

# WizFi630 User Manual

(Version 1.1)



© 2012 WIZnet Co., Ltd. All Rights Reserved.

For more information, please visit our website at <http://www.wiznet.co.kr>

## Certification Information

### CE for Class B ITE

#### INFORMATION TO THE USER

Hereby, WIZnet. Declares that this WizFi630 is in compliance with the essential requirements and other relevant provisions of directive 1999/5/EC and other relevant provisions of directive 1999/5/EC.

**WARNING:** This is a class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures

### FCC for Class B ITE

#### INFORMATION TO THE USER

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no Guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**WARNING:** This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made

## Document Revision History

Date	Revision	Changes
2012-07-02	1.0	Release
2012-07-17	1.1	Change WizFi630's picture at P10 Modify error sentence - P6, P18,P19 : WIZ630wi → WizFi630 - P24 : DNS server → DNS server address - P38 : WDS → WPS

## <Contents>

<b>1. Introduction .....</b>	<b>6</b>
1.1. Features .....	7
1.2. Wireless Specifications .....	8
1.3. Hardware Specifications.....	9
1.4. Software Specifications .....	10
1.5. EVB Construction .....	10
1.5.1. Contents.....	10
1.6. Block Diagram.....	12
<b>2. Operation Mode and Description of Menu.....</b>	<b>13</b>
2.1. Operation Mode .....	13
2.1.1. Access Point.....	13
2.1.2. Gateway.....	14
2.1.3. Client (Station).....	14
2.1.4. AP-Client Mode .....	15
2.1.5. Ad-hoc Mode .....	15
2.2. Menu List by Operation Mode .....	16
2.2.1. Access Point (Bridge) Mode .....	16
2.2.2. Gateway (Router) Mode.....	17
2.2.3. Client (Station) Mode .....	18
2.2.4. AP-Client Mode .....	19
2.2.5. Ad-hoc Mode .....	21
2.3. Internet Setting.....	23
2.3.1. Internet connection setting.....	23
2.3.2. Local network setting.....	25
2.3.3. DHCP Client Information .....	26
2.3.4. VPN setting.....	26
2.3.5. Static Routing Setting .....	27
2.3.6. QoS(802.1p) Setting.....	28
2.3.7. VLAN(802.1p).....	29
2.4. Wireless setting .....	30
2.4.1. Basic settings.....	30
2.4.2. Advanced Wireless Settings .....	32
2.4.3. Wireless Security.....	35
2.4.4. WDS(Wireless Distribution System) Setting.....	38
2.4.5. WPS Setting.....	39
2.4.6. Wireless network status.....	41
2.4.7. AP Wireless Statistics .....	42
2.4.8. Station QoS/DLS(Direct Link Setup) Configurations.....	44
2.4.9. Profile .....	45
2.4.10. Link Status.....	46
2.4.11. Site Survey .....	47
2.4.12. WI-FI Multi-Bridge settings.....	48
2.5. Serial to LAN(Wired and Wireless).....	49
2.5.1. Main Connection settings .....	50

2.5.2.	Aux Connection Settings .....	50
2.5.3.	Packing Condition (Incoming serial data packing condition).....	51
2.5.4.	Ethernet Data Tagging Option .....	51
2.6.	Firewall settings.....	52
2.6.1.	DMZ.....	52
2.6.2.	Port forwarding.....	53
2.6.3.	Packet filtering.....	54
2.6.4.	Contents filtering .....	55
2.6.5.	System Security.....	56
2.7.	Managements .....	57
2.7.1.	System Management.....	57
2.7.2.	Firmware .....	58
2.7.3.	Config Settings .....	59
2.7.4.	Port Setting.....	60
2.7.5.	Packet Statistics.....	61
2.7.6.	System Status.....	62
2.7.7.	System Log .....	63
<b>3.</b>	<b>Hardware Information .....</b>	<b>64</b>
3.1.	WizFi630 Pin Map.....	64
3.2.	Dimensions.....	66
<b>4.</b>	<b>Important Notice .....</b>	<b>67</b>

## 1. Introduction

WizFi630 is a gateway module that transforms the RS-232 protocol and TCP/IP protocol into IEEE802.11 b/g/n wireless LAN protocol. WizFi630 enables a device with RS-232 serial interface to connect to LAN or WLAN for remotely control, measuring, and administration. WizFi630 can also work as an IP router because of its internally embedded switch.

WizFi630 uses interfaces like Serial(UART), LAN, Wi-Fi(WLAN) to perform functions such as Serial(UART)-To-Wi-Fi, Serial-To-Ethernet, Ethernet-To-Wi-Fi. Users can connect to WizFi630's internal web server or use serial commands for simple Wi-Fi settings; not only serial devices but 8/16/32 bit micro controllers can also use UART for simple Wi-Fi settings.

WizFi630 can significantly reduce the processes for wireless module design, testing, and certification. Therefore, WizFi630 can be the best solution for users who lack wireless network experience.

WizFi630 follows the 802.11b/g/n standard and support up to 150Mbps speed in wireless interface.

WizFi630 provides a test board, pc software, and documents so that anyone can develop a wireless solution.

## 1.1. Features

- ◆ Complies with IEEE802.11b/g/n.
- ◆ Gateway/AP(Bridge)/AP-Client/Client(Station)/Ad-hoc Mode , WDS/Repeater supports
- ◆ 1T1R RF Interface
- ◆ Physical link rate up to 150Mbps
- ◆ Built-in 3 Ethernet Ports
- ◆ 2 Serial Ports supports
- ◆ Working as Wi-Fi Router
- ◆ WEP 64/128bit, WPA/WPA2-PSK TKIP, AES
- ◆ 802.1x (Only in AP mode)
- ◆ 802.11e and WMM (Wi-Fi Multimedia)
- ◆ Router and Firewall function supports

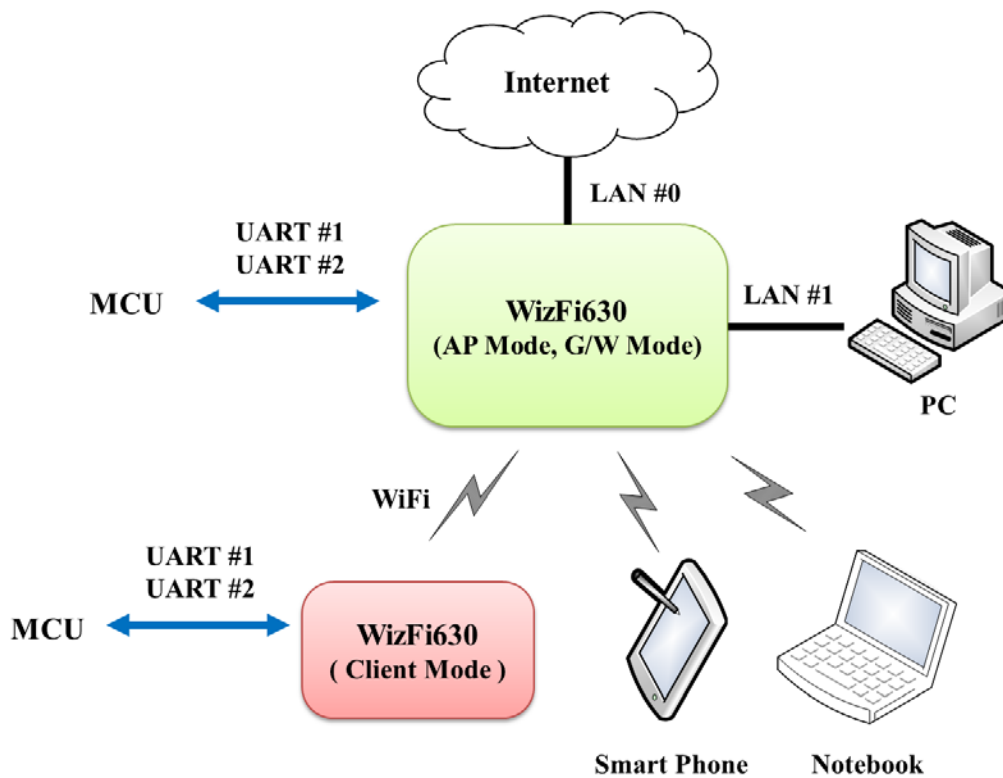


Figure 1. Example of WizFi630's Application

## 1.2. Wireless Specifications

Type	Description
<b>Wireless Standard</b>	IEEE802.11b/g/n
<b>Frequency Range</b>	USA: 2.400 ~ 2.483GHz Europe: 2.400 ~ 2.483GHz Japan: 2.400 ~ 2.497GHz China: 2.400 ~ 2.483GHz
<b>Operating Channels</b>	USA/Canada: 11(1 ~ 11) Major Europe Countries: 13(1 ~ 13) France: 4(10 ~ 13) Japan: 14 for 802.11b(1 ~ 14), 13 for 802.11g(1 ~ 13) Korea/China: 13(1 ~ 13)
<b>Output Power (Tolerance(+/-1dBm))</b>	802.11b: 17dBm@11Mbps 802.11g: 14dBm@54Mbps 802.11n: 14dBm@150Mbps/72Mbps
<b>Receive Sensitivity</b>	802.11b: -89dBm@11Mbps 802.11g: -74dBm@54Mbps 802.11n(40MHz): -66dBm@150Mbps 802.11n(20MHz): -70dBm@72Mbps
<b>Data Rates</b>	802.11b: 1,2,5.5,11Mbps 802.11g: 6,9,12,18,24,36,48,54Mbps 802.11n(20MHz): 7,14.5,21.5,28.5,43.5,57.5,65,72Mbps 802.11n(40MHz): 29.5,86.5,115,130,144,150Mbps
<b>Modulation Type</b>	11g: OFDM(64QAM, 16QAM, QPSK, BPSK) 11b: DSS(CCK, DQPSK, DBPSK)
<b>Antenna</b>	u.FL (EVB : 1T1R 2dBi)

Table 1. Wi-Fi Specifications



### 1.3. Hardware Specifications

Type	Description
Interface	Serial port : 2 EA LAN port : 3EA USB port : 1 USB Host Port ( Reserved )
	U.FL(wireless)
Temperature	Operation: -10°C~70°C
Humidity	Operation: 10% to 90%, Non-Condensing Storage: 5% to 90%, Non-Condensing
Serial	Baud Rate : 1200 ~ 921,600bps
	Stop bits: 1, 2
	Parity: None, Odd, Even
	Flow Control: UART1: XON/XOFF(software), CTS/RTS(hardware), none UART2: XON/XOFF, none
Input Power	DC 3.3V / 1A
Power Consumption	Max : 3.3V / 600mA
Dimension	33mm X 43mm X 4.5mm
Weight	6g

Table 2. WizFi630 Module Specifications



## 1.4. Software Specifications

Type	Description
<b>Operation Mode</b>	Access Point(Bridge), Client(Station), Gateway, AP-Client, ad-hoc
<b>Protocol</b>	TCP, UDP, ARP, ICMP, DHCP, PPPoE, HTTP
<b>Security</b>	WEP 64/128bit WPA/WPA2-PSK AES/TKIP 802.1x ( Only in AP Mode )
<b>Configuration</b>	Web Configuration, Serial Command, Configuration Tool
<b>Notification</b>	Event Logging
<b>Serial To Wi-Fi</b>	2 Serial Port supports

Table 3. SW Specifications

## 1.5. EVB Construction

### 1.5.1. Contents

Section	Qty.	Contents
WizFi630	1ea	WizFi630
		
WizFi630-EVB	1ea	WizFi630-EVB
		

<b>Antenna</b>	<b>1 ea</b>	2dBi WI-FI Antenna (Model : W5I-B0-08)
		
<b>Serial Cable</b>	<b>1 ea</b>	Serial Cable
		
<b>LAN Cable</b>	<b>1 ea</b>	LAN Cable
		
<b>Adapter</b>	<b>1ea</b>	DC 5V/2A Adapter
		

Table 4. WizFi630-EVB Contents

## 1.6. Block Diagram

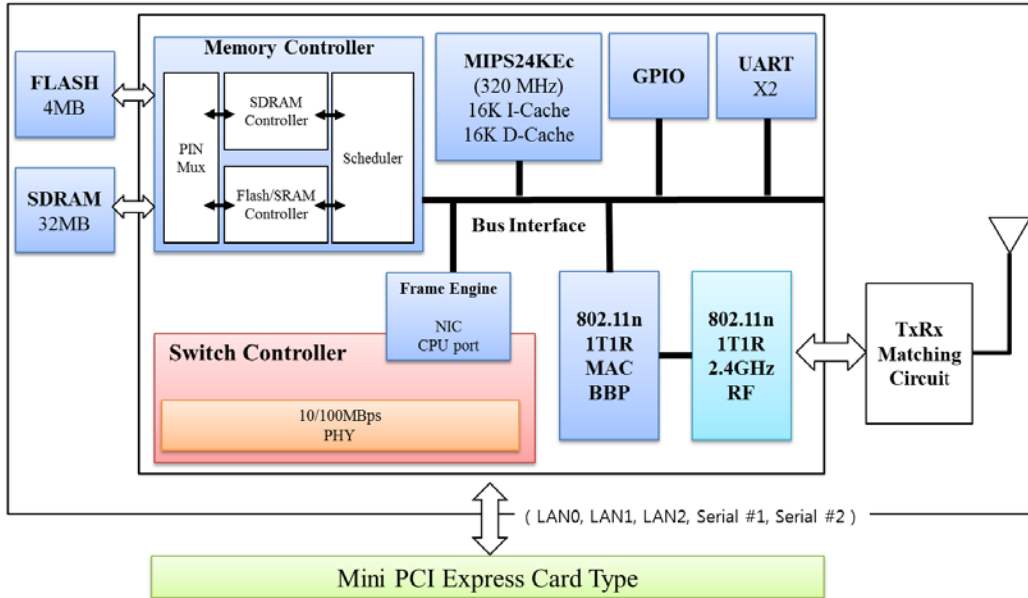
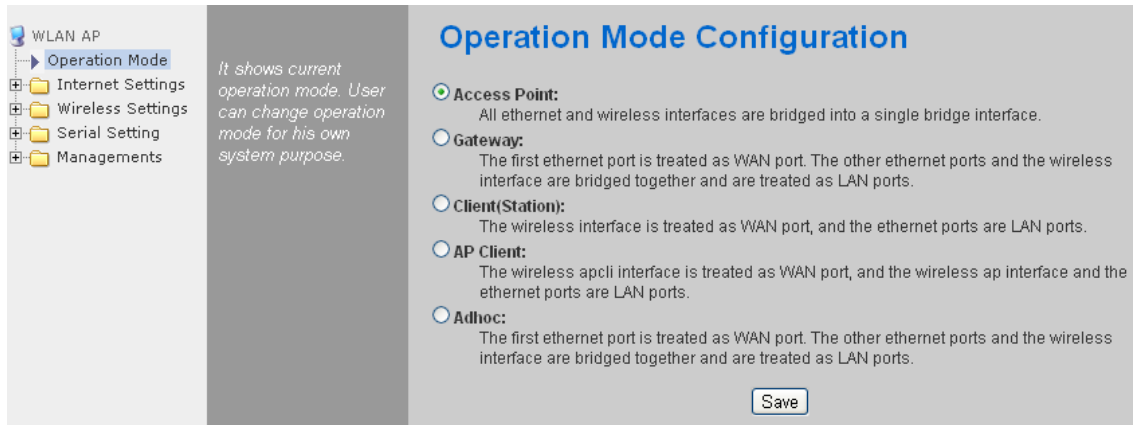


Figure 1. WizFi630 Block Diagram

## 2. Operation Mode and Description of Menu

### 2.1. Operation Mode

- ◆ User can select the operation mode.
- ◆ The default setting of WizFi630 is AP Mode. (DHCP Server Enabled)
- ◆ DHCP Server is usually disabled in AP mode, but for the user's convenience, DHCP Server will be enabled.

