



DG-WM2005SI

300Mbps CEILING MOUNT ACCESS POINT

User Manual

V1.0
2014-07-01

As our products undergo continuous development the specifications are subject to change without prior notice

Table of contents

1. INTRODUCTION.....	6
1.1 PACKAGE CONTENTS.....	6
1.2 HARDWARE INSTALLATION.....	7
1.2.1 WARNING.....	7
1.2.2 SYSTEM REQUIREMENTS.....	8
1.2.3 Hardware Configuration.....	9
1.2.4 Mounting on the Ceiling / Wall.....	10
1.2.5 LED Indicators.....	12
1.2.6 Button Definition.....	14
2.1 EASY SETUP VIA WEB UI.....	19
2.2 USE WEC BUTTON TO SETUP WIRELESS PROFILES.....	24
2.2.1 One Master and several isolated Slaves.....	25
2.2.2 One Master and a series of connected Slaves.....	27
3 MAKING CONFIGURATIONS.....	30
3.1 BASIC NETWORK.....	32
3.1.1 Ethernet LAN.....	33
3.1.2 Wireless.....	34
3.1.2.1 Wireless Setup.....	35
3.1.2.1.1 AP Only Mode.....	35
3.1.2.1.2 WDS Hybrid Mode.....	39
3.1.2.1.3 WDS Only Mode.....	43
3.1.2.1.4 Universal Repeater Mode.....	45
3.1.3 Advanced Wireless Setup.....	48
3.1.3.1 Advanced RF Module1 Settings.....	48
3.1.4 IPv6.....	50
3.2 ADVANCED NETWORK.....	51
3.2.1 Firewall.....	52
3.2.1.1 MAC Address Control.....	52
3.2.2 Management.....	53
3.2.2.1 UPNP.....	53
3.2.2.2 SNMP.....	54

3.3 SYSTEM.....	56
3.3.1 System Information.....	57
3.3.2 System Status.....	57
3.3.2.1 Web Log.....	57
3.3.2.2 Syslog.....	58
3.3.2.3 Email Alert.....	59
3.3.3 System Tools.....	59
3.3.3.1 Change Password.....	59
3.3.3.2 FW Upgrade.....	60
3.3.3.3 System Time.....	61
3.3.3.4 Others.....	62
3.3.4 MMI.....	64
3.3.4.1 Web UI.....	64
4 AP MANAGEMENT SOFTWARE.....	65
4.1 INSTALLATION PROCESS.....	67
4.2 GETTING STARTED.....	68
4.3 AP CONTROLLER UTILITY OVERVIEW.....	75
4.4 STATISTICS.....	80
4.5 AP LIST.....	84
4.6 STATUS.....	88
4.7 CONFIGURATION.....	89
4.8 WiFi CONFIGURATION.....	91
4.9 SYSTEM TOOLS.....	104
4.10 STA USERS.....	106
4.11 PROPOSALS.....	108
4.12 ACCOUNTS.....	110
5 TROUBLESHOOTING.....	113

COPYRIGHT

Copyright 2014 by Smartlink Network Systems Ltd. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

Trademarks:

DIGISOL™ is a trademark of Smartlink Network Systems Ltd. All other trademarks are the property of the respective manufacturers.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

1. Introduction

Congratulations on your purchase of this outstanding product: DG-WM2005SI WiFi 2.4G N 300 Ceiling Mount Access Point is designed for small and medium-sized businesses to extend the existing wired networks and has the ability to operate in different modes which can be used in a wide variety of wireless applications like AP, Point-to-Point and Universal. Repeater mode not only has an easier setup method, but also provides better performance and compatibility to create a virtually larger wireless network infrastructure by linking up other access points.

Supports Multiple-SSID capability to use one Physical AP to simultaneously emulate 8 APs with different ESSIDs by separating their packets via VLAN technology.

1.1 Package Contents

Before using this access point, please check if there is anything missing in the package, and contact your dealer of purchase to claim for missing items:

- DG-WM2005SI Ceiling Mount Access Point
- DC 12V Power Adapter
- Patch Cord
- Installation Guide CD
- Mounting Screws (2 Nylon washers, 2 Screws)

1.2 Hardware Installation

1.2.1 WARNING



Attention

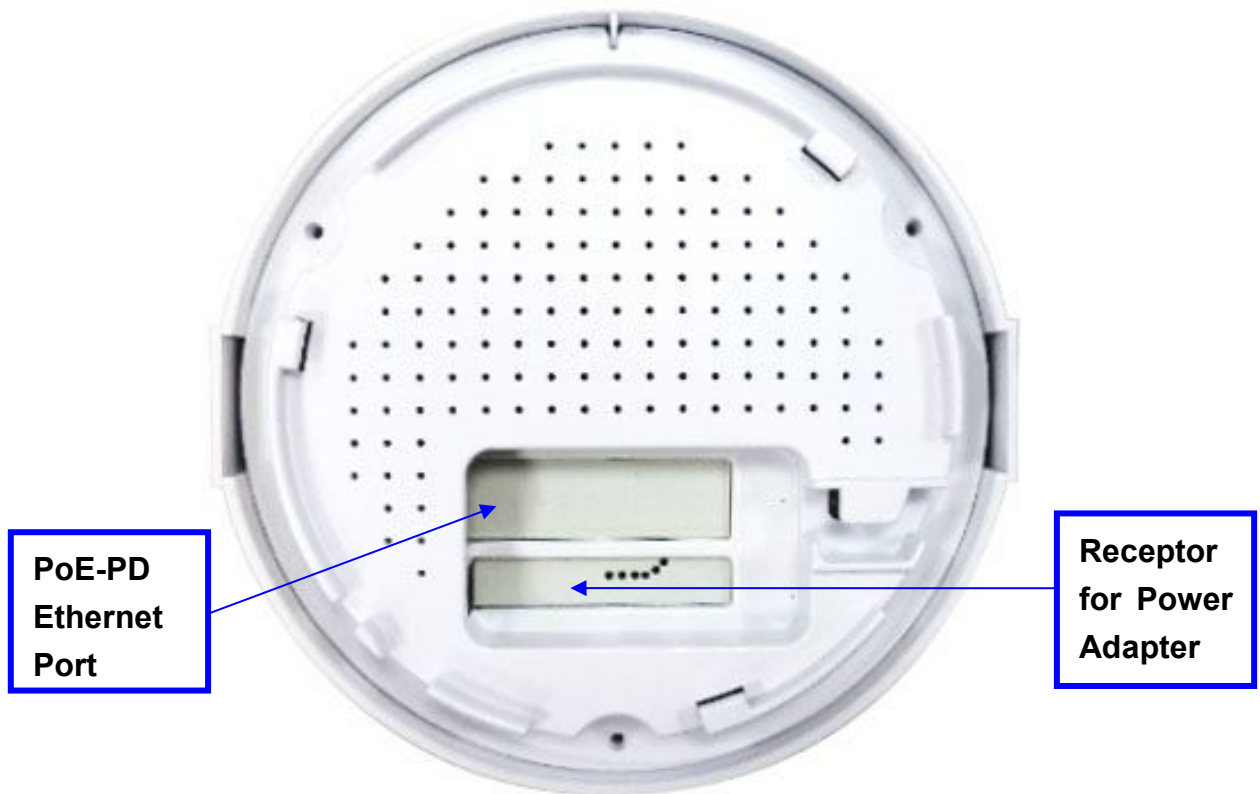
- Do not use the product in high humidity or high temperatures.
- Do not use the same power source for the Product as other equipment. Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the device.
- Do not open or repair the case yourself. If the Product is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Place the Product on a stable surface and avoid using this product and all accessories outdoors.

1.2.2 SYSTEM REQUIREMENTS

Network Requirements	<ul style="list-style-type: none">• An Ethernet-based Cable or DSL modem• IEEE 802.11n or 802.11b, g wireless clients• 10/100 Ethernet
Web-based Configuration Requirements	<p>Computer with the following:</p> <ul style="list-style-type: none">• Windows®, Macintosh, or Linux-based operating system• An installed Ethernet adapter <p>Browser Requirements:</p> <ul style="list-style-type: none">• Internet Explorer 6.0 or higher• Chrome 2.0 or higher• Firefox 3.0 or higher• Safari 3.0 or higher (with Java 1.3.1 or higher) <p>Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.</p>
AP Management Software Installation Requirements	<ul style="list-style-type: none">• PC with windows 7 or XP with service pack 2• An installed Ethernet Adapter

1.2.3 Hardware Configuration

Rear View:

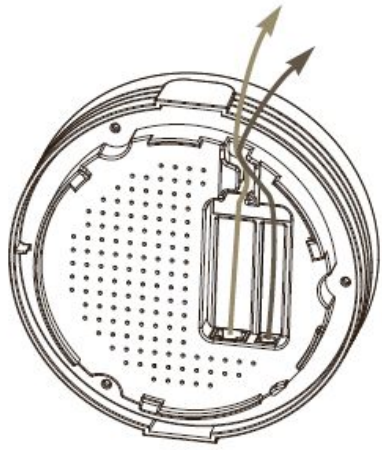
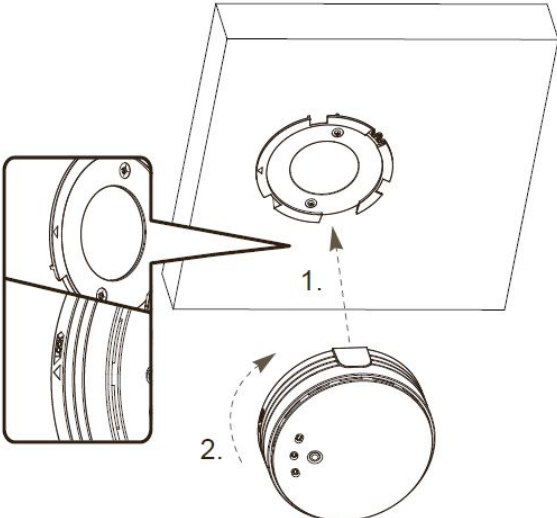
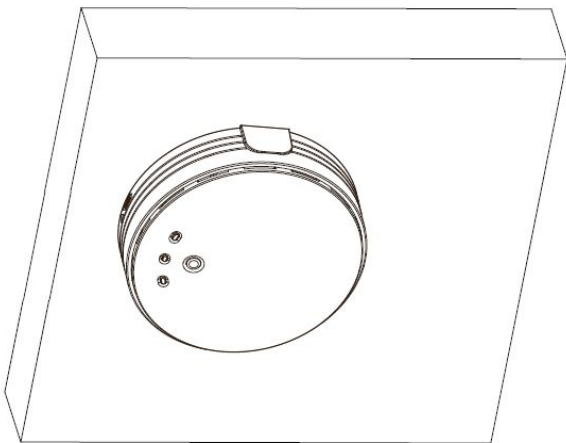


1.2.4 Mounting on the Ceiling / Wall

This device is designed for easily mounting on the ceiling or wall with a simple mount bracket. Before mounting it to the expected location, please make proper configuration for the device setting and run the PoE Ethernet cable to the location in advance.

The following illustrations show you how to mount this device on the ceiling / wall.

	Description	Illustration
A	Drill 2 holes for wall plugs. Self-tapping screws (Diameter : 3mm) If you run the cable above the ceiling (invisible cabling), you have to drill another big hole (about 10~20 mm diameter) to pull out the cable for connecting to the device.	
B	Screw the mounting bracket on the ceiling / wall.	

C	<p>Plug-in the cable (Ethernet cable, Power cord) to the connectors in the button side. Run the cables upward to proper location.</p>	
D	<p>Attached this device to mounting bracket by rotating it clock wisely to click into place.</p>	
E	<p>Installation completed.</p>	

1.2.5 LED Indicators



LED	Description
Status	When the device is booted up and ready: When WEC/Reset is triggered (with button pressed): Status LED flashes at different rate depending on how long the button is pressed Stage 1 (1 ~ 5 sec) : Flashes very fast Stage 2 (6 ~ 10 sec) : Flashes twice per second Stage 3 (11~15 sec) : Flashes once per second Stage 4 (16~30 sec) : Solid Green
	OFF: The device is powered off.
WiFi	<p>Green LED : Device is in Master Mode</p> <p>Amber LED: Device is in Slave Mode</p> LED flash: Data packet transferred. LED in fast flash per second during 2min: WPS PBC status OFF: Wireless Radio is disabled. LED in slow flash or Flash Green and Amber Alternately : Wireless

	Connection doesn't establish. LED in Solid: Wireless Connection established successfully.
LAN	OFF: No Ethernet connection. Solid Green: Ethernet connection is linked up. Flash Green: Data packet is transferred over the Ethernet link.

1.2.6 Button Definition

There is one multi-function push button “WEC/Reset” in this device. According to different button pressed duration, the device will take specific reaction. For ease of interacting with the device, you can also check the Status and WiFi LED to determine when to release the button. The Reset/WEC button behavior is defined below:

Function	Button	Description
Easy Configuration (Master to Slave)	WEC/Reset (Press 3 sec)	<p>There are two alternative AP modes defined for the device to operate with WEC (Wireless Easy Connection) feature. One is Master Mode (by default), and the other is Slave Mode.</p> <p>Please manually configure the Wireless Setting for the Master AP through web UI first, and also prepare a Slave AP that already been set to Slave Mode.</p> <p>Press the WEC/Reset button of the Master AP for 1~3 seconds, release it to trigger the WEC process. Then, WiFi Green LED flashes fast.</p> <p>Press the WEC/Reset button of the Slave AP for 1~3 seconds, release it to trigger the WEC process. Then, WiFi Amber LED flashes fast.</p> <p>Note: The Slave AP must be an un-configured one, if it has already been paired and configured before, please reset its Slave configuration first.</p> <p>After a few seconds (normally about 30~60 seconds). The Master and Slave APs can be paired automatically, and auto-duplicates the VAP1 wireless setting of the Master AP as that of the Slave AP.</p> <p>(If there is something wrong during paring the two devices, the process will be finished in 2 minutes.)</p> <p>Once the easy configuration process has completed, the Status LED will be recovered to its original behavior (prior to triggering). And the WiFi LED will be solid</p>

		when slave AP is connected to the network.
Easy Configuration (Slave to Slave)	WEC/Reset (Press 3 sec)	<p>Besides the above “Master to Slave” configuration, the easy configuration process also supports “Slave to Slave” configuration.</p> <p>Press the WEC/Reset button of the first Slave AP (say Slave1 that has been paired and configured) for 1~3 seconds, release it to trigger the WEC process. Then, the WiFi LED flashes fast.</p> <p>Press the WEC/Reset button of the second Slave AP (say Slave2 that is an un-configured Slave AP) for 1~3 seconds, release it to trigger the WEC process. Then, the WiFi LED flashes fast.</p> <p>After a few seconds (normally about 30~60 seconds). The Slave1 and Slave2 APs can be paired automatically, and auto-duplicates the wireless setting of the Slave1 as that of the Slave2.</p> <p>(If there is something wrong during paring the two devices, the process will be finished in 2 minutes.)</p> <p>Once the easy configuration process completed, the Status LED will be recovered to its original behavior (prior to triggering).</p>
AP Mode Toggling	WEC/Reset (Press 8 sec)	<p>There are two alternative AP modes defined for the device to operate with WEC (Wireless Easy Connection) feature. One is Master Mode (by default), and the other is Slave Mode.</p> <p>To change the AP mode from one to the other, you have to:</p> <p>Press the WEC/Reset button for 6~10 seconds, and then release it.</p> <p>The WiFi LED becomes OFF in 3 ~ 5 seconds, After about 20 ~ 25 seconds, the WiFi LED will be lit ON again to indicate that the AP Mode is changed.</p>

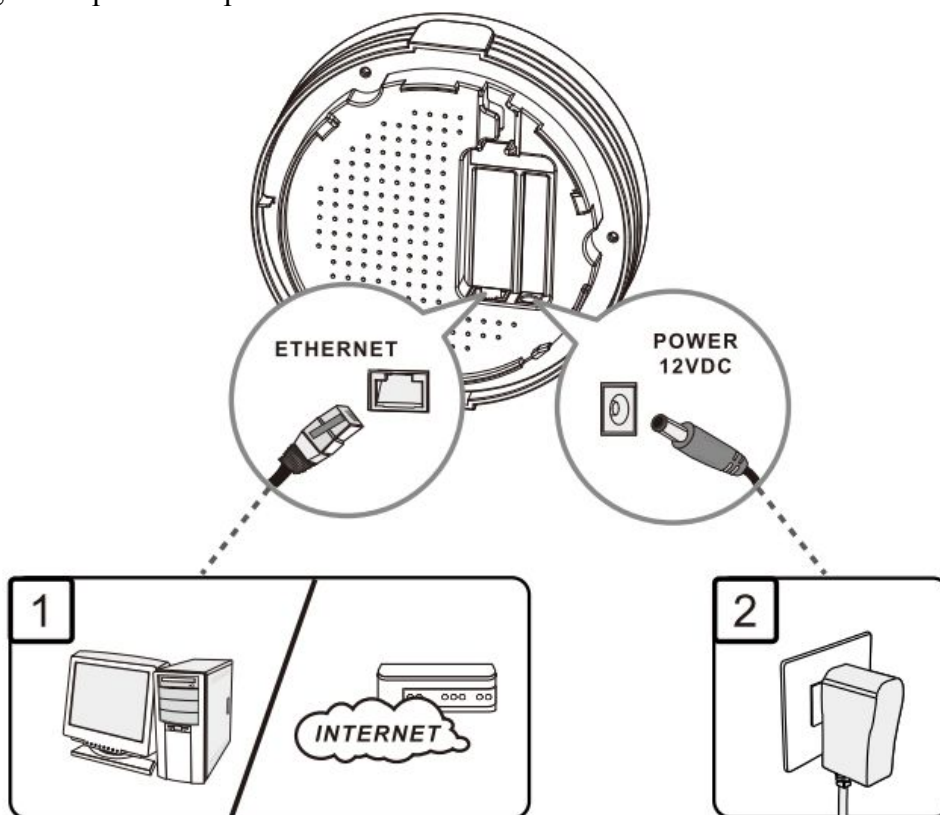
		<p>It takes about 36 seconds to change (toggle) the AP Mode completely.</p> <p>WiFi Green LED : Device is in Master Mode</p> <p>WiFi Amber LED: Device is in Slave Mode</p>
Reset Slave AP Configuration	WEC/Reset (Press 13 sec)	<p>Press the WEC/Reset button for about 11~15 seconds and release it.</p> <p>The Slave AP will be marked as an un-configured device, so that it can be paired with another Master or configured Slave AP later.</p> <p>For Master AP, there is no effect on the behavior of this button.</p>
Reset to Default	WEC/Reset (Press 20 sec)	<p>Press the Reset/WEC button for about 20 seconds till the Status LED becomes solid Green to indicate that the reset to default function is triggered. Release the button.</p> <p>Then, the device will reboot automatically and apply the factory default settings as well.</p> <p>It takes about 2 minutes to finish the reset to factory default operation.</p>

2. Getting Started

Before you can install this product to designated location and make it operate properly, you have to configure the device setting to fit in your network environment.

Hardware Preparation:

- a. Connect an Ethernet cable between this device and the computer that you will operate to set up the device.
- b. Power on the device by connecting the power adapter DC Plug to the DC Jack of this device and plug in the power adapter to an electrical outlet.



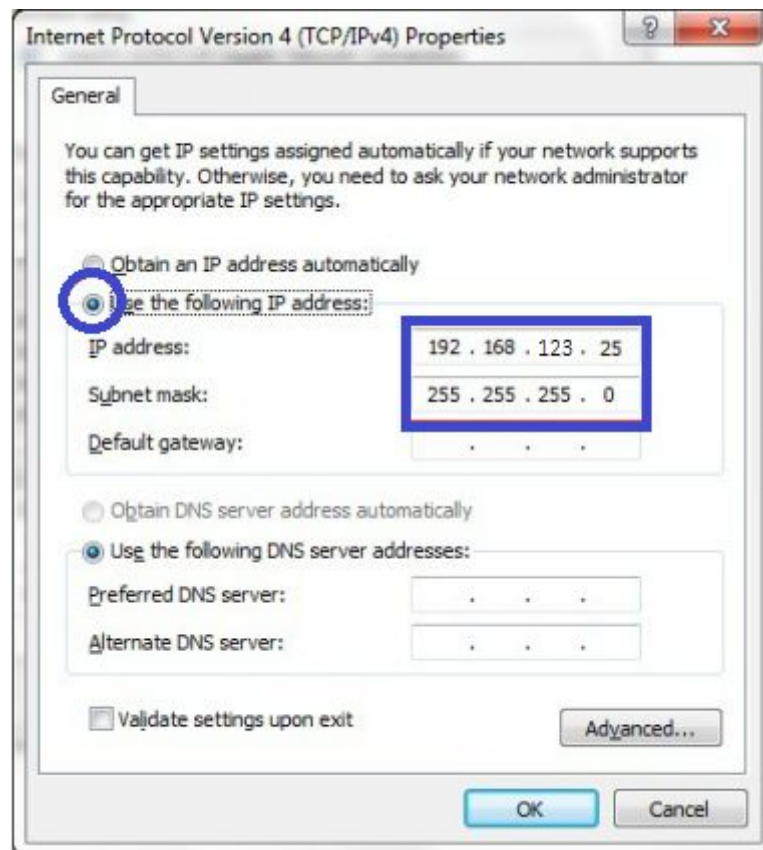
Software Preparation:

Most computers are connecting to a local network with dynamic IP (DHCP) setting. To access the web UI of the device, you have to change your computer's TCP/IPv4 settings into a static IP setting for the Ethernet Interface. You can refer to Appendix A for how to assign a Static IP address to your computer.

The device's default IP address is 192.168.123.50, and your computer must be assigned with a

192.168.123.x IP address to get access to the device.

Referring to Appendix A, set the TCP/IPv4 address of your computer to 192.168.123.25, and subnet mask to 255.255.255.0.



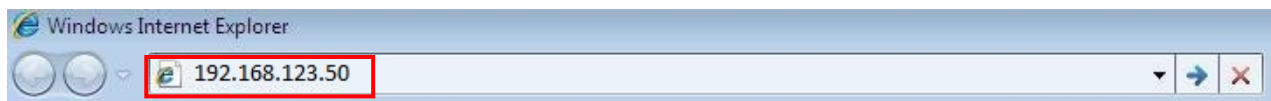
After applying this setting, you can now access the web UI for configuring the device.

2.1 Easy Setup via Web UI

You can browse web UI to configure the device. Firstly you need to launch the Setup Wizard browser first and then the Setup Wizard will guide you step-by-step to finish the basic setup process.

Activate the setup wizard:

Type in the IP Address (**http://192.168.123.50**)



Type the default password “**admin**” in the system authentication fields, and then click ‘**login**’ button.



Select “**Wizard**” for basic settings in a simple way or, you can go to **Basic Network / Advanced Network / System** to setup the configuration by your own selection.



The screen shown below will appear.



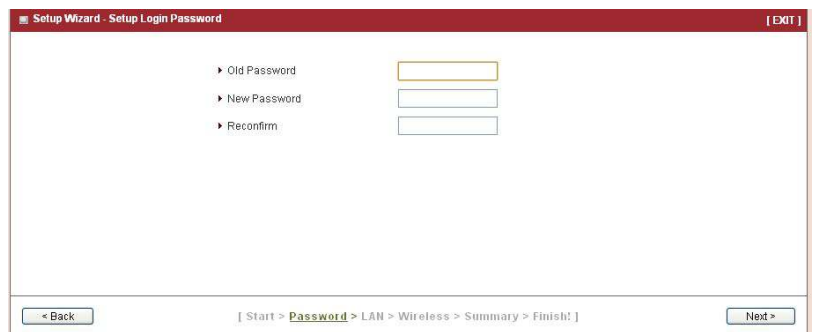
Press **“Wizard”** to start the Setup Wizard. Click on **“Next”**.



Configure with the Setup Wizard

Step 1

You can change the password of administrator here.



Step 2

LAN IP Address.

You have to change the IP address of this device according to your network configuration.



Step 3

Wireless settings.

You can specify the Wireless setting for VAP1.

Step 4

Wireless settings.

Specify VAP1's wireless authentication and encryption.

Step 5

Check the information again.

[Wireless Setting]	
Wireless	Enable
SSID	DG-WM2005SI
Channel	Auto
Authentication	Auto (Open/Shared)
Encryption	None

Step 6

System is applying the setting.

Step 7

Click finish

Setup Wizard - Apply settings

[EXIT]

Configuration is Completed.

Please click "Finish" to back to Status page.

LAN IP Address is changed, please reconnect manually.

< Back

[Start > Password > LAN > Wireless > Summary > **Finish**]

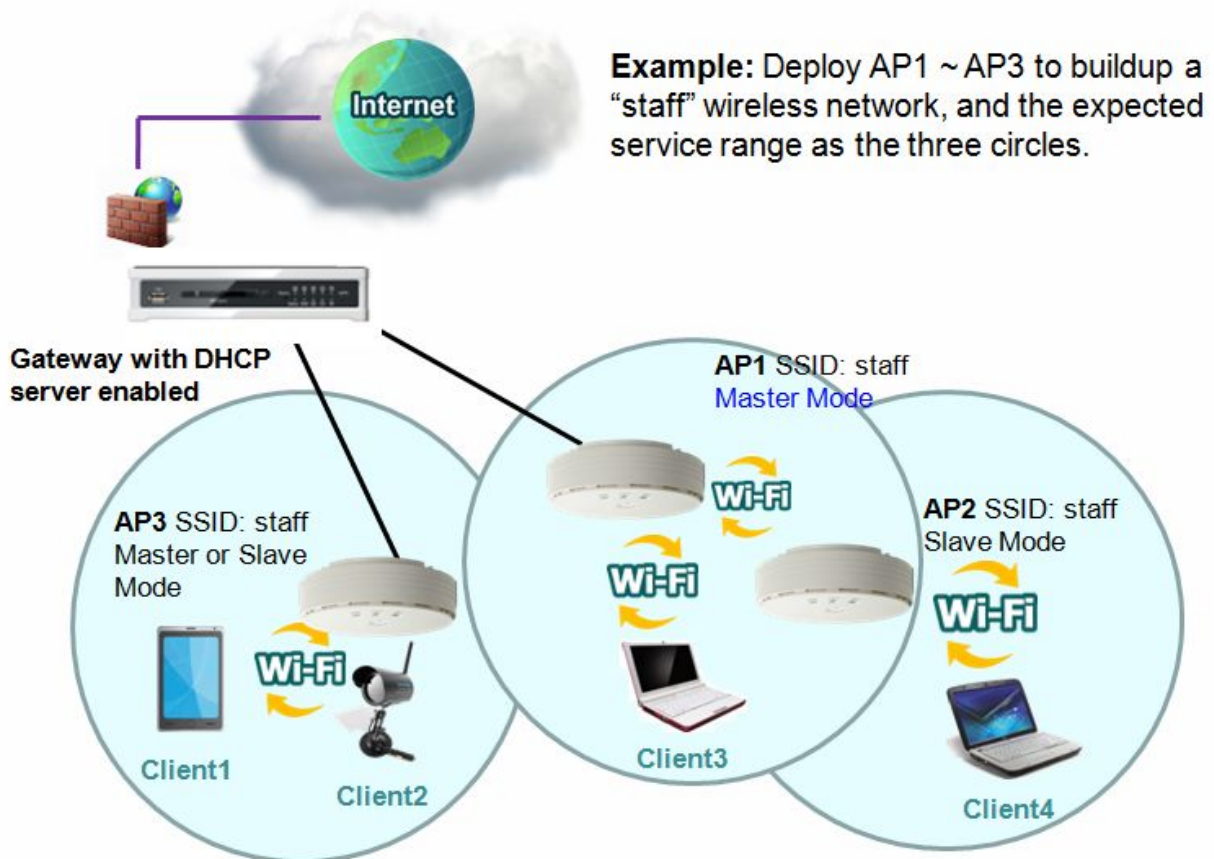
Finish

2.2 Use WEC Button to Setup Wireless Profiles

WEC (Wireless Easy Connection) is an easy configuration feature that is similar to well-known WPS function. It can be used to duplicate one device's wireless configuration to the other AP devices from the same manufacturer by clicking one button for both devices.

There are two alternative AP modes defined for the device to operate with WEC (Wireless Easy Connection) feature. One is the Master Mode (by default), and the other is the Slave Mode. Before starting to use WEC to configure your AP devices, you have to learn how to identify and set the device in the Master Mode, or the Slave Mode.

