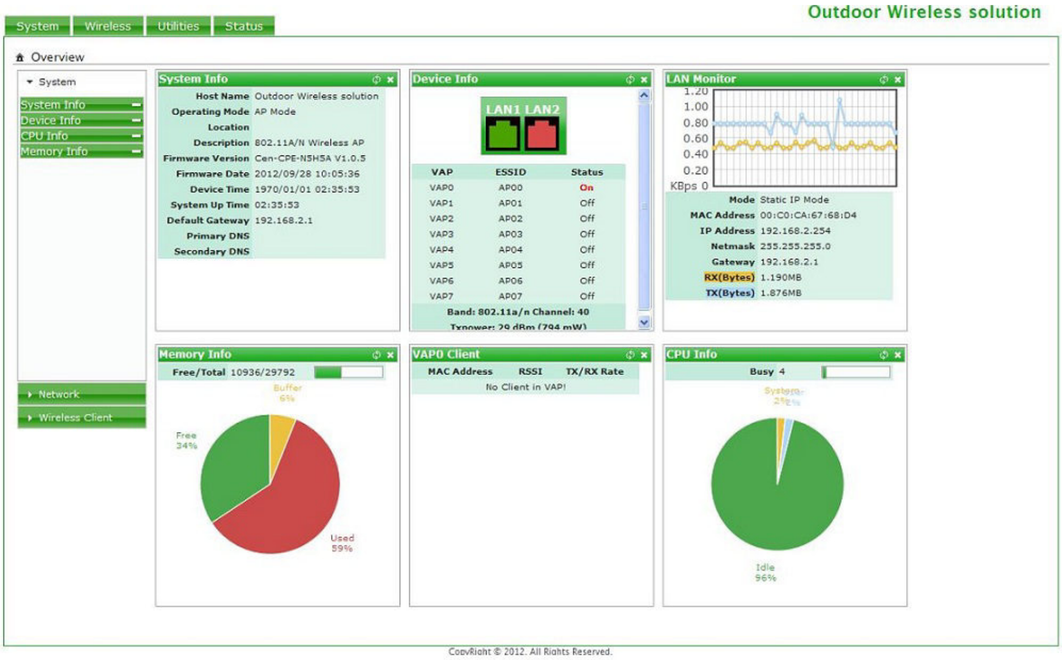
System is restarting, please wait for 47 seconds...

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. A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.

The **System Overview** page appears upon the completion of reboot.

System Status



System Info

Host Name	Outdoor Wireless solution
Operating Mode	AP Mode
Location	
Description	802.11A/N Wireless AP
Firmware Version	Cen-CPE-N5H5A V1.0.5
Firmware Date	2012/09/28 10:05:36
Device Time	1970/01/01 02:35:53
System Up Time	02:35:53
Default Gateway	192.168.2.1
Primary DNS	
Secondary DNS	

Device Info

VAP	ESSID	Status
VAP0	AP00	On
VAP1	AP01	Off
VAP2	AP02	Off
VAP3	AP03	Off
VAP4	AP04	Off
VAP5	AP05	Off
VAP6	AP06	Off
VAP7	AP07	Off

Band: 802.11a/n Channel: 40
Txpower: 29 dBm (794 mW)

LAN Monitor

Mode	Static IP Mode
MAC Address	00:C0:CA:67:68:D4
IP Address	192.168.2.254
Netmask	255.255.255.0
Gateway	192.168.2.1
RX(Bytes)	1.190MB
TX(Bytes)	1.876MB

Memory Info

Free/Total 10936/29792

VAP0 Client

MAC Address	RSSI	TX/RX Rate
No Client in VAP!		

CPU Info

Busy 4

This section breaks down into subsections of ***System Overview***, ***Extra Information*** and ***Event Log***.