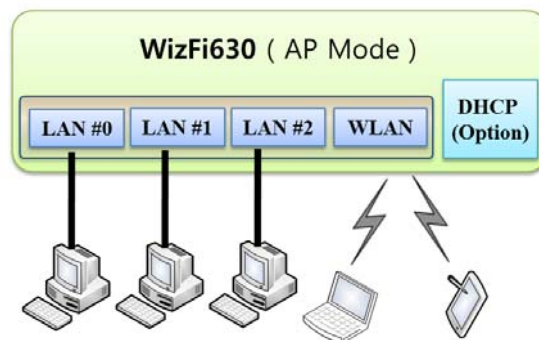


The screenshot shows the 'WLAN AP' configuration page. On the left is a navigation tree with 'Operation Mode' selected. A note states: 'It shows current operation mode. User can change operation mode for his own system purpose.' The main area is titled 'Operation Mode Configuration' and lists five modes with radio buttons:

- Access Point:** All ethernet and wireless interfaces are bridged into a single bridge interface.
- Gateway:** The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
- Client(Station):** The wireless interface is treated as WAN port, and the ethernet ports are LAN ports.
- AP Client:** The wireless apcli interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LAN ports.
- Adhoc:** The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

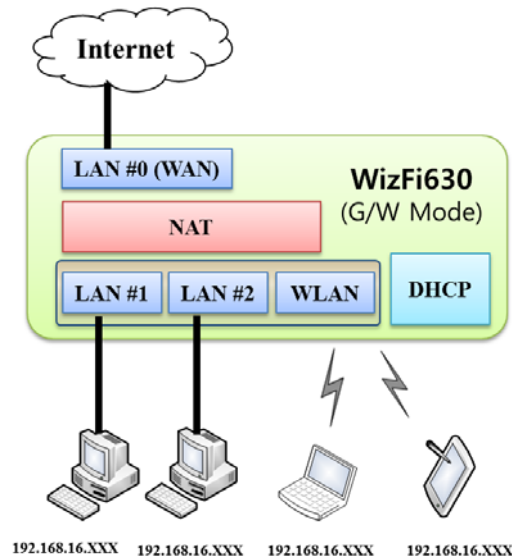
A 'Save' button is located at the bottom right of the configuration area.

#### 2.1.1. Access Point



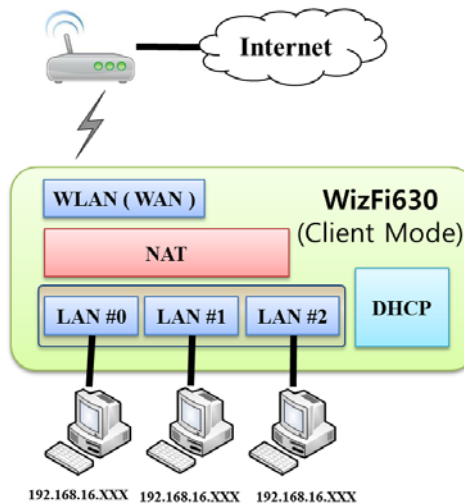
In this mode, all Ethernet ports and the wireless interface are bridged together. Wired/Wireless interface has the same IP address space with its top mesh. DHCP Server function is disabled and WizFi630 does not assign an IP. Wireless (LAN Port included) sending periodic Broadcast Packet to Station and maintains a connection with Station.

## 2.1.2. Gateway



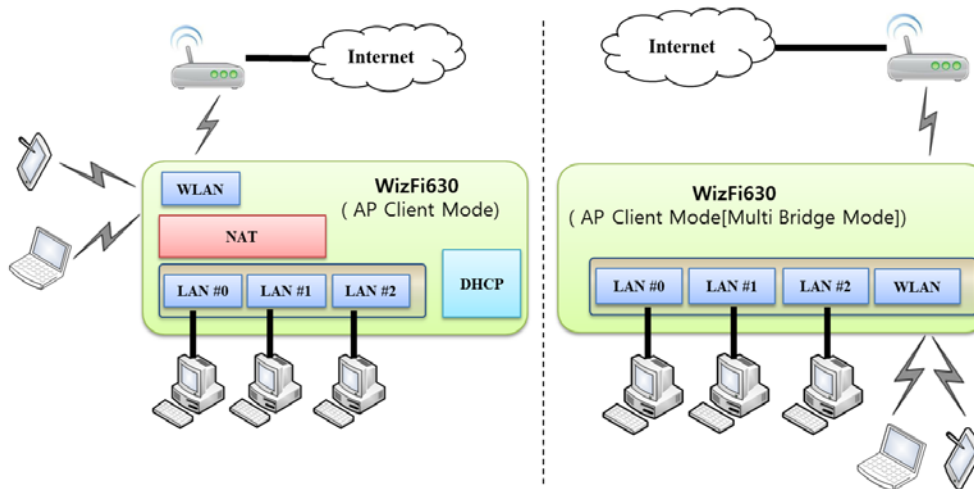
When operating in router mode, interfaces are separated into WAN I/F (Top Internet Business Network), LAN I/F (Sub Private Network: 192.168.16.xxx), and Wireless I/F (Sub Private Network: 192.168.16.xxx). Port # 0 will be assigned to the WAN Port. WizFi630 periodically sends Broadcast Packet to Sub-LAN (LAN Port included) and maintains connection with Station.

## 2.1.3. Client (Station)



Wireless I/F is assigned as WAN Port and all Ethernet Ports are bound to LAN Port. Set the profile and the WizFi630 is automatically connected to the AP when re-booting in the future. Devices that are connected through the LAN port are assigned a private IP. WizFi630 periodically sends PING Packet to AP Gateway and maintains connection with AP.

## 2.1.4. AP-Client Mode



Wireless I/F is assigned as WAN Port and all Ethernet Ports are bound to LAN Port. This mode is similar to Station mode, however the difference is that the Wireless I/F will operate as client with AP simultaneously. WizFi630 periodically sends Broadcast Packet to Sub-LAN (LAN Port included) and maintains connection with Station.

## 2.1.5. Ad-hoc Mode

This mode is similar to Gateway mode. The Wireless I/F operates as ad-hoc and connects to Station Point-to-Point. There is no communication between the LAN Port and Wireless I/F (ad-hoc).

WAN ↔ ad-hoc: OK

WAN ↔ LAN: OK

ad-hoc ↔ ad-hoc: OK

ad-hoc ↔ LAN: No Communication

## 2.2. Menu List by Operation Mode

### 2.2.1. Access Point (Bridge) Mode

Menu	Detailed Menu	Description ( Link )	List Number
Internet Setting	System IP	<a href="#">Internet connection setting</a>	2.3.1
	LAN	<a href="#">Local network setting</a>	2.3.2
	DHCP Clients	<a href="#">DHCP Client Information</a>	2.3.3
	VPN Config	<a href="#">VPN setting</a>	2.3.4
	QoS(802.1p)	<a href="#">QoS(802.1p) Setting</a>	2.3.6
Wireless Setting	Basic	<a href="#">Basic settings</a>	2.4.1
	Advanced	<a href="#">Advanced Wireless Settings ( AP Mode )</a>	2.4.2.1
	Security	<a href="#">Wireless Security setting</a>	2.4.3
	WDS	<a href="#">WDS Setting</a>	2.4.4
	WPS	<a href="#">WPS Setting ( AP Mode )</a>	2.4.5.1
	Station List	<a href="#">Wireless network status</a>	2.4.6
	Packet Statistics	<a href="#">AP Wireless Statistics ( AP Mode )</a>	2.4.7.1
Serial Setting	Serial Port #1	<a href="#">Serial to LAN(Wired and Wireless)</a>	2.5
	Serial Port #2		
Managements	System Mgmt	<a href="#">System Management</a>	2.7.1
	Firmware Mgmt	<a href="#">Firmware</a>	2.7.2
	Config Mgmt	<a href="#">Config Settings</a>	2.7.3
	Port Mgmt	<a href="#">Port Setting</a>	2.7.4
	Packet Statistics	<a href="#">Packet Statistics</a>	2.7.5
	System Status	<a href="#">System Status</a>	2.7.6
	System Log	<a href="#">System Log</a>	2.7.7



## 2.2.2. Gateway (Router) Mode

Menu	Detailed Menu	Description ( Link )	List Number
Internet Setting	WAN	<a href="#">Internet connection setting</a>	2.3.1
	LAN	<a href="#">Local network setting</a>	2.3.2
	DHCP Clients	<a href="#">DHCP Client Information</a>	2.3.3
	VPN Config	<a href="#">VPN setting</a>	2.3.4
	Routing	<a href="#">Static Routing Setting</a>	2.3.5
	Qos(802.1p)	<a href="#">QoS(802.1p) Setting</a>	2.3.6
	VLAN(802.1q)	<a href="#">VLAN(802.1q)</a>	2.3.7
Wireless Setting	Basic	<a href="#">Basic settings</a>	2.4.1
	Advanced	<a href="#">Advanced Wireless Settings ( AP Mode )</a>	2.4.2.1
	Security	<a href="#">Wireless Security setting</a>	2.4.3
	WDS	<a href="#">WDS Setting</a>	2.4.4
	WPS	<a href="#">WPS Setting ( AP Mode )</a>	2.4.5.1
	Station List	<a href="#">Wireless network status</a>	2.4.6
	Packet Statistics	<a href="#">AP Wireless Statistics ( AP Mode )</a>	2.4.7.1
Serial Setting	Serial Port #1	<a href="#">Serial to LAN(Wired and Wireless)</a>	2.5
	Serial Port #2		
Firewall	DMZ	<a href="#">DMZ</a>	2.6.1
	Port Forwarding	<a href="#">Port forwarding</a>	2.6.2
	Packet Filtering	<a href="#">Packet filtering</a>	2.6.3
	Contents Filtering	<a href="#">Contents filtering</a>	2.6.4
	System Security	<a href="#">System Security</a>	2.6.5
Managements	System Mgmt	<a href="#">System Management</a>	2.7.1
	Firmware Mgmt	<a href="#">Firmware</a>	2.7.2
	Config Mgmt	<a href="#">Config Settings</a>	2.7.3
	Port Mgmt	<a href="#">Port Setting</a>	2.7.4
	Packet Statistics	<a href="#">Packet Statistics</a>	2.7.5
	System Status	<a href="#">System Status</a>	2.7.6
	System Log	<a href="#">System Log</a>	2.7.7

## 2.2.3. Client (Station) Mode

- ◆ WizFi630 works as a Wi-Fi client(station) which is always paired with a Wi-Fi AP.
- ◆ Users can take Client Mode as an opposite of Gateway Mode

Menu	Detailed Menu	Description ( Link )	List Number
Internet Setting	WAN	<a href="#">Internet connection setting</a>	2.3.1
	LAN	<a href="#">Local network setting</a>	2.3.2
	DHCP Clients	<a href="#">DHCP Client Information</a>	2.3.3
	VPN Config	<a href="#">VPN setting</a>	2.3.4
	Routing	<a href="#">Static Routing Setting</a>	2.3.5
	QoS(802.1p)	<a href="#">QoS(802.1p) Setting</a>	2.3.6
	VLAN(802.1q)	<a href="#">VLAN(802.1q)</a>	2.3.7
Wireless Setting	Profile	<a href="#">Profile</a>	2.4.9
	Link Status	<a href="#">Link Status</a>	2.4.10
	Site Survey	<a href="#">Site Survey</a>	2.4.11
	Packet Statistics	<a href="#">AP Wireless Statistics ( Client Mode )</a>	2.4.7.2
	Advance	<a href="#">Advanced Wireless Settings(Client Mode)</a>	2.4.2.2
	QoS	<a href="#">Station QoS/DLS(Direct Link Setup) Configurations</a>	2.4.8
	WPS	<a href="#">WPS Settings ( Client Mode )</a>	2.4.5.2
Serial Setting	Serial Port #1	<a href="#">Serial to LAN(Wired and Wireless)</a>	2.5
	Serial Port #2		
Firewall	DMZ	<a href="#">DMZ</a>	2.6.1
	Port Forwarding	<a href="#">Port forwarding</a>	2.6.2
	Packet Filtering	<a href="#">Packet filtering</a>	2.6.3
	Contents Filtering	<a href="#">Contents filtering</a>	2.6.4
	System Security	<a href="#">System Security</a>	2.6.5
Managements	System Mgmt	<a href="#">System Management</a>	2.7.1
	Firmware Mgmt	<a href="#">Firmware</a>	2.7.2
	Config Mgmt	<a href="#">Config Settings</a>	2.7.3
	Port Mgmt	<a href="#">Port Setting</a>	2.7.4
	Packet Statistics	<a href="#">Packet Statistics</a>	2.7.5
	System Status	<a href="#">System Status</a>	2.7.6
	System Log	<a href="#">System Log</a>	2.7.7

## 2.2.4. AP-Client Mode

- ◆ AP-Client Mode Settings are very similar to the Gateway Mode Settings.
- ◆ The table below shows the added features of AP-Client mode.
- ◆ One module can operate as both AP and Station.
- ◆ The wireless module connects to a different AP and functions as WAN port.
- ◆ The channel of WizFi630 must be identical to the channel of AP to be connected
- ◆ Support wireless bridge.