2.2.1 One Master and several isolated Slaves



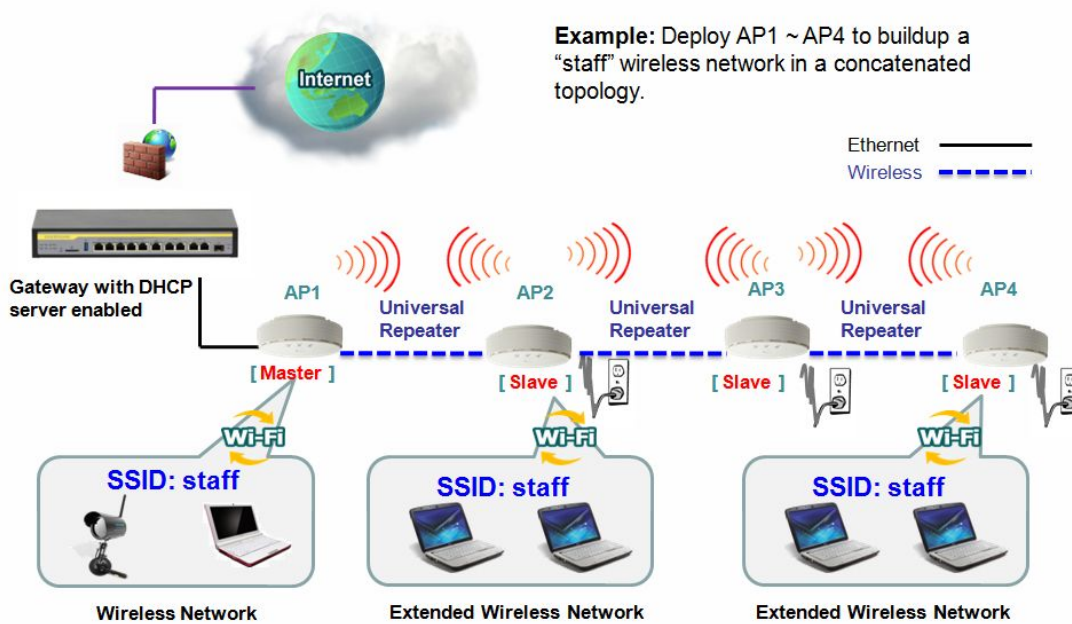
As illustrated in the above figure, how to configure the three APs (AP1, AP2, AP3) to build up the “staff” wireless network. You can follow the procedure mentioned below:

Step	Button	Description
1	Set AP1 in Master Mode, and configure it via web UI.	<ol style="list-style-type: none"> 1. Make sure AP1 is in Master Mode (WiFi LED should be “Green” color, if not, you have to toggle its AP mode by pressing the WEC button for 9~10 seconds) 2. Login in to AP1 web UI and configure the wireless settings as what you want (LAN IP, SSID, encryption key, etc.)
2	Set AP2 and AP3 in Slave Mode.	<ol style="list-style-type: none"> 1. Make sure AP2 / AP3 is in Slave Mode (WiFi LED should be “Amber” color, if not, you have to toggle its AP mode by pressing the WEC button for 9~10 seconds)
3	Easy configure AP2 via WEC.	Master to Slave WEC: <ol style="list-style-type: none"> 1. Trigger AP1 into WEC configuration process by pressing the WEC button for 3 second. 2. Trigger AP2 into WEC configuration process by pressing the WEC button for 3 second. 3. It takes 30 ~ 60 seconds for the device to finish the WEC configuration process.
4	Easy configure AP3 via WEC.	Master to Slave WEC: <ol style="list-style-type: none"> 1. Trigger AP1 into WEC configuration process by pressing the WEC button for 3 second. 2. Trigger AP3 into WEC configuration process by pressing the WEC button for 3 second. 3. It takes 30 ~ 60 seconds for the device to finish the WEC configuration process.
5	Mount the devices AP1,	<ol style="list-style-type: none"> 1. Install AP1 to its location first and verify its wireless

	<p>AP2 and AP3 to expected locations.</p>	<p>network connectivity with a client device (Client3).</p> <ol style="list-style-type: none"> 2. Install AP2 to its location and verify its wireless network connectivity with a client device (Client4) at the location beyond the service range of AP1. Besides, you can also check the AP2's WiFi LED, it should be "Solid Amber" if AP2 already connected to a Master AP AP1. 3. Install AP3 to its location and verify its wireless network connectivity with a client device (Client1) at the location beyond the service range of AP1. In this case, AP3 is located out of the service range of AP1, you don't have to check AP3's WiFi LED, but you have to connect the AP3 with an Ethernet cable to the gateway.
--	---	---

2.2.2 One Master and a series of connected Slaves

This device also supports universal repeater function, you can easily extend the wireless network with a series of repeaters that are wirelessly concatenated to build up the wireless network without running Ethernet cables to each repeater.



As illustrated in above figure, if you intend to deploy 4 APs (AP1 ~ AP4) to create a “Staff” wireless network, you can follow the procedure below:

Step	Button	Description
1	Set AP1 in Master Mode, and configure it via web UI.	Make sure AP1 is in Master Mode (WiFi LED should be “Green” color, if not, you have to toggle its AP mode by pressing the WEC button for 8 seconds). Login in to AP1 web UI and configure the wireless settings as what you want (LAN IP, SSID, encryption key, etc).
2	Set AP2, AP3, AP4 in Slave Mode.	Make sure AP2 / AP3 / AP4 is in Slave Mode (WiFi LED should be “Amber” color, if not, you have to toggle its AP mode via pressing the WEC button for 8 seconds)
3	Easy configure AP2 via WEC.	Master to Slave WEC: Trigger AP1 into WEC configuration process by pressing the WEC button for 3 second. Trigger AP2 into WEC configuration process by pressing the WEC button for 3 second. It takes 30 ~ 60 seconds for the device to finish the WEC configuration process.
4	Easy configure AP3 via WEC.	Slave to Slave WEC: Trigger AP2 into WEC configuration process by pressing the WEC button for 3 second. Trigger AP3 into WEC configuration process by pressing the WEC button for 3 second. It takes 30 ~ 60 seconds for the device to finish the WEC configuration process.
5	Easy configure AP4 via WEC.	Slave to Slave WEC: Trigger AP3 into WEC configuration process by

		<p>pressing the WEC button for 3 second.</p> <p>Trigger AP4 into WEC configuration process by pressing the WEC button for 3 second.</p> <p>It takes 30 ~ 60 seconds for the device to finish the WEC configuration process.</p>
6	<p>Mount the devices AP1, AP2, AP3, and AP4 to expected locations.</p>	<p>Install AP1 to its location first and verify its wireless network connectivity with a client device.</p> <p>Install AP2 to its location and verify its wireless network connectivity with a client device at the location beyond the service range of AP1.</p> <p>Besides, You can also check the AP2's WiFi LED, it should be "Solid Amber" if AP2 already connected to a Master AP AP1.</p> <p>Install AP3 to its location and verify its wireless network connectivity with a client device at the location beyond the service range of AP2.</p> <p>Besides, You can also check the AP3's WiFi LED, it should be "Solid Amber" if AP3 already connected AP2.</p> <p>Install AP4 to its location and verify its wireless network connectivity with a client device at the location beyond the service range of AP3.</p> <p>Besides, You can also check the AP4's WiFi LED, it should be "Solid Amber" if AP4 already connected to a AP3.</p>

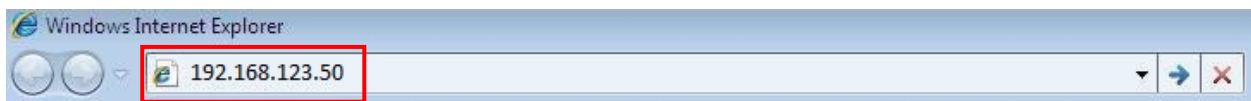
Although such wireless repeater function is available, there are limitations for such topology.

First, the available bandwidth for AP2 ~ AP4 will be decayed since it is connected to its peer AP wirelessly. It depends on the data rate and environment. Besides, if one of the AP, say AP2, is disconnected, the AP's behind it will be disconnected as well. Such topology needs more maintenance effort to keep the whole wireless network connectivity.

If Ethernet cable is reachable, connecting each AP to an Ethernet Uplink is recommended. Above WEC configuration process is also suitable for running Ethernet cables to AP2 ~ AP4 to get a better wireless network.

3 Making Configurations

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the device. The default IP Address is: 192.168.123.50. In the configuration section you may want to check the connection status of this device, to do Basic or Advanced Network setup or to check the system status. These task buttons can be easily found in the cover page of the UI (User Interface).



Enter the default password “**admin**” and then click ‘**login**’ button.



The screenshot shows the web interface for the DIGISOL DG-WM2005SI device. The top header includes the DIGISOL logo, the device model "DG-WM2005SI", and the SSID "DG-WM2005SI" and FW Version "BMQM0.1005_06101700".

On the left side, there is a login section with a "Password:" label, a text input field, a "Login" button, and the text "(default: admin)".

The main content area features a central graphic of a wireless router with a "Client:0" indicator. Below this are two tables:

IPv4 System Status [HELP]		
Item	LAN Status	Sidenote
IP Address	192.168.123.50	Static IP
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	

Statistics Information		
	Receive	Transmit
LAN	437 Packets	698 Packets
WLAN	0 Packets	0 Packets

At the bottom of the main content area, there is a "Refresh" button and the text "Device Time: Thu, 01 Jan 1970 00:10:55 +0000".

Afterwards, you can go Wizard, Basic Network, Advanced Network, Application or System respectively on left hand side of web page.

SSID : DG-WM2005SI
FW Version : BMQM0.1005_06101700

Logout

IPv4 System Status [HELP]

Item	LAN Status	Sidenote
IP Address	192.168.123.50	Static IP
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	<input type="button" value="Edit"/>

Statistics Information

	Receive	Transmit
LAN	203 Packets	257 Packets
WLAN	0 Packets	0 Packets

Device Time: Thu, 01 Jan 1970 00:06:27 +0000

Note: You can see the Connection Status screen below after you log in.

Wireless Module AP 1		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	DG-WM2005SI	<input type="button" value="Edit"/>
Channel	Auto	
Security	Auto	(None)
MAC address	00:17:7C:37:1C:A0	

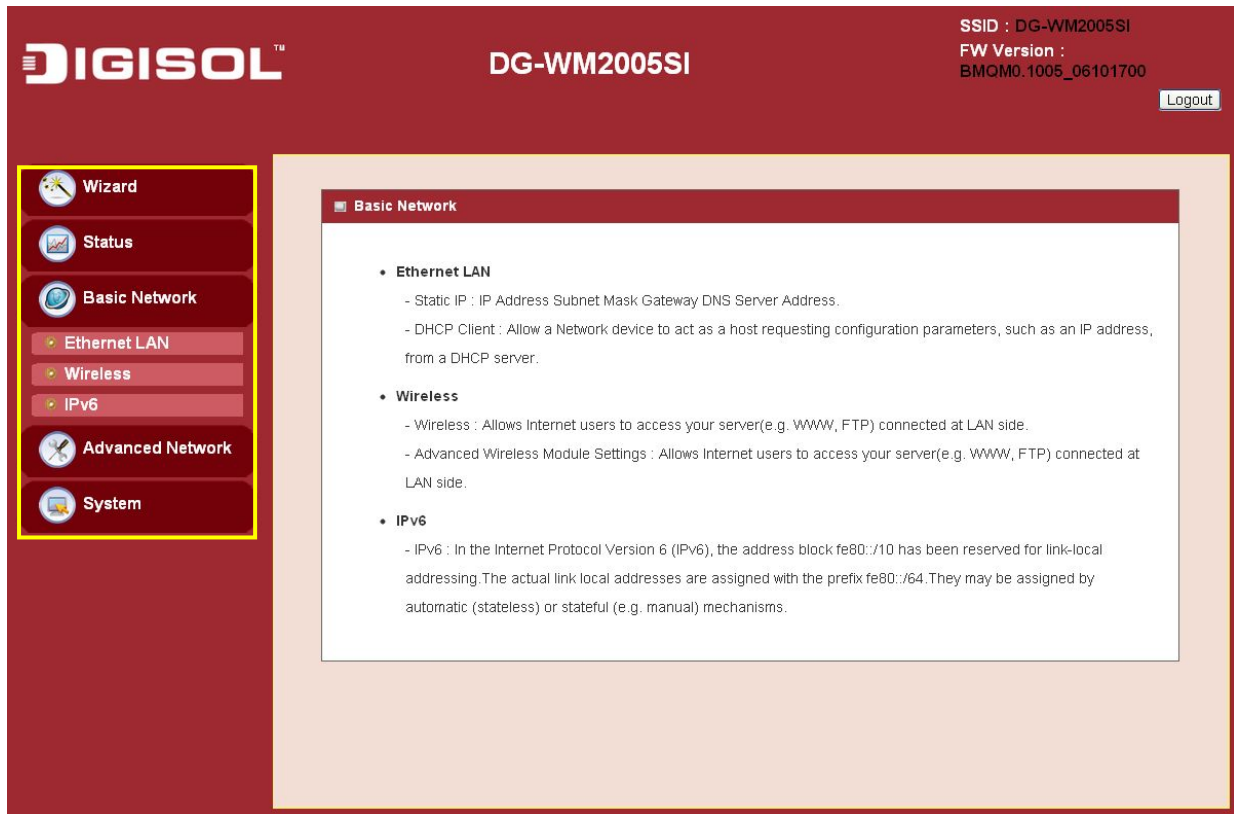
Wireless Module AP 2		
Item	WLAN Status	Sidenote
Wireless mode	Disable	(B/G/N Mixed)
SSID	default	<input type="button" value="Edit"/>
Channel	Auto	
Security	Open	(None)
MAC address	02:17:7C:37:1C:A0	

Wireless Module AP 3		
Item	WLAN Status	Sidenote
Wireless mode	Disable	(B/G/N Mixed)
SSID	default	<input type="button" value="Edit"/>
Channel	Auto	
Security	Open	(None)
MAC address	06:17:7C:37:1C:A0	

Note: You can see the status of this device in the 'Status' main menu section.

3.1 Basic Network

You can enter Basic Network for Ethernet LAN, Wireless and IPv6 settings in this web page.



3.1.1 Ethernet LAN

▶ Ethernet LAN

■ Device Network Type

Item	Setting
▶ Device Network Type	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
▶ LAN IP Address	<input type="text" value="192.168.123.50"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0"/> ▼
▶ Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>

1. **Device Network Type:** This device supports two network types for connecting to your local network.

Static IP: Allow a device to act as a Static host. If you need Static host please enter IP Address.

DHCP: Allow a device to act as a host requesting configuration parameters, such as an IP address from a DHCP server.

Note: Please check if there is DHCP server in your Network, first.

2. **LAN IP Address, Subnet Mask, Gateway, Primary / Secondary DNS:** If you selected the Static IP network type for this device, you have to further specify the LAN IP Address, Subnet mask, Gateway and optional Primary / Secondary DNS settings for connecting to your local network.

3.1.2 Wireless

Wireless settings allow you to set the WLAN (wireless LAN) configuration items. When the wireless configuration is done, your wireless network is ready for supporting your local WiFi devices such as your laptop PC, wireless printer and some portable devices.

SSID : DG-WM2005SI
FW Version :
BQM0.1005_06101700

Logout

Wizard
Status
Basic Network
Ethernet LAN
Wireless
IPv6
Advanced Network
System

Wireless Module Advanced Wireless Module Settings

Item	Setting
Wireless Module	<input checked="" type="checkbox"/> Enable
Wireless Operation Mode	AP Only Mode
Green AP	<input type="checkbox"/> Enable
AP Number	AP 1 <input checked="" type="checkbox"/> Enable
Network ID(SSID)	DG-WM2005SI
SSID Broadcast	<input checked="" type="checkbox"/> Enable
VLAN ID	<input type="checkbox"/> Enable 3 (3~4094)
Max Supported Stations	<input type="checkbox"/> Enable (1~16)
WLAN Partition	<input type="checkbox"/> Enable
Channel	Auto
Wireless Mode	B/G/N mixed
Bandwidth	Auto
Authentication	Auto
Encryption	None

Save Undo WPS Setup... Wireless Client List...

The embedded RF Module1 is an IEEE 802.11b/g/n compliant 2.4GHz Wireless Module.

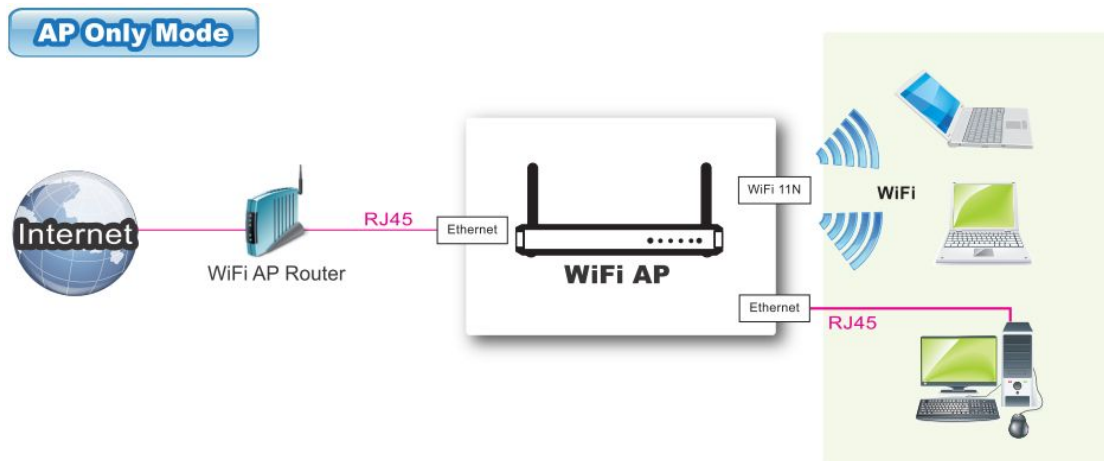
3.1.2.1 Wireless Setup

There are several wireless operation modes provided by this device. They are: “AP Only Mode”, “WDS Hybrid Mode”, “WDS Only Mode” and “Universal Repeater Mode”. You can choose the expected mode and configure the device manually.

Besides manually configuring the devices to be deployed one by one, you can also configure your devices via the simple WEC configuration approach as stated in last Chapter. By default,

the Master AP is set to the WDS-hybrid Mode, and the Slave APs are set to the Universal Repeater mode. You just have to manually configure the Master AP via the web UI configuration, and use the WEC process for the rest Slave APs.

3.1.2.1.1 AP Only Mode



When acting as an access point, this device connects all the wireless stations to a wired network.

Wireless Setting [HELP]	
Item	Setting
▶ Wireless Module	<input checked="" type="checkbox"/> Enable
▶ Wireless Operation Mode	AP Only Mode
▶ Green AP	<input type="checkbox"/> Enable
▶ AP Number	AP 1 <input checked="" type="checkbox"/> Enable
▶ Network ID(SSID)	DG-WM2005SI
▶ SSID Broadcast	<input checked="" type="checkbox"/> Enable
▶ VLAN ID	<input type="checkbox"/> Enable 3 (3~4094)
▶ Max Supported Stations	<input type="checkbox"/> Enable (1~16)
▶ WLAN Partition	<input type="checkbox"/> Enable
▶ Channel	Auto
▶ Wireless Mode	B/G/N mixed
▶ Bandwidth	Auto
▶ Authentication	Auto
▶ Encryption	None

1. **Wireless Module:** Enable the wireless function.
2. **Wireless Operation Mode:** Choose “**AP Only Mode**” from the list.
3. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
4. **AP Number:** This device supports up to 8 SSIDs at the same time for you to manage your wireless networks. You can select AP1 ~ AP8 and configure each wireless network individually.
5. **Network ID (SSID):** Network ID is used for identifying a Wireless LAN. Client stations can roam freely over this device and other Access Points that have the same Network ID. The factory default SSID is “default”, you can change it to a meaningful identifier for the wireless users to easy find it out.
6. **SSID Broadcast:** By default, the SSID Broadcast setting is “Enable”, and the device will broadcast beacons that have some information, including SSID, to the air, so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, you can hide the wireless network from been scanned by wireless clients. Those who know the SSID can manually specify the SSID on their client device to connect the hidden wireless network.
7. **VLAN ID:** This device supports mapping of a SSID to a certain VLAN ID to separate workgroups across wireless and wired domains. By default, it is not enabled. If you enabled this function, you have to specify a VLAN ID for the wireless network.
8. **Max Supported Stations:** You can specify the number of maximum stations that can associate to the SSID simultaneously.
9. **WLAN Partition:** WLAN Partition: You can check the WLAN Partition function to separate the wireless clients associated to the same VAP. The wireless clients can't communicate with each other, but they can access the internet and other Ethernet LAN devices.
10. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection. It's recommended to choose a channel that is not used in your environment to reduce radio interference.
11. **Wireless Mode:** The RF1 module supports 802.11b/g/n modes. You can also choose “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
12. **Bandwidth:** The default setting for Bandwidth is “Auto”. You can change it to

“20MHz” with care if some clients are suffering from the connectivity problem in higher bandwidth setting.

13. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open (include 802.1x), Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

- **Open**

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP's configuration.

In this mode you can also enable the 802.1x feature if you have another RADIUS server for user authentication. You need to input IP address, port, shared key of RADIUS server here.

▶ 802.1X	<input checked="" type="checkbox"/> Enable
▶ Encryption	None ▾
▶ RADIUS Server IP	0.0.0.0
▶ RADIUS port	1812
▶ RADIUS Shared Key	

In this mode, you can only choose “None” or “WEP” in the encryption field.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The gateway will select appropriate authentication method (Open or Shared) according to the WiFi client's request automatically.

- **WPA-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-shared key.

- **WPA**

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

- **WPA2-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA2**

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

- **WPA-PSK/WPA2-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key.

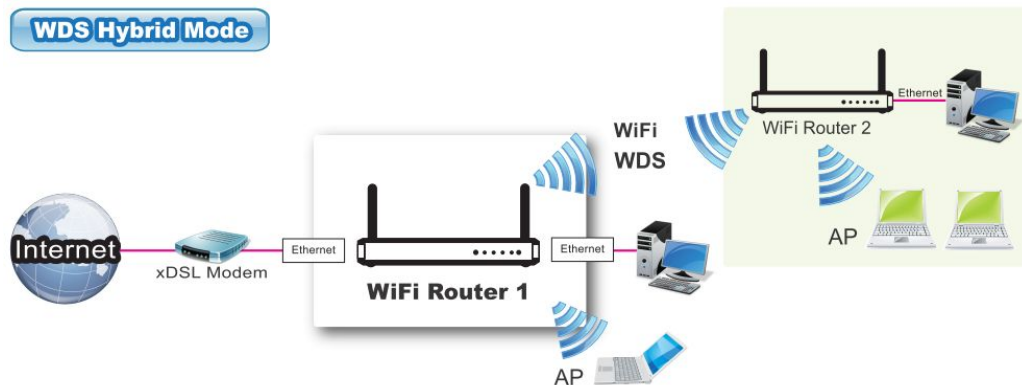
- **WPA/WPA2**

If some of wireless clients can only support WPA, but most of them can support WPA2. You can choose this option to support both of them. Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.1.2.1.2 WDS Hybrid Mode

This mode makes device act as a wireless bridge but also have AP function. While acting as a wireless Bridge, Wireless Router 1 and Wireless Router 2 can communicate with each other through wireless interface (with WDS). Thus All Stations can communicate with each other and are able to access Internet if Wireless Router 1 has the Internet connection.



Wireless Module > Advanced Wireless Module Settings	
Wireless Setting [HELP]	
Item	Setting
Wireless Module	<input checked="" type="checkbox"/> Enable
Wireless Operation Mode	WDS Hybrid Mode
Lazy Mode	<input type="checkbox"/> Enable
Green AP	<input type="checkbox"/> Enable
AP Number	AP 1 <input checked="" type="checkbox"/> Enable
Network ID (SSID)	DG-WM2005SI
SSID Broadcast	<input checked="" type="checkbox"/> Enable
VLAN ID	<input type="checkbox"/> Enable 3 (3~4094)
Max Supported Stations	<input type="checkbox"/> Enable (1~16)
WLAN Partition	<input type="checkbox"/> Enable
Channel	Auto
Wireless Mode	B/G/N mixed
Bandwidth	Auto
Authentication	Auto
Encryption	None
Scan Remote AP's MAC List	Scan
Remote AP MAC1	
Remote AP MAC2	
Remote AP MAC3	
Remote AP MAC4	

Save Undo WPS Setup... Wireless Client List...

1. **Lazy Mode:** This device supports the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers MAC address filled.
2. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
3. **AP Number:** This device supports up to 8 SSIDs at the same time for you to manage your wireless networks. You can select AP1 ~ AP8 and configure each wireless network individually.
4. **Network ID (SSID):** Network ID is used for identifying a Wireless LAN. Client stations can roam freely over this device and other Access Points that have the same Network ID. The factory default SSID is "default", you can change it to a meaningful identifier for the wireless users to easily find it out.
5. **SSID Broadcast:** By default, the SSID Broadcast setting is "Enable", and the device will broadcast beacons that have some information, including SSID, to the air, so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as "Disable", you can hide the wireless network from being scanned by wireless clients. Those who know the SSID can manually specify the SSID on their client device to connect the hidden wireless network.
6. **VLAN ID:** This device supports mapping of a SSID to a certain VLAN ID to separate workgroups across wireless and wired domains. By default, it is not enabled. If you enable this function, you have to specify a VLAN ID for the wireless network.
7. **Max Supported Stations:** You can specify the number of maximum stations that can associate to the SSID simultaneously.
8. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection. It's recommended to choose a channel that is not used in your environment to reduce radio interference.
9. **Wireless Mode:** The RF1 module supports 802.11b/g/n modes. You can also choose "N only", "G/N mixed" or "B/G/N mixed". The factory default setting is "B/G/N mixed".
10. **Bandwidth:** The default setting for Bandwidth is "Auto". You can change it to "20MHz" with care if some clients are suffering from the connectivity problem in higher bandwidth setting.
11. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open (include 802.1x), Shared, Auto, WPA-PSK and

WPA2-PSK.

- **Open**

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP's configuration.

In this mode you can also enable the 802.1x feature if you have another RADIUS server for user authentication. You need to input IP address, port, shared key of RADIUS server here.

▶ 802.1X	<input checked="" type="checkbox"/> Enable
▶ Encryption	None ▾
▶ RADIUS Server IP	<input type="text" value="0.0.0.0"/>
▶ RADIUS port	<input type="text" value="1812"/>
▶ RADIUS Shared Key	<input type="text"/>

In this mode, you can only choose “None” or “WEP” in the encryption field.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The gateway will select appropriate authentication method (Open or Shared) according to the Wi-Fi client's request automatically.

- **WPA-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-shared key.

- **WPA2-PSK**

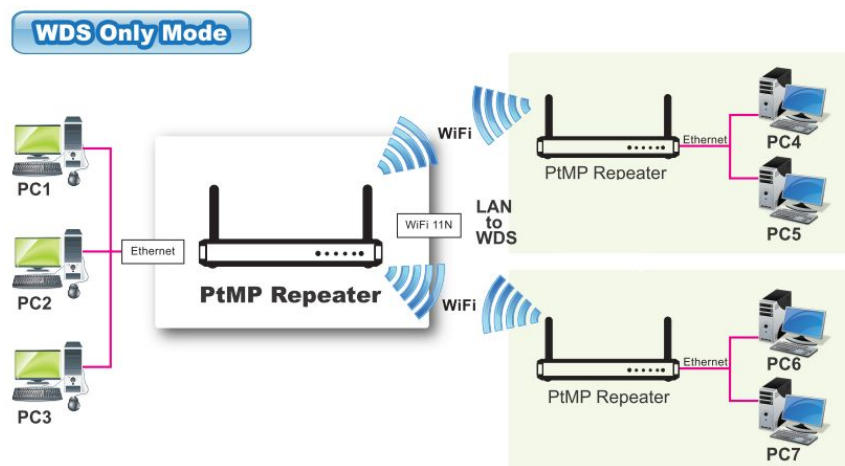
Select Encryption mode and enter the Pre-shared Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-shared key.

12. **Remote AP MAC 1 ~ Remote AP MAC 4:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.2.1.3 WDS Only Mode

WDS (Wireless Distributed System) function lets AP’s acts as a wireless LAN bridge. All stations associated with WDS AP’s could see each other and roam through APs without changing Wi-Fi configurations. You can use this feature to build up a large wireless network in a large space like airports, hotels, schools etc.



▶ Wireless Module ▶ Advanced Wireless Module Settings

■ Wireless Setting [HELP]

Item	Setting
▶ Wireless Module	<input checked="" type="checkbox"/> Enable
▶ Wireless Operation Mode	WDS Only Mode ▼
▶ Green AP	<input type="checkbox"/> Enable
▶ Channel	Auto ▼
▶ Authentication	Auto ▼
▶ Encryption	None ▼
▶ Scan Remote AP's MAC List	<input type="button" value="Scan"/>
Remote AP MAC1	<input type="text"/>
Remote AP MAC2	<input type="text"/>
Remote AP MAC3	<input type="text"/>
Remote AP MAC4	<input type="text"/>

1. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
2. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection. It's recommended to choose a channel that is not used in your environment to reduce radio interference
3. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open (include 802.1x), Shared, Auto, WPA-PSK and WPA2-PSK.

- **Open**

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP's configuration.

In this mode you can also enable the 802.1x feature if you have another RADIUS server for user authentication. You need to input IP address, port, shared key of RADIUS server here.

▶ 802.1X	<input checked="" type="checkbox"/> Enable
▶ Encryption	None ▼
▶ RADIUS Server IP	0.0.0.0
▶ RADIUS port	1812
▶ RADIUS Shared Key	

In this mode, you can only choose "None" or "WEP" in the encryption field.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The gateway will select appropriate authentication method (Open or Shared) according to the Wi-Fi client's request automatically.

- **WPA-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key.

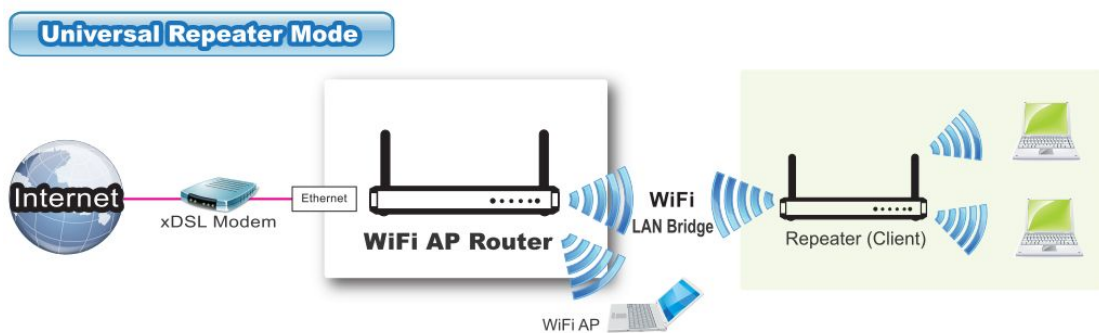
- **WPA2-PSK**

Select Encryption mode and enter the Pre-shared Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-shared key.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.1.2.1.4 Universal Repeater Mode

Universal Repeater is a technology used to extend wireless coverage. It provides the function to act as Adapter (Client) and AP at the same time and can use this function to connect to a Root AP and use AP (SSID name must be the same as that of Root AP) function to service all wireless stations within its coverage. All the stations within the coverage of this access point can be bridged to the Root AP.



Wireless Module > Advanced Wireless Module Settings	
Wireless Setting [HELP]	
Item	Setting
Wireless Module	<input checked="" type="checkbox"/> Enable
Wireless Operation Mode	Universal Repeater
Green AP	<input type="checkbox"/> Enable
Network ID(SSID)	DG-WM2005SI
Destination AP MAC	
Destination AP MAC2	<input type="checkbox"/> Enable
WEC Config Status	UNCONFIGURED Release
SSID Broadcast	<input checked="" type="checkbox"/> Enable
VLAN ID	<input type="checkbox"/> Enable 3 (3~4094)
Max Supported Stations	<input type="checkbox"/> Enable (1~16)
WLAN Partition	<input type="checkbox"/> Enable
Channel	Auto
Bandwidth	Auto
Authentication	Auto
Encryption	None

1. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
2. **Network ID (SSID):** Network ID is used for identifying a Wireless LAN. Client stations can roam freely over this device and other Access Points that have the same Network ID. The factory default SSID is “default”, you have to change it to the same SSID of the peer AP to be associated under the Universal Repeater Mode.
3. **Destination AP MAC:** Besides, to have the same SSID of the peer AP to be associated under the Universal Repeater mode, you also have to specify the MAC address of the peer AP to avoid making wrong connection with other AP that has the same SSID.
4. **WEC Config Status:** Displays the status of the WEC button which is also used to push the master configuration to the slave.
5. **SSID Broadcast:** By default, the SSID Broadcast setting is “Enable”, and the device will broadcast beacons that have some information, including SSID, to the air, so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, you can hide the wireless network from being scanned by wireless clients. Those who know the SSID can manually specify the SSID on their client device to connect the hidden wireless network.