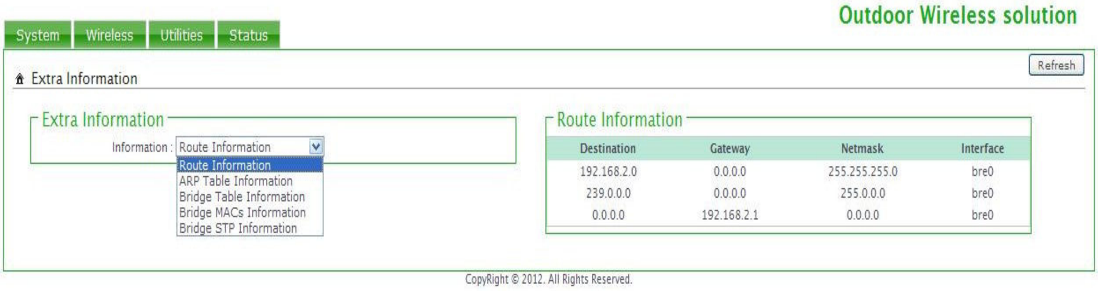
System Overview

Display detailed information of ***System, Network, Wireless Client*** in the System Overview page.

System Information : Display the information of the system.

Networking Information : Display the information of the network.

Wireless Client Information : Display the information of the wireless clients.



Extra Information

Extra Information

Information : Route Information

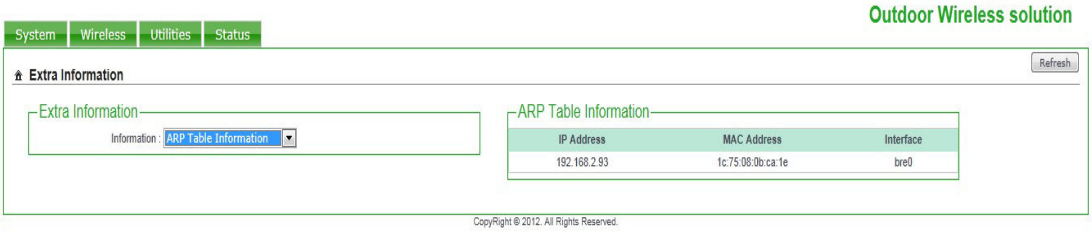
Route Information

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
0.0.0.0	192.168.2.1	0.0.0.0	bre0

CopyRight © 2012. All Rights Reserved.

Extra Information

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.



Extra Information

Extra Information

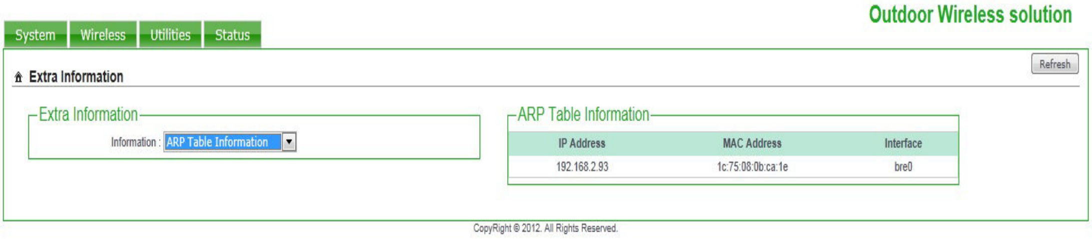
Information : ARP Table Information

ARP Table Information

IP Address	MAC Address	Interface
192.168.2.93	1c:75:08:0b:ca:1e	bre0

CopyRight © 2012. All Rights Reserved.

Route information : Select "**Route table information**" on the drop-down list to display route table. ST58T8 SERIES 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

Extra Information

Information : ARP Table Information

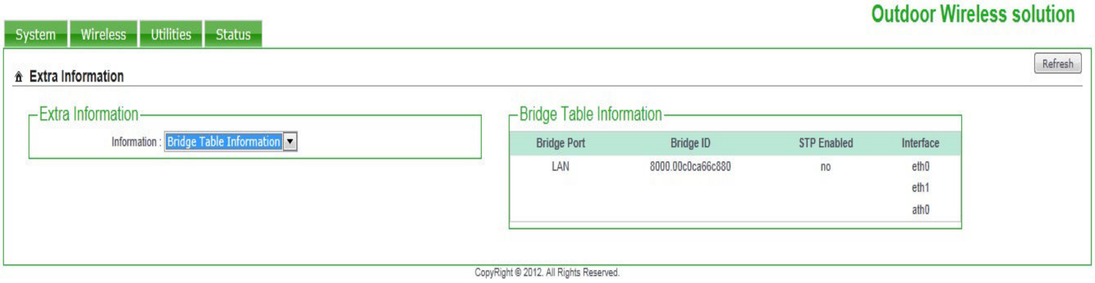
ARP Table Information

IP Address	MAC Address	Interface
192.168.2.93	1c:75:08:0b:ca:1e	bre0

CopyRight © 2012. All Rights Reserved.