Menu	Detailed Menu	Description ( Link )	List Number
Internet Setting	WAN	<a href="#">Internet connection setting</a>	2.3.1
	LAN	<a href="#">Local network setting</a>	2.3.2
	DHCP Clients	<a href="#">DHCP Client Information</a>	2.3.3
	VPN Config	<a href="#">VPN setting</a>	2.3.4
	Routing	<a href="#">Static Routing Setting</a>	2.3.5
	Qos(802.1p)	<a href="#">QoS(802.1p) Setting</a>	2.3.6
Wireless Setting	Basic	<a href="#">Basic settings</a>	2.4.1
	Advanced	<a href="#">Advanced Wireless Settings ( AP Mode )</a>	2.4.2.1
	Security	<a href="#">Wireless Security setting</a>	2.4.3
	WDS	<a href="#">WDS Setting</a>	2.4.4
	WPS	<a href="#">WPS Setting ( AP Mode )</a>	2.4.5.1
	WIFI Multi Bridge	<a href="#">WIFI Multi-Bridge settings</a>	2.4.12
	Station List	<a href="#">Wireless network status</a>	2.4.6
	Packet Statistics	<a href="#">AP Wireless Statistics ( AP Mode )</a>	2.4.7.1
Serial Setting	Serial Port #1	<a href="#">Serial to LAN(Wired and Wireless)</a>	2.5
	Serial Port #2		
Firewall	DMZ	<a href="#">DMZ</a>	2.6.1
	Port Forwarding	<a href="#">Port forwarding</a>	2.6.2
	Packet Filtering	<a href="#">Packet filtering</a>	2.6.3
	Contents Filtering	<a href="#">Contents filtering</a>	2.6.4
	System Security	<a href="#">System Security</a>	2.6.5
Managements	System Mgmt	<a href="#">System Management</a>	2.7.1
	Firmware Mgmt	<a href="#">Firmware</a>	2.7.2
	Config Mgmt	<a href="#">Config Settings</a>	2.7.3
	Port Mgmt	<a href="#">Port Setting</a>	2.7.4
	Packet Statistics	<a href="#">Packet Statistics</a>	2.7.5

	System Status	<a href="#">System Status</a>	2.7.6
	System Log	<a href="#">System Log</a>	2.7.7

## 2.2.5. Ad-hoc Mode

- ◆ Settings for ad-hoc mode are almost the same as settings for Client (Station) Mode as previously shown.
- ◆ The difference with Client mode is that Client mode is used to connect AP.
- ◆ Client Mode connects to AP, whereas ad-hoc Mode connects with stations that use the same SSID.
- ◆ Both 1:1 connection and 1:N connection are possible
- ◆ In case of 1:N, N is possible up to 255

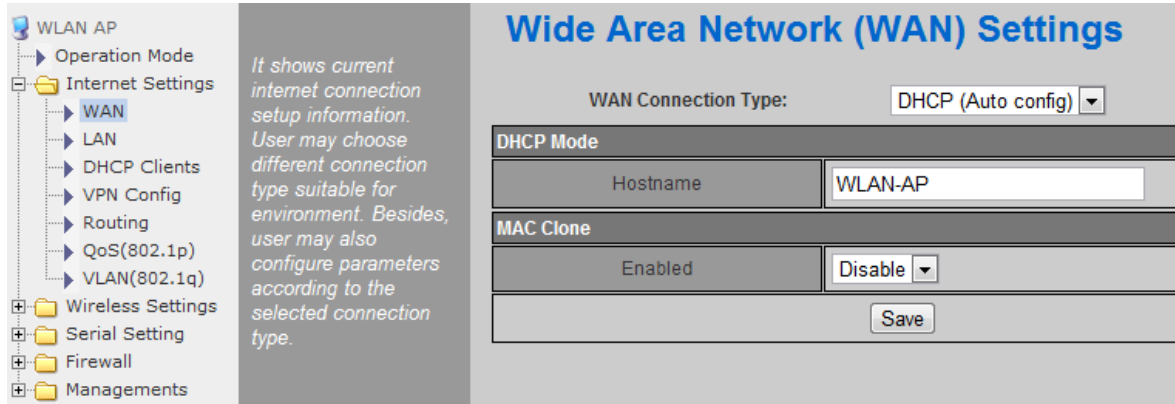
Menu	Detailed Menu	Description ( Link )	List Number
Internet Setting	WAN	<a href="#">Internet connection setting</a>	2.3.1
	LAN	<a href="#">Local network setting</a>	2.3.2
	DHCP Clients	<a href="#">DHCP Client Information</a>	2.3.3
	VPN Config	<a href="#">VPN setting</a>	2.3.4
	Routing	<a href="#">Static Routing Setting</a>	2.3.5
	Qos(802.1p)	<a href="#">QoS(802.1p) Setting</a>	2.3.6
Wireless Setting	Profile	<a href="#">Profile</a>	2.4.9
	Link Status	<a href="#">Link Status</a>	2.4.10
	Site Survey	<a href="#">Site Survey</a>	2.4.11
	Packet Statistics	<a href="#">AP Wireless Statistics ( Client Mode )</a>	2.4.7.2
	Advance	<a href="#">Advanced Wireless Settings(Client Mode)</a>	2.4.2.2
	QoS	<a href="#">Station QoS/DLS(Direct Link Setup) Configurations</a>	2.4.8
	WPS	<a href="#">WPS Settings ( Client Mode )</a>	2.4.5.2
Serial Setting	Serial Port #1	<a href="#">Serial to LAN(Wired and Wireless)</a>	2.5
	Serial Port #2		
Firewall	DMZ	<a href="#">DMZ</a>	2.6.1
	Port Forwarding	<a href="#">Port forwarding</a>	2.6.2
	Packet Filtering	<a href="#">Packet filtering</a>	2.6.3
	Contents Filtering	<a href="#">Contents filtering</a>	2.6.4
	System Security	<a href="#">System Security</a>	2.6.5
Managements	System Mgmt	<a href="#">System Management</a>	2.7.1
	Firmware Mgmt	<a href="#">Firmware</a>	2.7.2
	Config Mgmt	<a href="#">Config Settings</a>	2.7.3
	Port Mgmt	<a href="#">Port Setting</a>	2.7.4
	Packet Statistics	<a href="#">Packet Statistics</a>	2.7.5
	System Status	<a href="#">System Status</a>	2.7.6

	System Log	<a href="#">System Log</a>	2.7.7
--	------------	----------------------------	-------

## 2.3. Internet Setting

### 2.3.1. Internet connection setting

- ◆ Select the internet service type and WizFi630 can connect to the internet
- ◆ If users would like access to Internet, Gateway Mode should be selected.



WLAN AP

- Operation Mode
- Internet Settings
  - WAN**
  - LAN
  - DHCP Clients
  - VPN Config
  - Routing
  - QoS(802.1p)
  - VLAN(802.1q)
- Wireless Settings
- Serial Setting
- Firewall
- Managements

*It shows current internet connection setup information. User may choose different connection type suitable for environment. Besides, user may also configure parameters according to the selected connection type.*

### Wide Area Network (WAN) Settings

WAN Connection Type: DHCP (Auto config) ▼

**DHCP Mode**

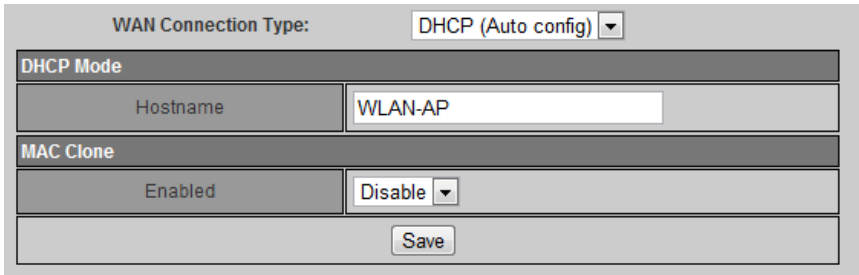
Hostname: WLAN-AP

**MAC Clone**

Enabled: Disable ▼

Save

Type	Description
<b>WAN Connection Type</b>	Select the communication ways for Internet's connection <ul style="list-style-type: none"> <li>- Static(Fixed IP)</li> <li>- DHCP (Auto config)</li> <li>- PPPoE</li> </ul>
<b>Host Name</b>	Settings about module's host name
<b>Mac Clone</b>	Some ISPs require that you register a MAC address. Users can directly enter MAC address or use the MAC Clone function

Type	Description
<b>DHCP(Auto config)</b>	User should choose DHCP Mode when the user connects to the internet service such as FTTH, cable modems, VDSL, or IP-ADSL 
<b>Static(Fixed IP)</b>	Static IP setting window. If user receives static IP from ISP, user should set the Fixed IP

	<div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p style="text-align: right; margin: 0;">WAN Connection Type: <span style="border: 1px solid #ccc; padding: 2px;">STATIC (fixed IP)</span> ▼</p> <p><b>Static Mode</b></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr><td style="width: 40%;">IP Address</td><td style="border: 1px solid #ccc; padding: 2px;">192.168.123.70</td></tr> <tr><td>Subnet Mask</td><td style="border: 1px solid #ccc; padding: 2px;">255.255.255.0</td></tr> <tr><td>Default Gateway</td><td style="border: 1px solid #ccc; padding: 2px;">192.168.123.254</td></tr> <tr><td>Primary DNS Server</td><td style="border: 1px solid #ccc; padding: 2px;">61.41.153.2</td></tr> <tr><td>Secondary DNS Server</td><td style="border: 1px solid #ccc; padding: 2px;">203.248.252.2</td></tr> </table> <p><b>MAC Clone</b></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr><td style="width: 40%;">Enabled</td><td style="border: 1px solid #ccc; padding: 2px;">Disable ▼</td></tr> </table> <p style="text-align: center; margin: 0;"><input type="button" value="Save"/></p> </div> <p style="margin-top: 10px;">Input the network information that got from ISP (such as IP, Subnet, Gateway, DNS)</p>	IP Address	192.168.123.70	Subnet Mask	255.255.255.0	Default Gateway	192.168.123.254	Primary DNS Server	61.41.153.2	Secondary DNS Server	203.248.252.2	Enabled	Disable ▼
IP Address	192.168.123.70												
Subnet Mask	255.255.255.0												
Default Gateway	192.168.123.254												
Primary DNS Server	61.41.153.2												
Secondary DNS Server	203.248.252.2												
Enabled	Disable ▼												
<b>PPPoE(ADSL)</b>	<div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p style="text-align: right; margin: 0;">WAN Connection Type: <span style="border: 1px solid #ccc; padding: 2px;">PPPoE (ADSL)</span> ▼</p> <p><b>PPPoE Mode</b></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr><td style="width: 40%;">User Name</td><td style="border: 1px solid #ccc; padding: 2px;">pppoe_user</td></tr> <tr><td>Password</td><td style="border: 1px solid #ccc; padding: 2px;">.....</td></tr> <tr><td>Verify Password</td><td style="border: 1px solid #ccc; padding: 2px;">.....</td></tr> <tr><td rowspan="2">Operation Mode</td><td style="border: 1px solid #ccc; padding: 2px;">Keep Alive ▼</td></tr> <tr><td style="border: 1px solid #ccc; padding: 2px;">Keep Alive Mode: Redial Period <span style="border: 1px solid #ccc; padding: 2px;">60</span> seconds On demand Mode: Idle Time <span style="border: 1px solid #ccc; padding: 2px;">5</span> minutes</td></tr> </table> <p><b>MAC Clone</b></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr><td style="width: 40%;">Enabled</td><td style="border: 1px solid #ccc; padding: 2px;">Disable ▼</td></tr> </table> <p style="text-align: center; margin: 0;"><input type="button" value="Save"/></p> </div> <p style="margin-top: 10px;">         -. User Name: Setting the User Name received from ISP          -. Password: Password assigned by ISP          -. Operation Mode: This mode is used for re-connecting when connection is bad       </p>	User Name	pppoe_user	Password	.....	Verify Password	.....	Operation Mode	Keep Alive ▼	Keep Alive Mode: Redial Period <span style="border: 1px solid #ccc; padding: 2px;">60</span> seconds On demand Mode: Idle Time <span style="border: 1px solid #ccc; padding: 2px;">5</span> minutes	Enabled	Disable ▼	
User Name	pppoe_user												
Password	.....												
Verify Password	.....												
Operation Mode	Keep Alive ▼												
	Keep Alive Mode: Redial Period <span style="border: 1px solid #ccc; padding: 2px;">60</span> seconds On demand Mode: Idle Time <span style="border: 1px solid #ccc; padding: 2px;">5</span> minutes												
Enabled	Disable ▼												



## 2.3.2. Local network setting

- ◆ WizFi630 internal IP setting, DHCP server setting and DHCP.

WLAN AP

- ▶ Operation Mode
- ▶ Internet Settings
  - ▶ WAN
  - ▶ LAN
  - ▶ DHCP Clients
  - ▶ VPN Config
  - ▶ Routing
  - ▶ QoS(802.1p)
  - ▶ VLAN(802.1q)
- ▶ Wireless Settings
- ▶ Serial Setting
- ▶ Firewall
- ▶ Managements

*It show local networking information and user can setup the local networking function for user's network environments.*

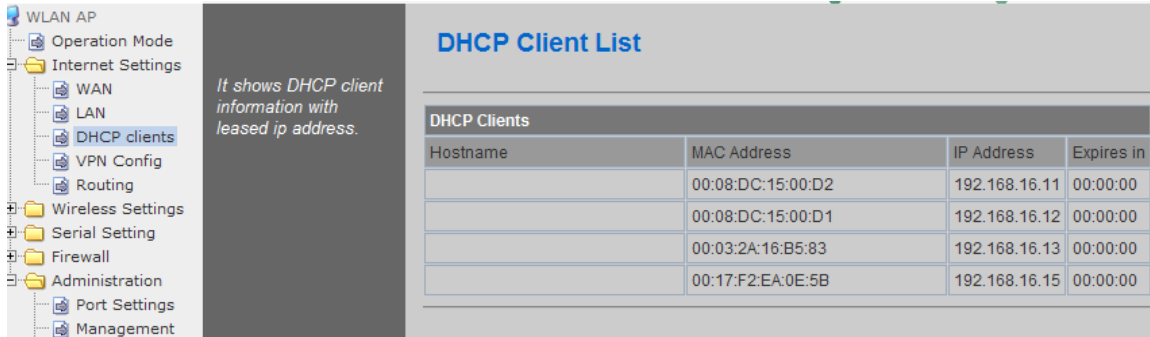
### Local Area Network (LAN) Settings

LAN Setup	
IP Address	<input type="text" value="192.168.16.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
MAC Address	00:50:38:08:38:B8
DHCP Server	<input type="button" value="Enable"/>
Start IP Address	<input type="text" value="192.168.16.11"/>
End IP Address	<input type="text" value="192.168.16.50"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text" value="168.126.63.1"/>
Lease Time	<input type="text" value="3600"/> sec(60-86400, default:3600)
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
IGMP Proxy	<input type="button" value="Enable"/> <input type="button" value="Group List"/>
DNS Proxy	<input type="button" value="Disable"/>
<input type="button" value="Save"/>	

Type	Description
<b>IP Address</b>	Enter the module's IP. (Default Value : 192.168.16.254)
<b>Subnet Mask</b>	Enter the module's subnet mask.
<b>MAC Address</b>	MAC Address of module's LAN port (Wireless included). (Read Only)
<b>DHCP Server</b>	Decide whether the module's DHCP server will be used.
<b>Start IP Address</b>	Set the start IP address that will be assigned from the DHCP server
<b>End IP Address</b>	Set the end IP address that will be assigned from the DHCP server.
<b>Subnet Mask</b>	Enter the value of subnet mask.
<b>Primary DNS Server</b>	Enter the primary DNS server address.
<b>Secondary DNS Server</b>	Enter the secondary DNS server address.
<b>Lease Time</b>	Enter the lease time when IP address is assigned.
<b>Statically Assigned</b>	Maximum of three IP can be statically assigned when IP address is assigned.

### 2.3.3. DHCP Client Information

- ◆ The IP information that is assigned from the DHCP server is shown.