6. **VLAN ID:** This device supports mapping of a SSID to a certain VLAN ID to separate the work groups across wireless and wired domains. By default, it is not enabled. If you enable this function, you have to specify a VLAN ID for the wireless network.
7. **Max Supported Stations:** You can specify the number of maximum stations that can associate to the SSID simultaneously.
8. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients associated to the same VAP. The wireless clients can't communicate with each other, but they can access the internet and other Ethernet LAN devices
9. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection. It's recommended to choose a channel that is not used in your environment to reduce radio interference
10. **Bandwidth:** The default setting for Bandwidth is "Auto". You can change it to "20MHz" with care if some clients are suffering from the connectivity problem in higher bandwidth setting.
11. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open Shared, Auto, WPA-PSK and WPA2-PSK.

Afterwards, click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

3.1.3 Advanced Wireless Setup

This device provides advanced wireless setup for professional users to optimize the wireless performance under the specific installation environment.

3.1.3.1 Advanced RF Module1 Settings

Advanced Wireless Module Settings [HELP]	
Item	Setting
▶ Regulatory Domain	(1-11)
▶ Beacon Interval	<input type="text" value="100"/> (msec, range: 1~1000)
▶ Transmit Power	<input type="text" value="100%"/>
▶ RTS Threshold	<input type="text" value="2347"/> (1~2347)
▶ Fragmentation	<input type="text" value="2346"/> (256~2346)
▶ DTIM Interval	<input type="text" value="3"/> range (1~255)
▶ WMM Capable	<input checked="" type="checkbox"/> Enable
▶ AP Isolation	<input type="text" value="On"/>
▶ Short GI	<input type="text" value="400ns"/>
▶ TX Rates	<input type="text" value="Best"/>

- 1. Beacon interval:** Beacons are packets sent by a wireless router to synchronize wireless devices.
- 2. Transmit Power:** Normally the wireless transmission power operates at 100% out power specification of this device. You can lower down the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.
- 3. RTS Threshold:** If an excessive number of wireless packet collision occurred, the wireless performance will be affected. It can be improved by adjusting the RTS/CTS (Request to Send/Clear to Send) threshold value.
- 4. Fragmentation:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage.
- 5. DTIM interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered

broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.

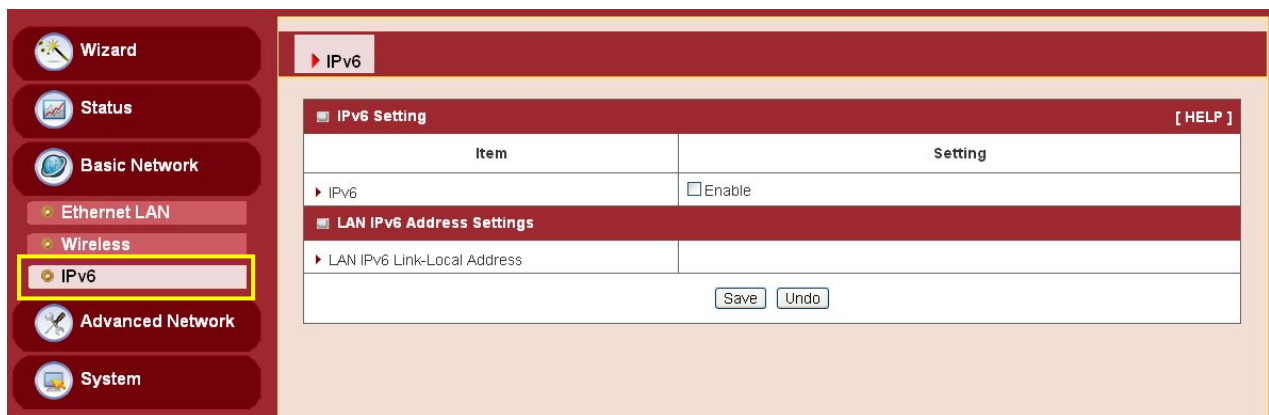
6. **WMM Capable:** WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
7. **AP Isolation:** If you enable multiple VAPs in this device, you can further decide whether the wireless clients associated to different VAPs can access to each other or not. When you enable the AP Isolation function, each VAP is isolated to the others consequently.
8. **Short GI:** Short GI can guard intervals are used to ensure that distinct transmissions do not interfere with one another.
9. **TX Rate:** For Wi-Fi transmit rate, you can choose “Best” for auto-adjustment according to Wi-Fi signal quality in your environment, or you can fix it in certain TX rate. Please note the Wi-Fi connection may be dropped if you fix at a higher data rate but in a noisy (poor RF signal quality) environment.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.1.4 IPv6

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6 (Internet Protocol version 6)** is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers.

This device supports IPv6, it works as an IPv6 bridge, you can use it to build an IPv6 network.

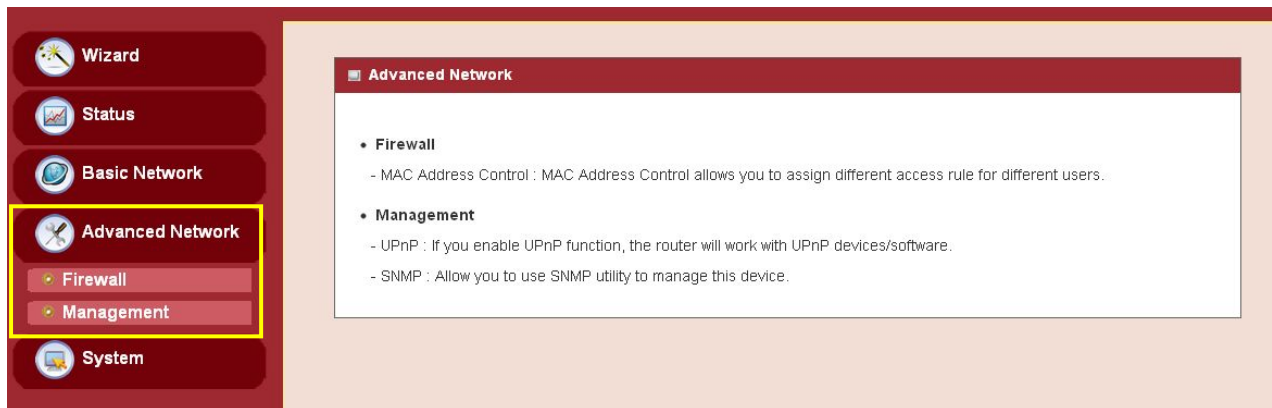


LAN IPv6 address settings: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

“2001:0db8:85a3:0000:0000:8a2e:0370:7334”

3.2 Advanced Network

This device also supports other advanced network features for you to further manage the device. You can finish the configuration for Firewall, and Management in this section.



3.2.1 Firewall

3.2.1.1 MAC Address Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

▶ MAC Address Control
[HELP]

■ MAC Address Control
[HELP]

Item	Setting
▶ MAC Address Control	<input type="checkbox"/> Enable
<input type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and <input type="text" value="allow"/> unspecified MAC addresses to associate.

ID	MAC Address	A
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

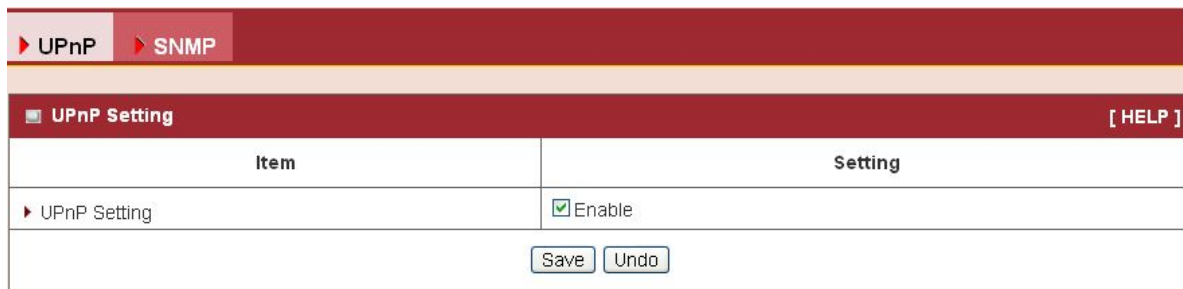
1. **MAC Address Control:** Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.
2. **Association control:** Check "Association control" to enable the control of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.2.2 Management

3.2.2.1 UPnP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some Network device. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming



Item	Setting
▶ UPnP Setting	<input checked="" type="checkbox"/> Enable

This device supports the UPnP Internet Gateway Device (IGD) feature. By default, it is enabled.

3.2.2.2 SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

▶ UPNP ▶ SNMP	
■ SNMP Setting [HELP]	
Item	Setting
▶ Enable SNMP	<input checked="" type="checkbox"/> Local(LAN)
▶ SNMP Version	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input type="checkbox"/> v3
▶ Get Community	<input type="text" value="public"/>
▶ Set Community	<input type="text" value="private"/>
■ Username 1	
▶ User 1	<input type="checkbox"/> Enable
▶ SNMPv3 Settings: User 1	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write
▶ User 1 AUTH Mode	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
▶ User 1 Privacy Mode	<input type="radio"/> noAuthNoPriv <input checked="" type="radio"/> authNoPriv <input type="radio"/> authPriv
▶ Username 1	<input type="text"/>
▶ Password 1(len>=8)	<input type="text"/>
▶ User 1 Priv Key	<input type="text"/>
■ Username 2	
▶ User 2	<input type="checkbox"/> Enable
▶ SNMPv3 Settings: User 2	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write
▶ User 2 AUTH Mode	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
▶ User 2 Privacy Mode	<input type="radio"/> noAuthNoPriv <input checked="" type="radio"/> authNoPriv <input type="radio"/> authPriv
▶ Username 2	<input type="text"/>
▶ Password 2(len>=8)	<input type="text"/>
▶ User 2 Priv Key	<input type="text"/>
■ Trap Event Receiver	
▶ Trap Event Receiver 1	<input type="text"/>
▶ Trap Event Receiver 2	<input type="text"/>
▶ Trap Event Receiver 3	<input type="text"/>
▶ Trap Event Receiver 4	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **Enable SNMP:** Enable this Function.
2. **SNMP Version:** Supports SNMP V1, V2c, and V3.
3. **Get Community:** The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
4. **Set Community:** The community of SetRequest that this device will accept.
5. **SNMPv3 Settings: User 1:** This device supports up to two SNMP management accounts. You can specify the account permission as “Read” or “Read/Write” respectively.
6. **User 1 AUTH Mode:** Select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.
7. **User 1 Privacy Mode:** You can configure the SNMP privacy mode. There are three modes for you to choose: “noAuthNoPriv” for both authentication and private key are not required, “authNoPriv” for no private key required, and “authPriv” for both authentication and private key required.
8. **Username 1:** Use this field to identify the user name for the specified level of access.
9. **Password 1:** Use this field to set the password for the specified level of access.
10. **User 1 Priv Key:** Use this field to define the encryption key for the specified level of access.
11. **Trap Event Receiver 1 ~ 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify the IP address, so that the device can send SNMP Trap message to the management PCs consequently.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.3 System

In this section you can see system information, system logs, use system tools for system update and do service scheduling and system administration setting.

3.3.1 System Information

You can view the System Information in this page.

Item	Setting
▶ Display time	Thu, 01 Jan 1970 01:18:05 +0000

3.3.2 System Status

3.3.2.1 Web Log

Web Log		Syslogd	Email Alert
Log Types			
Item	Setting		
Log Types	<input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Debug		
<input type="button" value="Save"/> <input type="button" value="Undo"/>			
Web Log			
Time	Log		
Page: 0/0 (Log Number: 0)			
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="First Page"/> <input type="button" value="Last Page"/>			
<input type="button" value="Refresh"/> <input type="button" value="Download"/> <input type="button" value="Clear logs"/>			

1. **Log Types:** You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop” and “Debug” types for you to select.
2. **Web Log:** You can browse, refresh, download and clear logs.

3.3.2.2 Syslog

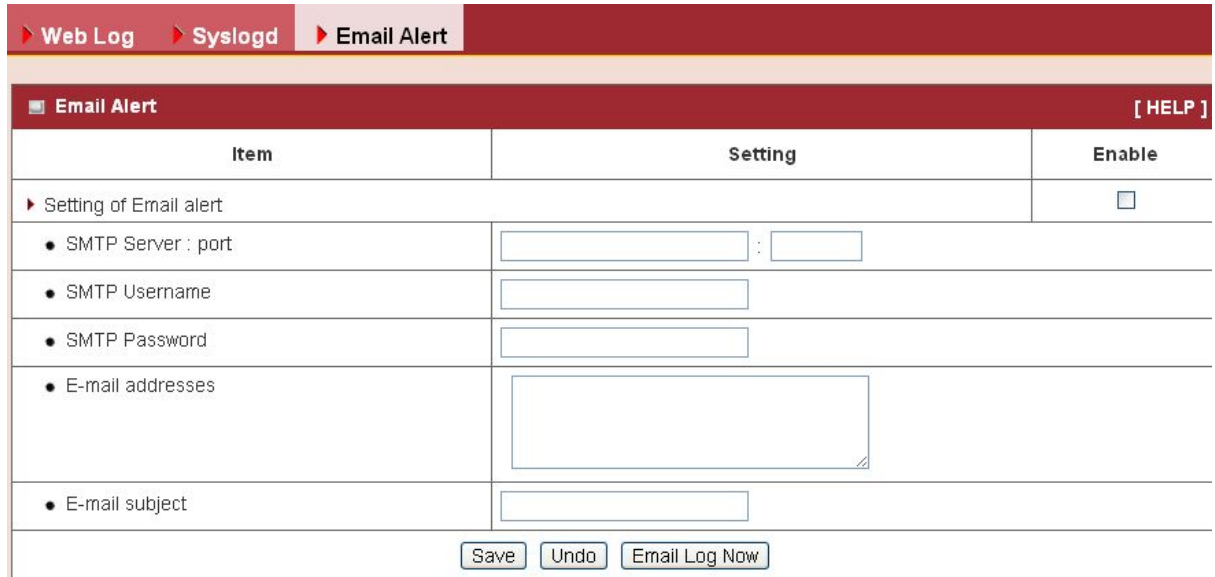
This device also can export system logs to specific destination by means of syslog (UDP) and SMTP (TCP). With enabled Syslog function, this device will send log to a certain host periodically. You need to install a syslog utility on a host to receive syslogs.

Web Log		Syslogd	Email Alert
System Log			[HELP]
Item	Setting	Enable	
IP address for syslogd	<input type="text"/>	<input type="checkbox"/>	
<input type="button" value="Save"/> <input type="button" value="Undo"/>			

The items you have to setup include:

1. **IP Address for syslogd:** Host IP of destination where syslog will be sent to. Check **Enable** to enable this function.

3.3.2.3 Email Alert



Item	Setting	Enable
▶ Setting of Email alert		<input type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

This device can also export system logs via sending emails to specific recipients. The items you have to setup include:

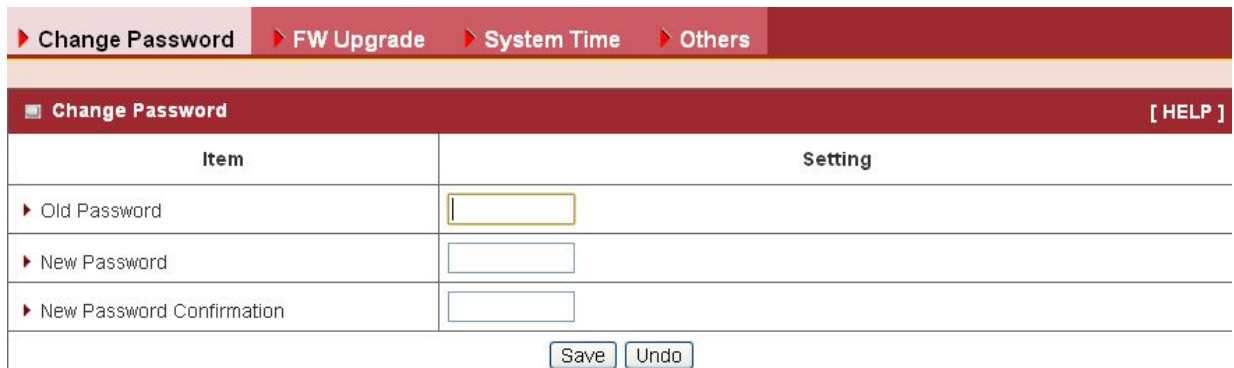
1. **Setting of Email alert:** Check if you want to enable Email alert (send syslog via email).
2. **SMTP Server: Port:** Input the SMTP server IP and port, which are connected with '!' If you do not specify port number, the default value is 25.
For example, "mail.your_url.com" or "192.168.1.100:26".
3. **SMTP Username:** Enter the Username offered by your ISP.
4. **SMTP Password:** Enter the password offered by your ISP.
5. **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than one recipient, using ';' or ',' to separate these email addresses.
6. **E-mail Subject:** The subject of email alert is optional.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.3.3 System Tools

3.3.3.1 Change Password

You can change the System Password here. We **strongly** recommend you to change the system password for security reasons. Click on “Save” to store your settings or click “Undo” to give up the changes.



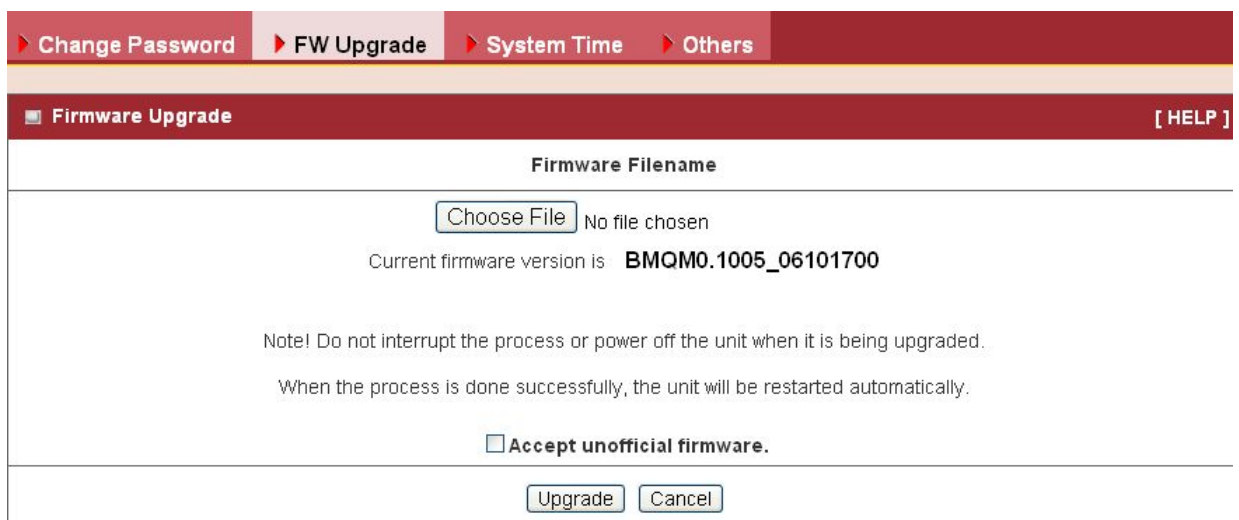
The screenshot shows the 'Change Password' section of the web interface. At the top, there is a navigation bar with tabs for 'Change Password', 'FW Upgrade', 'System Time', and 'Others'. Below this, the 'Change Password' section is active, with a '[HELP]' link on the right. The main area contains a table with two columns: 'Item' and 'Setting'.

Item	Setting
▶ Old Password	<input type="password"/>
▶ New Password	<input type="password"/>
▶ New Password Confirmation	<input type="password"/>

At the bottom of the form, there are two buttons: 'Save' and 'Undo'.

3.3.3.2 FW Upgrade

If new firmware is available, you can upgrade device firmware through the WEB GUI here.



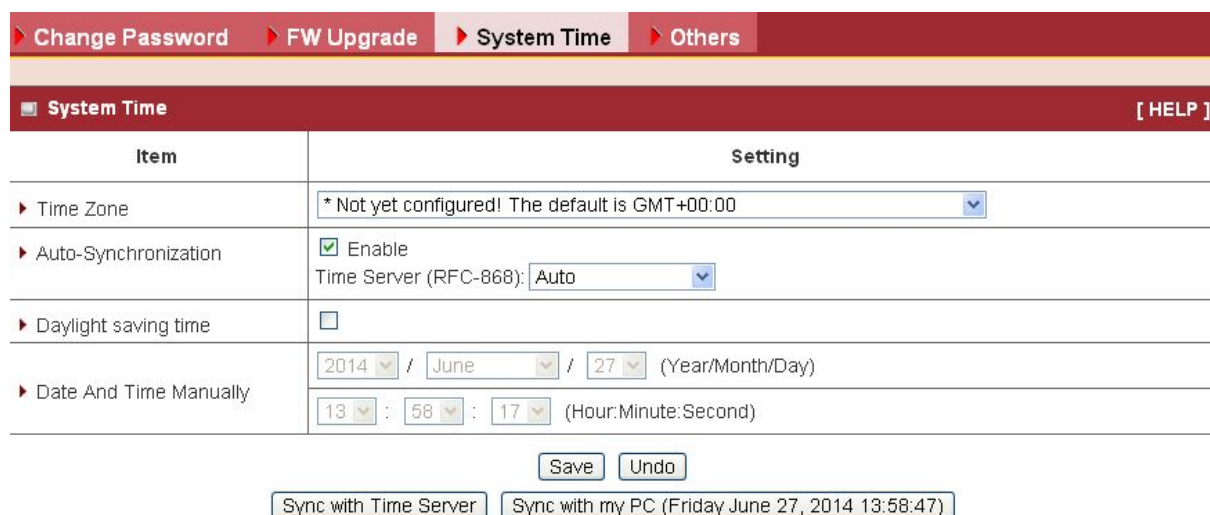
The screenshot shows the 'FW Upgrade' section of the web interface. At the top, there is a navigation bar with tabs for 'Change Password', 'FW Upgrade', 'System Time', and 'Others'. Below this, the 'FW Upgrade' section is active, with a '[HELP]' link on the right. The main area contains a 'Firmware Filename' section with a 'Choose File' button and the text 'No file chosen'. Below this, it displays 'Current firmware version is **BMQM0.1005_06101700**'. A note states: 'Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.' There is a checkbox labeled 'Accept unofficial firmware.' which is currently unchecked. At the bottom, there are two buttons: 'Upgrade' and 'Cancel'.

Press “Choose File” button to indicate the file name of new firmware, and then press Upgrade button to start to upgrade new firmware on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS IN PROGRESS.

3.3.3.3 System Time

If new firmware is available, you can upgrade device firmware through the WEB GUI here.



Item	Setting
▶ Time Zone	* Not yet configured! The default is GMT+00:00
▶ Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): Auto
▶ Daylight saving time	<input type="checkbox"/>
▶ Date And Time Manually	2014 / June / 27 (Year/Month/Day) 13 : 58 : 17 (Hour:Minute:Second)

1. **Time Zone:** Select a time zone where this device locates.
2. **Auto-Synchronization:** Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Daylight saving time:** is the practice of advancing clocks during the summer months that have more daylight so that people get up earlier in the morning and experience more daylight in the evening. Enable the checkbox to enable the field.
4. **Date and Time Manually:** Enter the date and time manually
5. **Sync with Time Server:** Click on the button if you want to set Date and Time by NTP Protocol.
6. **Sync with my PC:** Click on the button if you want to set Date and Time using the PC’s Date and Time.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.3.3.4 Others

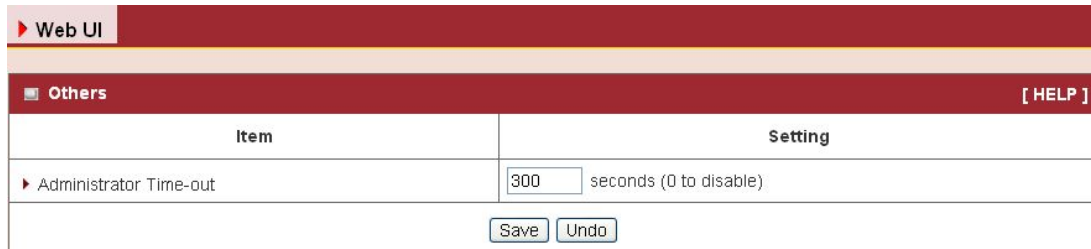
In this section you can do system backup, reset to default, system reboot settings and ping test.

▶ Change Password ▶ FW Upgrade ▶ System Time ▶ Others	
■ Others [HELP]	
Item	Setting
▶ Backup Setting	<input type="button" value="Backup"/>
▶ Reset to Default	<input type="button" value="Reset"/>
▶ Reboot	<input type="button" value="Reboot"/>
▶ Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>
▶ Domain Name or IP address for Traceroute	<input type="text"/> <input type="button" value="Traceroute"/>

1. **Backup Setting:** You can backup your settings by clicking the “**Backup**” button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.
2. **Reset to Default:** You can also reset this device to factory default settings by clicking the “**Reset**” button.
3. **Reboot:** You can also reboot this device by clicking the “**Reboot**” button.
4. **Domain Name or IP address for Ping Test:** This allows you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.
5. **Domain Name or IP address for Traceroute:** Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point

3.3.4 MMI

3.3.4.1 Web UI



The screenshot shows a web interface with a red header. The main content area has a dark red bar with 'Web UI' on the left and '[HELP]' on the right. Below this is a table with two columns: 'Item' and 'Setting'. The 'Item' column contains 'Administrator Time-out'. The 'Setting' column contains a text input field with the value '300' and the text 'seconds (0 to disable)'. Below the table are two buttons: 'Save' and 'Undo'.

Item	Setting
Administrator Time-out	<input type="text" value="300"/> seconds (0 to disable)

You can set UI administration time-out duration in this page. If the value is “0”, means the time-out is unlimited.

4 AP Management Software

Ranger view AP management software is a PC-based network management utility. It allows administrator to deploy AP mesh quickly and easily across IP network, and configure all trusted APs based on pre-defined configuration profiles individually or simultaneously. The system supports a smart discovery of trusted APs via UPnP and CAPWAP protocols and a quick AP searching based on AP's name, MAC address or IP address from the trusted AP list. It also monitors online status of managed APs and real-time network traffic for each AP, each virtual AP and each STA client graphically. To collect all categorized traps in the control center from trusted APs and make several statistics diagrams, administrator can have an easy analysis based on these diagrams and take adequate and instant reactions to the events. Full control functions to all trusted APs include reboot, reset, FW upgrade and backup/restore settings. And further, AP Load Balance function leverages the loading of all AP members in the AP mesh to get best communication performance in the whole network. Besides, an optional function of remote AP management also can be activated via a pre-established VPN tunnel.

Following diagram shows two application scenarios example. One is for SMB office that AP Management Software manages the AP mesh in SMB office to grant staff to access both Internet and Intranet, but to grant visiting guests to access Internet only. The other application scenario is for hospitality that AP Management Software manages the AP mesh in a hotel. It allows all valid room guests to play their mobile devices or notebooks for Internet surfing via WiFi network at their rooms or public areas, like lobby and parking lot.



AP Management Software has following feature sets:

- **Easy-to-use User Interface**
 - Centralized management of various AP devices.
 - Auto-discover APs and show their current status.
 - Quick search by AP Name, MAC address or IP address.

- **Real-time AP & STA User Statistics**
 - Monitor traffic load by AP, virtual AP and STA client.
 - Graphic Statistics for administrator to analyze easily and take instant reactions.

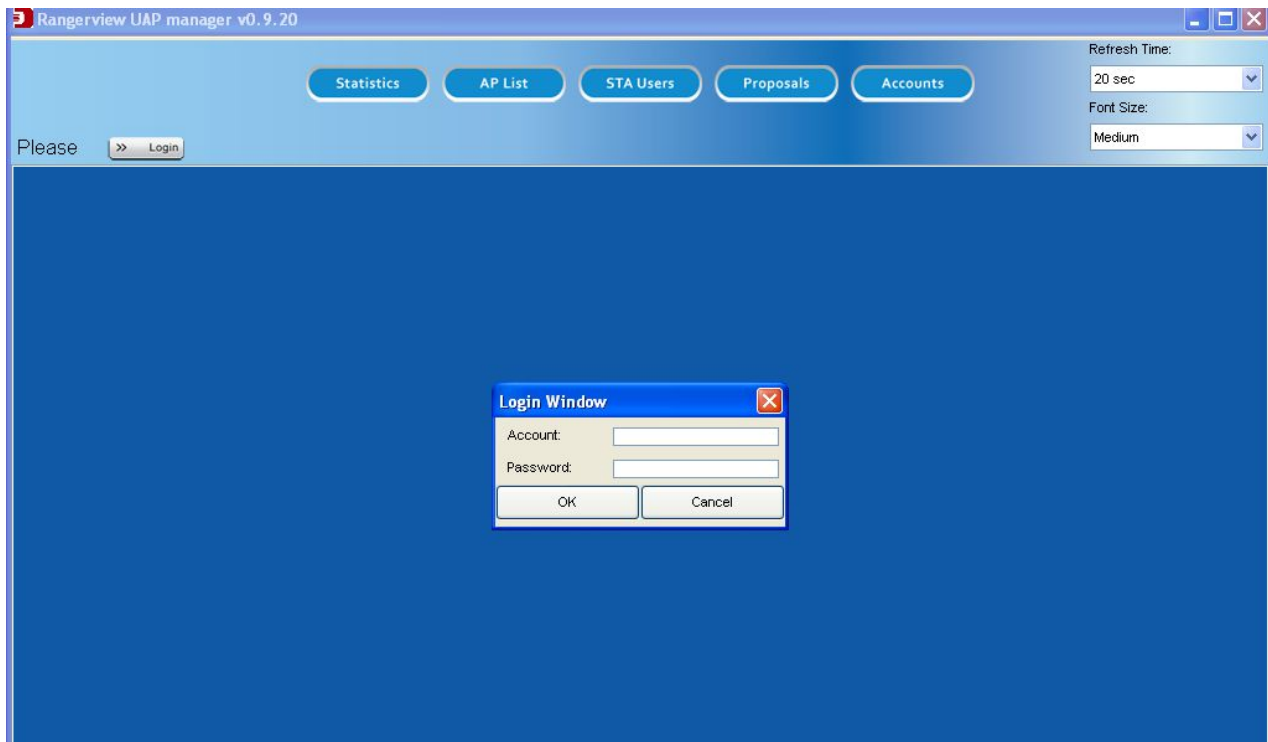
- **Support Multi-site AP Management and Control**
 - Define various kinds of AP configuration proposals for different APs.
 - Apply pre-defined proposals to adequate APs individually or simultaneously.
 - AP configuration includes WiFi, LAN & VLAN, IPv6, MAC Control, Packet Filters and QoS & BWM configurations and System Controls.