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

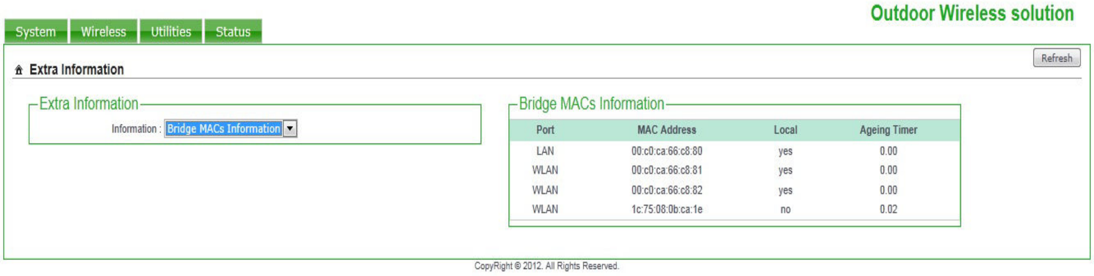
Information : Bridge Table Information

Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
LAN	8000.00c0ca66c880	no	eth0 eth1 ath0

CopyRight © 2012. All Rights Reserved.

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. eth0, eth1 and ath0).



Extra Information

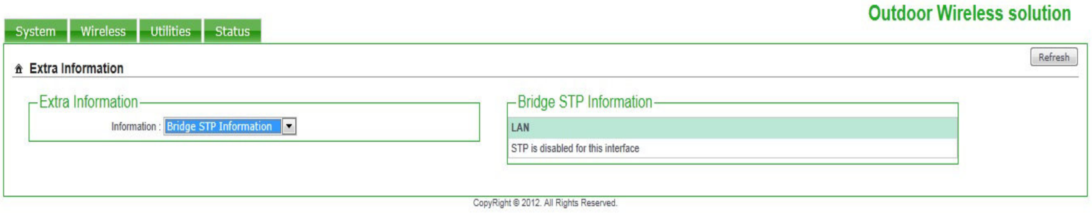
Information : Bridge MACs Information

Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:c0:ca:66:c8:80	yes	0.00
WLAN	00:c0:ca:66:c8:81	yes	0.00
WLAN	00:c0:ca:66:c8:82	yes	0.00
WLAN	1c:75:08:0b:ca:1e	no	0.02

CopyRight © 2012. All Rights Reserved.

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.