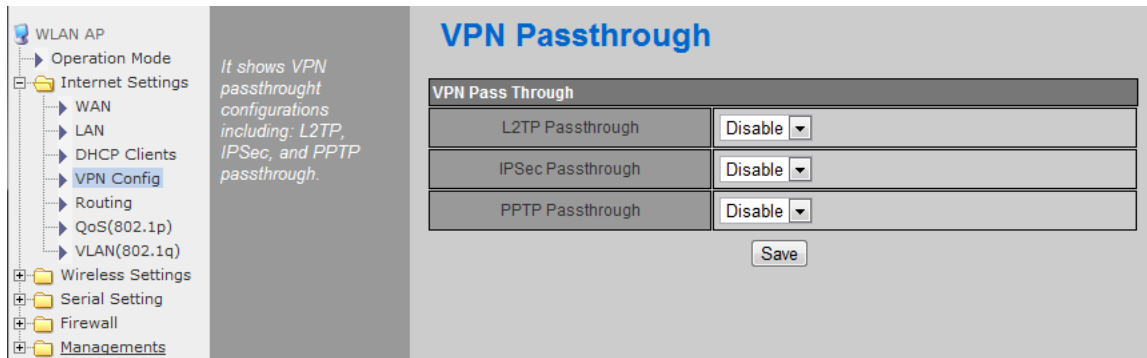
*It shows DHCP client information with leased ip address.*

Hostname	MAC Address	IP Address	Expires in
	00:08:DC:15:00:D2	192.168.16.11	00:00:00
	00:08:DC:15:00:D1	192.168.16.12	00:00:00
	00:03:2A:16:B5:83	192.168.16.13	00:00:00
	00:17:F2:EA:0E:5B	192.168.16.15	00:00:00

Type	Description
<b>Host name</b>	Client's host name is shown
<b>Mac Address</b>	Client's MAC address is shown.
<b>IP Address</b>	Client's IP address is shown.
<b>Expires in</b>	The usable time of client's IP address is shown.

### 2.3.4. VPN setting

- ◆ This section will explain on VPN packet settings.



*It shows VPN passthrough configurations including: L2TP, IPsec, and PPTP passthrough.*

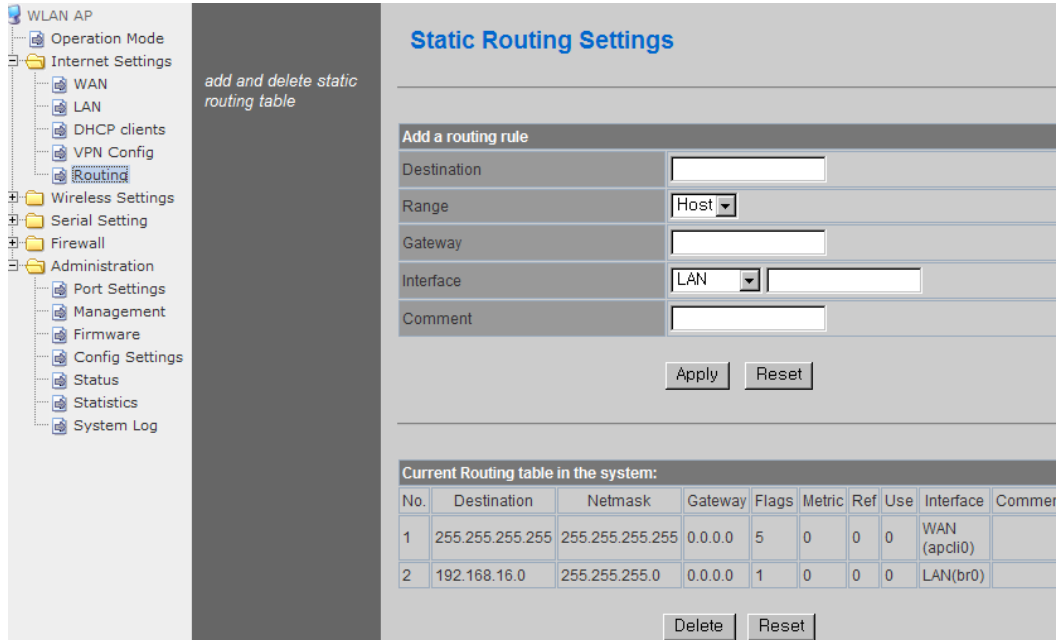
VPN Pass Through	
L2TP Passthrough	Disable
IPsec Passthrough	Disable
PPTP Passthrough	Disable

Save

Type	Description
<b>L2TP Pass-through</b>	Enable : VPN L2TP packet is passed through WAN. Disable : VPN L2TP packet is not passed through WAN. (Default value)
<b>IPsec Pass-through</b>	Enable : VPN IPsec packet is passed through WAN. Disable : VPN IPsec packet is not passed through WAN. (Default value)
<b>PPTP Pass-through</b>	Enable : VPN PPTP packet is passed through WAN. Disable : VPN PPTP packet is not passed through WAN. (Default value)

## 2.3.5. Static Routing Setting

- ◆ User can modify the routing table at static routing settings.
- ◆ We do not recommend any modification.



*add and delete static routing table*

### Static Routing Settings

**Add a routing rule**

Destination:

Range:

Gateway:

Interface:

Comment:

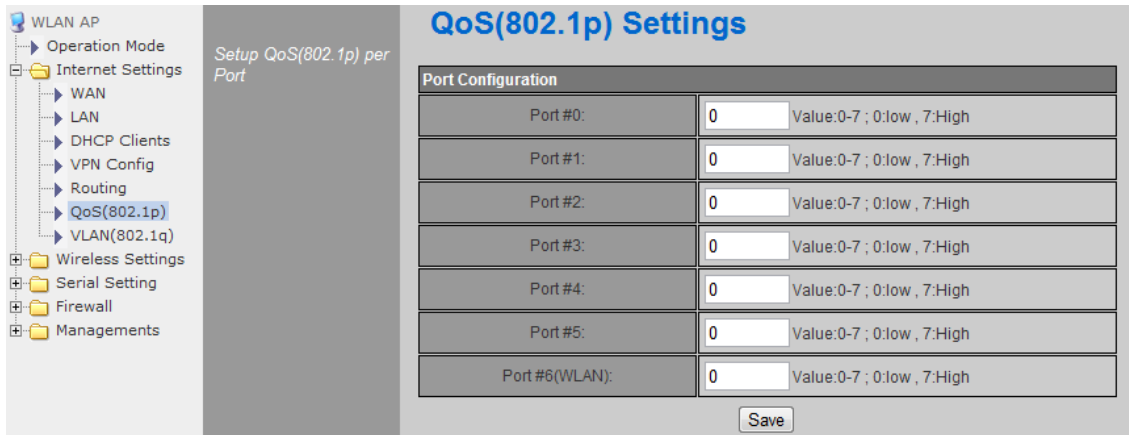
**Current Routing table in the system:**

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Commer
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	WAN (apcli0)	
2	192.168.16.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	

Type	Description
<b>Destination</b>	Enter the Target IP address or network address.
<b>Range</b>	Select whether the routing table is HOST or NETWORK
<b>Netmask</b>	If Range is NETWORK, enter subnet mask.
<b>Gateway</b>	Enter the gateway address to be passed when communicating with target.
<b>Interface</b>	Select whether the target is LAN or WAN.

## 2.3.6. QoS(802.1p) Setting

- ◆ Settings for QoS / DLS in Station mode.



WLAN AP

- Operation Mode
- Internet Settings
  - WAN
  - LAN
  - DHCP Clients
  - VPN Config
  - Routing
  - QoS(802.1p)**
  - VLAN(802.1q)
- Wireless Settings
- Serial Setting
- Firewall
- Managements

Setup QoS(802.1p) per Port

### QoS(802.1p) Settings

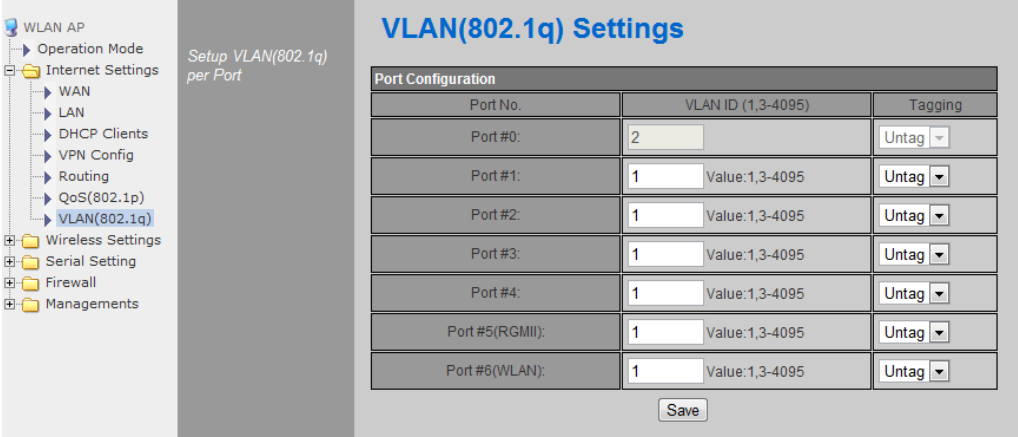
Port Configuration		
Port #0:	<input type="text" value="0"/>	Value:0-7 ; 0:low , 7:High
Port #1:	<input type="text" value="0"/>	Value:0-7 ; 0:low , 7:High
Port #2:	<input type="text" value="0"/>	Value:0-7 ; 0:low , 7:High
Port #3:	<input type="text" value="0"/>	Value:0-7 ; 0:low , 7:High
Port #4:	<input type="text" value="0"/>	Value:0-7 ; 0:low , 7:High
Port #5:	<input type="text" value="0"/>	Value:0-7 ; 0:low , 7:High
Port #6(WLAN):	<input type="text" value="0"/>	Value:0-7 ; 0:low , 7:High

Save

Type	Description
<b>Port #0 ~ Port#5</b>	Set a QoS value from 0~7
<b>Port #6(WLAN)</b>	Set a QoS value from 0~7

## 2.3.7. VLAN(802.1p)

- ◆ Settings for VLAN ID value and Tag/Untag.



**VLAN(802.1q) Settings**

Port No.	VLAN ID (1,3-4095)	Tagging
Port #0:	<input type="text" value="2"/>	Untag
Port #1:	<input type="text" value="1"/> Value:1,3-4095	Untag
Port #2:	<input type="text" value="1"/> Value:1,3-4095	Untag
Port #3:	<input type="text" value="1"/> Value:1,3-4095	Untag
Port #4:	<input type="text" value="1"/> Value:1,3-4095	Untag
Port #5(RGMII):	<input type="text" value="1"/> Value:1,3-4095	Untag
Port #6(WLAN):	<input type="text" value="1"/> Value:1,3-4095	Untag

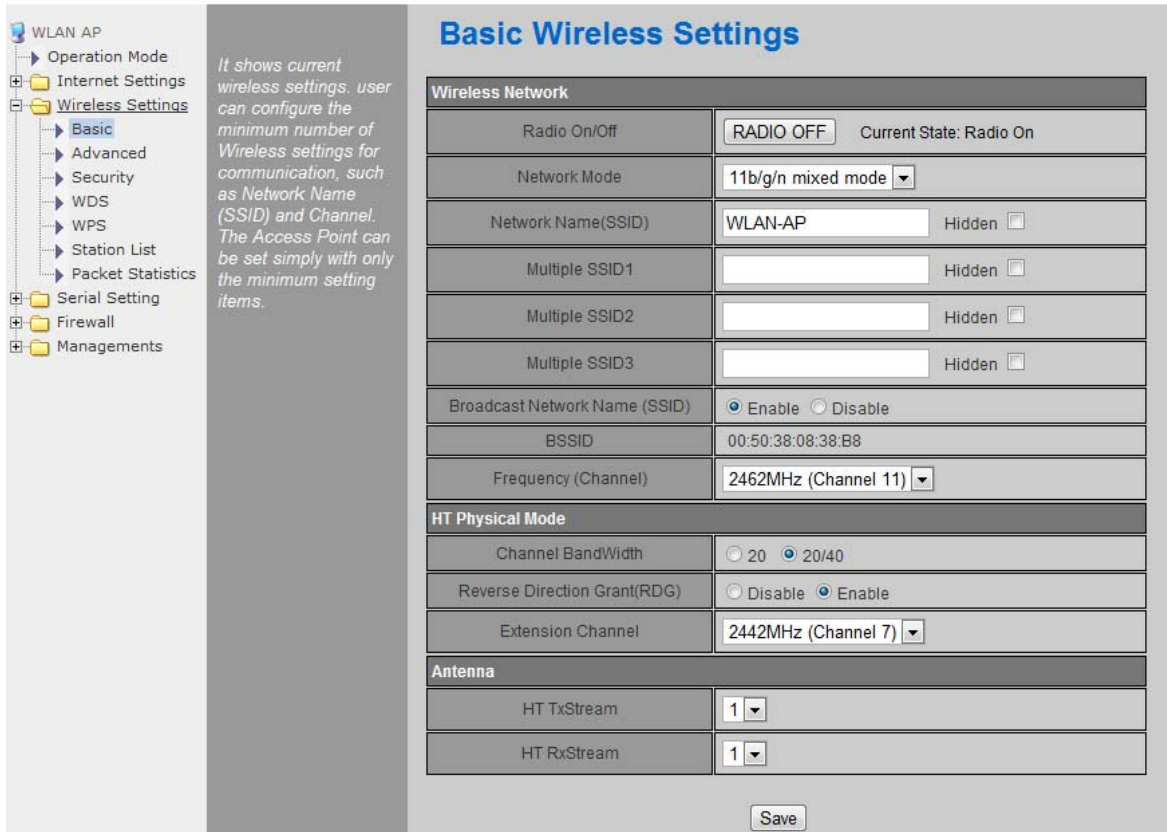
Save

Type	Description
<b>VLANID</b>	ID for connection with VLAN.
<b>Tagging</b>	Select to add information related to VLAN.

## 2.4. Wireless setting

### 2.4.1. Basic settings

- ◆ This chapter is about basic setting for wireless LAN.