- **Collect and Report Network Trap Events**
 - Collect all trap events from trusted APs all the time.
 - Activate alerting system based on administrator's management policy.
 - Comprehensive alerting approaches include AP Management Software screen, Email, SMS, and syslogd.

- **Advanced Functions to Improve Intranet Traffic Performance and Extend Management Range**
 - AP Load Balance function leverages the loading of all APs to get best Intranet traffic throughput.
 - An optional function of remote AP management is activated via a pre-established VPN tunnel.

4.1 Installation Process

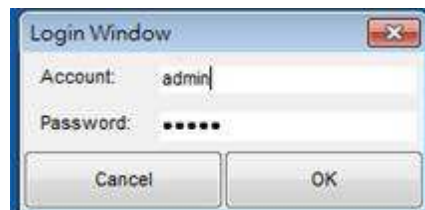
- a. Extract the RangerView files in the local Drive of computer.
- b. Double click on the “**Rangerview UAP manager.exe**” file icon to execute the utility. If you can see the login window, it will run successfully as shown in below diagram.



4.2 Getting Started

Easy Setup

- Make sure all APs in your Intranet to be operated normally.
- Make sure the AP Controller Utility is running at the computer connected to the Intranet via its Ethernet adaptor.
- At login window, input default account and password to start the controller.
- By default, account and password is “admin” and “admin”. Please be noted that account “admin” can’t be removed or modified. Besides, please change the password when you log in successfully first time by using “Accounts” function in the controller utility as below diagrams.

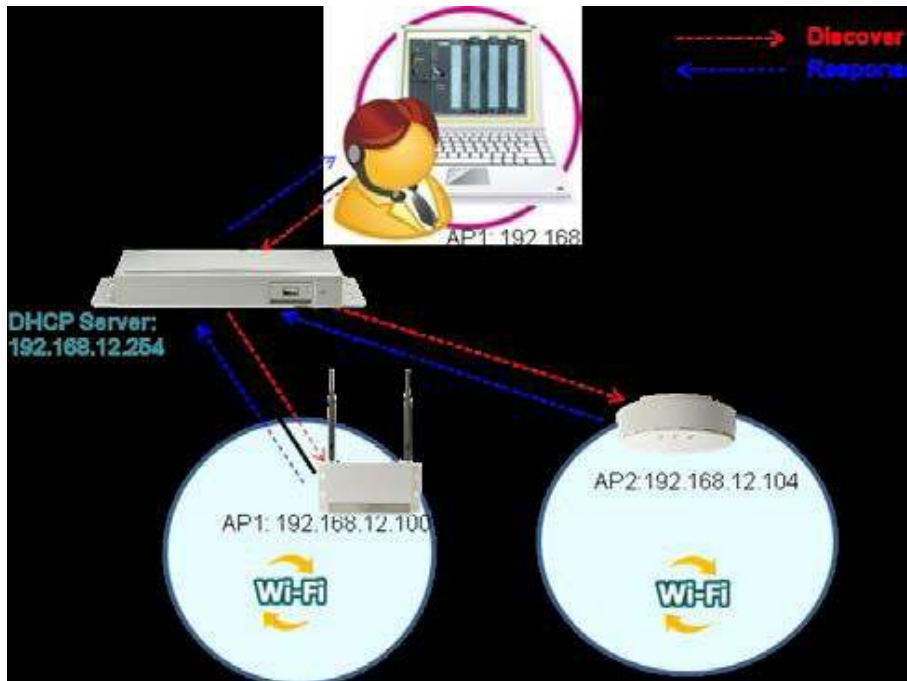


Discover Trusted APs

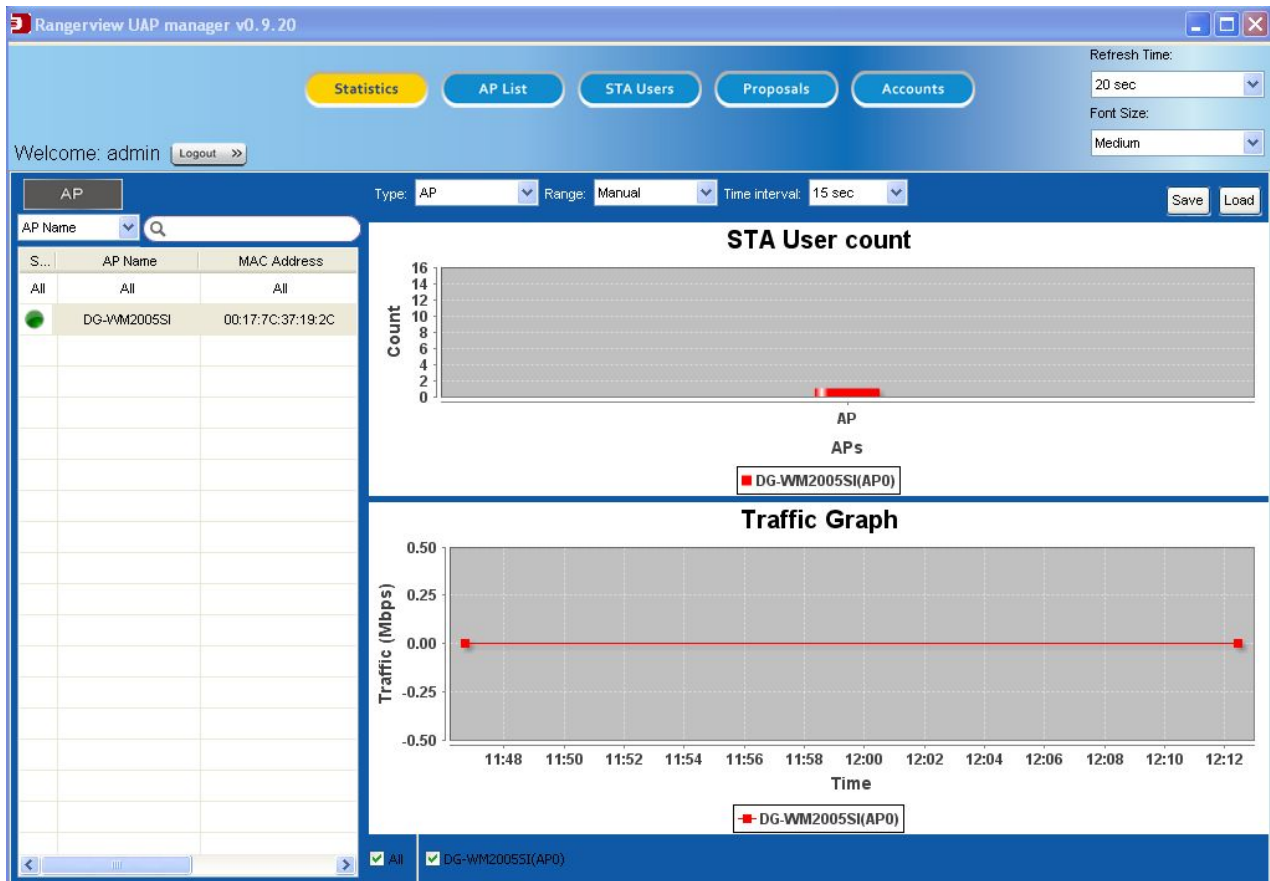
- a. AP Controller can operate at three network situations well

First situation is there is a DHCP server in the Intranet for IP assignment to AP Controllers and all APs. All devices are existed in the same subnet that is dominated by the DHCP server. The second situation is AP controller owns its static IP address and configures found APs with different IP addresses after discovery process. All devices are existed in the same subnet that is dominated by the AP controller. The last one is AP controller is configured to be “Auto IP” with 169.254.x.x subnet. It will configure all found trusted APs to be also “Auto IP” so that they all can communicate with each other in the same subnet.

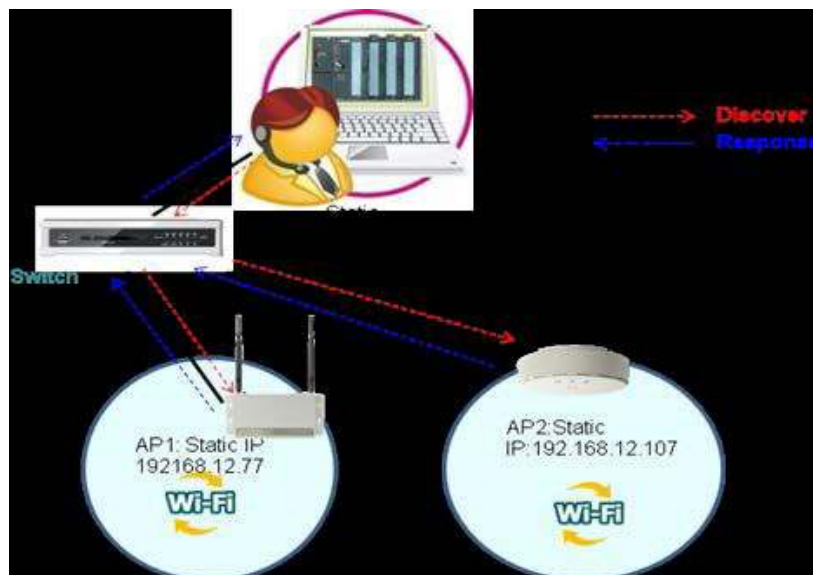
a.1 One DHCP server in the Intranet



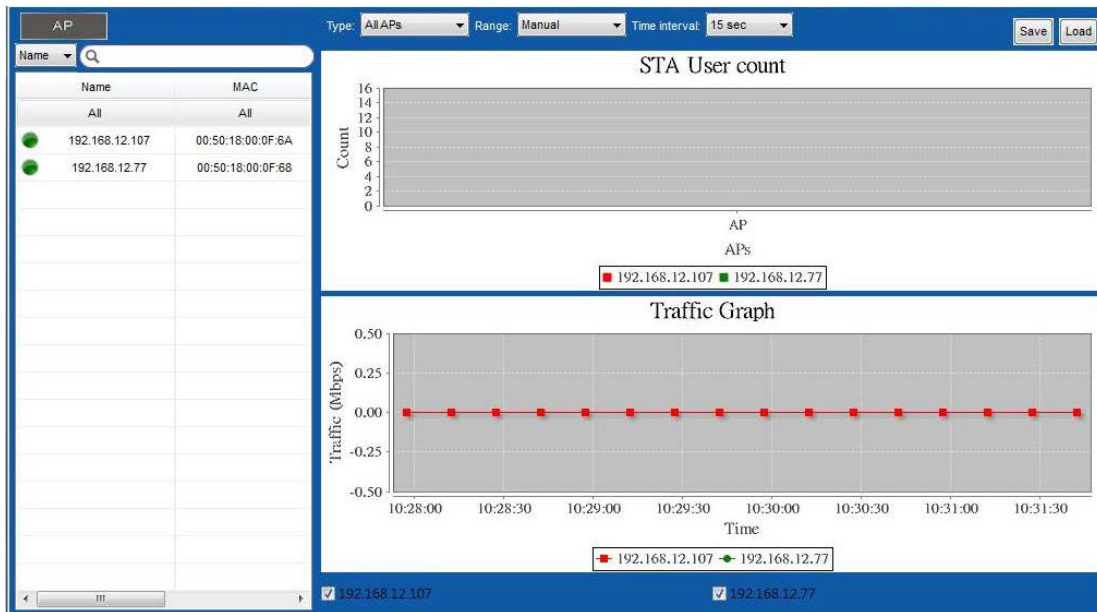
AP controller and APs get their IP addresses from the DHCP server as above diagram. They are existed in the same subnet and communicate each other. AP controller can discover APs and APs can respond the discovery request from AP controller in the Intranet. The found AP list will show at the AP controller screen as below.



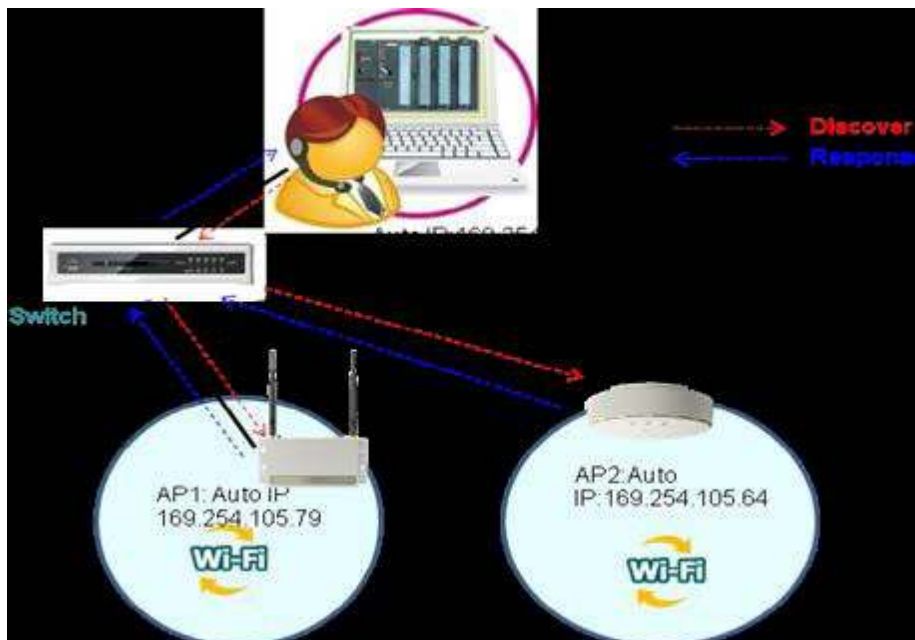
a.2 AP controller owns a static IP address



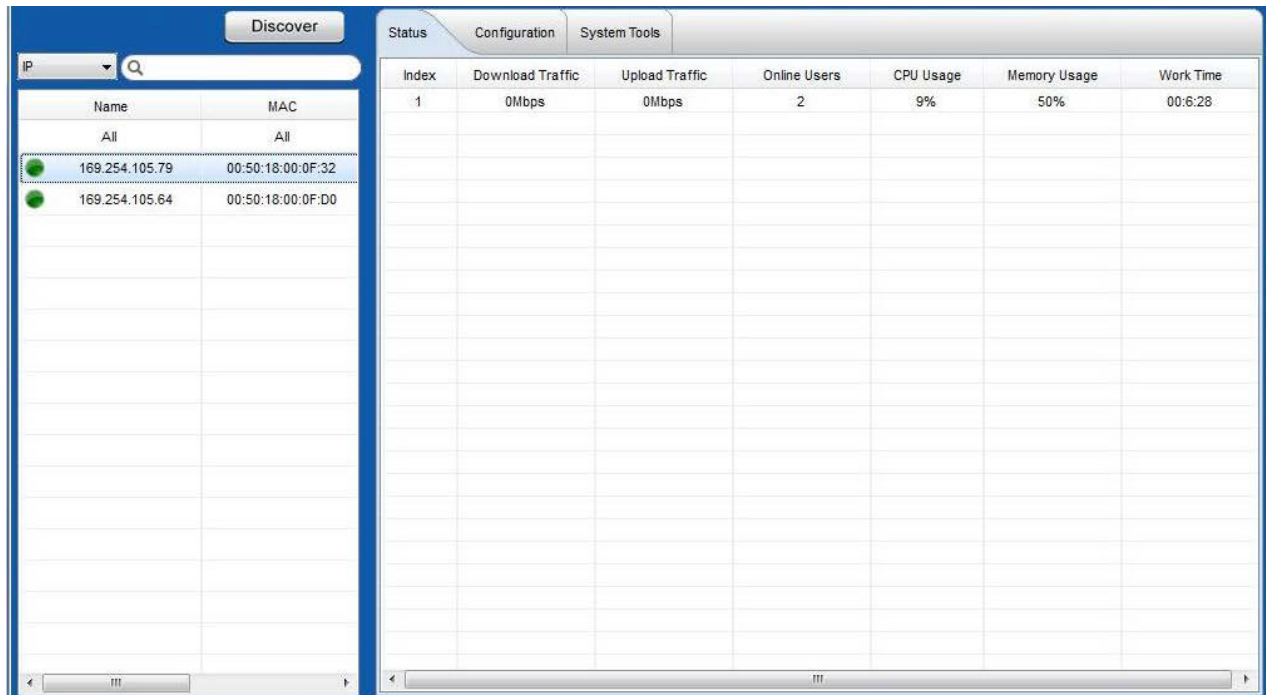
AP controller owns a static IP address: 192.168.12.123 as above diagram. It broadcasts the discovery request and specifies the IP range of managed APs. All existed APs will respond AP controller with their chosen IP addresses, and they will also change their IP addresses again once IP address conflict between them has been detected. AP controller shows the discovery results as below.



a.3 AP controller uses “Auto IP”



AP controller uses “Auto IP” and gets the IP address: 169.254.105.202 as above diagram. It broadcasts the discovery request and specifies the IP range of managed APs with 169.254.x.x subnet. All existed APs will respond AP controller with their chosen IP addresses, and they will also change their IP addresses again once IP address confliction between them has been detected. AP controller shows the discovery results as below.



The screenshot displays the 'Discover' tab of the AP controller's web interface. On the left, there is a search bar for IP addresses and a table listing discovered APs. The table has columns for 'Name' and 'MAC'. Two APs are listed: one with IP 169.254.105.79 and MAC 00:50:18:00:0F:32, and another with IP 169.254.105.64 and MAC 00:50:18:00:0F:D0. On the right, there is a detailed status table for the selected AP (Index 1). The status table has columns for 'Index', 'Download Traffic', 'Upload Traffic', 'Online Users', 'CPU Usage', 'Memory Usage', and 'Work Time'. The values for Index 1 are: Download Traffic: 0Mbps, Upload Traffic: 0Mbps, Online Users: 2, CPU Usage: 9%, Memory Usage: 50%, and Work Time: 00:6:28.

Name	MAC
All	All
169.254.105.79	00:50:18:00:0F:32
169.254.105.64	00:50:18:00:0F:D0

Index	Download Traffic	Upload Traffic	Online Users	CPU Usage	Memory Usage	Work Time
1	0Mbps	0Mbps	2	9%	50%	00:6:28

a.4 Once AP is rebooted

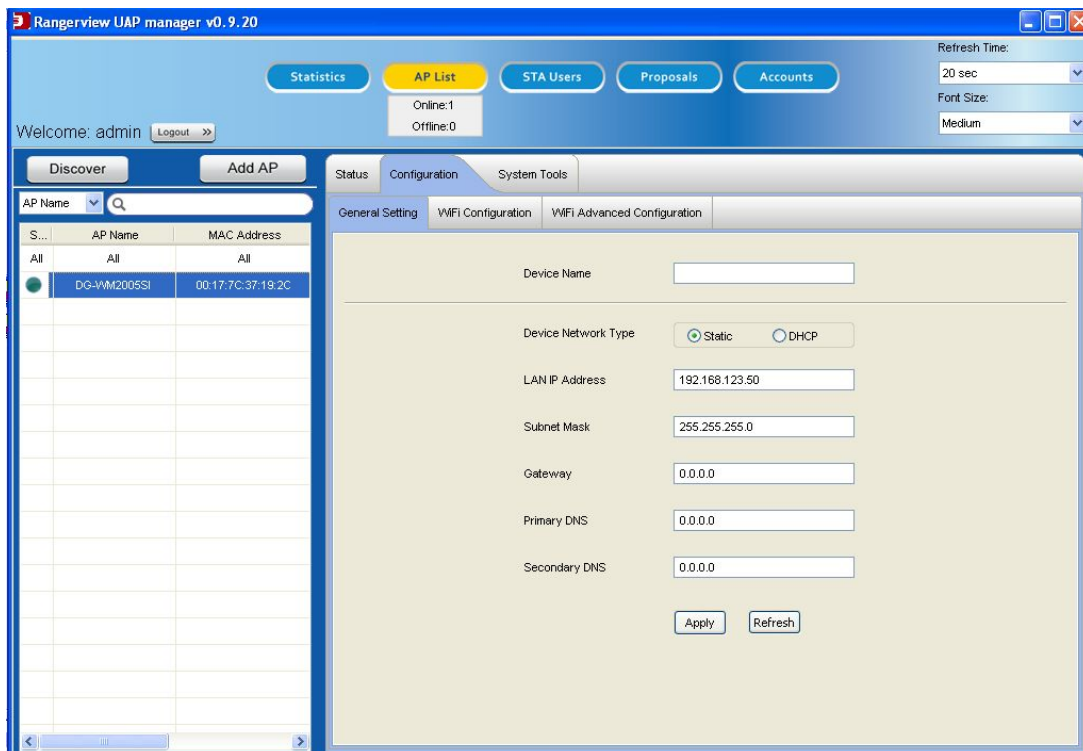
Once one AP is rebooted, it will use the original IP address to communicate with AP controller normally as same as before rebooting in the Intranet. But if AP controller or DHCP server is gone after AP rebooting, the AP will use its default IP address, 192.168.123.50 to let user make further configuration to that AP via Web UI by using a computer's browser with <http://192.168.123.50> URL.

a.5 Let APs with their device names

Here, we suggest strongly that user should let all managed APs have their corresponding device names. After that, user can identify one specific AP easily by its name. Refer to below diagram to configure AP's device name by following steps:

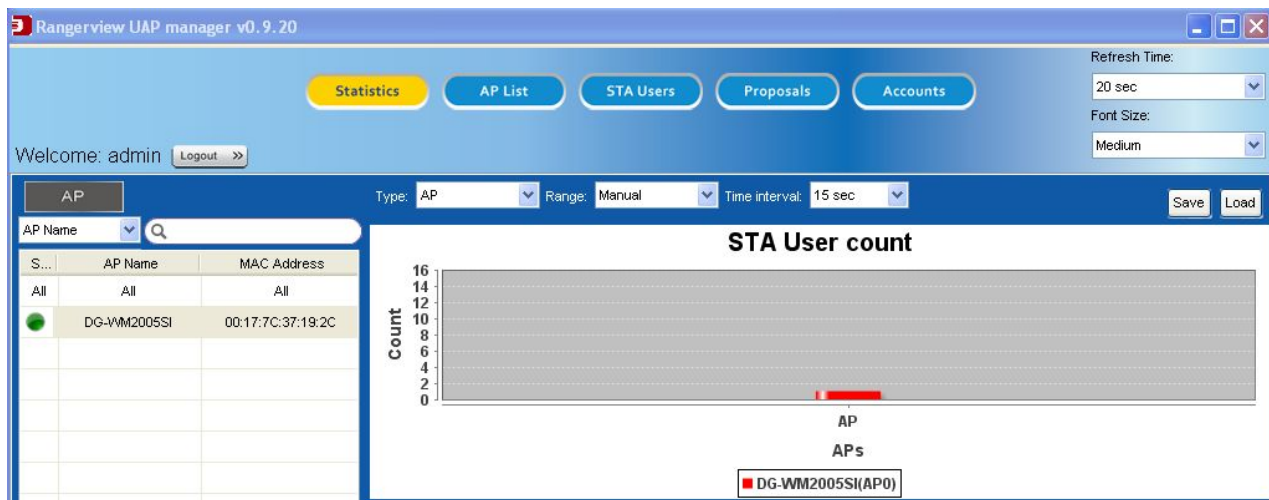
Step 1: Choose “AP List” function in AP controller screen and specify the target AP from the AP list in left window.

Step 2: Choose “Configuration” tag and “General Settings” sub-tab, you can input the “Device Name” for that AP.



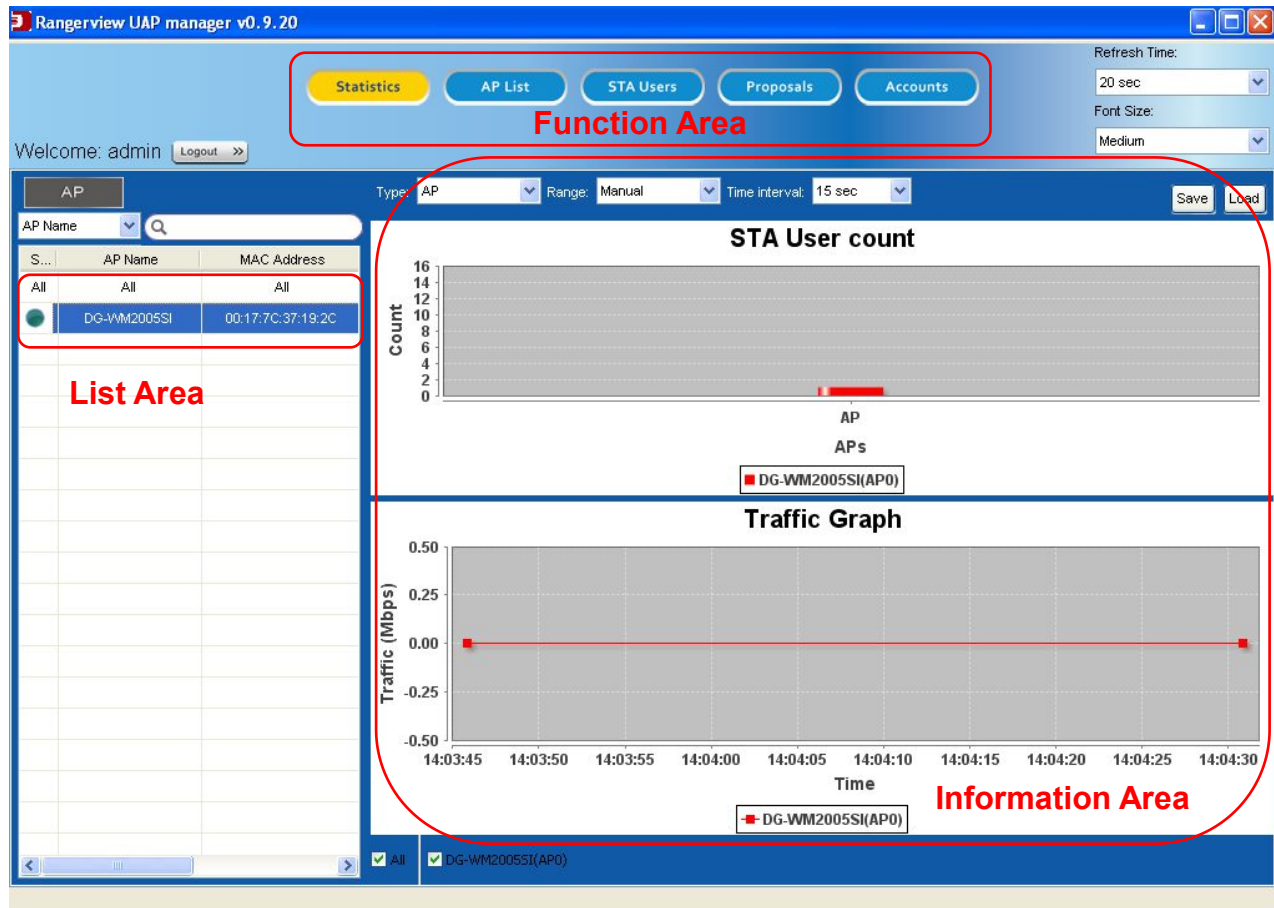
b. AP controller starts to discover Trusted AP's in the intranet

After user logins successfully, AP Controller will discover APs automatically at either situation of above mentioned from a.1 to a.3, and then list all found APs in left window of screen. Among the found AP list, user can search his dedicated AP by Name, MAC Address, IP Address or Model Name by inputting a keyword in searching field and to find it in the AP list. Green led at the front of each AP record means AP is online, gray led means AP is offline or isn't detectable in a short period by controller as shown as below diagram.



4.3 AP Controller Utility Overview

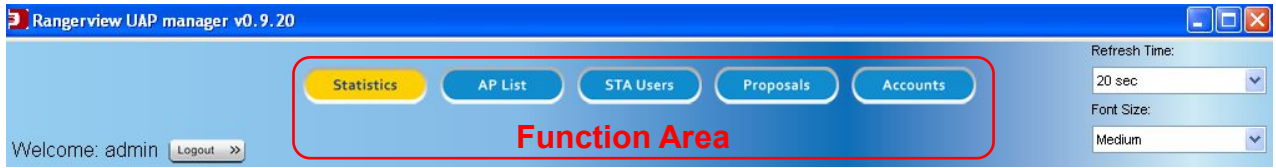
There are three areas in the AP controller screen: Function Area, List Area and Information Area as below diagram.



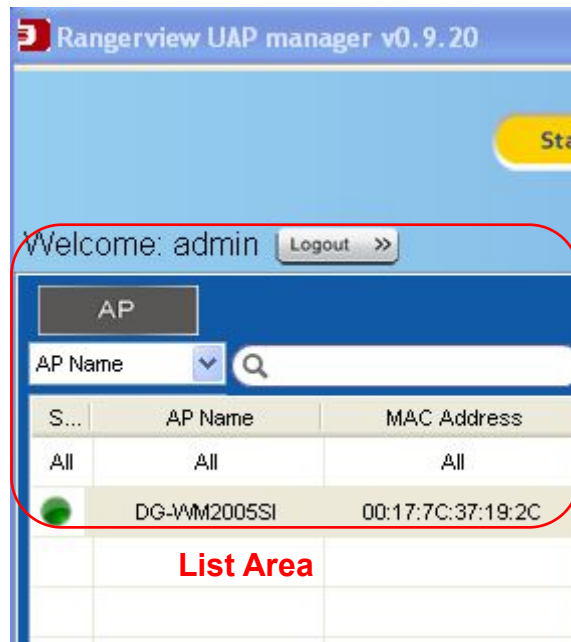
Function area shows the major functions in the AP controller. These functions include Statistics, AP List, STA Users, Proposals and Accounts. Introduce them in details at Chapter 3. List area will show some lists based on different functions. For example, AP list for Statistics, AP List and Proposals functions; STA user list for STA Users function; and Group list for Accounts function. However, information area will shows some statistics, AP status, STA status, proposal contents and user account status, even it provides the interface to let manager configure one AP or control it.