Extra Information

Information : Bridge STP Information

Bridge STP Information

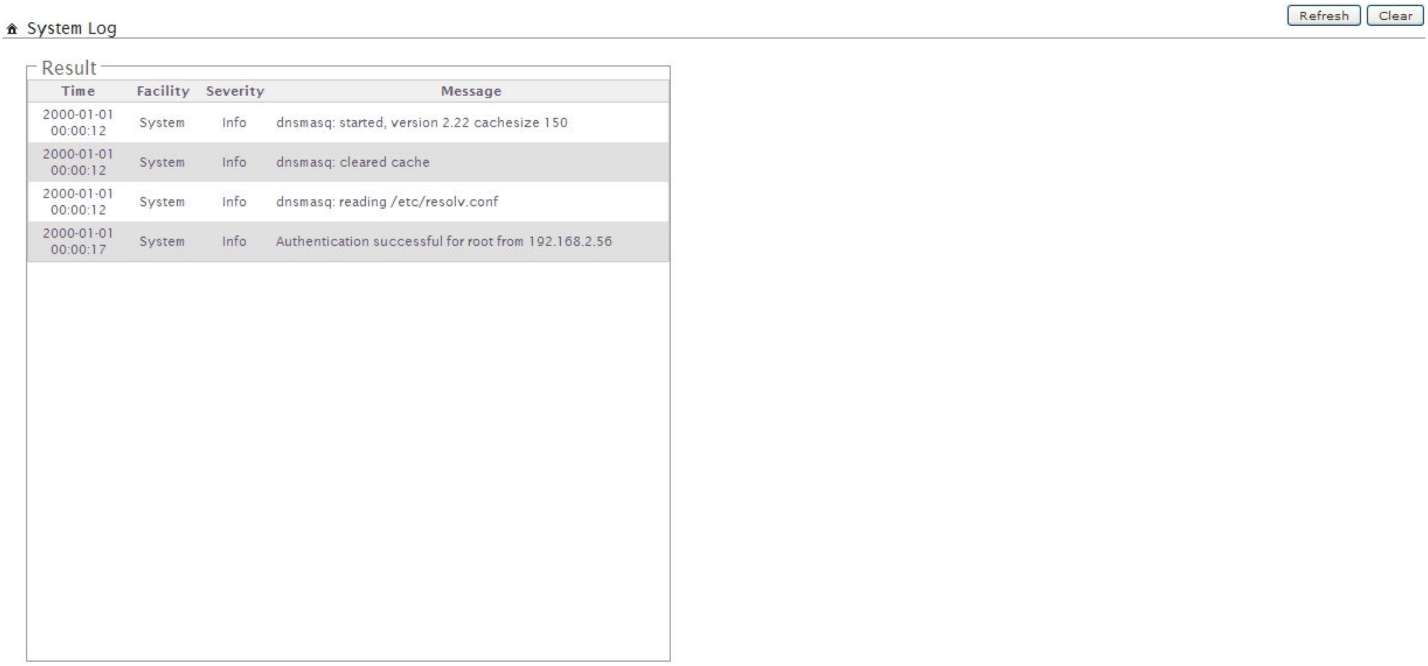
LAN

STP is disabled for this interface

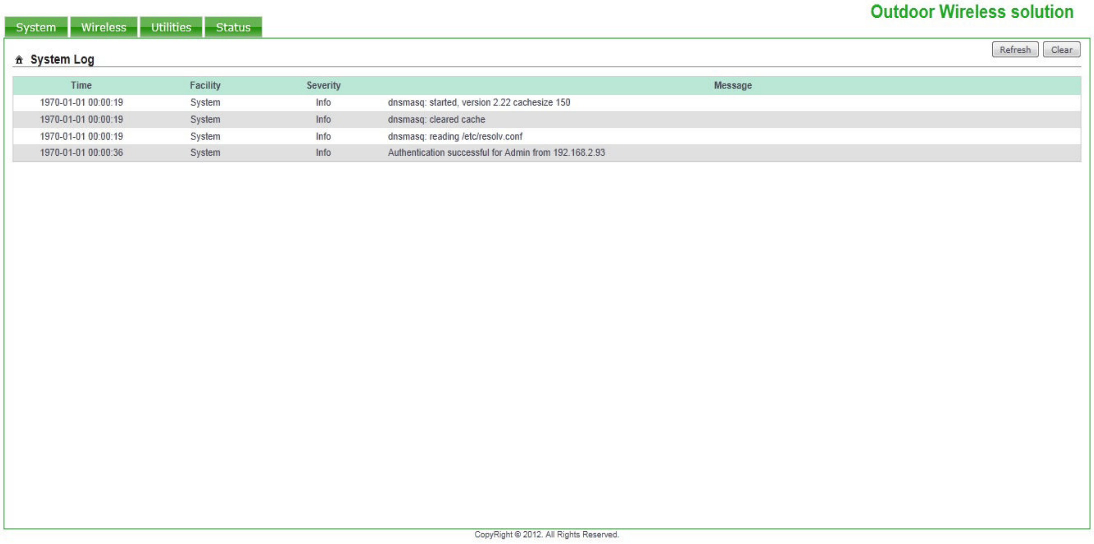
CopyRight © 2012. All Rights Reserved.