WLAN AP

- Operation Mode
- Internet Settings
- Wireless Settings
  - Basic
  - Advanced
  - Security
  - WDS
  - WPS
  - Station List
  - Packet Statistics
- Serial Setting
- Firewall
- Managements

*It shows current wireless settings. user can configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.*

### Basic Wireless Settings

Wireless Network	
Radio On/Off	RADIO OFF Current State: Radio On
Network Mode	11b/g/n mixed mode
Network Name(SSID)	WLAN-AP Hidden <input type="checkbox"/>
Multiple SSID1	Hidden <input type="checkbox"/>
Multiple SSID2	Hidden <input type="checkbox"/>
Multiple SSID3	Hidden <input type="checkbox"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
BSSID	00:50:38:08:38:B8
Frequency (Channel)	2462MHz (Channel 11)
HT Physical Mode	
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2442MHz (Channel 7)
Antenna	
HT TxStream	1
HT RxStream	1

Save

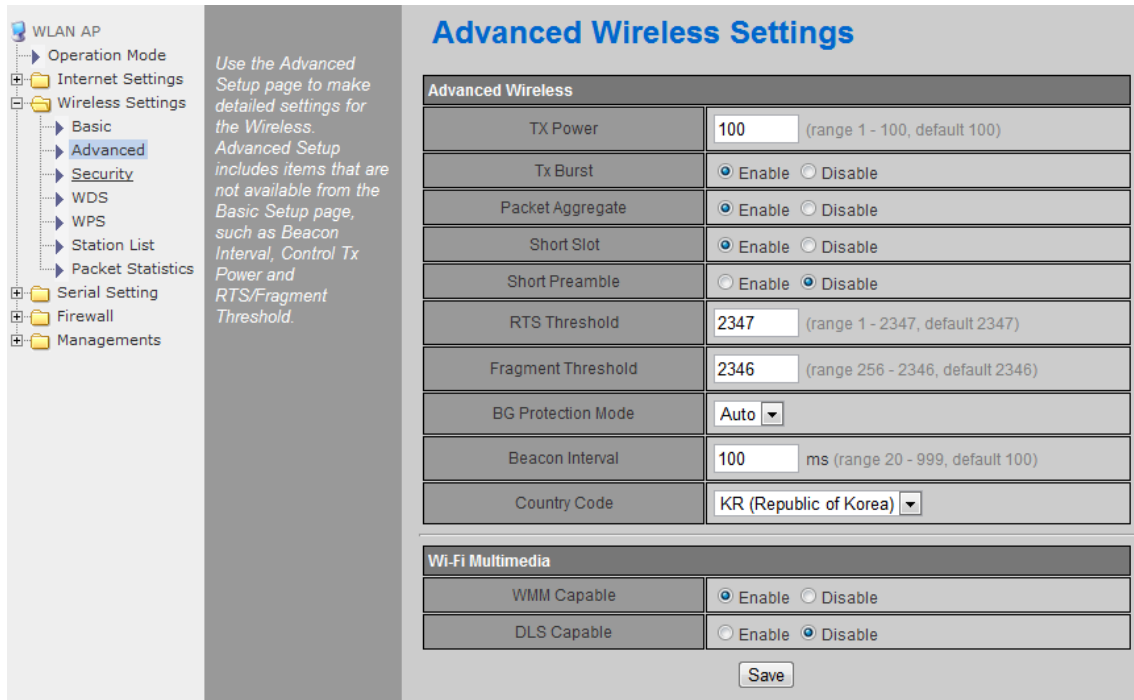
Type	Description
<b>Radio On/Off</b>	Decide radio on/off of wireless AP function.
<b>Network Mode</b>	11b/g/n mixed mode: 802.11b/g/n are supported. 11b/g mixed mode: 802.11b/g are supported. 11b only: only 802.11b is supported. 11g only: only 802.11g is supported. 11n only: only 802.11n is supported
<b>SSID</b>	Enter the name of the wireless network.
<b>Broadcast Network Name</b>	AP or Wireless network status can be checked by notifying the SSID to the wireless device. AP cannot be searched if this function is disabled.
<b>Frequency(Channel)</b>	Select the channel of wireless network.
<b>Channel Bandwidth</b>	Fix bandwidth channel to 20MHz. Use 40MHz as bandwidth in case connection with wireless station that supports 11n channel bonding..
<b>Reverse Direction Grant(RDG)</b>	The wireless performance can be improved using Reverse Direct Grant, 11n's RDG technology.

Type	Description
<b>Extension Channel</b>	Setting for the other 20MHz area when channel bandwidth is set to 40MHz
<b>HT TxStream</b>	Setting for number of Tx antennas of 2T2R system.
<b>HT RxStream</b>	Setting for number of Rx antennas of 2T2R system.

## 2.4.2. Advanced Wireless Settings

### 2.4.2.1. Advanced Wireless Settings ( AP Mode )

- ◆ Only works at the AP Mode, Gateway Mode, and AP-Client Mode
- ◆ This chapter is about higher-level setting for wireless LAN.



**Advanced Wireless Settings**

**Advanced Wireless**

TX Power	100	(range 1 - 100, default 100)
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Packet Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
RTS Threshold	2347	(range 1 - 2347, default 2347)
Fragment Threshold	2346	(range 256 - 2346, default 2346)
BG Protection Mode	Auto	
Beacon Interval	100	ms (range 20 - 999, default 100)
Country Code	KR (Republic of Korea)	

**Wi-Fi Multimedia**

WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Save

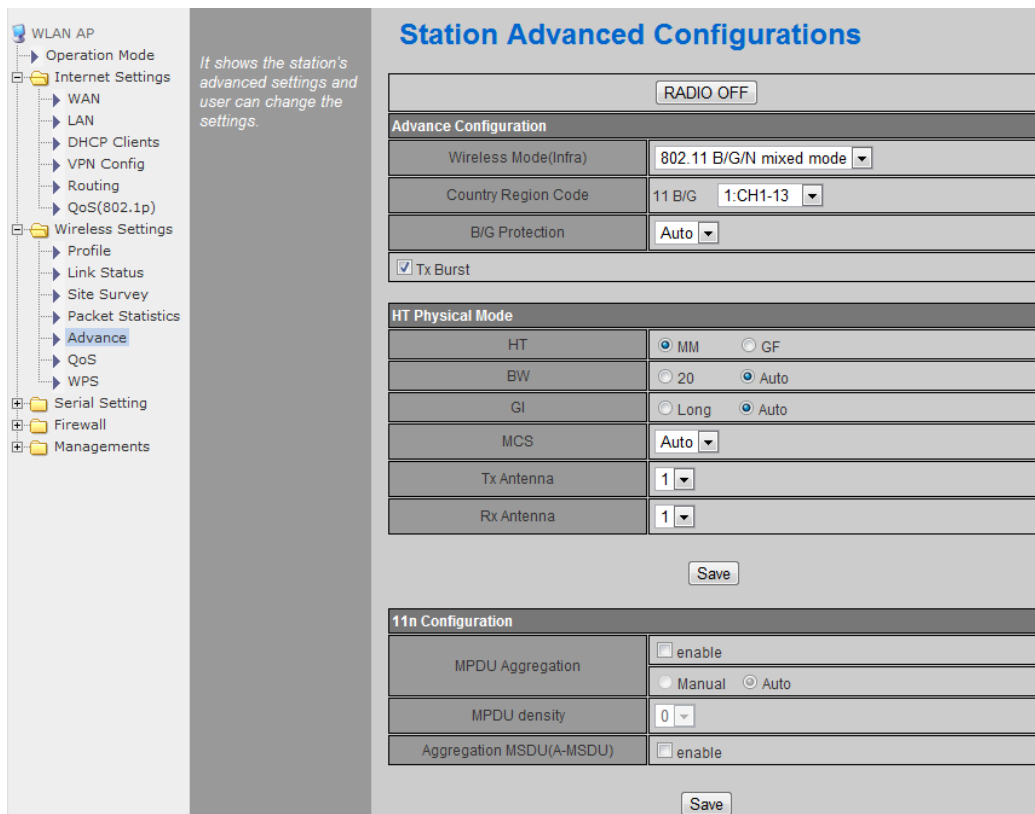
Type	Description
<b>Tx Power</b>	Controls the range of wireless radio being sent. The range of wireless radio being sent gets larger as the value is larger.
<b>Tx Burst</b>	The wireless speed can be maximized by enabling this function. However, it is recommended to disable this function for stable connection when numerous stations are connected together..
<b>Packet Aggregate</b>	Numerous packets can be transmitted in one MPDU by enabling this function
<b>Short Slot</b>	The performance of wireless station connected to 11g can be improved by enabling Short Slot. However, it is recommended to disable Short Slot if there is a wireless station with unstable connection.
<b>Short Preamble</b>	If user enables Short Preamble, performance might slightly improve. However, the compatibility with wireless LAN card when connecting could decrease. It is recommended to disable Short Preamble for best compatibility.
<b>RTS Threshold</b>	When a data is larger than the threshold size, it can be sent RTS/CTS. Smaller threshold size may enable more stable wireless communication; however the maximum speed is lower. Smaller threshold size is recommended in case of more wireless stations are connected at the same time. The setting range is 1~2347.
<b>Fragmentation</b>	When a data is larger than the threshold size, it is fragmented and sent. Smaller



<b>Threshold</b>	threshold size may enable more stable wireless communication; however the maximum speed is lower. Smaller threshold size is recommended in case of many interruptions from surrounding signals. The setting range is 256~2346.
<b>BG Protection</b>	Setting for wireless communication when using both 11b and 11g LAN cards. Recommended for automatic settings in general.
<b>Beacon Interval</b>	Controls the interval of sending beacon. The setting range is 20~999 and 100ms is usually used.
<b>Country Code</b>	Setting for country code. Example: KR(Republic of Korea), US(United State), FCC(Europe), JP(Japan), FR(France), ES(Spain)
<b>WMM (Wi-Fi Multimedia)</b>	Decide whether or not to use WMM function.
<b>DLS</b>	Decide whether or not to use DLS (Direct Link Setup) function.

### 2.4.2.2. Advanced Wireless Settings ( Client Mode )

- ◆ Set Station advanced configurations in station mode.



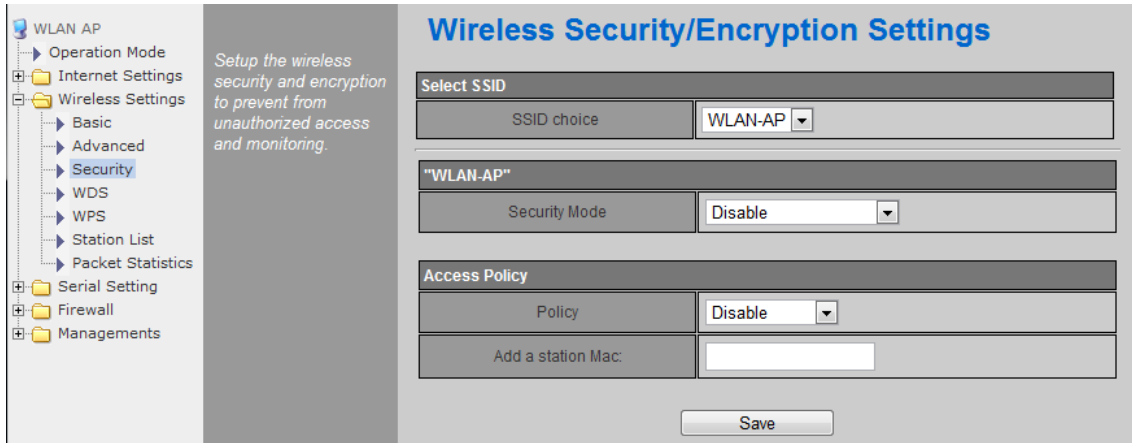
Type	Description
<b>RADIO OFF</b>	Enable / Disable wireless LAN. User cannot use wireless LAN if user clicks RADIO OFF.
<b>Wireless Mode</b>	Selects wireless mode.
<b>Country Region Code</b>	Selects the country / regional code.
<b>B/G Protection</b>	Setting for better wireless communication when both 11b and 11g LAN cards are used.

---

	We recommend Auto.
<b>HT</b>	Select whether the PHY Mode of wireless to be Mixed Mode or GreenField Mode.
<b>BW</b>	Fix the channel bandwidth to 20MHz: 20MHz. 20/40MHz: Use 40MHz when wireless station that supports 11n channel bonding.
<b>GI</b>	Long: 800nsec, short: 400nsec
<b>MCS</b>	Controls link rate.
<b>Tx Antenna</b>	Select number of Tx antenna in 2T2R system.
<b>Rx Antenna</b>	Select number of Rx antenna in 2T2R system.
<b>MPDU Aggregation</b>	Aggregates multiple MPDU to a single MPDU.
<b>MPDU density</b>	MPDU Variable Factor
<b>Aggregation MSDU (A-MSDU)</b>	Aggregates multiple MPDU to a single MPDU.

## 2.4.3. Wireless Security

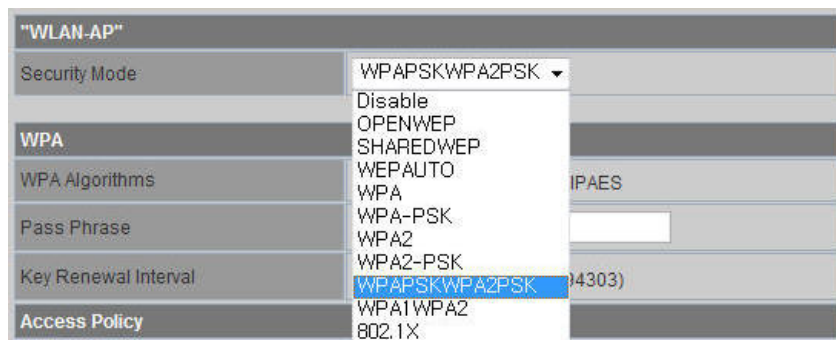
- ◆ This chapter is about settings for wireless network security



Type	Description
<b>SSID choice</b>	If multiple SSID are in use, choose the corresponding SSID for security.
<b>Security Mode</b>	Select security mode.
<b>Access Policy</b>	Disable : Access Control function will be disabled. Allow Listed : allows communication with listed MAC client. Reject Listed: blocks communication with listed MAC client.
<b>Add a station MAC</b>	Enter the client's MAC address for controlling.

### 2.4.3.1. Wireless Security setting

- ◆ Authentication settings



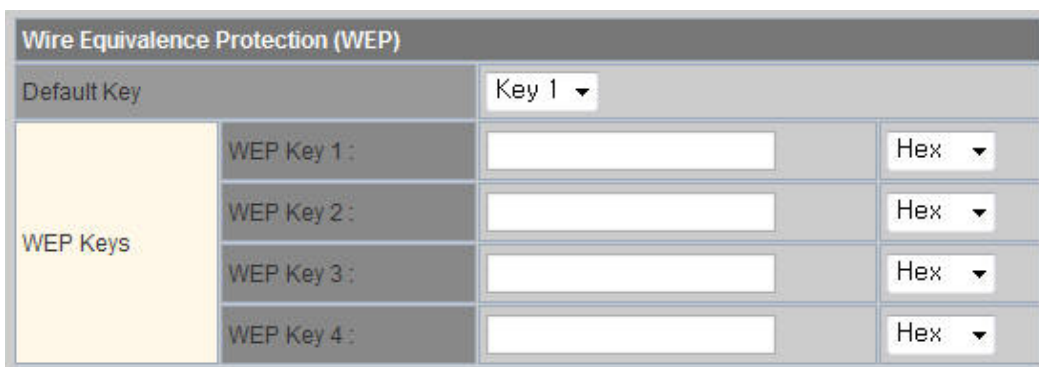
Type	Description
<b>OPENWEP</b>	All users are authorized.
<b>SHAREDWEP</b>	Users only with correct network key are authorized.
<b>WEPAUTO</b>	OPEN/SHARED Mode is selected automatically.
<b>WPA-PSK</b>	WPA certified standard with improved security.
<b>WPA2-PSK</b>	Improved WPA certified standard
<b>WPAPSKWPA2PSK</b>	Both WPZ-PSK and WPZ2-PSK are supported.
<b>WPA</b>	WPA certified standard including 802.1x.
<b>WPA2</b>	Improved WPA certified standard.
<b>WPA1WPA2</b>	Both WPA and WPA2 are supported.
<b>802.1x</b>	Radius authentication through WEP Key.