One example of showing the statistics of all APs is shown as below by following steps:

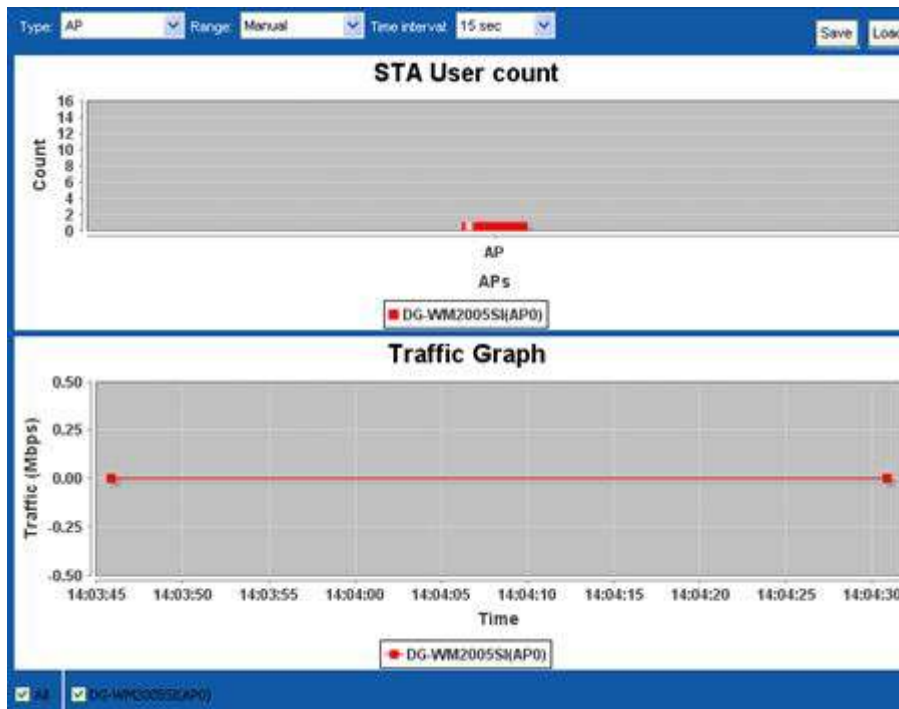
Step 1: Select “Statistics” function



Step 2: Specify “All” APs in list area.

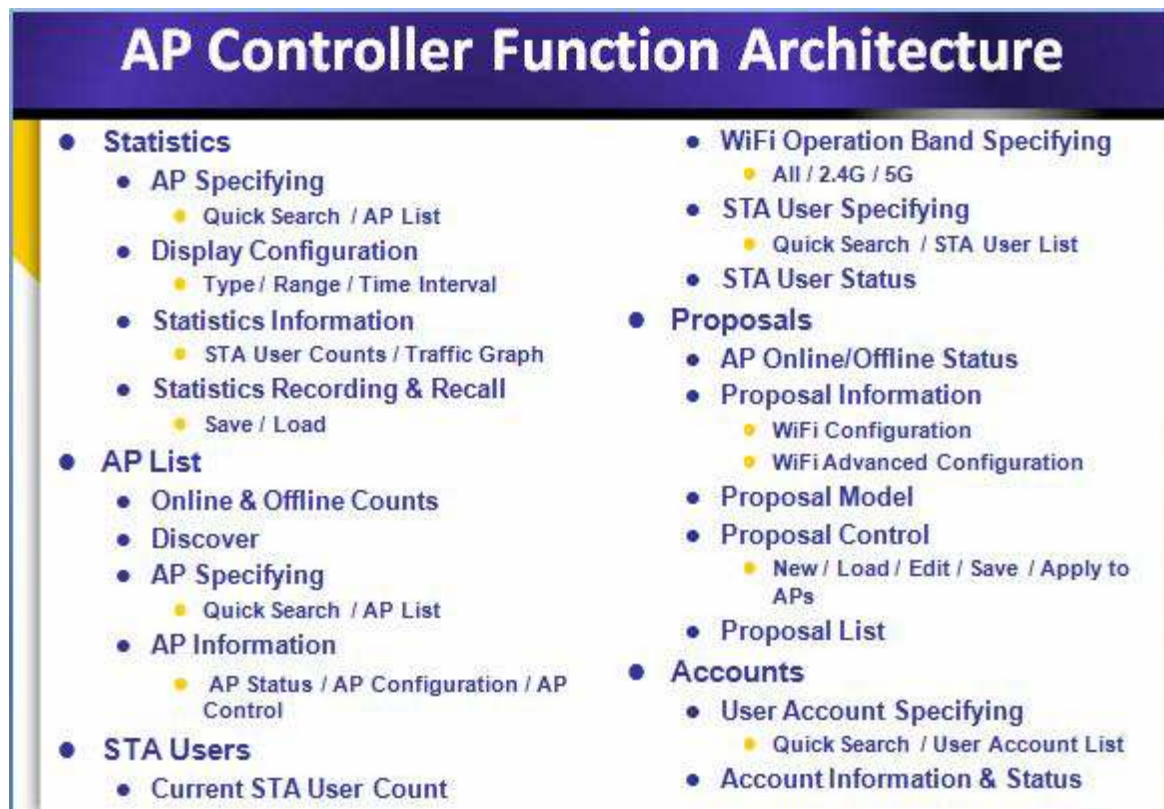


Step 3: Information area will show two statistics information of all APs, including the number of STA Users and its traffic loads for each AP.



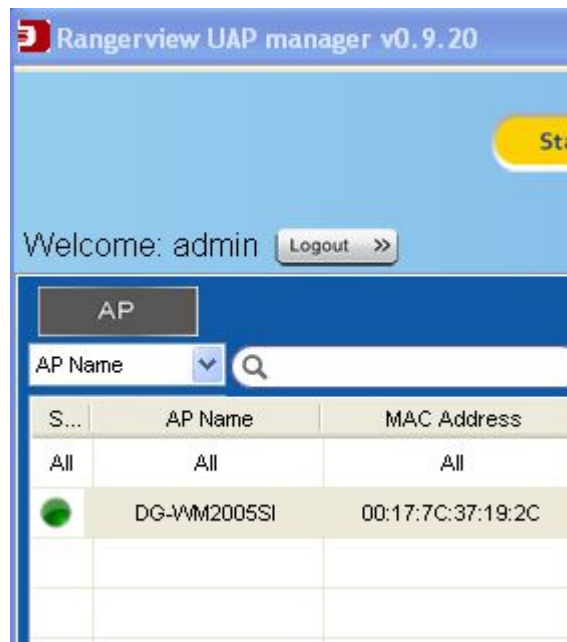
Ranger View Controller Functions

Use one function structure diagram to show all functions of AP Controller as below. There are five major functions including Statistics, AP List, STA Users, Proposals and Accounts. Describe them in details at following sections.



4.4 Statistics

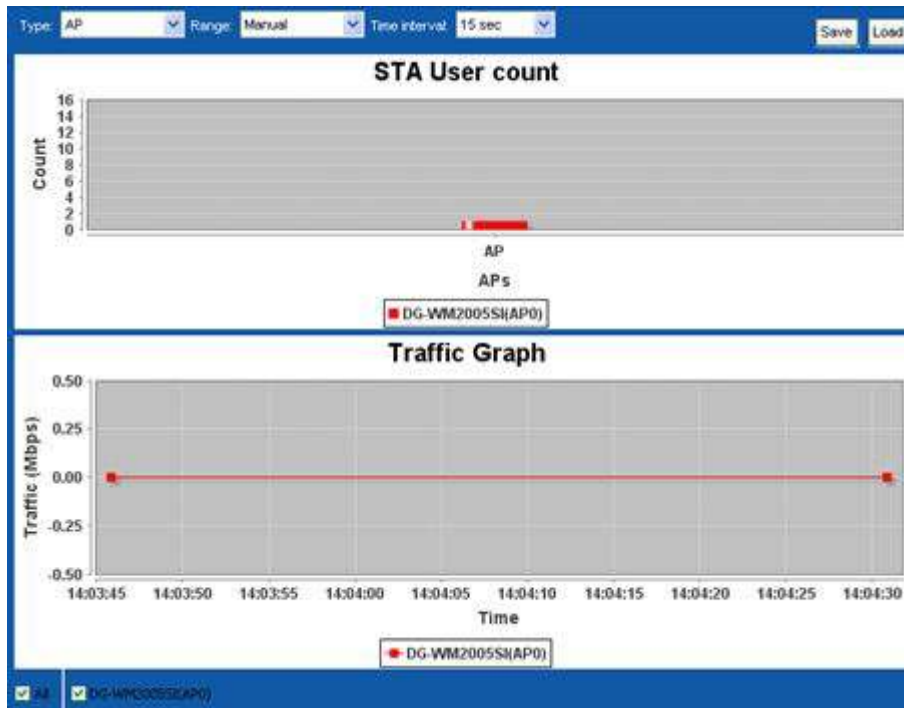
When manager clicks on the “Statistics” function button, the screen will be divided into 4 sectors for the function. At the left window, it is AP specifying part, including the quick search and AP list. Quick search can let manager input a keyword to find the target AP that he wants based on Device Name, MAC Address, IP Address or Model Name. AP list shows out all found APs by system. AP specifying part is shown as right side.



The second part is the configuration of how to display the statistics information, including AP type (physical AP or virtual AP or loaded data), displaying time range. Manual displaying time range means that manager can specify the traffic graph display window by using mouse to mark an area on current one. Display configuration part is shown as below.



The third part is statistics information. It includes two statistics data. One is the current count of STA users for each AP. The other is the traffic curve for each physical AP or virtual AP based on Displaying AP Type. An example of statistics information part is shown as below. At the bottom of display area, manager can choose what physical APs or what virtual APs to show their traffic curves.



The last part is the recording and recall of statistics data. There are two command buttons in this area, Save and Load. Save command button can record current traffic graph as a PNG file in computer storage and Load command button can load in the recorded statistics data to display. Recording and recall of statistics data part is shown as below.

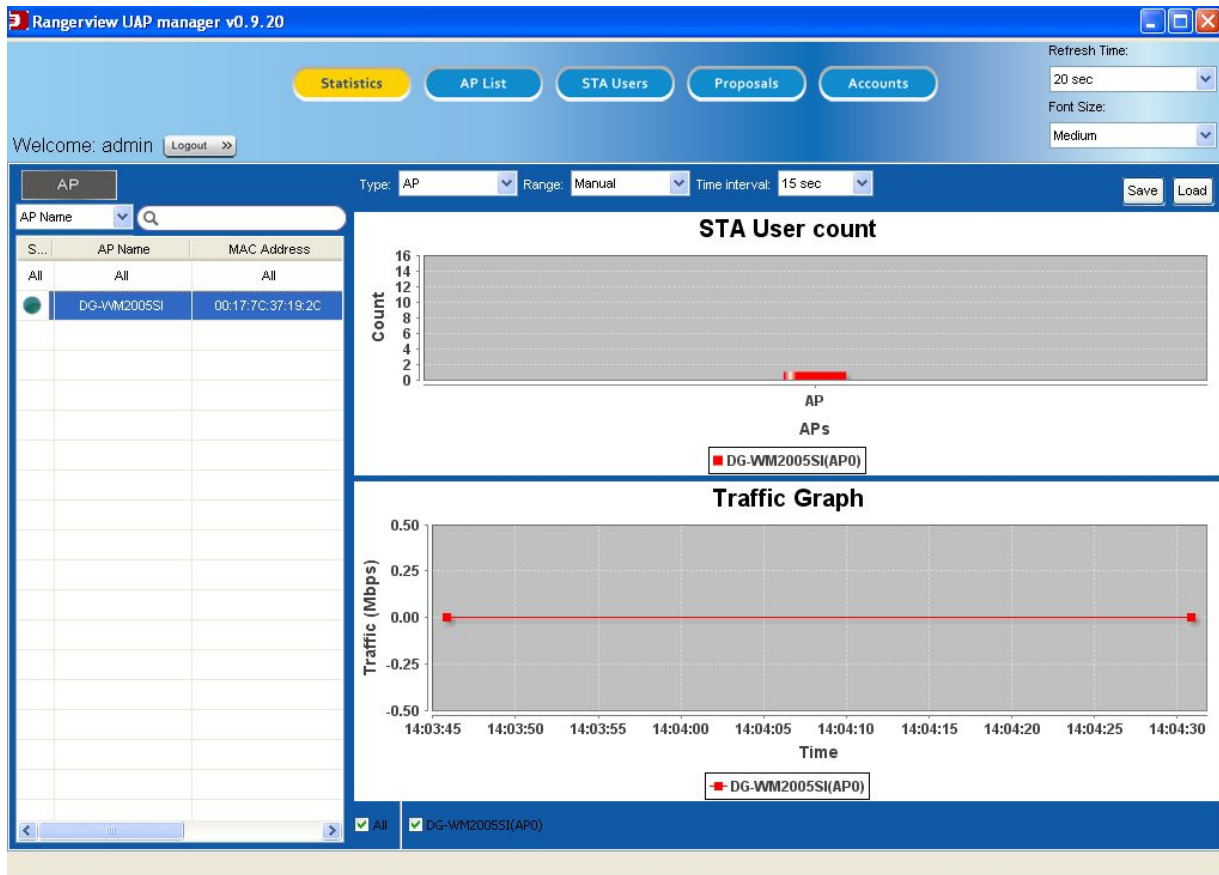


An example to show the statistics of all APs as following steps:

Step 1: Click on the “Statistics” function button.

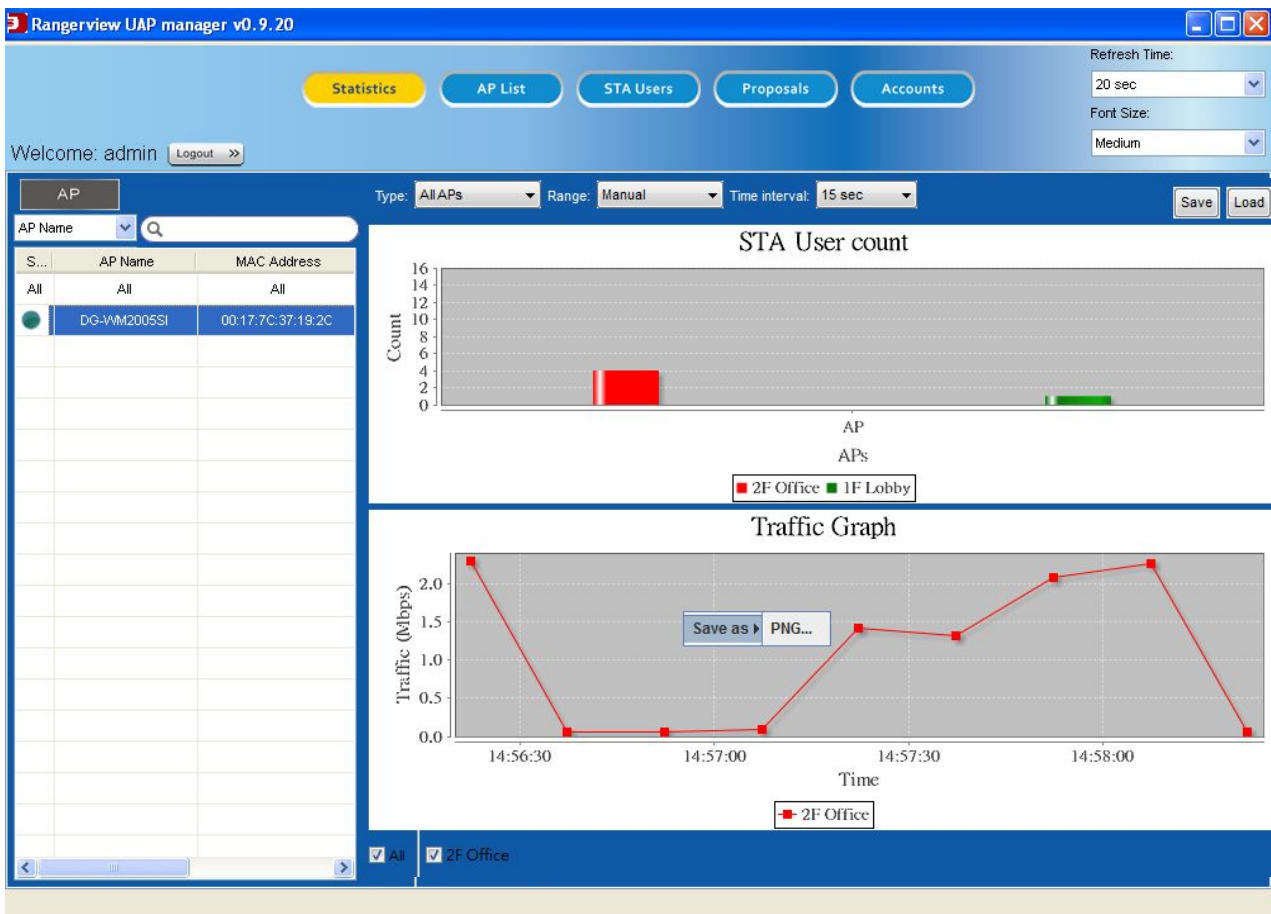
Step 2: Click on the “All” name of record in the found AP list.

Step 3: You can see STA user counts and statistics graph of all APs as below diagram.

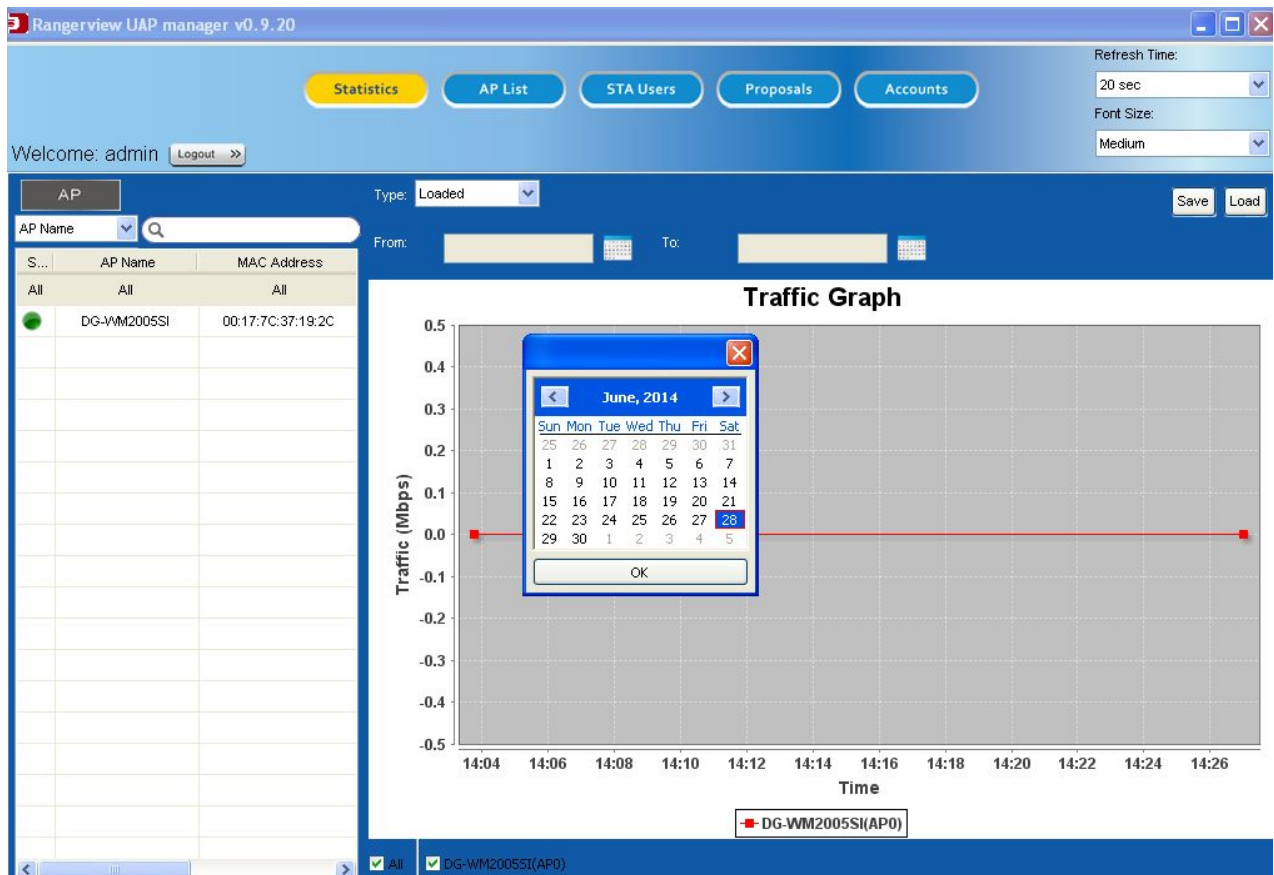


Step 4: You also can see the traffic curves of some specific APs by checking them at the bottom of statistics information area dynamically.

If manager wants to focus on the statistics monitoring of one specific AP, he can choose that AP from the AP list at Step 2 of above procedure. One example is shown as below.



Besides, manager wants to save the traffic curves as a file in computer by clicking on the “Save” command button at right-top corner of screen. And he can re-load it by clicking on the “Load” command button and show its contents on the traffic curve screen with displaying AP type is “Loaded”. Following is an example diagram.



Manager can choose the period of from date-time and to date-time to check the traffic curves during the period.

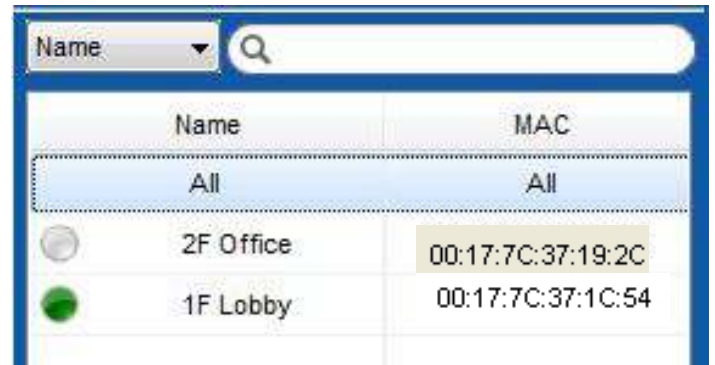
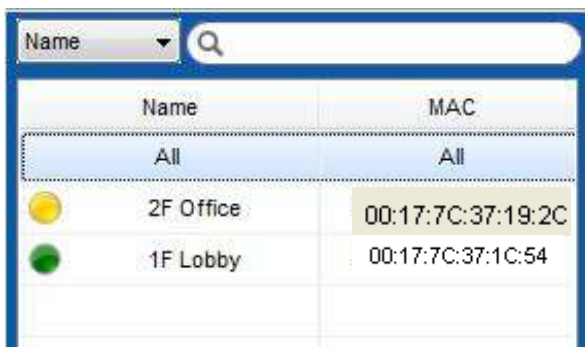
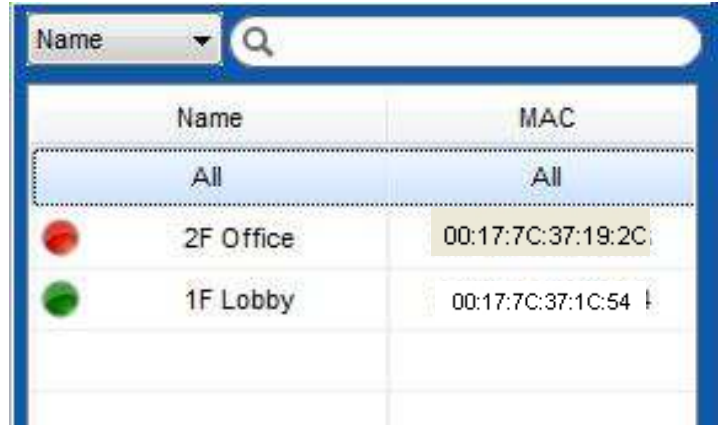
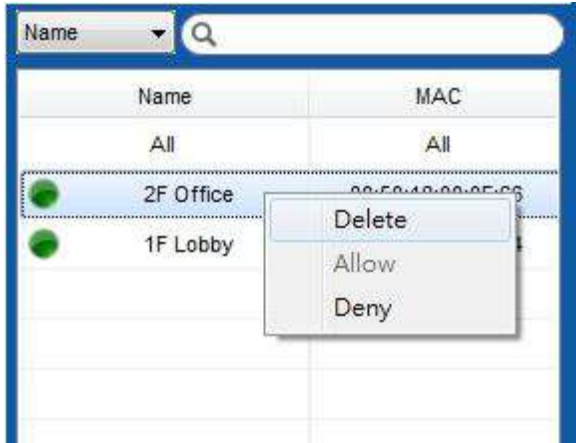
4.5 AP List

When manager moves his mouse over or clicks on the “AP List” function button, the counts of online APs and offline APs will show beneath “AP List” button. Clicking on the button, the screen will be divided into 3 sectors for the function. At the top-left corner, it is a Discover sector where there is a “Discover” command button there. Clicking on the “Discover” command button, AP controller will try to find existed trusted AP in the Intranet automatically. Shown as below:



Left window is AP specifying part, including the quick search and AP list. It is the second part and it is same as the one of “Statistics” function. By using the right button of mouse, manager can delete, deny or allow one AP from the AP list, shown as below. The red indicator marked at the front of AP record indicates all STA clients under that AP will be denied to access the Intranet and

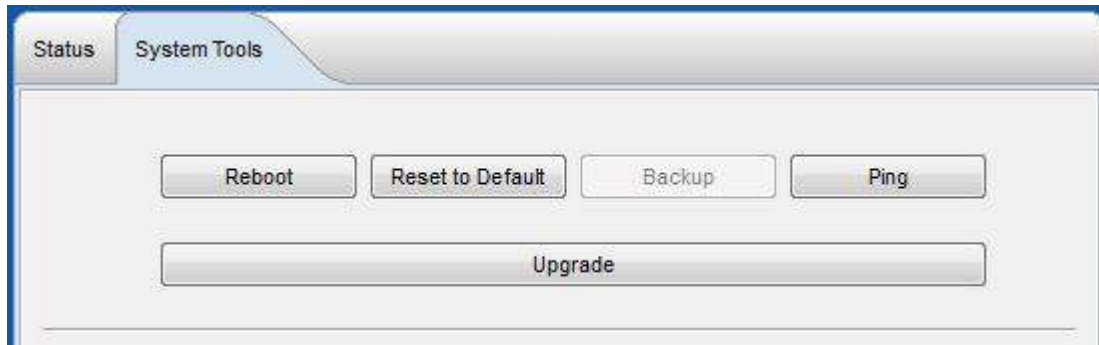
Internet. Yellow indicator indicates that the AP is busy. Green indicator indicates AP is online and gray indicator indicates AP is offline.



The last part is the AP information area. It includes the status displaying (Status tab), AP configuration (Configuration tab) and AP controlling (System Tools tab) for one dedicated AP. When “All” APs are specified at AP List, there are only Status and System Tools tabs are shown as below diagram.

Status		System Tools				
Index	2.4G Channel / 5G Channel	Download Traffic	Upload Traffic	Online Users	CPU Usage	Memory
1	Auto / Auto	0Mbps	0Mbps	0	8%	53
2	Auto / Auto	0Mbps	0Mbps	0	10%	51

Status tab will display the channel, download traffic, upload traffic, the number of online users, CPU usage, memory usage and work time for each AP. Besides, in System Tools tab, system provide “Reboot”, “Reset to Default”, “Ping” and “Upgrade” tools to execute corresponding actions to all APs. They are shown as below.



But if manager specifies one dedicated AP from the AP list, there is one more Configuration tab to be provided for AP configuration. And the displayed contents are different at Status tab between all APs and one specific AP. For one specific AP situation, Status tab will display the AP status as same as All AP situation, but also the status of virtual APs of dedicated AP is displayed beneath AP status. This can be checked from following diagram.

Detail Info

Connection Type: DHCP
WiFi Operation Mode: WDSHybrid

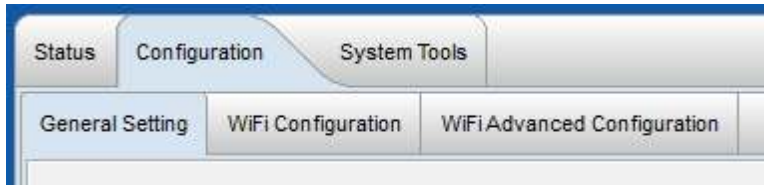
AP Info:

Index	2.4G Channel / 5G Channel	Download Traffic	Upload Traffic	Online Users	CPU Usage
1	Auto / Auto	0Mbps	0Mbps	0	9%

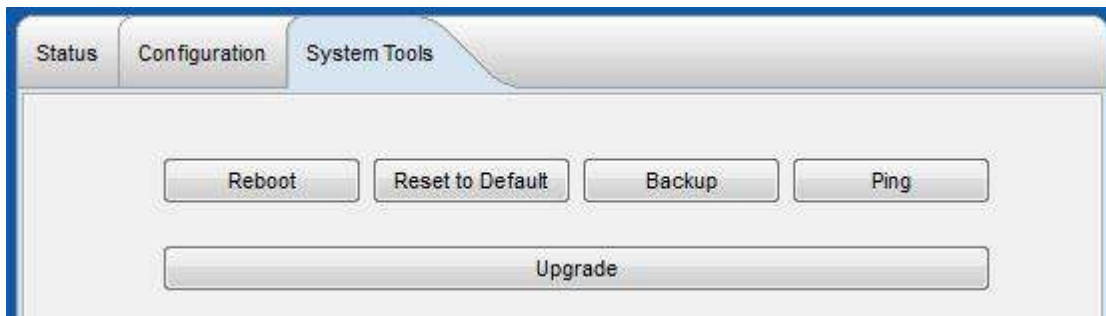
VAP Info:

SSID	Enable/Disable	VLAN ID	Number of Associated Stations	Authentication
default (2.4G VAP1)	Enable	Disable	0	Auto
default (2.4G VAP2)	Enable	Disable	0	Open
default (2.4G VAP3)	Enable	Disable	0	Open
default (2.4G VAP4)	Enable	Disable	0	Open
default (2.4G VAP5)	Enable	Disable	0	Open
default (2.4G VAP6)	Enable	Disable	0	Open
default (2.4G VAP7)	Enable	Disable	0	Open
default (2.4G VAP8)	Enable	Disable	0	Open

Configuration tab will appear only in specific AP situation, not All AP situation, as described as above. Manger wants to configure the dedicated AP about its general settings, WiFi configuration and WiFi advanced configuration as below diagram.



In System Tools tab for specific AP situation, system provide “Reboot”, “Reset to Default”, “Ping” and “Upgrade” tools as same as the ones for All AP situation, but there is one more command button “Backup” is activated to backup all configuration parameters of specific AP in the computer. They are shown as below.



Following sub-sections will describe these three functions for AP List in details.