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

Event Log



Time	Facility	Severity	Message
2000-01-01 00:00:12	System	Info	dnsmasq: started, version 2.22 cachesize 150
2000-01-01 00:00:12	System	Info	dnsmasq: cleared cache
2000-01-01 00:00:12	System	Info	dnsmasq: reading /etc/resolv.conf
2000-01-01 00:00:17	System	Info	Authentication successful for root from 192.168.2.56


Outdoor Wireless solution
System
Wireless
Utilities
Status
System Log
Refresh
Clear
CopyRight © 2012. All Rights Reserved.

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 00:00:36	System	Info	Authentication successful for Admin from 192.168.2.93

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

Time : The date and time when the event occurred.

Facility : It helps users to identify source of events such “System” or “User”

Severity : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.

Message : Description of the event.

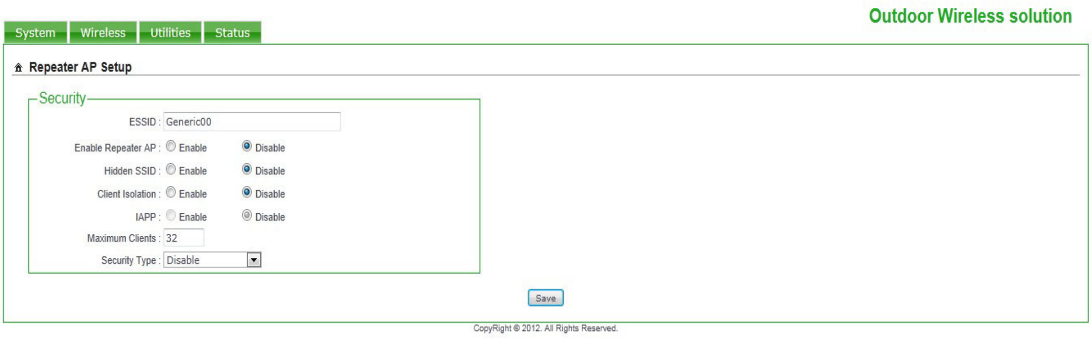
Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

■ Client Bridge + Universal Repeater Configuration

When Client Bridge+Universal Repeater mode is activated, the system can be configured as an **Access Point** and **Client Station** simultaneously. This section provides information in configuring the Client Bridge+Universal Repeater mode with graphical illustrations. ST58T8 SERIES provides functions as stated below where they can be configured via a user-friendly web based interface.

It can be used as an Client Bridge or Universal Repeater to receive and repeat wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, ST58T8 SERIES is enabled with DHCP Server functions. The wired clients of ST58T8 SERIES are in **the same** subnet from Main Base Station and it **accepts** wireless connections from wireless client devices.

When the ST58T8 SERIES 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 ST58T8 SERIES to Main Base Station and wireless client to ST58T8 SERIES, but security type can be different.



Repeater AP Setup

Security

ESSID : Generic00

Enable Repeater AP : ○ Enable ● Disable

Hidden SSID : ○ Enable ● Disable

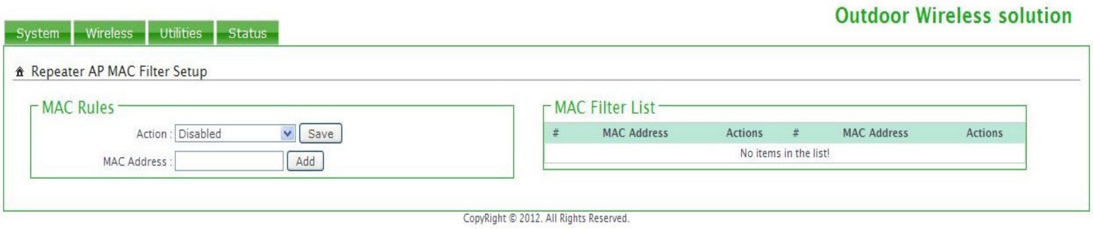
Client Isolation : ○ Enable ● Disable

IAPP : ○ Enable ● Disable

Maximum Clients : 32

Security Type : Disable

CopyRight © 2012. All Rights Reserved.