### 2.4.3.2. Wireless Authentication Setting

Encryption	Type	Description
<b>None</b>	OPEN	Encryption algorithm is not used.
<b>WEP64</b>	SHARED/ WEPAUTO/802.1x	WEP encryption algorithm is used with 64bit key.
<b>WEP128</b>		WEP encryption algorithm is used with 128 bit key.
<b>TKIP</b>	WPA/WPA2/ WPA-PSK/ WPA2-PSK/ WPA1WPA2/ WPAPSKWPA2PSK	More complex encryption algorithm than WEP Is used.
<b>AES</b>		New encryption algorithm is used.
<b>TKIP/AES</b>		Support TKIP/AES simultaneously

#### 2.4.3.2.1. WEP

- ◆ Enter key for WEP64 or WEP128 network.
- ◆ Use either character string or hex character when entering key.
- ◆ Select 1~4 for 'Default Key..
- ◆ Enter at least one WEP Key.
- ◆ The entered WEP key is used for connection from wireless terminal.



The screenshot shows the 'Wire Equivalence Protection (WEP)' configuration window. At the top, there is a 'Default Key' dropdown menu currently set to 'Key 1'. Below this, there is a section labeled 'WEP Keys' which contains four rows. Each row has a label (WEP Key 1, WEP Key 2, WEP Key 3, WEP Key 4), an empty text input field, and a 'Hex' dropdown menu.

### 2.4.3.2.2. TKIP/AES authentication

- ◆ Enter at least 8 characters of character string for the network key value.

WPA	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	<input type="text" value="12345678"/>
Key Renewal Interval	<input type="text" value="3600"/> seconds (0 ~ 4194303)

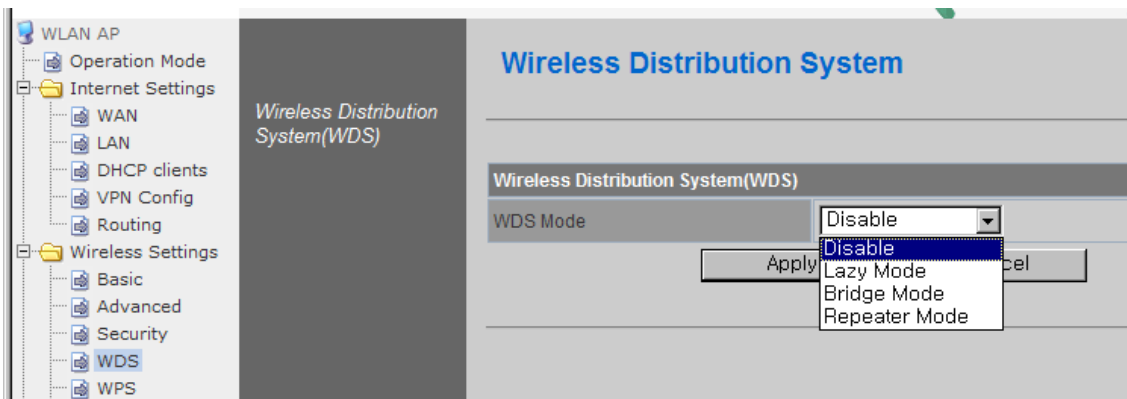
### 2.4.3.2.3. Wireless 802.1x authentication

- ◆ Enter the value for linking with the Radius Server.
- ◆ The values related to the Radius Server are provided by the internet service company.

"WLAN-AP"	
Security Mode	<input type="text" value="802.1X"/>
802.1x WEP	
WEP	<input type="radio"/> Disable <input type="radio"/> Enable
Radius Server	
IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="0"/>
Idle Timeout	<input type="text"/>
Access Policy	
Policy	<input type="text" value="Disable"/>
Add a station Mac:	<input type="text"/>
<input type="button" value="Save"/>	

## 2.4.4. WDS(Wireless Distribution System) Setting

- ◆ Connection with different AP is possible with WDS (Wireless Distribution System) function.
- ◆ Maximum of four APs can connect through WDS function.
- ◆ 2 APs must use the same channel and authentication / encryption method

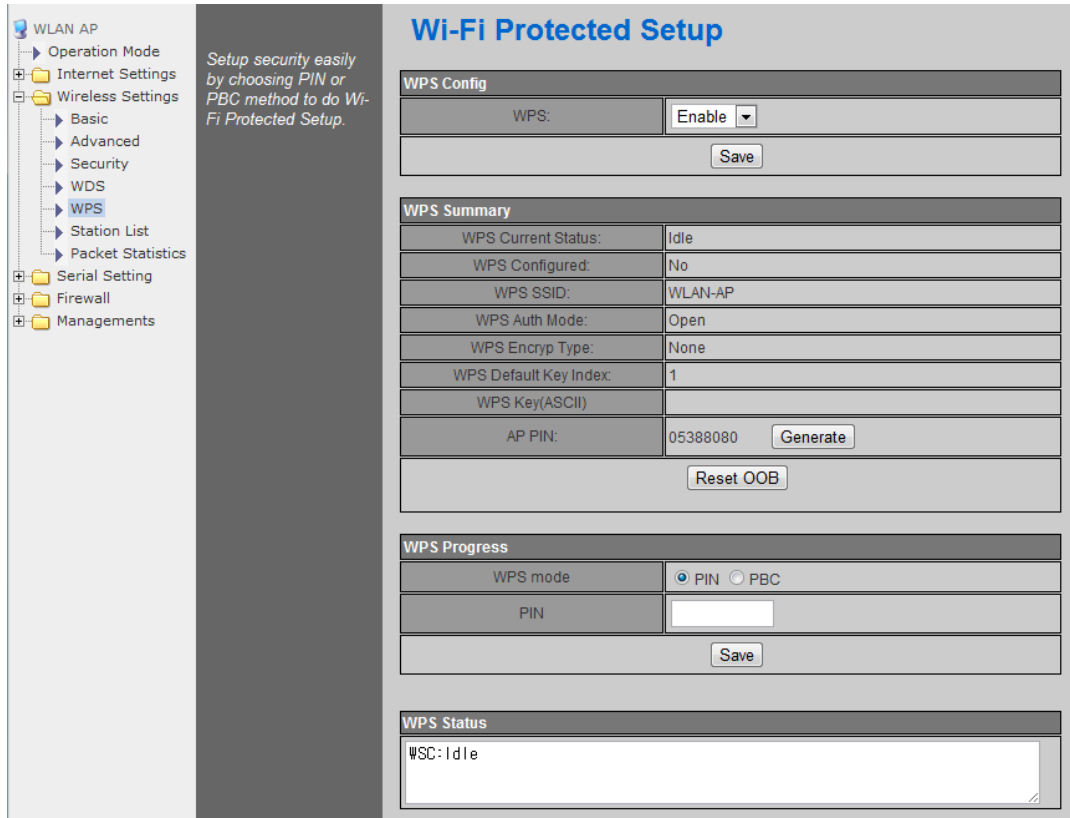


Type	Description
<b>Disable</b>	WDS function is not used. (Default disable)
<b>Lazy Mode</b>	Do not register the MAC of AP to be connected. Connect the AP's MAC to the registered AP. AP function is provided.
<b>Bridge Mode</b>	Register the MAC of AP to be connected. Connect the registered MAC to the AP. AP function is not provided.
<b>Repeater Mode</b>	Register the MAC of AP to be connected. Connect the registered MAC to the AP. AP function is provided. (The performance of WDS is best in Repeater Mode.)

## 2.4.5. WPS Setting

### 2.4.5.1. WPS Setting ( AP Mode )

- ◆ Only work at the AP Mode, Gateway Mode and AP-Client Mode
- ◆ The WPS function enables easier wireless network setting.



**WLAN AP**

- Operation Mode
- Internet Settings
- Wireless Settings
  - Basic
  - Advanced
  - Security
  - WDS
  - WPS**
  - Station List
  - Packet Statistics
- Serial Setting
- Firewall
- Managements

*Setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.*

### Wi-Fi Protected Setup

**WPS Config**

WPS:

**WPS Summary**

WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	WLAN-AP
WPS Auth Mode:	Open
WPS Encrypt Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	05388080 <input type="button" value="Generate"/>

**WPS Progress**

WPS mode:  PIN  PBC

PIN:

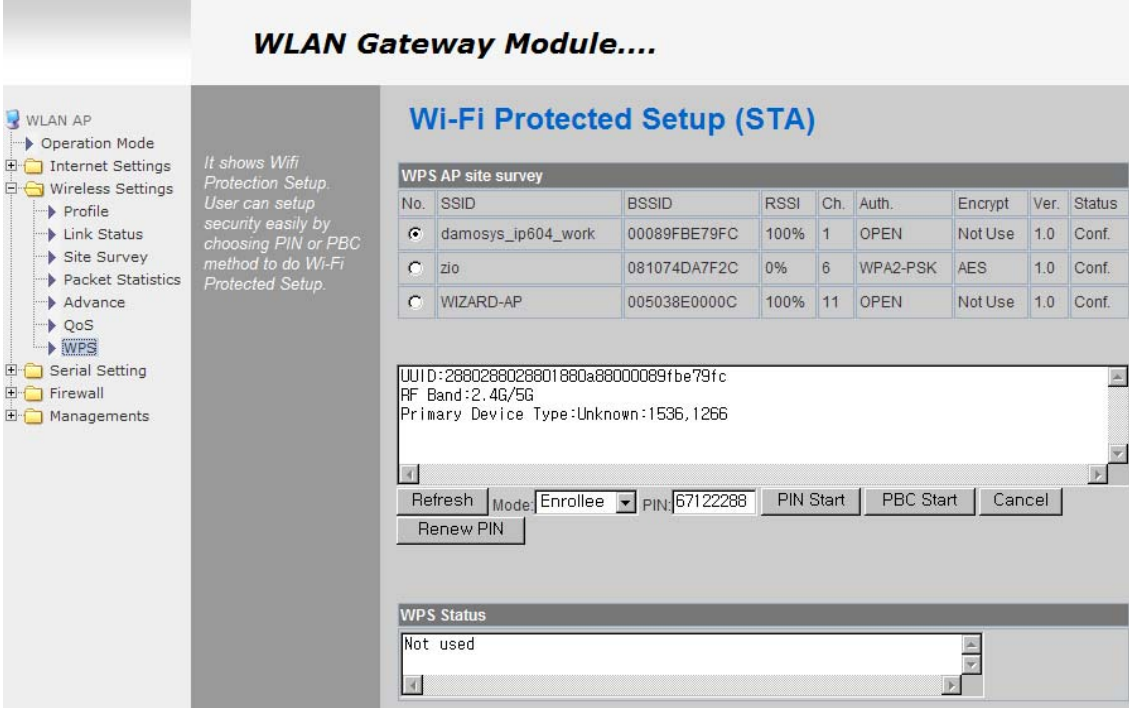
**WPS Status**

WSC: Idle

Type	Description
<b>WPS</b>	Enable / Disable WPS.
<b>WPS Current Status</b>	Shows whether WPS is used or not for the connection with station.
<b>WPS Configured</b>	Shows whether WPS is configured or not.
<b>WPS SSID</b>	Shows the SSID connected to the station.
<b>WPS Auth Mode</b>	Shows the authentication used with WPS.
<b>WPS Encrypt Type</b>	Shows the Encryption used with WPS.
<b>WPS Default Key Index</b>	Shows the default key ID used with WPS.
<b>WPS Key(ASCII)</b>	Shows the WPS Key.
<b>AP PIN</b>	Shows the PIN value used when connecting to station.
<b>WPS Mode</b>	Select PIN or PBC.

## 2.4.5.2. WPS Settings ( Client Mode )

- ◆ WPS settings in Station Mode.



The screenshot shows the 'WLAN Gateway Module...' configuration page. On the left is a navigation tree with 'WPS' selected under 'Wireless Settings'. The main area is titled 'Wi-Fi Protected Setup (STA)'. It contains a 'WPS AP site survey' table, a text box for device information, and control buttons for 'Refresh', 'Mode', 'Enrollee', 'PIN', 'PIN Start', 'PBC Start', 'Cancel', and 'Renew PIN'. Below these is a 'WPS Status' section showing 'Not used'.

**WPS AP site survey**

No.	SSID	BSSID	RSSI	Ch.	Auth.	Encrypt	Ver.	Status
1	damosys_ip604_work	00089FBE79FC	100%	1	OPEN	Not Use	1.0	Conf.
2	zio	081074DA7F2C	0%	6	WPA2-PSK	AES	1.0	Conf.
3	WIZARD-AP	005038E0000C	100%	11	OPEN	Not Use	1.0	Conf.

UIID: 2880288028801880a88000089fbc79fc  
 RF Band: 2.4G/5G  
 Primary Device Type: Unknown: 1536, 1266

Refresh Mode: Enrollee PIN: 67122288 PIN Start PBC Start Cancel  
 Renew PIN

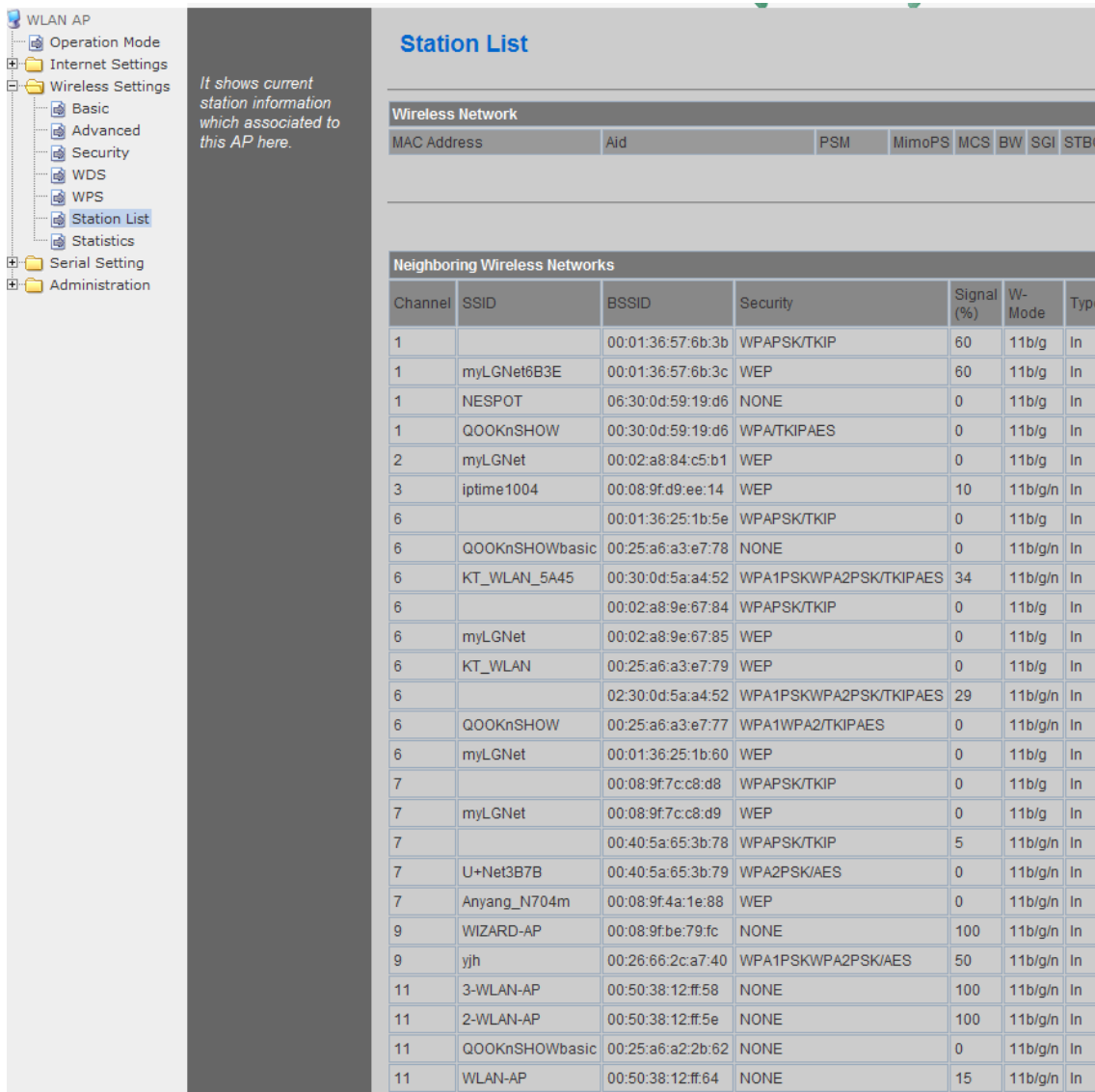
WPS Status  
 Not used

Type	Description
<b>Refresh</b>	Searches for WPS function activated AP.
<b>PIN Start</b>	Attempts connection with AP using PIN value.
<b>PBC Start</b>	Attempts connection with AP by virtually clicking the PBC button.
<b>Cancel</b>	Cancel the AP connection attempt.
<b>Renew PIN</b>	Renews the PIN value of WizFi630.