4.6 Status

The screenshot displays the 'Rangerview UAP manager v0.9.20' interface. At the top, there are navigation buttons for 'Statistics', 'AP List', 'STA Users', 'Proposals', and 'Accounts'. A 'Welcome: admin' message is visible with a 'Logout' link. The 'AP List' button is highlighted, and a dropdown shows 'Online:1' and 'Offline:0'. On the right, there are settings for 'Refresh Time' (20 sec) and 'Font Size' (Medium). The main interface is divided into 'Discover' and 'Add AP' sections on the left, and a 'Status' section on the right. The 'Status' section is further divided into 'Status', 'Configuration', and 'System Tools' tabs. The 'Detail Info' tab is active, showing the following information:

Connection Type: Static
 WiFi Operation Mode: AP Only Mode

AP Info:

Index	2.4G Channel / 5G Channel	Download Traffic	Upload Traffic	Online Users	CPU Usage
1	Auto / Auto	0Mbps	0Mbps	1	4.70%

VAP Info:

SSID	Enable/Disable	VLAN ID	Number of Associated Stations	Authentication
smartlink (2.4G VAP1)	Enable	Disable	1	WPA2-PSK
default (2.4G VAP2)	Disable	Disable	0	Open
default (2.4G VAP3)	Disable	Disable	0	Open
default (2.4G VAP4)	Disable	Disable	0	Open
default (2.4G VAP5)	Disable	Disable	0	Open
default (2.4G VAP6)	Disable	Disable	0	Open
default (2.4G VAP7)	Disable	Disable	0	Open
Guest (2.4G VAP8)	Enable	Disable	0	Open

1. Connection Type: The connection type of the specified AP is Static or DHCP.
 2. WiFi Operation Mode: The WiFi Operation Mode of the specified AP is AP Only mode, WDS Hybrid mode, WDS Only mode or Universal Repeater.
 AP Info: (Physical AP)
 3. 2.4G Channel / 5G Channel: The operation frequency band of the specified AP is 2.4G or 5G.
 4. Download Traffic: The download usage bandwidth of the specified AP (Mbps).
 5. Upload Traffic: The upload usage bandwidth of the specified AP (Mbps).
 6. Online Users: The number of current online users on the specified AP.
 7. CPU Usage: The current CPU usage of the specified AP (%).
 8. Memory Usage: The current memory usage of the specified AP (%).
 9. Work Time: The work time of the specified AP from powering on.
- VAP Info: (Virtual AP)

1. SSID: The network ID of the specified VAP.
2. Enable/Disable: The specified VAP is enabled or disabled.
3. VLAN ID : The VLAN ID of the specified VAP.
4. Number of Associated Stations: The number of associated station links to the specified VAP.
5. Authentication: The adopted authentication protocol of the specified VAP.

4.7 Configuration

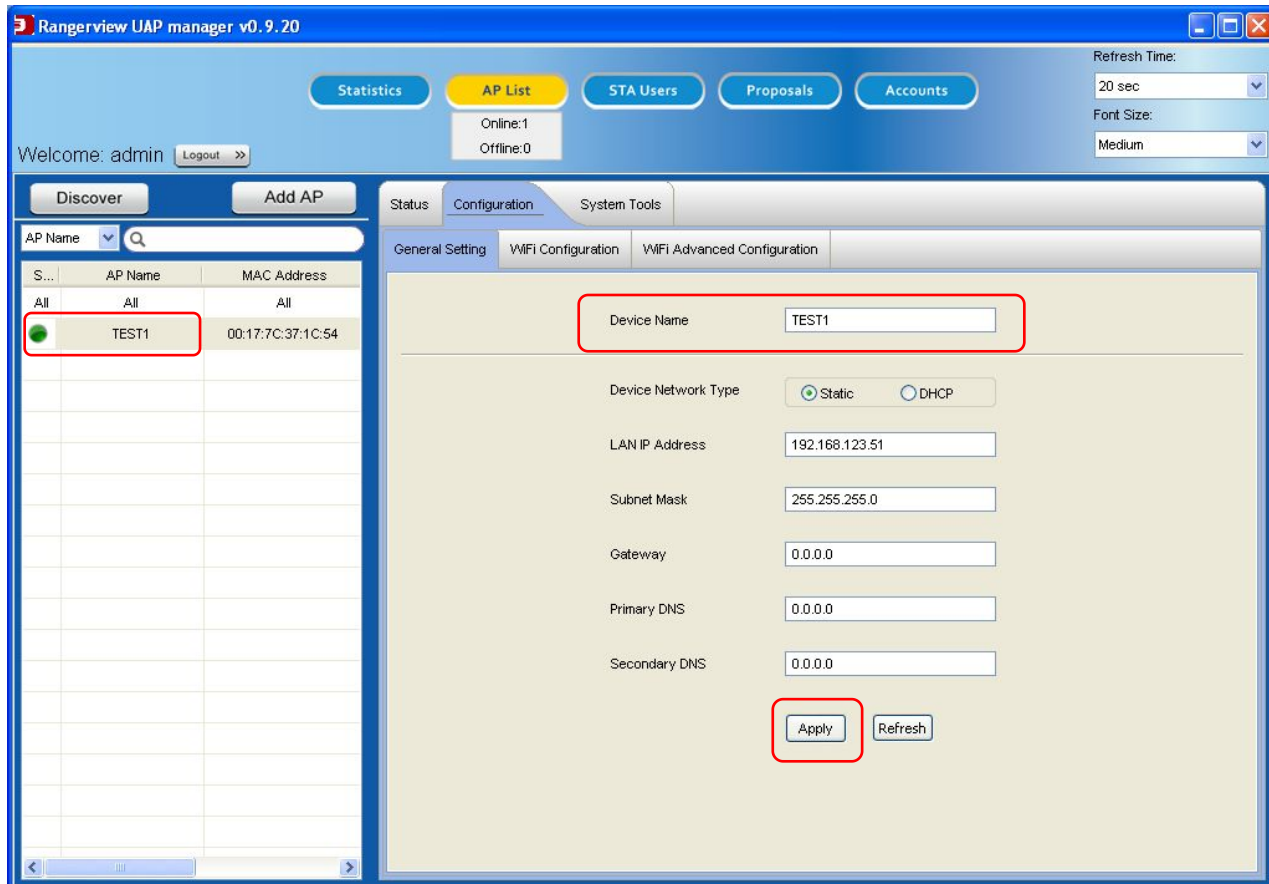
General Configuration

Device Name

You can enter the device name of specified AP on the “Device Name” field and click on the “Apply” button (red circle) to finish the setting. “Apply” button will be changed to inactivated state during the setting process, and the blue circle represents current value or state.

The screenshot shows the 'Rangerview UAP manager v0.9.20' web interface. The top navigation bar includes 'Statistics', 'AP List', 'STA Users', 'Proposals', and 'Accounts'. The 'AP List' section shows a table with columns for 'S...', 'AP Name', and 'MAC Address'. A row is highlighted with a blue circle, showing 'WIFI Access Point' and MAC address '00:17:7C:37:1C:54'. The main configuration area is titled 'Configuration' and includes tabs for 'General Setting', 'WIFI Configuration', and 'WIFI Advanced Configuration'. The 'Device Name' field is set to 'TEST1' and is highlighted with a red circle. Below it, there are fields for 'Device Network Type' (Static/DHCP), 'LAN IP Address' (192.168.123.51), 'Subnet Mask' (255.255.255.0), 'Gateway' (0.0.0.0), 'Primary DNS' (0.0.0.0), and 'Secondary DNS' (0.0.0.0). The 'Apply' button is highlighted with a blue circle, and the 'Refresh' button is also visible.

After setting is done, the status bar show “saved” and current value is changed (red circle), and “Apply” button will become activated.



1. Devcie Name: The custom name of the specified AP device. The factory default setting is empty. It’s recommended to set a custom device name for identifying the AP device.
2. Network Type: Please check the network enviroment with the selected AP, and select “Static” or “Dynamic” accordingly. If you select “Static” option, you have to specify additional “LAN IP Address”, “Subnet Mask”, and “Gateway”, and “ Primary DNS”, and “Secondary DNS” settings provided by your ISP.
3. IP address / Subnet Mask / Gateway: Enter the IP address, subnet mask, and gateway address if necessary.
4. Primary DNS / Secondary DNS: Input the Primary/Secondary DNS if necessary.

4.8 WiFi Configuration

You can change WiFi setting and click on the “Apply” button, then the status led of specified AP becomes yellow and status bar will show the progress (red circle)

The screenshot displays the Rangerview UAP manager v0.9.20 interface. The top navigation bar includes buttons for Statistics, AP List (highlighted), STA Users, Proposals, and Accounts. A status bar shows 'Online:1' and 'Offline:0'. The main content area is divided into 'Status', 'Configuration', and 'System Tools' tabs. Under 'Configuration', there are sub-tabs for 'General Setting', 'WiFi Configuration' (selected), and 'WiFi Advanced Configuration'. On the left, a table lists APs with columns for 'S...', 'AP Name', and 'MAC Address'. The first row shows 'TEST1' with MAC address '00:17:7C:37:1C:54'. The right pane shows the 'WiFi Configuration' settings for 'AP 1', including: Operation Band (2.4G Single Band), Wireless Module (checked), Wireless Operation Mode (AP Only Mode), Green AP (unchecked), AP Number (AP 1, checked), Network ID (SSID) (smartlink), SSID Broadcast (checked), VLAN ID (unchecked, 3), Max Supported Stations (unchecked, 0), WLAN Partition (unchecked), Channel (Auto), Wireless Mode (B/G/N mixed), Bandwidth (Auto), Authentication (WPA2-PSK), Encryption (AES), and Preshare Key (987654321). The 'Apply' button is highlighted with a red circle.

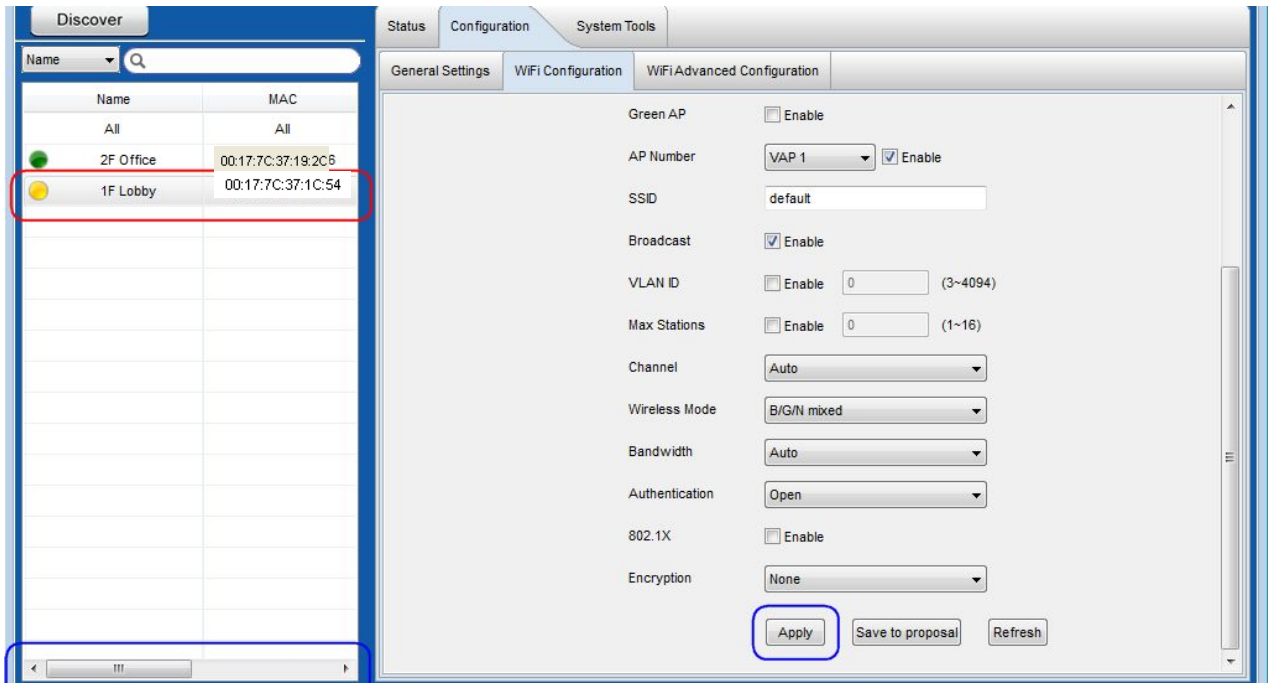
S...	AP Name	MAC Address
All	All	All
●	TEST1	00:17:7C:37:1C:54

WiFi Configuration Settings:

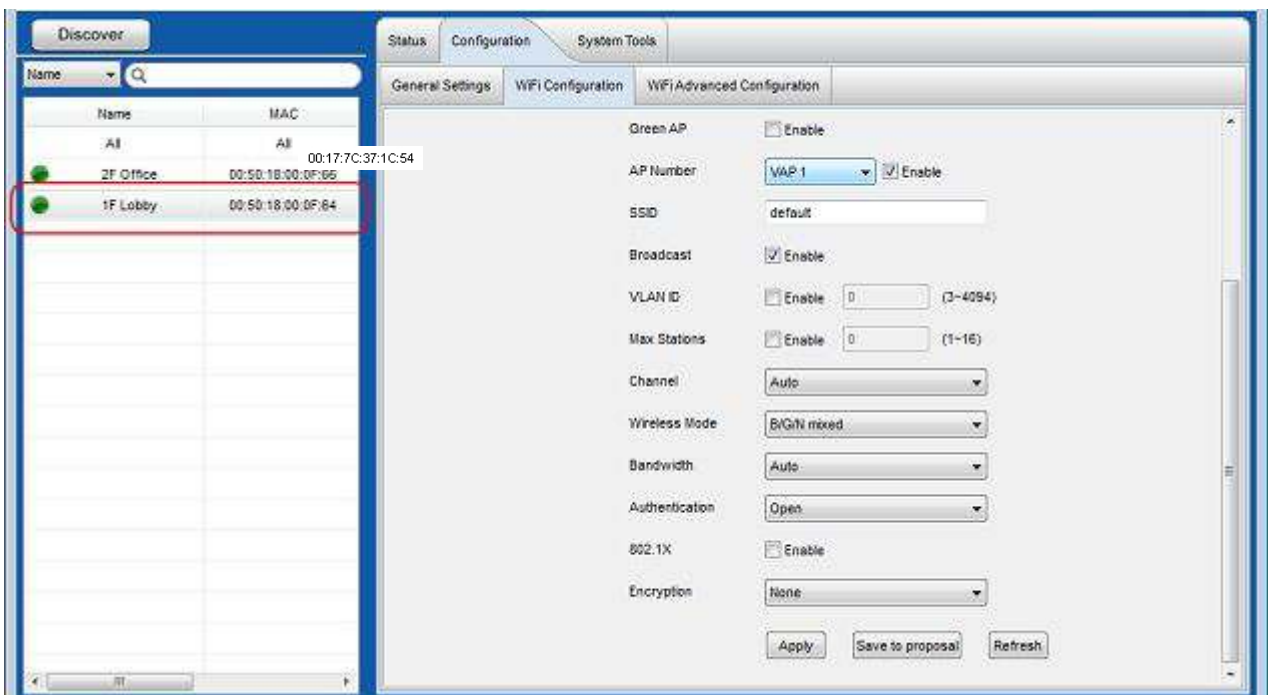
- Operation Band: 2.4G Single Band
- Wireless Module: Enable
- Wireless Operation Mode: AP Only Mode
- Green AP: Enable
- AP Number: AP 1 Enable
- Network ID (SSID): smartlink
- SSID Broadcast: Enable
- VLAN ID: Enable 3 (3~4094)
- Max Supported Stations: Enable 0 (1~16)
- WLAN Partition: Enable
- Channel: Auto
- Wireless Mode: B/G/N mixed
- Bandwidth: Auto
- Authentication: WPA2-PSK
- Encryption: AES
- Preshare Key: 987654321

Buttons: Apply, Save to proposal, Refresh

After the dedicated AP receives the request from AP controller, status bar will show “saved” and status led is still yellow (red mark).

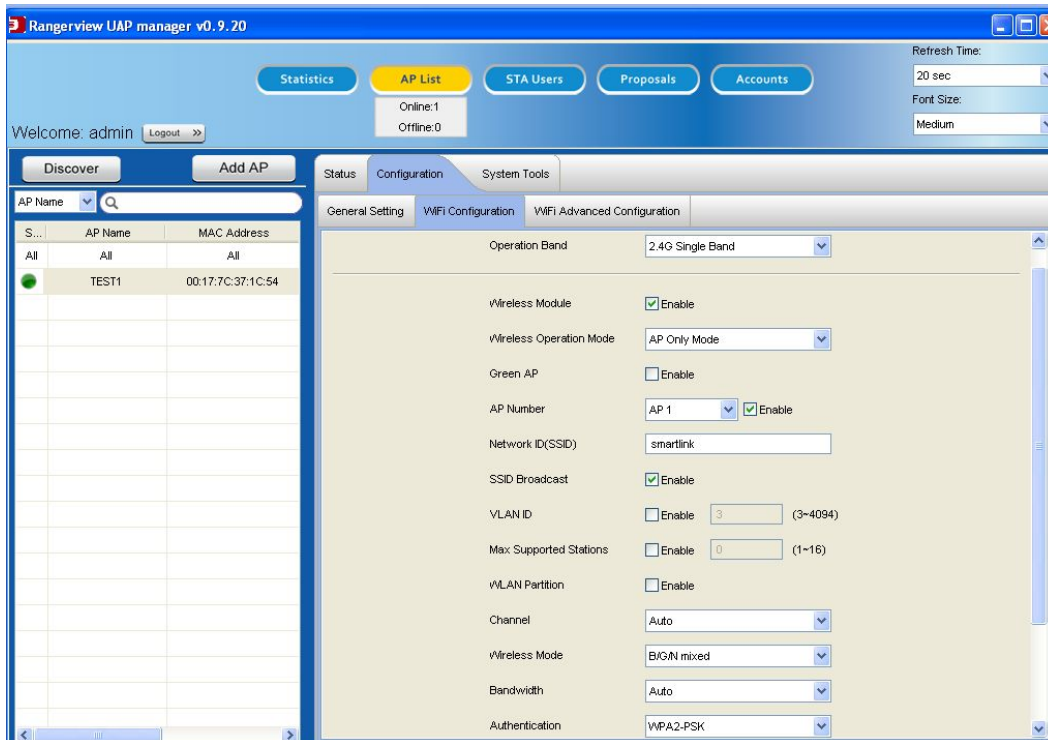


Status led will become green again when setting is done.



Trusted APs support 4 kinds of WiFi operation modes as described in the following 4 sections.

AP Only Mode



1. Wireless Module: Enable the wireless function.
2. Operation Mode: Choose “AP Only Mode” from the list.
3. Green AP: Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
4. AP Number: A physical AP can support up to 8 virtual APs (VAP-1 ~ VAP-8) for you to deploy your wireless network based on different applied services. Each virtual AP owns its property, like different SSID. For example, “Guest” SSID can let guest users access network resources via “Guest” virtual AP. You can select one virtual AP from VAP-1 to VAP-8 and configure its property beneath this field.
5. Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID.
6. Broadcast: The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients cannot find the device from beacons.

7.VLAN ID: Enable VLAN function and set the VLAN ID of virtual AP that will be carried out in uplink Ethernet port to represent the packets from the virtual AP.

8.Max Stations: Configure the maximum number of accepted client stations.

9.Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection. It's recommended to choose a channel that is not used in your environment to reduce radio interference.

10.Wireless Mode: This gateway supports 802.11a/b/g/n modes. For 2.4GHz operation band, you can also choose "N only", "G/N mixed" or "B/G/N mixed", and for 5GHz operation band, you can choose "A only", "N only", or "A/N mixed" according to your requirement. The factory default setting is "B/G/N mixed" for 2.4GHz and "A/N mixed" for 5GHz.

11. Bandwidth: The Bandwidth of the Channel Width. You may select 20 MHz or Auto.

12. Authentication & Encryption: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA/WPA2.

- Open

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router (WiFi gateway) containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration. In this mode you can enable 802.1x feature if you have another RADIUS server for users authentication. You need to input IP address, port, shared key of RADIUS server here.

- Shared

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

- Auto

The gateway will select appropriate authentication method according to WiFi client's request automatically.

- WPA-PSK

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don’t need additional RADIUS server for user authentication.

- WPA

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

- WPA2-PSK

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don’t need additional RADIUS server for user authentication.

- WPA2

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

- WPA-PSK/WPA2-PSK

If some of wireless clients can only support WPA-PSK, but most of them can support WPA2-PSK. You can choose this option to support both of them. Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. In this mode, you don’t need additional RADIUS server for user authentication.

- WPA/WPA2

If some of wireless clients can only support WPA, but most of them can support WPA2. You can choose this option to support both of them. Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

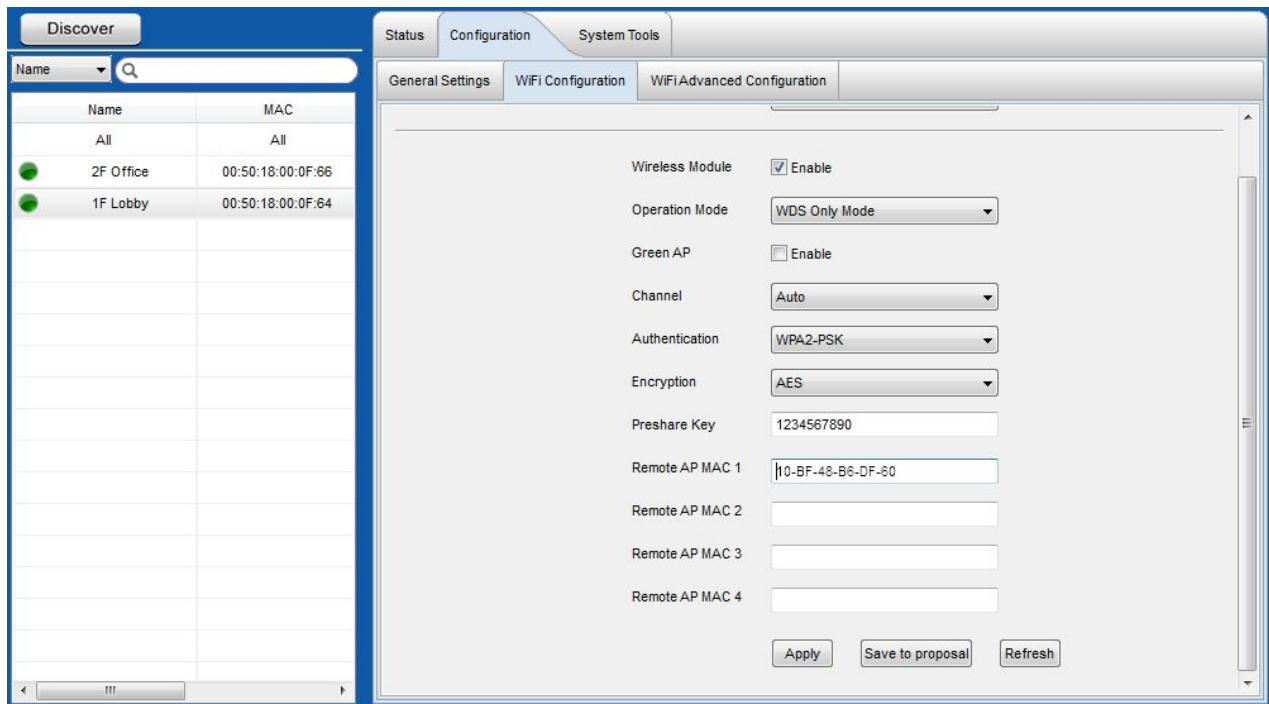
WDS Hybrid Mode

The screenshot displays the Rangerview UAP manager v0.9.20 web interface. The top navigation bar includes buttons for Statistics, AP List, STA Users, Proposals, and Accounts. A status bar shows 'Welcome: admin' with a Logout button and 'Online:1 Offline:0'. A 'Refresh Time' dropdown is set to 20 sec, and 'Font Size' is set to Medium. The main content area is divided into 'Status', 'Configuration', and 'System Tools' tabs. Under 'Configuration', there are sub-tabs for 'General Setting', 'WIFI Configuration', and 'WIFI Advanced Configuration'. The 'WIFI Configuration' sub-tab is active, showing various settings: Operation Band (2.4G Single Band), Wireless Module (checked Enable), Wireless Operation Mode (WDS Hybrid Mode), Lazy Mode (unchecked Enable), Green AP (unchecked Enable), AP Number (AP 1, checked Enable), Network ID (SSID) (smartlink), SSID Broadcast (checked Enable), VLAN ID (unchecked Enable, 3, (3~4094)), Max Supported Stations (unchecked Enable, 0, (1~16)), WLAN Partition (unchecked Enable), Channel (Auto), Wireless Mode (B/G/N mixed), and Bandwidth (Auto). On the left, there is a table for APs with columns for AP Name and MAC Address. The table contains one entry: TEST1 with MAC Address 00:17:7C:37:1C:54.

While acting as a wireless Bridge, Wireless Router 1 and Wireless Router 2 can communicate with each other through wireless interface (with WDS). Thus all Stations can communicate each other and are able to access Internet if Wireless Router 1 has the Internet connection.

1. Wireless Module: Enable the wireless function.
2. Operation Mode: Choose “WDS Hybrid Mode” from the list.
3. Lazy Mode: This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.
4. Green AP: Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
5. AP Number: A physical AP can support up to 8 virtual APs (VAP-1 ~ VAP-8) for you to deploy your wireless network based on different applied services. Each virtual AP owns its property, like different SSID. For example, “Guest” SSID can let guest users access network resources via “Guest” virtual AP. You can select one virtual AP from VAP-1 to VAP-8 and configure its property beneath this field.
6. Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID.
7. Broadcast: The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find this gateway through wireless network scan.
8. VLAN ID: Enable VLAN function and set the VLAN ID of virtual AP that will be carried out in uplink Ethernet port to represent the packets from the virtual AP.
9. Max Stations: Configure the maximum number of accepted client stations.
10. Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. In Hybrid WDS WiFi mode, this channel number needs to be same as the channel number of peer APs.
11. Wireless Mode: This gateway supports 802.11a/b/g/n modes. For 2.4GHz operation band, you can also choose “N only”, “G/N mixed” or “B/G/N mixed”, and for 5GHz operation band, you can choose “A only”, “N only”, or “A/N mixed” according to your requirement. The factory default setting is “B/G/N mixed” for 2.4GHz and “A/N mixed” for 5GHz.
12. Authentication & Encryption: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA2-PSK.
13. Remote AP MAC 1 ~ Remote AP MAC 4: If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

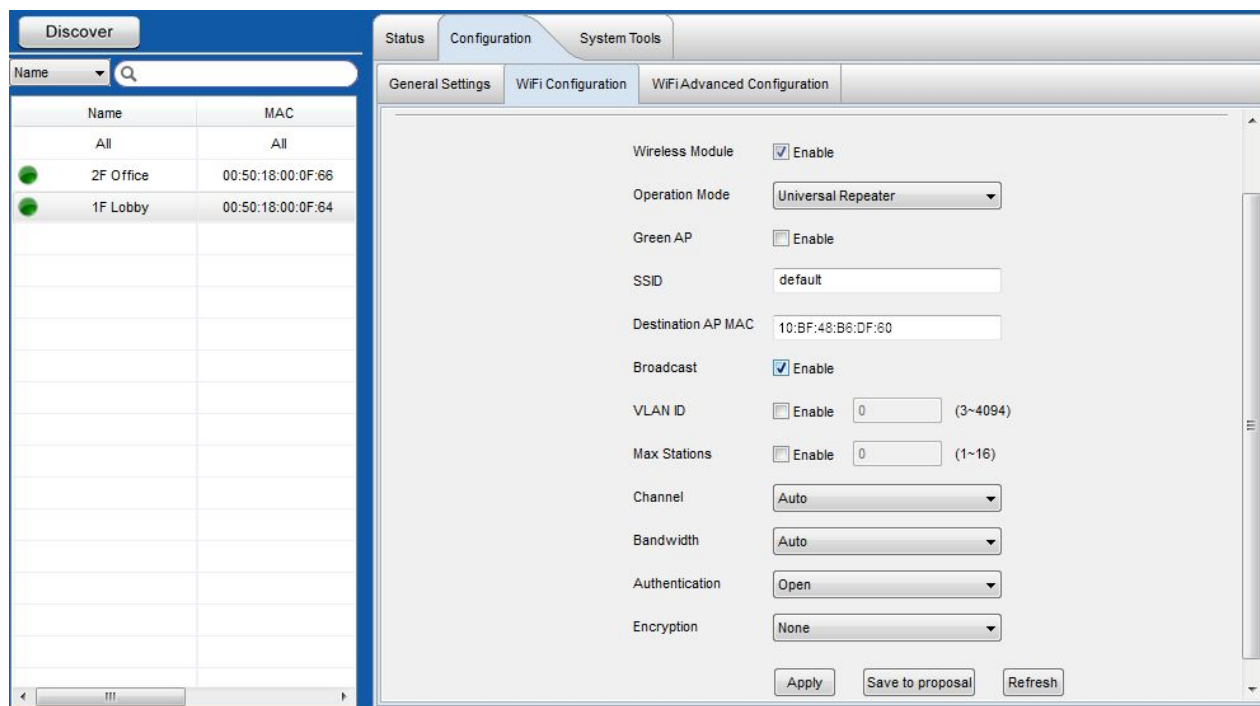
WDS Only Mode



WDS (Wireless Distributed System) function let this access point acts as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels, schools etc.

1. Wireless Module: Enable the wireless function.
2. Operation Mode: Choose “WDS Only Mode” from the list.
3. Green AP: Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
4. Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. In WDS Only WiFi mode, this channel number needs to be same as the channel number of peer APs.
5. Authentication & Encryption: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA2-PSK.
6. Remote AP MAC 1 ~ Remote AP MAC 4: You have to enter the wireless MAC address for each WDS peer one by one.