Repeater AP MAC Filter Setup

MAC Rules

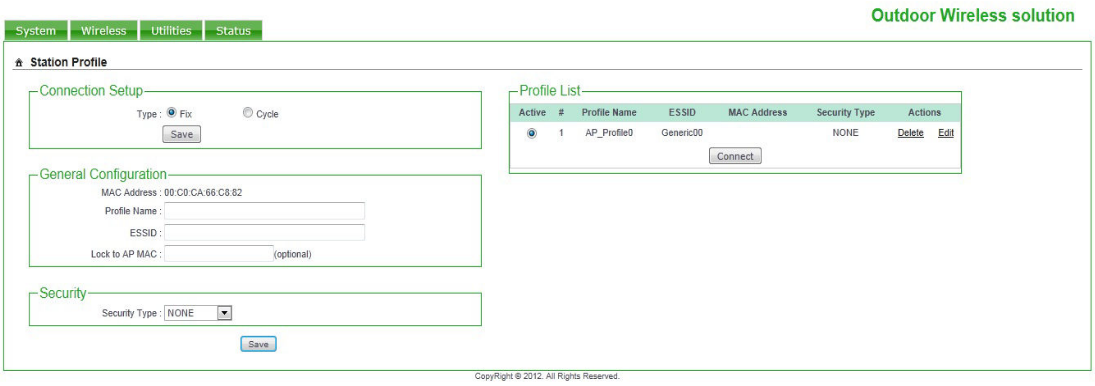
Action : Disabled

MAC Address :

MAC Filter List

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

CopyRight © 2012. All Rights Reserved.



Station Profile

Connection Setup

Type : ● Fix ○ Cycle

Profile List

Active	#	Profile Name	ESSID	MAC Address	Security Type	Actions
●	1	AP_Profile0	Generic00		NONE	Delete Edit

General Configuration

MAC Address : 00:C0:CA:66:C8:82

Profile Name :

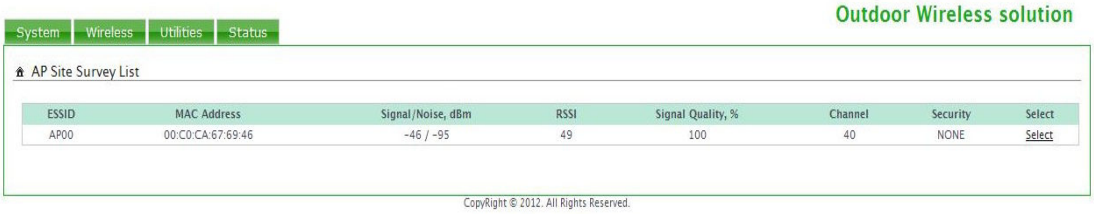
ESSID :

Lock to AP MAC : (optional)

Security

Security Type : NONE

CopyRight © 2012. All Rights Reserved.



AP Site Survey List

ESSID	MAC Address	Signal/Noise, dBm	RSSI	Signal Quality, %	Channel	Security	Select
AP00	00:C0:CA:67:69:46	-46 / -95	49	100	40	NONE	Select

CopyRight © 2012. All Rights Reserved.

Site Survey

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

ESSID : Available Extend Service Set ID of surrounding Access Points.

MAC Address : MAC addresses of surrounding Access Points.