## 2.4.6. Wireless network status

- ◆ The status of the station that is connected to WizFi630 is shown.
- ◆ The surrounding wireless AP's status are shown.



*It shows current station information which associated to this AP here.*

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
Neighboring Wireless Networks							
Channel	SSID	BSSID	Security	Signal (%)	W-Mode	Type	
1		00:01:36:57:6b:3b	WPAPSK/TKIP	60	11b/g	In	
1	myLGNNet6B3E	00:01:36:57:6b:3c	WEP	60	11b/g	In	
1	NESPOT	06:30:0d:59:19:d6	NONE	0	11b/g	In	
1	QOOKnSHOW	00:30:0d:59:19:d6	WPA/TKIPAES	0	11b/g	In	
2	myLGNNet	00:02:a8:84:c5:b1	WEP	0	11b/g	In	
3	iptime1004	00:08:9f:d9:ee:14	WEP	10	11b/g/n	In	
6		00:01:36:25:1b:5e	WPAPSK/TKIP	0	11b/g	In	
6	QOOKnSHOWbasic	00:25:a6:a3:e7:78	NONE	0	11b/g/n	In	
6	KT_WLAN_5A45	00:30:0d:5a:a4:52	WPA1PSKWPA2PSK/TKIPAES	34	11b/g/n	In	
6		00:02:a8:9e:67:84	WPAPSK/TKIP	0	11b/g	In	
6	myLGNNet	00:02:a8:9e:67:85	WEP	0	11b/g	In	
6	KT_WLAN	00:25:a6:a3:e7:79	WEP	0	11b/g	In	
6		02:30:0d:5a:a4:52	WPA1PSKWPA2PSK/TKIPAES	29	11b/g/n	In	
6	QOOKnSHOW	00:25:a6:a3:e7:77	WPA1WPA2/TKIPAES	0	11b/g/n	In	
6	myLGNNet	00:01:36:25:1b:60	WEP	0	11b/g	In	
7		00:08:9f:7c:c8:d8	WPAPSK/TKIP	0	11b/g	In	
7	myLGNNet	00:08:9f:7c:c8:d9	WEP	0	11b/g	In	
7		00:40:5a:65:3b:78	WPAPSK/TKIP	5	11b/g/n	In	
7	U+Net3B7B	00:40:5a:65:3b:79	WPA2PSK/AES	0	11b/g/n	In	
7	Anyang_N704m	00:08:9f:4a:1e:88	WEP	0	11b/g/n	In	
9	WIZARD-AP	00:08:9f:be:79:fc	NONE	100	11b/g/n	In	
9	yjh	00:26:66:2c:a7:40	WPA1PSKWPA2PSK/AES	50	11b/g/n	In	
11	3-WLAN-AP	00:50:38:12:ff:58	NONE	100	11b/g/n	In	
11	2-WLAN-AP	00:50:38:12:ff:5e	NONE	100	11b/g/n	In	
11	QOOKnSHOWbasic	00:25:a6:a2:2b:62	NONE	0	11b/g/n	In	
11	WLAN-AP	00:50:38:12:ff:64	NONE	15	11b/g/n	In	

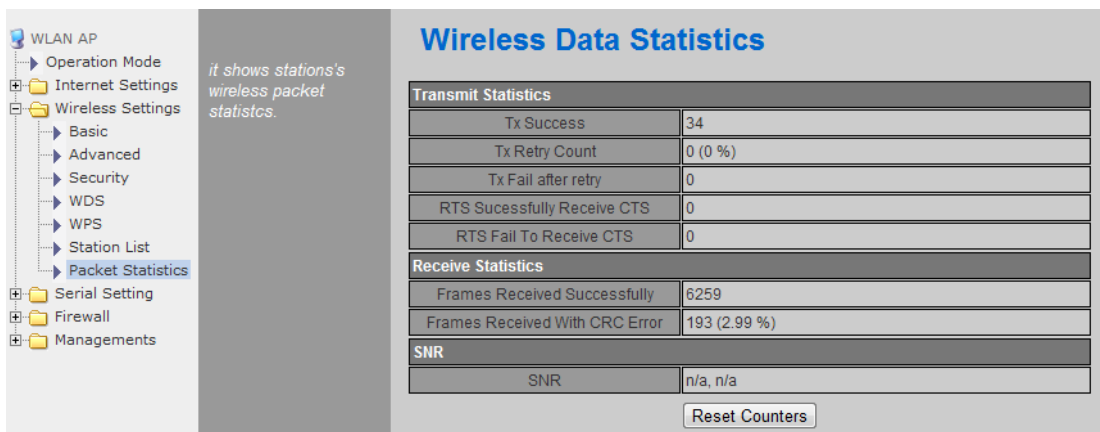
Type	Description
<b>Channel</b>	Channel information of AP
<b>SSID</b>	SSID of AP
<b>BSSID</b>	MAC address of AP
<b>Security</b>	Encryption method of AP
<b>Signal</b>	Signal strength with AP
<b>W-Mode</b>	Wireless mode of AP
<b>Type</b>	Network Type of finding AP In: Infrastructure, Ad: ad-hoc

## 2.4.7. AP Wireless Statistics

- ◆ The Statistics of wireless communication is shown.

### 2.4.7.1. AP Wireless Statistics ( AP Mode )

- ◆ Only work at the AP Mode, Gateway Mode and AP-Client Mode



WLAN AP

- Operation Mode
- Internet Settings
- Wireless Settings
  - Basic
  - Advanced
  - Security
  - WDS
  - WPS
  - Station List
  - Packet Statistics
- Serial Setting
- Firewall
- Managements

*it shows stations's wireless packet statistics.*

### Wireless Data Statistics

Transmit Statistics	
Tx Success	34
Tx Retry Count	0 (0 %)
Tx Fail after retry	0
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	6259
Frames Received With CRC Error	193 (2.99 %)
SNR	
SNR	n/a, n/a

Reset Counters

Type	Description
<b>Tx Success</b>	Number of successfully transmitted frames
<b>Tx Retry Count</b>	Number of retransmitted frames
<b>Tx Fail after retry</b>	Number of failed frames
<b>RTS Successfully Receive CTS</b>	Number of frames that successfully received CTS
<b>RTS Fail To Receive CTS</b>	Number of frames that failed to receive CTS
<b>Frames Receive Successfully</b>	Number of frames successfully received
<b>Frames Received With CRC Error</b>	Number of frames that failed due to CRC error
<b>SNR</b>	Receiving signal strength

## 2.4.7.2. AP Wireless Statistics ( Client Mode )

- ◆ Station statistics shows the information of wireless data packet in station mode.

**WLAN Gateway Module....**

WLAN AP

- ▶ Operation Mode
- ▶ Internet Settings
- ▶ Wireless Settings
  - ▶ Profile
  - ▶ Link Status
  - ▶ Site Survey
  - ▶ **Packet Statistics**
  - ▶ Advance
  - ▶ QoS
  - ▶ WPS
- ▶ Serial Setting
- ▶ Firewall
- ▶ Managements

**Station Statistics**

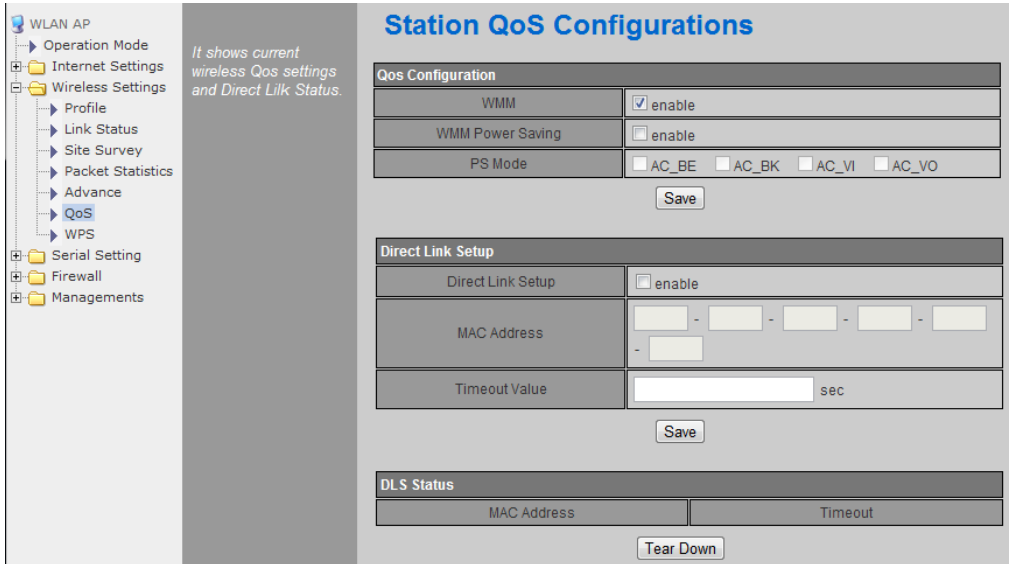
Transmit Statistics	
Frames Transmitted Successfully	3847
Frames Transmitted Successfully Without Retry	0
Frames Transmitted Successfully After Retry(s)	3847 (100.00 %)
Frames Fail To Receive ACK After All Retries	218
RTS Frames Successfully Receive CTS	0
RTS Frames Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	5174
Frames Received With CRC Error	38908 (88.26 %)
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	7

*it shows stations's wireless packet statistics.*

Type	Description
<b>Frames Transmitted Successfully</b>	Number of frames successfully transmitted.
<b>Frames Transmitted Successfully Without Retry</b>	Number of frames successfully transmitted without a retry.
<b>Frames Transmitted Successfully After Retry(s)</b>	Number of frames transmitted successfully after retry.
<b>Frames Fail To Receive ACK After All Retries</b>	Number of frames failed to receive ACK after all retries.
<b>RTS Frames Successfully Receive CTS</b>	Number of RTS frames that successfully received CTS
<b>RTS Frames Fail To Receive CTS</b>	Number of RTS frames failed to receive CTS.
<b>Frames Received Successfully</b>	Number of frames successfully received.
<b>Frames Received With CRC Error</b>	Number of frames received with CRC error.
<b>Frames Dropped Due To Out-of-Resources</b>	Number of frames dropped due to out of resources.
<b>Duplicate Frames Received</b>	Number of duplicate frames received.

## 2.4.8. Station QoS/DLS(Direct Link Setup) Configurations

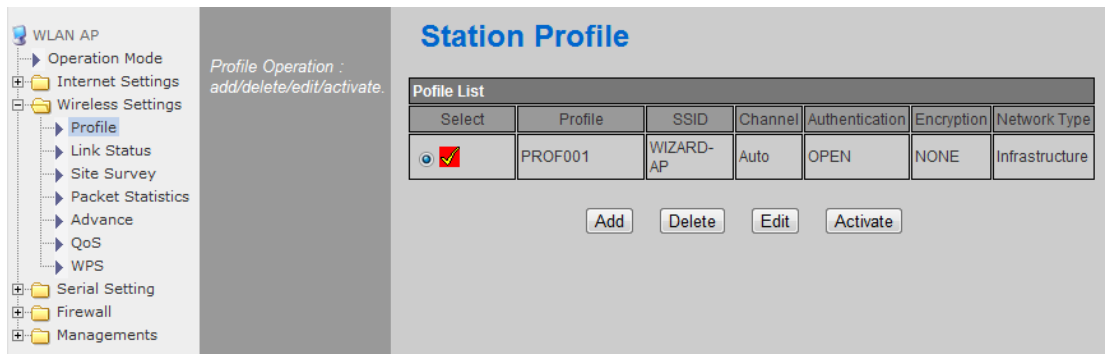
- ◆ Set Station QoS / DLS configurations in station mode



Type	Description
<b>WMM(Wi-Fi Multimedia)</b>	Enable WMM function or not.
<b>WMM Power Saving</b>	Enable Power Saving function or not.
<b>Direct Link Setup</b>	Enable Direct Link function or not. In order to use Direct Link function, the AP connected to WizFi630 and the Station to be connected must support Direct Link function.
<b>MAC Address</b>	Enter the MAC Address of the station to be connected using direct link function.
<b>Timeout Value</b>	Cancels the link if there are no traffic between stations for a period of time.

## 2.4.9. Profile

- ◆ Shows the profile of the connected AP.  
The profile information can be modified.  
By using "Site Survey", it is very convenient to find and connect with an AP.
- ◆ Administration of maximum of two AP is possible after adding to profile.
- ◆ The module automatically connects to the active AP (selected AP) upon booting.



Type	Description
<b>Profile</b>	Profile Name
<b>SSID</b>	SSID of AP to be connected
<b>Channel</b>	Channel information of AP to be connected. Channel information is needed only when connecting with ad-hoc.
<b>Authentication</b>	Authentication method of AP to be connected.
<b>Encryption</b>	Encryption method of AP to be connected.
<b>Network Type</b>	Select AP / ad-hoc.

## 2.4.10.Link Status

- ◆ Shows the link status between wireless LAN and AP.

**WLAN Gateway Module....**

WLAN AP

- ▶ Operation Mode
- ▶ Internet Settings
- ▶ Wireless Settings
  - ▶ Profile
  - ▶ **Link Status**
  - ▶ Site Survey
  - ▶ Packet Statistics
  - ▶ Advance
  - ▶ QoS
  - ▶ WPS
- ▶ Serial Setting
- ▶ Firewall
- ▶ Managements

*It shows module's WiFi link status. it is seen at the client (station) mode.*

### Station Link Status

Link Status		
Status	WIZARD-AP <--> 00-50-38-E0-00-0C	
Extra Info	Link is Up	
Channel	11 <--> 2462000 KHz; Central Channel: 9	
Link Speed	Tx(Mbps) 135.0	Rx(Mbps) 1.0
Throughput	Tx(Kbps) 5.0	Rx(Kbps) 58.9
Link Quality	Good 92%	
Signal Strength1	Good 90%	<input type="checkbox"/> dBm format
Signal Strength2	Weak 0%	
Signal Strength3	Weak 0%	
Noise Level	Low 0%	

HT	
BW	40
GI	long
STBC	none
MCS	7
SNR0	26
SNR1	n/a

Type	Description
<b>Status</b>	SSID and BSSID of connected AP.
<b>Extra Info</b>	Link status.
<b>Channel</b>	Channel information of connected AP.
<b>Link Speed</b>	Link speed rate of connected AP.
<b>Throughput</b>	Real performance through communication.
<b>Link Quality</b>	Link quality of connected AP.
<b>Signal Strength</b>	Signal strength of connected AP.
<b>Noise Level</b>	Noise level of connected AP.