Universal Repeater Mode

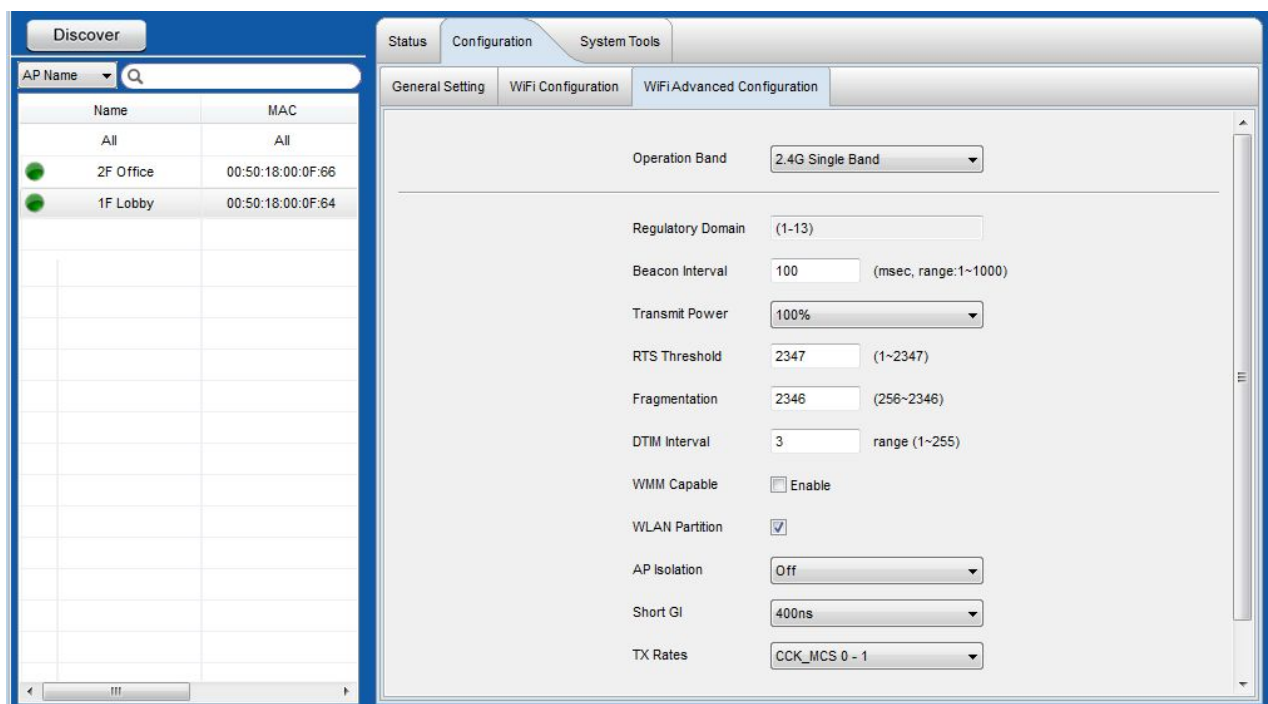


Universal Repeater is a technology used to extend wireless coverage. It provides the function to act as Adapter (client) and AP at the same time and can use this function to connect to a Root AP and use AP (SSID name is same with Root AP) function to service all wireless stations within its coverage. All the stations within the coverage of this access point can be bridged to the Root AP.

1. Wireless Module: Enable the wireless function.
2. Operation Mode: Choose "Universal Repeater Mode" from the list.
3. Green AP: Enable the Green AP function to reduce the power consumption when there is no wireless traffic.
4. Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID.
5. Destination AP MAC: The MAC address of the Destination AP.
6. Broadcast: The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as "Disable", the wireless clients can not find this gateway through wireless network scan.

7. VLAN ID: Enable VLAN function and set the VLAN ID of virtual AP that will be carried out in uplink Ethernet port to represent the packets from the virtual AP.
8. Max Stations: Configure the maximum number of accepted client stations.
9. Channel: The radio channel number. The permissible channels depend on the regulatory Domain. The factory default setting is auto channel selection. It's recommended to choose a channel that is not used in your environment to reduce radio interference.
10. Bandwidth: The Bandwidth of the Channel Width. You may select 20 MHz or Auto.
11. Authentication & Encryption: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA2-PSK.

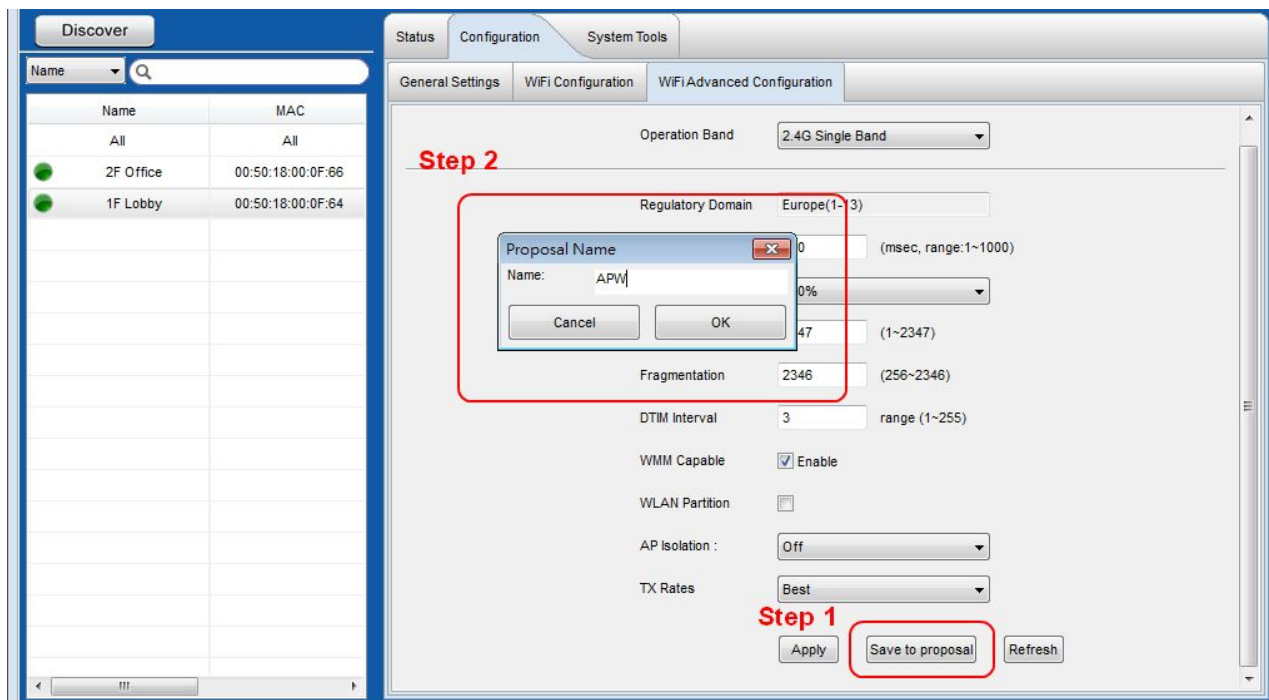
WiFi Advanced Configuration



1. Beacon interval: Beacons are packets sent by a wireless router to synchronize wireless devices.
2. Transmit Power: Normally the wireless transmission power operates at 100% out power specification of this device. You can lower down the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

3. RTS Threshold: If an excessive number of wireless packet collision occurred, the wireless performance will be affected. It can be improved by adjusting the RTS/CTS (Request to Send/Clear to Send) threshold value.
4. Fragmentation: Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage.
5. DTIM interval: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.
6. WMM Capable: WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
7. WLAN Partition: You can check the WLAN Partition function to separate the wireless clients. The wireless clients can't communicate each other, but they can access the internet and other Ethernet LAN devices.
8. AP Isolation: You can enable the AP Isolation function to prevent mobile devices connected to an AP from communicating directly with each other.
9. Short GI: Short GI can guard intervals which is used to ensure that distinct transmissions do not interfere with one another.
10. TX Rate: For WiFi transmit rate, you can choose "Best" for auto-adjustment according to WiFi signal quality in your environment, or you can fix it in certain TX rate. Please note the WiFi connection may be dropped if you fix at a higher data rate but in a noisy (poor RF signal quality) environment.

Save to Proposal



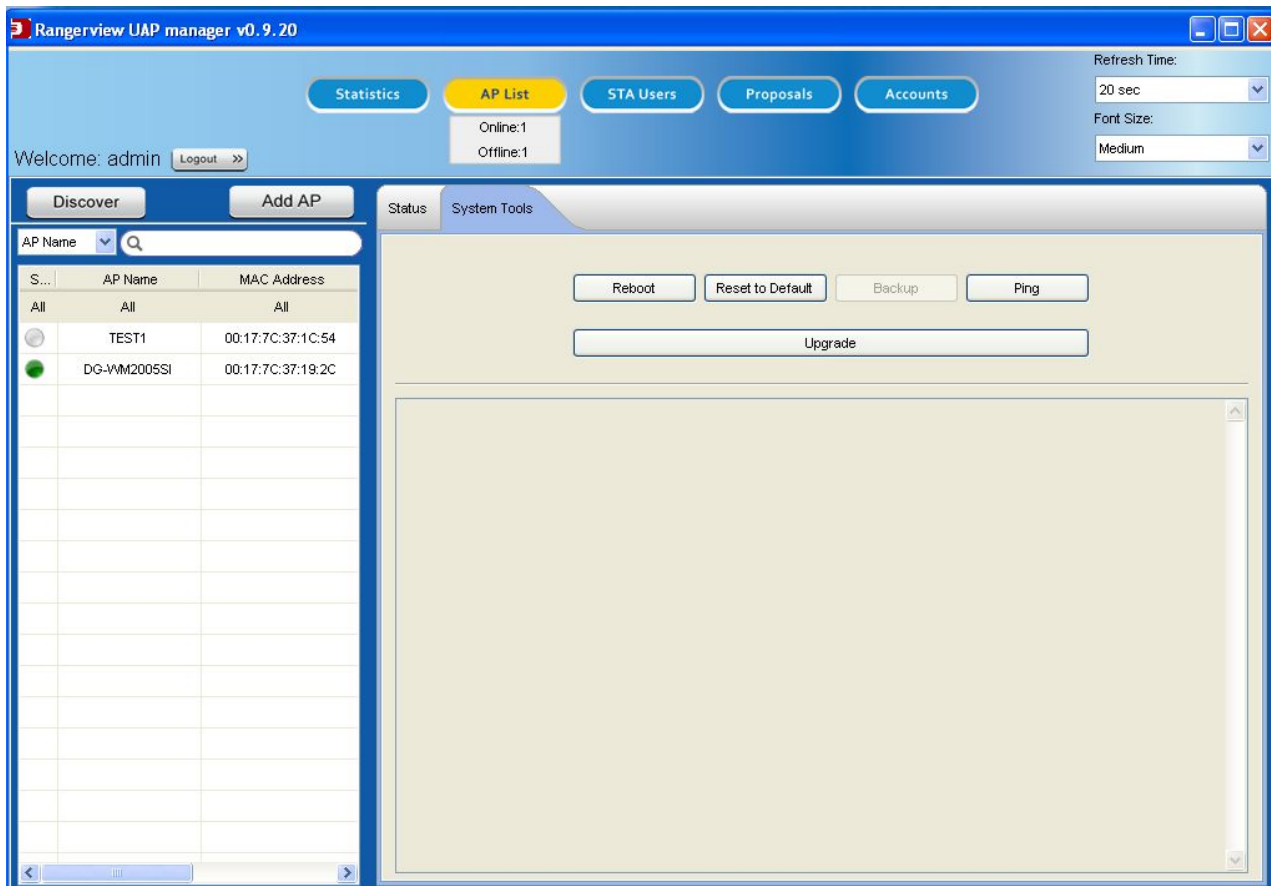
By clicking on the “Save to proposal” button, system will try to get current AP’s settings and save its contents to a proposal file in computer. Manager can check if it is existed or not by using “Proposal” function and searching the proposal list at the right side of window. An example is shown as below.

The screenshot displays the WiFi Configuration interface, divided into three main sections:

- Left Panel:** A table listing Access Points (APs) with columns for Name and MAC. Two APs are listed: "2F Office" (MAC: 00:50:18:00:0F:66) and "1F Lobby" (MAC: 00:50:18:00:0F:64).
- Center Panel:** The "WiFi Advanced Configuration" tab is active, showing various settings for the selected AP. Settings include:
 - Operation Band: 2.4G Single Band
 - Wireless Module: Enable
 - Operation Mode: AP Only Mode
 - Green AP: Enable
 - AP Number: VAP 1 Enable
 - SSID: (empty text field)
 - Broadcast: Enable
 - VLAN ID: Enable (3~4094)
 - Max Stations: Enable (1~16)
 - Channel: Auto
 - Wireless Mode: N only
 - Bandwidth: 20Mhz
 - Authentication: Open
 - 802.1X: Enable
- Right Panel:** A control area with buttons for "New", "Load", "Edit", and "Save", followed by an "Apply to APs" button. Below these is a list of AP names, with "1F" and "APW" visible. The "APW" entry is highlighted with a red rectangle.

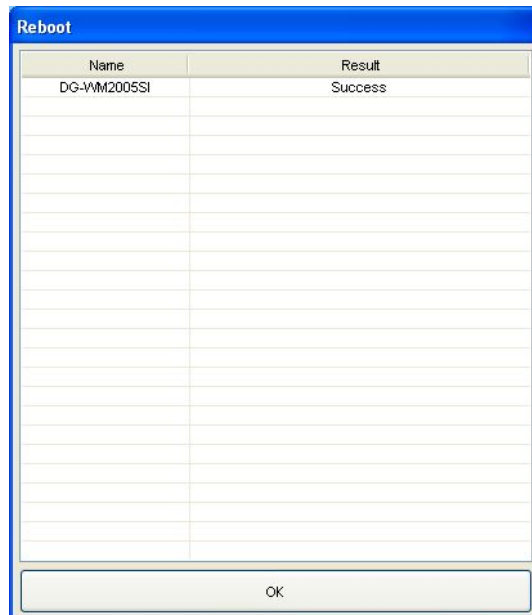
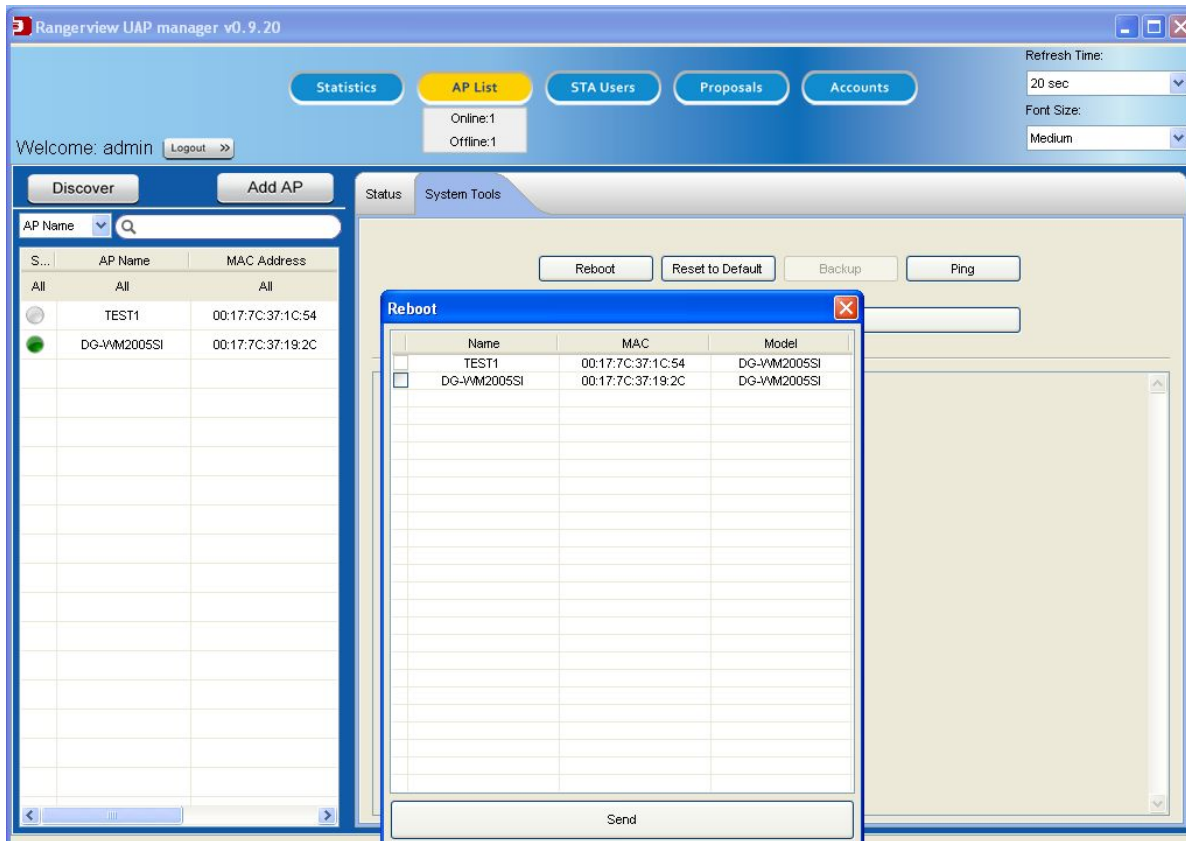
4.9 System Tools

There are totally 5 tools buttons for controlling one specific AP or all APs. They are “Reboot”, “Reset to Default”, “Backup”, “Ping”, and “Upgrade”. But “Backup” button will be inactive when manager choose “All” APs in AP list that he want to access. Other four buttons are active at both one specific AP and all APs cases. Following diagram shows the case of accessing one specific AP.



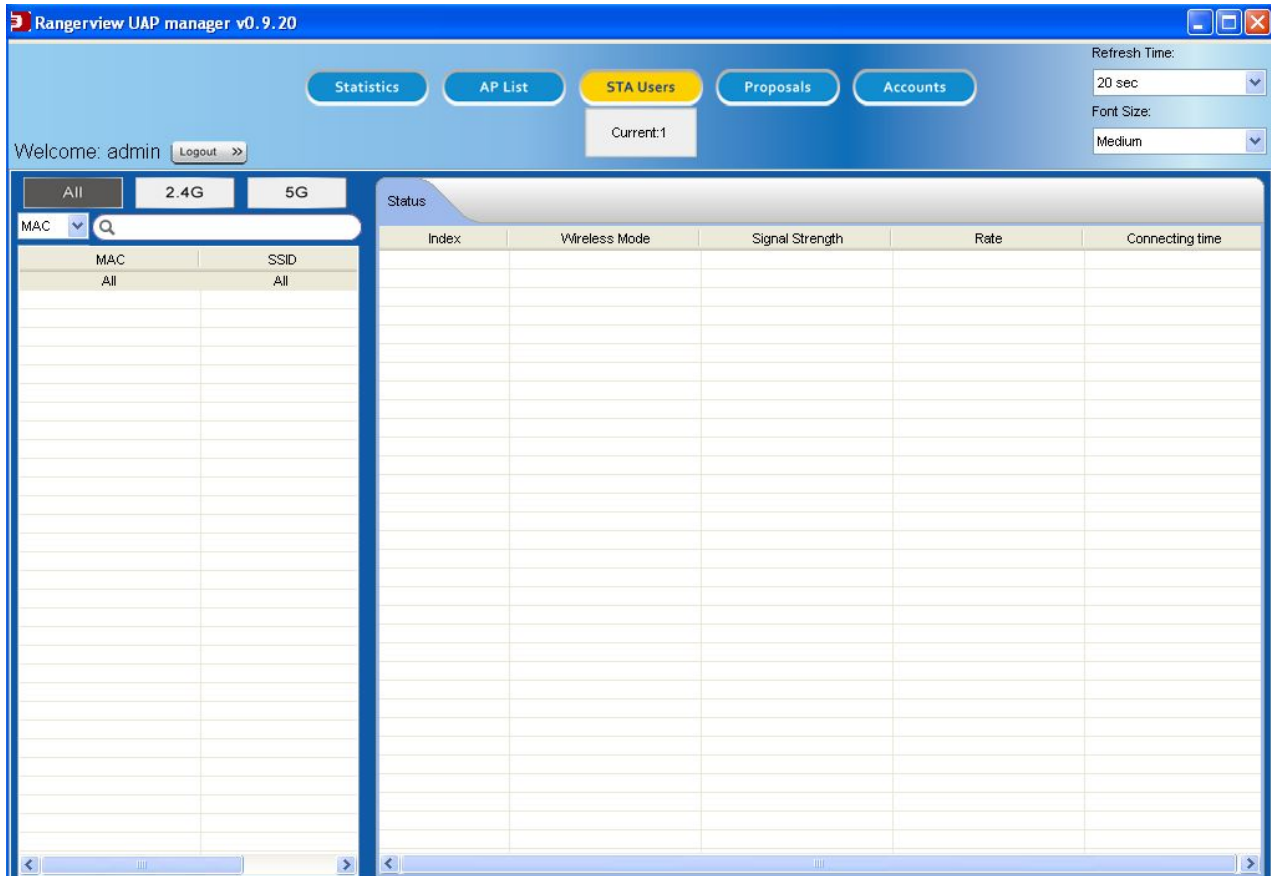
1. Reboot: Reboot the specified AP or all APs.
2. Reset to Default: Reset the specified AP or all APs to default configuration.
3. Backup: Backup the specified AP’s settings to PC.
4. Ping: Ping the specified AP or all APs to check if they are live or not.
5. Upgrade: Upgrade the specified AP or all APs with chosen FW or configuration binary file by manager.

You can select multiple APs to reboot/reset/ping/upgrade when selecting “All” in AP list. System will show the operation results for all chosen APs as shown as below.



4.10 STA Users

When manager moves his mouse over or clicks on the “STA Users” function button, the count of current STA users will show beneath “AP List” button. It is shown as below.



Clicking on the button, the screen will be divided into 2 windows for the function. At the left window, it is STA user specifying part, including the selection of 2.4G WiFi, 5G WiFi or both, the quick search and the STA user list. However, at the right window, it is the status of one specific STA user or all STA users, including their wireless mode, signal strength, data rate and working time, as shown as below.

Rangerview UAP manager v0.9.20

Statistics AP List **STA Users** Proposals Accounts

Refresh Time: 20 sec
 Font Size: Medium

Welcome: admin Logout >> Current:1

All 2.4G 5G

MAC All 70-F1-A1-2F-03-B2

Index	Wireless Mode	Signal Strength	Rate	Connecting time
1	G	88	54	00:02:14

Manager can view the status of all STA users that are existed in the Intranet by using “STA Users” function with following steps.

Step 1: Click on the “STA Users” function button.

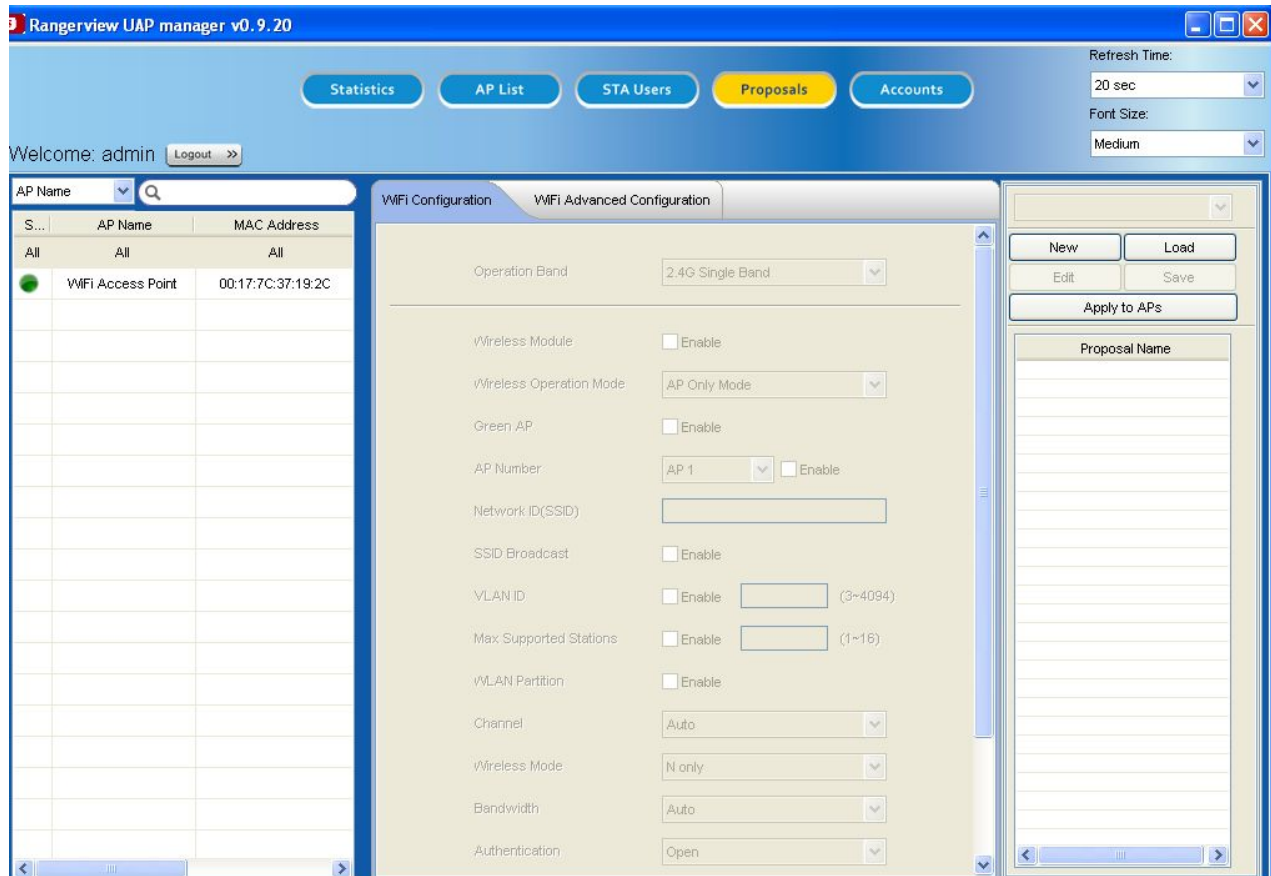
Step 2: Choose 2.4G WiFi, 5G WiFi or both of STA users to check their status.

Step 3: You also can choose one base type of MAC, SSID or Name in the Quick Search, and input one keyword in searching field to find target STA user.

Step 4: AP controller will show their or its status.

4.11 Proposals

Here, proposal means WiFi configurations, AP Management software supports multiple APs to configuration in this section simultaneously.

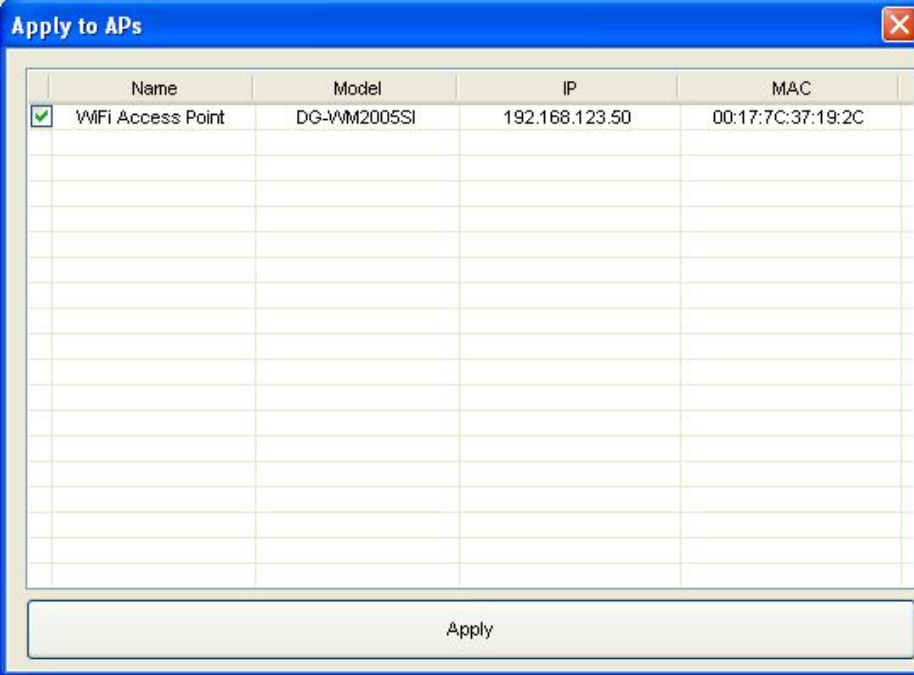


New: Add one proposal.

Load: Load proposal in the Folders of Desktop

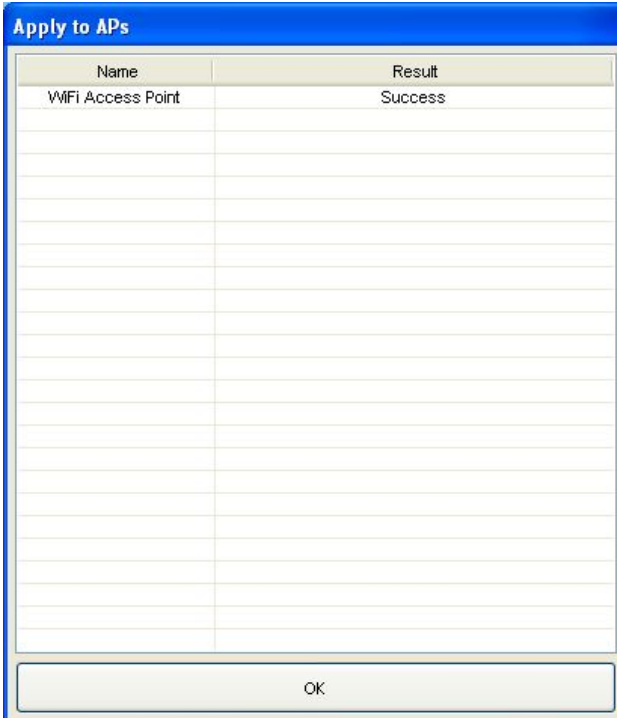
Edit and Save: Click on Edit to edit the access point details and click on Save to save the settings.

Apply to APs: Select one Proposal to store APs.



	Name	Model	IP	MAC
<input checked="" type="checkbox"/>	WiFi Access Point	DG-WM2005SI	192.168.123.50	00:17:7C:37:19:2C

Apply



Name	Result
WiFi Access Point	Success

OK

4.12 Accounts

There are two groups: One is Admin, the other is User. Accounts in Admin Group can discover and configure APs. Accounts in User Group only can browse, and there are some different permission in Accounts.