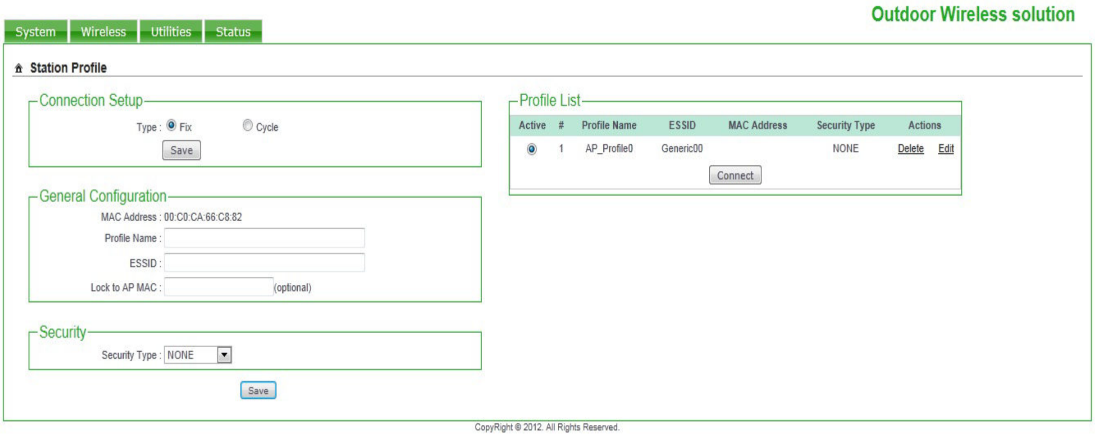
Signal : Received signal strength of all found Access Points.

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 Profile** Setup. However, more settings are needed including Security Key.



Station Profile

Connection Setup

Type : ● Fix ○ Cycle

General Configuration

MAC Address : 00:C0:CA:66:C8:82

Profile Name :

ESSID :

Lock to AP MAC : (optional)

Security

Security Type : NONE

Profile List

Active	#	Profile Name	ESSID	MAC Address	Security Type	Actions
●	1	AP_Profile0	Generic00		NONE	Delete Edit

CopyRight © 2012. All Rights Reserved.

Create Station Profile

The administrator can configure station profiles via this page. Please click on **Wireless -> Station Profile** and follow the below setting.

Connection Setup: Type "Fix" or "Cycle", default is "Fix".
MAC Address : The MAC address of the Wireless Station is displayed here.
Profile Name : Set different profiles for quick connection uses.

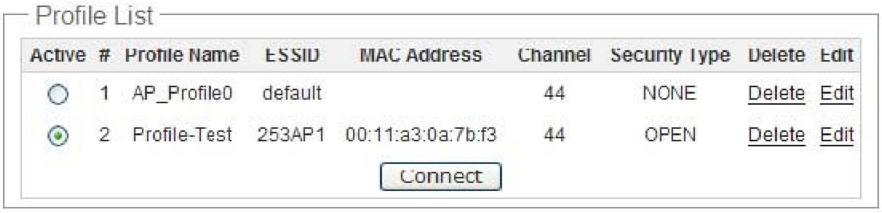
ESSID : Assign Service Set ID for the wireless system.

Lock to AP MAC : This allows the station to always maintain connection to a particular AP with a specific MAC address. This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.

Security Type : Select the desired security type from the drop-down list; the options are "**NONE**""**OPEN**", "**SHARED**", "**WPA-PSK**" and "**WPA2-PSK**".

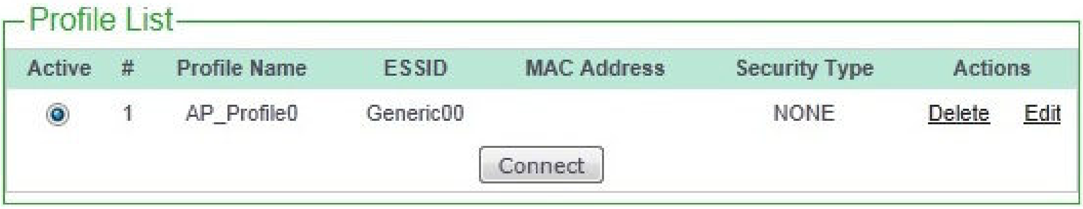
OPEN / SHARED : OPEN and SHARED require the user to set a WEP key to exchange data.