Admin group (Default admin): Add / Edit / Delete account

Admin group (Limited admin) : Browse account

User group : Browse account

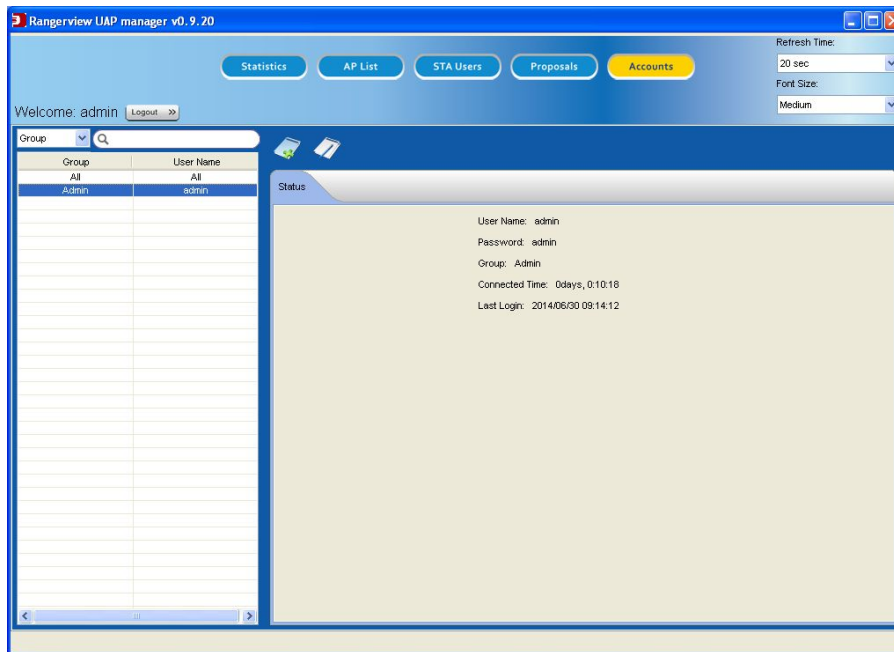
Default admin selects All (Add)

The screenshot displays the 'Accounts' page in the Rangerview UAP manager v0.9.20. The interface includes a navigation bar with buttons for 'Statistics', 'AP List', 'STA Users', 'Proposals', and 'Accounts'. A 'Welcome: admin' message and a 'Logout' button are visible. On the right, there are settings for 'Refresh Time' (20 sec) and 'Font Size' (Medium). The main content area features a 'Group' dropdown menu and a search bar. Below this, there are two tables. The first table lists user groups, and the second table shows the status of the 'admin' user.

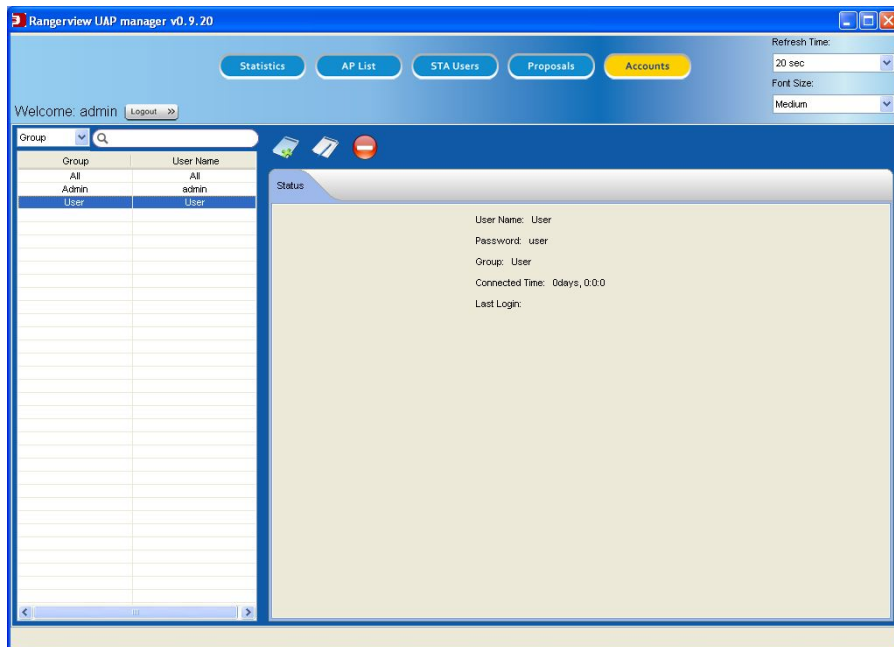
Group	User Name
All	All
Admin	admin

User Name	Connected Time	Last Login Time
admin	0days, 0:8:51	2014/06/30 09:14:12

Default admin selects default admin (Add / Edit)



Default admin selects other account (Add / Edit / Delete)



Admin / User group (Read only)

Group:

Group	User Name
All	All
Admin	admin
User	User

Status

User Name	Connected Time	Last Login Time
admin	0days, 0:12:14	2014/06/30 09:14:12
User	0days, 0:0:0	

5 Troubleshooting

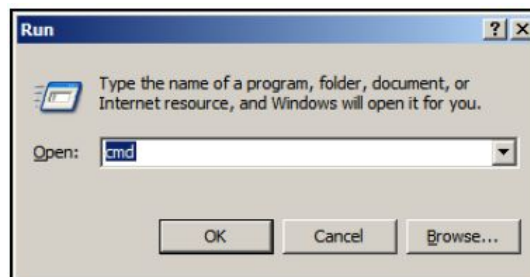
This Chapter provides solutions to problems for the installation and operation of the Wi-Fi DG-WM2005SI. You can refer to the following if you are having problems.

1 Why can't I configure the device even if the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the Wi-Fi Access Point is responding.

Go to **Start > Run**.

1. Type **cmd**.



2. Press **OK**.
3. Type **ipconfig** to get the IP of default gateway.
4. Type "**ping 192.168.123.50**". Assure that you ping the correct IP Address assigned to the WiFi DG-WM2005SI. It will show four replies if you ping correctly.

```
Pinging 192.168.123.254 with 32 bytes of data:  
Reply from 192.168.123.50: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.50: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.50: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.50: bytes=32 time<1ms TTL=64
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The

installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on “My Computer” > Properties**.
2. **Select the Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on **“Network Adapters”**.
5. Right-click on **Wireless Card bus Adapter** or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click **“OK”**.

2 What can I do if my Ethernet connection does not work properly?

- A. Make sure the RJ45 cable connects with the device.
- B. Ensure that the setting on your Network Interface Card is “Enabled”.
- C. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and using a patch cable is recommended.
- D. If the connection still does not work properly, then you can reset it to default.

3 Something wrong with the wireless connection?

A. Can’t setup a wireless connection?

- I. Ensure that the SSID and the encryption settings are exactly the same to the Clients.
- II. Move the Wi-Fi DG-WM2005SI and the wireless client into the same room, and then test the wireless connection.

- III. Disable all security settings such as **WEP** and **MAC Address Control**.
- IV. Turn off the Wi-Fi DG-WM2005SI and the client, then restart it and then turn on the client again.
- V. Ensure that the LEDs are indicating normally. If not, make sure that the power and Ethernet cables are firmly connected.
- VI. Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- VII. If you are using other wireless devices, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motor.

B. What can I do if my wireless client cannot access the Internet?

- I. Out of range: Put the device closer to your client.
- II. Wrong SSID or Encryption Key: Check the SSID or Encryption setting.
- III. Connect with wrong AP: Ensure that the client is connected with the correct Access Point.
 - i. **Right-click** on the **Local Area Connection icon** in the taskbar.
 - ii. Select **View Available Wireless Networks in Wireless Configure**. Ensure you have selected the correct available network.
 - iii. Reset the Wi-Fi DG-WM2005SI to default setting

C. Why does my wireless connection keep dropping?

- I. Antenna Orientation.
 - i. Try different antenna orientations for the Wi-Fi DG-WM2005SI.

- ii. Try to keep the antenna at least 6 inches away from the wall or other objects.
- II. Try changing the channel on the Wi-Fi DG-WM2005SI, and your Access Point and Wireless adapter to a different channel to avoid interference.
- III. Keep your product away from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4 What to do if I forget my encryption key?

1. Go back to advanced setting to set up your Encryption key again.
2. Reset the Wi-Fi DG-WM2005SI to default setting

5 How to reset to default?

1. Ensure the Wi-Fi DG-WM2005SI is powered on
2. Find the **Reset** button on the right side
3. Press the **Reset** button for 8 seconds and then release.
4. After the Wi-Fi DG-WM2005SI reboots, it goes back to the factory **default** settings.

6 Why do I get an error after executing AP Management software Controller?

This error is generated because AP Management Software can't detect any network. You can follow the steps below to check network:

- a. Make sure the RJ45 cable connects with the router.
- b. Ensure that the setting on your Network Interface Card adapter is "Enabled" and ensure it has an IP Address (not "0.0.0.0").
- c. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and use a patch cable is recommended.

7 Why can't I find any AP?

- a. Make sure the RJ45 cables are connected to APs.
- b. Make sure the AP is DIGISOL.
- c. Please add windows firewall exception for AP Management software Controller or disable the windows firewall.
- d. If AP Management software Controller still can't find any AP, you can reset AP to default and discover again by using AP Management software Controller.

8 Why can't I configure settings by using AP Management software Controller?

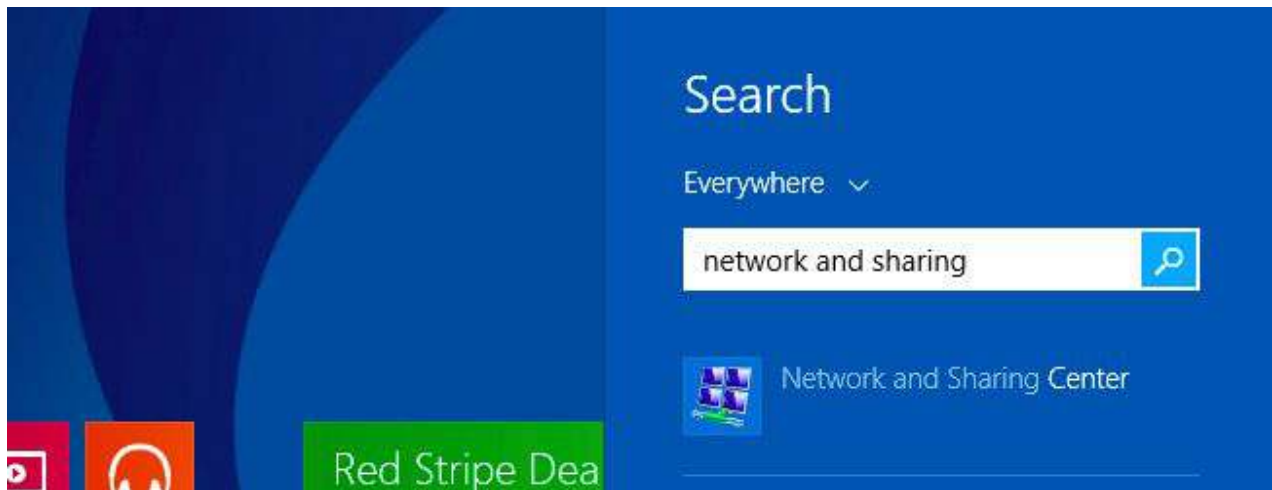
May be the AP status is busy (yellow light), please wait for the AP status to become normal (green light).

Appendix A. Assigning a Static IP in Windows PC

When organizing your local network it's easier to assign each computer it's own IP address than using DHCP. Here we will take a look at doing it in XP, Windows 7, Windows 8 and Windows 8.1.

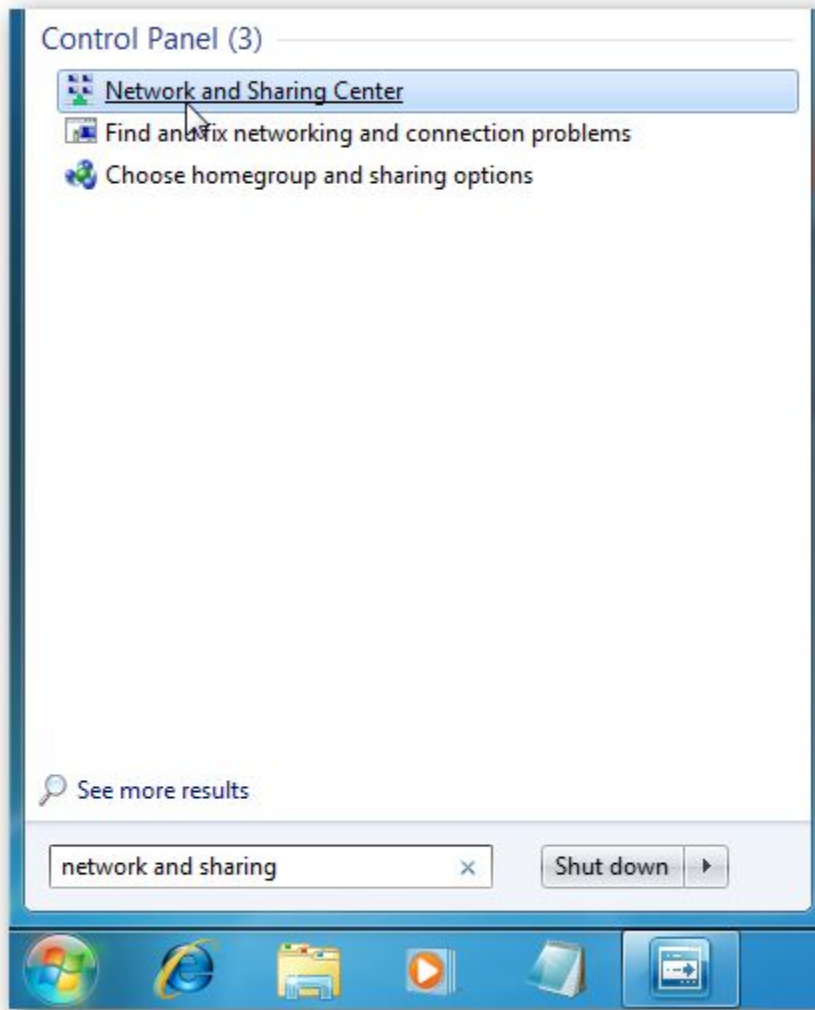
If you have a home network with several computers and devices, it's a good idea to assign each of them a specific address. If you use DHCP (*Dynamic Host Configuration Protocol*), each computer will request and be assigned an address every time it's booted up. When you have to do troubleshooting on your network, it's annoying going to each machine to figure out what IP they have.

Using Static IPs prevents address conflicts between devices and allows you to manage them more easily. Assigning IPs to Windows is essentially the same process, but getting to where you need to be varies between each version.

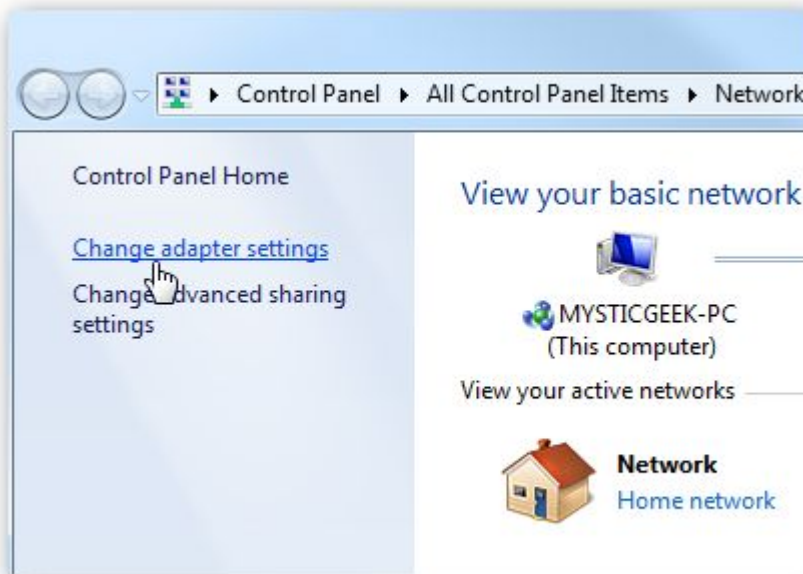


Windows 7 or Windows 8.x

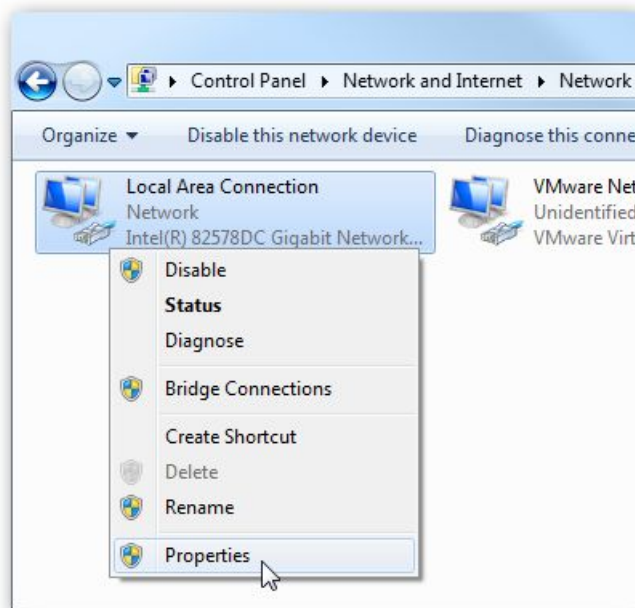
To change the computer's IP address in Windows 7, type *network and sharing* into the Search box in the Start Menu and select Network and Sharing Center when it comes up. If you are in Windows 8.x it will be on the Start Screen itself, like the screenshot at the top of this article.



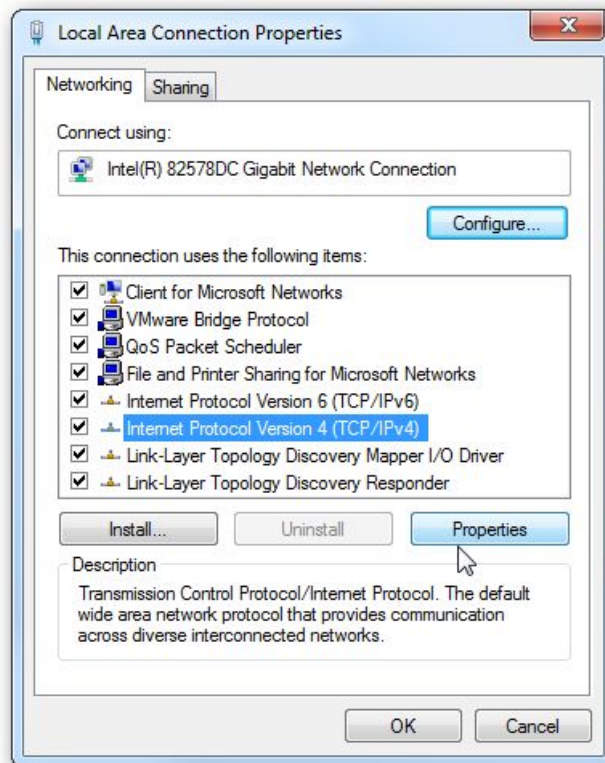
Then when the Network and Sharing Center opens, click on *Change adapter settings*. This will be the same on Windows 7 or 8.x.



Right-click on your local adapter and select Properties.

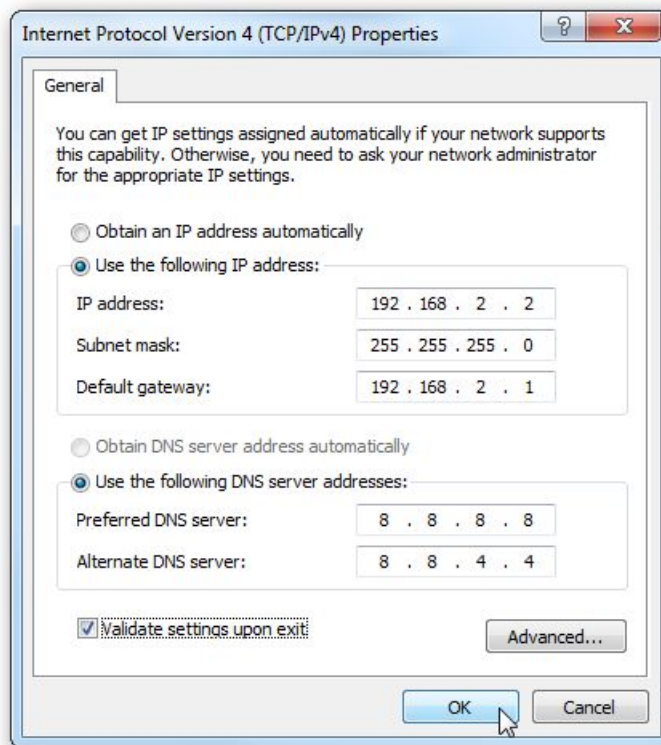


In the Local Area Connection Properties window highlight *Internet Protocol Version 4 (TCP/IPv4)* then click the Properties button.

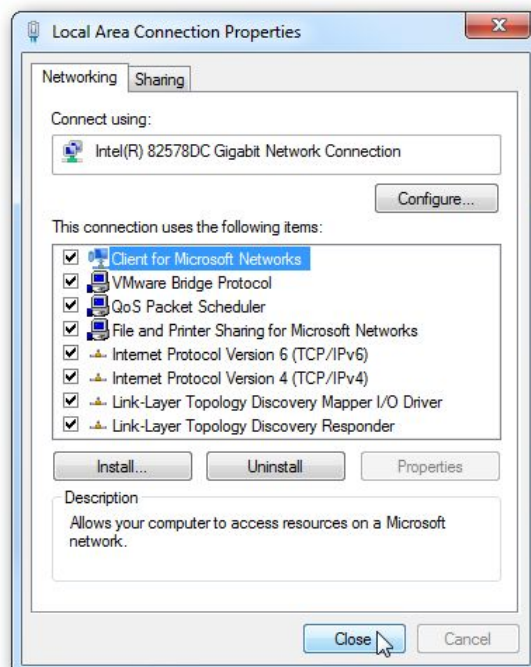


Now select the radio button *Use the following IP address* and enter in the correct IP, Subnet mask, and Default gateway that corresponds with your network setup. Then enter your Preferred and Alternate DNS server addresses. Here we're on a home network using a simple Class C network configuration and Google DNS.

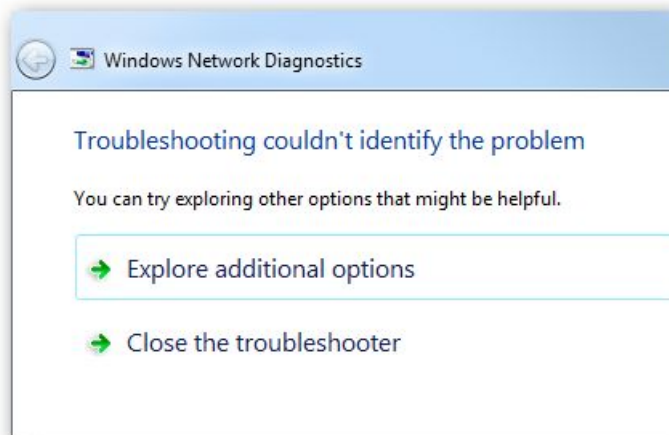
Check *Validate settings upon exit* so Windows can find any problems with the addresses you entered. When you're finished click OK.



Now come out of the Local Area Connections Properties window.



Windows 7 will run network diagnostics and verify that the connection is good. Here we had no problems with it, but if you did, you could run the network troubleshooting wizard.



Now you can open the command prompt and do an *ipconfig* to see the network adapter settings have been successfully changed.

```
Windows IP Configuration

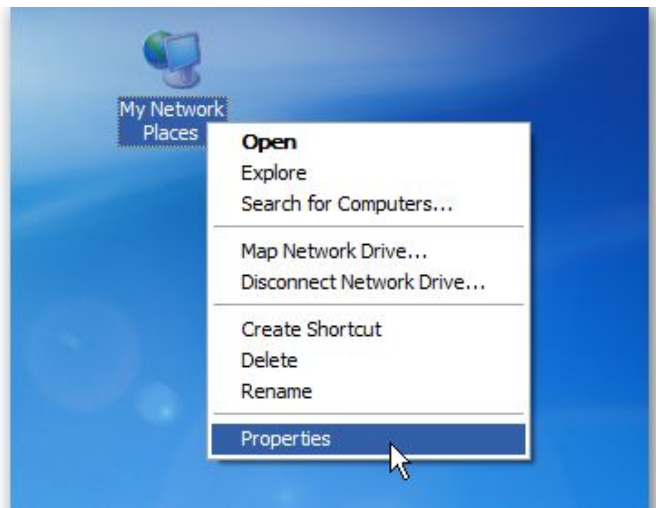
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::11e3:1d23:a...
    IPv4 Address. . . . . : 192.168.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1
```

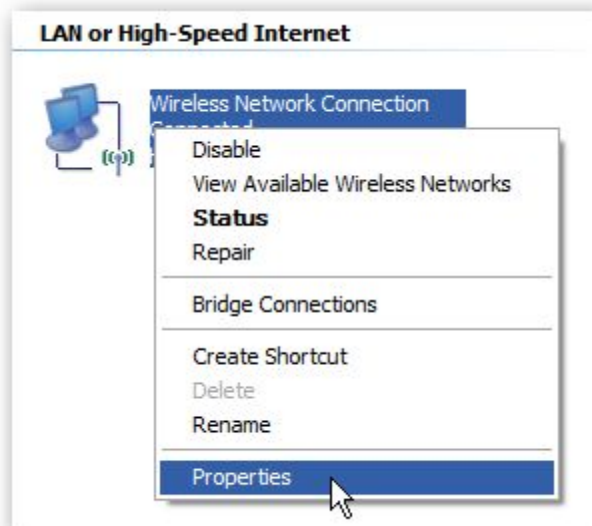
Windows XP

In this example we're using XP SP3 Media Center Edition and changing the IP address of the Wireless adapter.

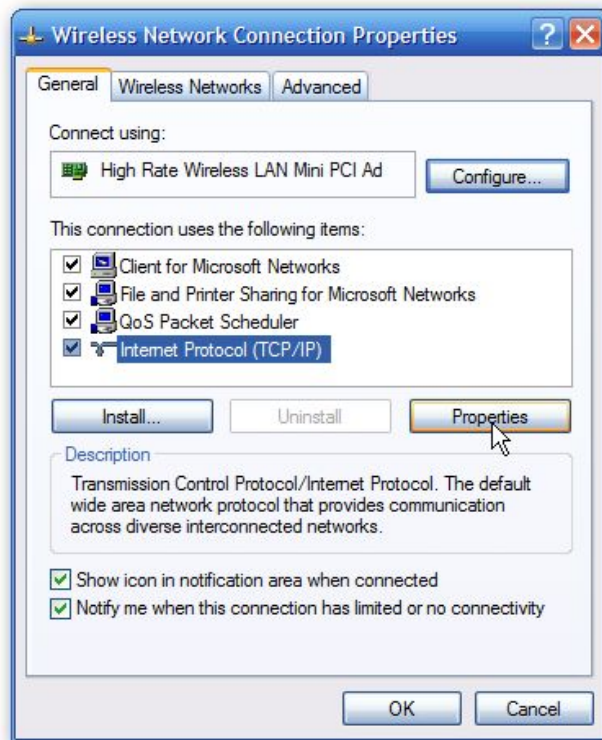
To set a Static IP in XP right-click on My Network Places and select Properties.



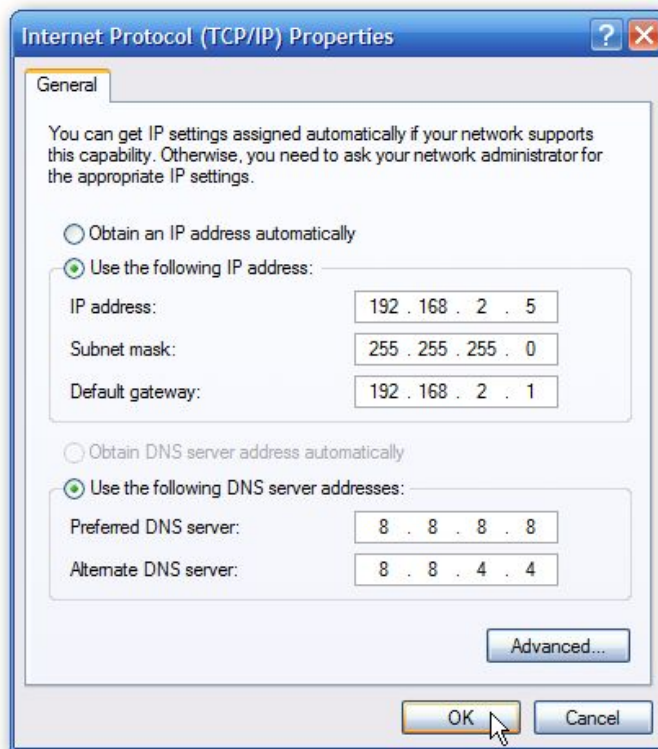
Right-click on the adapter you want to set the IP for and select Properties.



Highlight *Internet Protocol (TCP/IP)* and click the Properties button.



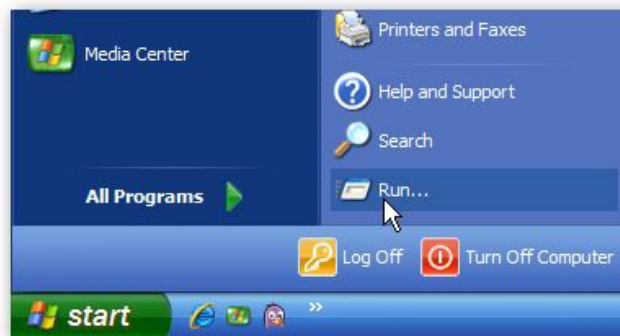
Now change the IP, Subnet mask, Default Gateway and DNS Server Addresses. When you're finished click OK.



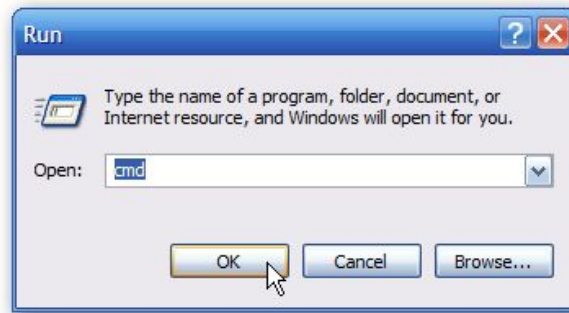
You will need to come out of the Network Connection Properties screen before the changes go into effect.



Again you can verify the settings by doing an *ipconfig* in the command prompt. In case you're not sure how to do this, click on Start then Run.



In the Run box type in *cmd* and click OK.



Then at the prompt type in *ipconfig* and hit Enter. This will show the IP address for the network adapter you changed.

```
C:\Documents and Settings\XP Geek>ipconfig
Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . : 
    IP Address. . . . . : 192.168.2.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\Documents and Settings\XP Geek>
```

If you have a small office or home network, assigning each computer a specific IP address makes it a lot easier to manage and troubleshoot network connection problems.

[Source: How to Assign a Static IP Address in Windows 7, 8, XP, or Vista; <http://www.howtogeek.com/howto/19249/how-to-assign-a-static-ip-address-in-xp-vista-or-windows-7/>]

Please refer www.digisol.com for warranty information in your region.