Profile List



Profile List

Active	#	Profile Name	ESSID	MAC Address	Channel	Security Type	Delete	Edit
○	1	AP_Profile0	default		44	NONE	Delete	Edit
●	2	Profile-Test	253AP1	00:11:a3:0a:7b:f3	44	OPEN	Delete	Edit



Profile List

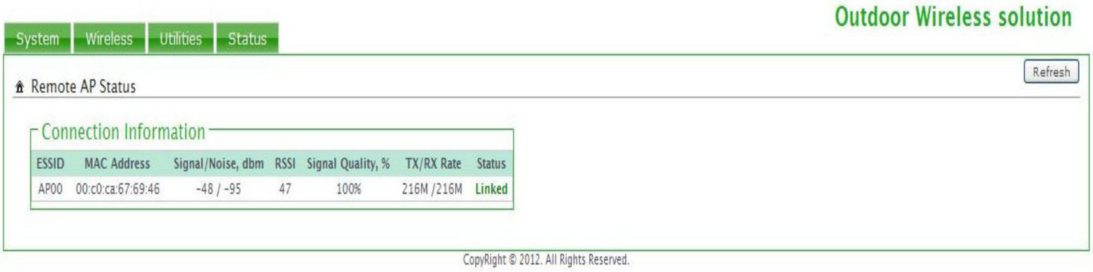
Active	#	Profile Name	ESSID	MAC Address	Security Type	Actions
●	1	AP_Profile0	Generic00		NONE	Delete Edit

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

Click ""**Edit**" an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click "**Save**" button to save the profile.

Click "**Delete**" to remove profile.

Click and Select a profile from list, then click the "**Connect**" button to connecting to the wireless network with the profile setting. After clicking "**Connect**" button, the system should be jump to **Remote AP Page**, you can verify connecting status on **Remote AP Page**.



Remote AP Status

Connection Information

ESSID	MAC Address	Signal/Noise, dbm	RSSI	Signal Quality, %	TX/RX Rate	Status
AP00	00:c0:ca:67:69:46	-48 / -95	47	100%	216M /216M	Linked

CopyRight © 2012. All Rights Reserved.

Remote AP Status

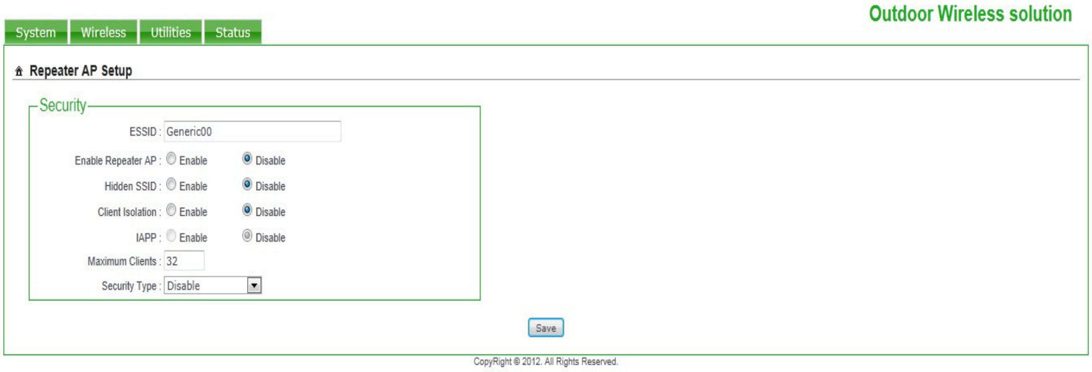
SSID, MAC address and RSSI for associated AP are available.

ESSID : Shows the current ESSID, which must be the same on the wireless client and AP in order for communication to be established.

MAC Address : Display MAC address of associated AP.

RSSI : Shows the wireless signal strength of the connection between system and an access point.

Status : Shows the current link status between system and access point.



Repeater AP Setup

Security

ESSID : Generic00

Enable Repeater AP : ○ Enable ● Disable

Hidden SSID : ○ Enable ● Disable

Client Isolation : ○ Enable ● Disable

IAPP : ○ Enable ● Disable

Maximum Clients : 32

Security Type : Disable

CopyRight © 2012. All Rights Reserved.

Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations and security type settings. Please click on **Wireless -> Repeater AP Setup**.

The Repeater AP Setup page appears.

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's clients associated with the specified AP.

Enable Repeater AP : By default, it's "***Disable***" for repeater AP. Select "***Enable***" to activate Repeater AP or click "***Disable***" to deactivate this function

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's 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.
WMM : Select Enable, the packets with QoS WMM will has higher priority.
IAPP Support : 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.

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