- ◆ The HT section only appears when connected with 802.11n AP.

Type	Description
<b>BW</b>	Channel Bandwidth. 20MHz or 40MHz.
<b>GI</b>	Guard Interval Long: 800nsec, Short: 400nsec
<b>STBC</b>	Supported only when value of MCS is 0-7.
<b>MCS</b>	Shows link rate.
<b>SNR</b>	Shows the receiving signal strength.

## 2.4.11.Site Survey

- ◆ Site Survey searches for AP surrounding WizFi630.
- ◆ Select an AP and click the connect button (If the module is rebooted, the module will connect to the previous profile).
- ◆ Click "Add Profile" if user wishes to add to profile.

**WLAN Gateway Module....**

WLAN AP

- ▶ Operation Mode
- ▶ Internet Settings
- ▶ Wireless Settings
  - ▶ Profile
  - ▶ Link Status
  - ▶ Packet Statistics
  - ▶ **Site Survey**
  - ▶ Advance
  - ▶ QoS
  - ▶ WPS
- ▶ Serial Setting
- ▶ Firewall
- ▶ Managements

**Station Site Survey**

*It show shows site survey information of APs nearby. User can choose one of these APs connecting or adding it to profile.*

Select	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Network Type
<input type="radio"/>	Semitron_AP	00:1d:7e:54:eb:8b	100%	11	Not Use	OPEN	In
<input checked="" type="radio"/>	WIZARD-AP	00:50:38:e0:00:0c	100%	11	Not Use	OPEN	In
<input type="radio"/>	visitor	00:11:21:f8:f0:20	65%	2	WEP	Unknown	In
<input type="radio"/>	Semi-AP-Anygate	00:1f:1f:41:db:24	60%	11	Not Use	OPEN	In
<input type="radio"/>	WIZARD-AP-chi	00:50:38:12:45:00	50%	11	Not Use	OPEN	In
<input type="radio"/>	Semi_AP_DLink_24G	00:24:01:db:aa:ec	50%	6	AES	WPA2-PSK	In
<input type="radio"/>	WLANAP	00:50:38:12:45:01	50%	11	Not Use	OPEN	In
<input type="radio"/>	damosys_ip604_work	00:08:9f:be:79:fc	29%	1	Not Use	OPEN	In
<input type="radio"/>	802.1x	74:91:1a:ab:74:69	29%	1	AES	WPA2	In
<input type="radio"/>	ruckus	74:91:1a:2b:74:69	20%	1	AES	WPA2-PSK	In
<input type="radio"/>	McTiVia	e0:69:95:76:74:32	15%	1	Not Use	OPEN	In
<input type="radio"/>	kimkyong	00:08:9f:d9:fa:08	15%	11	Not Use	OPEN	In
<input type="radio"/>	UTIS-AUTH	0a:0b:6b:2b:ca:29	0%	7	AES	WPA; WPA2	In
<input type="radio"/>	U+Net0E4B	00:40:5a:98:0e:49	0%	3	AES	WPA2-PSK	In
<input type="radio"/>	zio	08:10:74:da:7f:2c	0%	6	AES	WPA2-PSK	In
<input type="radio"/>	iptime	00:26:66:a8:24:dc	0%	11	Not Use	OPEN	In

Connected <--> WIZARD-AP

Type	Description
<b>SSID</b>	SSID of searched AP
<b>BSSID</b>	Wireless MAC Address of searched AP.
<b>RSSI</b>	Signal strength of searched AP.
<b>Channel</b>	Channel of searched AP.
<b>Encryption</b>	Encryption method of searched AP.
<b>Authentication</b>	Authentication method of searched AP.
<b>Network Type</b>	Network type of searched AP. In: Infrastructure, Ad: ad-hoc
<b>Connected</b>	SSID of AP connected with WizFi630.
<b>Connect</b>	Connects with AP.
<b>Rescan</b>	Rescans for surrounding AP.
<b>Add Profile</b>	Adds to profile.

## 2.4.12. WIFI Multi-Bridge settings

- ◆ Set WI-FI Multi Bridge Mode in AP-Client mode.

WLAN Gateway Module....

- WLAN AP
- ▶ Operation Mode
- ▶ Internet Settings
- ▶ Wireless Settings
  - ▶ Basic
  - ▶ Advanced
  - ▶ Security
  - ▶ WDS
  - ▶ WPS
  - ▶ **WIFI Multi Bridge**
  - ▶ Station List
  - ▶ Packet Statistics
- ▶ Serial Setting
- ▶ Firewall
- ▶ Managements

You could configure AP Client parameters here.

### AP Client Feature

**Wireless multi-bridge configuration**

Operation Mode	<input checked="" type="radio"/> WiFi is WAN <input type="radio"/> Multi-Bridge Mode	
SSID	<input type="text" value="WLAN_AP_1"/> <input type="button" value="Search AP"/>	
Frequency (Channel)	<input type="text" value="2412MHz (Channel 1)"/>	
MAC Address (Optional)	<input type="text" value="00:50:38:e0:10:20"/>	
Security Mode	<input type="text" value="Open"/>	
Encryption Type	<input type="text" value="None"/>	
WEP Default Key	<input type="text" value="Key 1"/>	
WEP Keys	WEP Key 1 :	<input type="text"/> <input type="text" value="ASCII"/>
	WEP Key 2 :	<input type="text"/> <input type="text" value="ASCII"/>
	WEP Key 3 :	<input type="text"/> <input type="text" value="ASCII"/>
	WEP Key 4 :	<input type="text"/> <input type="text" value="ASCII"/>

Type	Description
<b>Operation Mode</b>	Select Gateway or Bridge Mode. Wi-Fi is WAN: operates in Gateway Mode. Multi-Bridge Mode: operates in Bridge Mode.
<b>SSID</b>	SSID of AP to be connected.
<b>Frequency (Channel)</b>	Channel of AP to be connected.
<b>MAC Address</b>	MAC Address of AP to be connected. (optional)
<b>Security</b>	Select the same security option with AP to be connected.

© Copyright 2012 WIZnet Co., Ltd. All rights reserved.

48



## 2.5. Serial to LAN(Wired and Wireless)

- ◆ Individual settings for serial #1 and serial #2 are possible.
- ◆ Set the serial parameters for serial to wireless (Ethernet) function.
- ◆ Set two channels (Main connection, Aux connection) for each serial port
- ◆ Setting management of Serial #1 and #2 (Main connection, Aux connection)

### WLAN Gateway Module....

WLAN AP

- ▶ Operation Mode
- ▶ Internet Settings
  - ▶ WAN
  - ▶ LAN
  - ▶ DHCP Clients
  - ▶ VPN Config
  - ▶ Routing
  - ▶ QoS(802.1p)
  - ▶ VLAN(802.1q)
- ▶ Wireless Settings
  - ▶ Basic
  - ▶ Advanced
  - ▶ Security
  - ▶ WDS
  - ▶ WPS
  - ▶ Station List
  - ▶ Packet Statistics
- ▶ Serial Setting
  - ▶ **Serial Port#1**
  - ▶ Serial Port#2
- ▶ Firewall
- ▶ Managements

#### Serial-to-Ethernet(Serial #1)

*It shows current Serial to LAN conguration for serial port #1. user can change it.*

Main Connection Configuration	
Status:	<input checked="" type="checkbox"/> Enable
Protocol:	<input type="radio"/> UDP <input checked="" type="radio"/> TCP
Mode:	<input type="radio"/> Server <input checked="" type="radio"/> Client <input type="radio"/> Mixed
Server IP:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="123"/> or <input style="width: 100px;" type="text"/>
Server Port:	<input type="text" value="5000"/>
Reconnect Interval:	<input type="text" value="10"/> Seconds(1-30, default: 10)
Connection Option:	<input checked="" type="radio"/> System BootUp <input type="radio"/> Serial Data In
Baudrate:	<input type="text" value="38400"/>
Databits:	<input type="text" value="8"/>
Parity:	<input type="text" value="None"/>
Stopbits:	<input type="text" value="1"/>
Flowcontrol:	<input type="text" value="None"/>

Aux Connection Configuration	
Status:	<input type="checkbox"/> Enable
Protocol:	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Mode:	<input checked="" type="radio"/> Server <input type="radio"/> Client
Server IP:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="123"/> or <input style="width: 100px;" type="text"/>
Server Port:	<input type="text" value="5050"/>

Data Packing Condition	
Time:	<input type="text" value="0"/> milli-second(100-5000, default: 0)
Size:	<input type="text" value="0"/> Bytes(0-1500, default: 0)
Char:	<input type="text" value="00"/> Hexacode(00-ff, default: 0)
Inactivity Time:	<input type="text" value="0"/> Seconds(00-60, default: 0)
Command Mode:	<input type="checkbox"/> Enable(Enable: H/W GPIO Used)

Ethernet Data Tagging Option	
Status:	<input type="checkbox"/> Enable
Main Port:	<input type="text" value="!MAIN!"/> string(1-16 chars)
Aux Port:	<input type="text" value="!AJX!"/> string(1-16 chars)

## 2.5.1. Main Connection settings

Type	Description
<b>Status</b>	Enable checked : Serial to LAN is used. Enable un-check: Serial to LAN is not used.
<b>Protocol</b>	Protocol used in Serial to LAN communication -TCP -UDP
<b>Mode</b>	Serial to LAN operation mode. ( Client Mode recommended) - Server : waits for connection. - Client : connected to the remote server of WizFi630 - Mixed : not recommended
<b>Server IP</b>	Enter the IP address for WizFi630 setting.
<b>Server Port</b>	Enter the port number for remote serial data server host PC.
<b>Reconnect Interval</b>	Interval of TCP reconnection.
<b>Connection</b>	Connection Type of WizFi630's Serial LAN. ( TCP Only ) System Bootup : connected to the remote server upon bootup. Serial Data In : once serial data comes in, connect to remote server. (end connection after inactive time)
<b>Baud rate</b>	Select the serial communication speed.
<b>Databits</b>	Select the databits.
<b>Parity</b>	Select the method for parity check.
<b>Stopbits</b>	Select the stopbits.
<b>FlowControl</b>	Select the method for flow control. (Option: none, Xon/Xoff, RTS/CTS)

## 2.5.2. Aux Connection Settings

Type	Description
<b>Status</b>	Select whether to enable serial port or not.
<b>Protocol</b>	Protocol used in Serial to LAN communication.
<b>Mode</b>	Select Server or Client Mode.
<b>Server IP</b>	Enter the IP address for WizFi630 setting.
<b>Server Port</b>	Enter the port number for remote serial data server host PC.

### 2.5.3. Packing Condition (Incoming serial data packing condition)

Type	Description
<b>Time</b>	Data packing until the set time and then sent to server after the set time.
<b>Size</b>	Data packing until the set size and then sent to the server.
<b>Character</b>	Data packing until the set character and then sent to the server.
<b>Inactivity Time:</b>	TCP/IP connection is discontinued if there is neither serial data nor network data during the set time.
<b>H/W CMD switch</b>	- . Enable/Disable the H/W CMD switch pin. - . H/W CMD switch pin is the switch for sending commands from CPU to WizFi630.

### 2.5.4. Ethernet Data Tagging Option

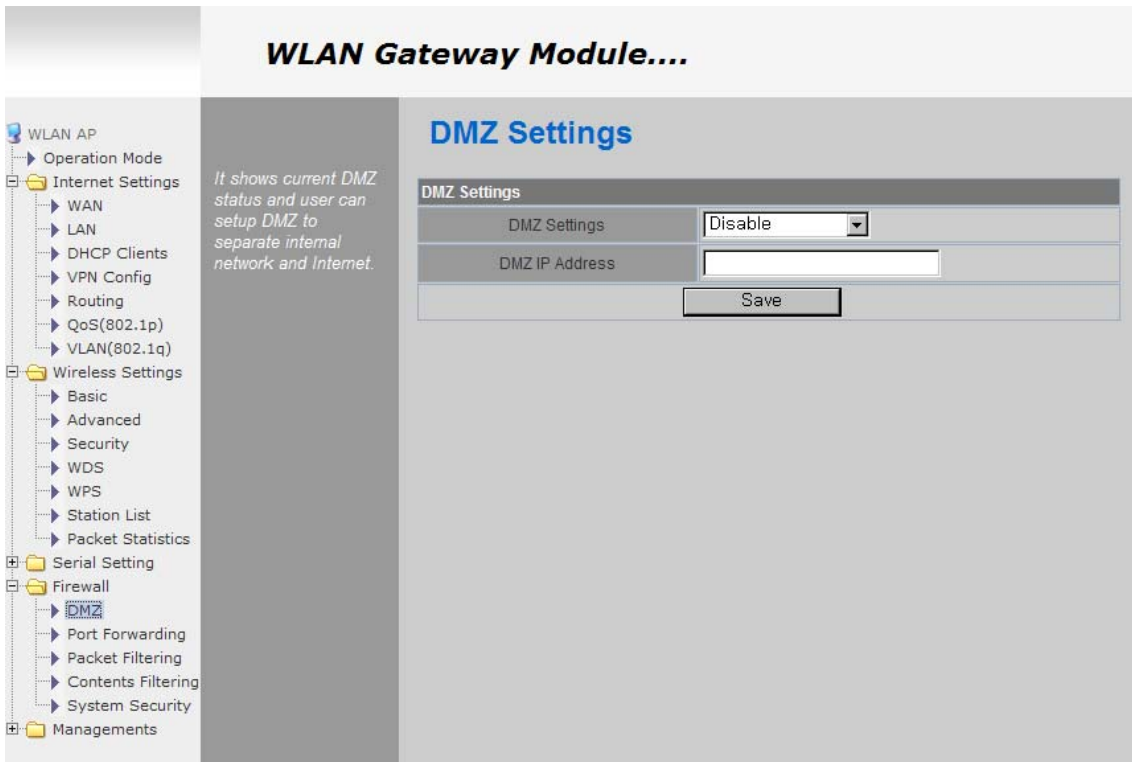
This option is used to help serial device to identify who is the received serial data's source; the received serial data comes from Main Port or Aux Port.

Type	Description
<b>Status</b>	Enable or disable this option (Checked : Enable, Un-Check : Disable)
<b>Main Port</b>	Before sending data from Main port to serial port, WizFi630 added a TAG in the front of payload. For example: In-come LAN Data : "abcdefg" Output data to Serial Port : "!MAIN!abcdefg"
<b>Aux Port</b>	Before sending data from Aux port to serial port, WizFi630 added a TAG in the front of payload. For example: In-come LAN Data : "abcdefg" Output data to Serial Port : "!AUX!abcdefg"

## 2.6. Firewall settings

### 2.6.1. DMZ

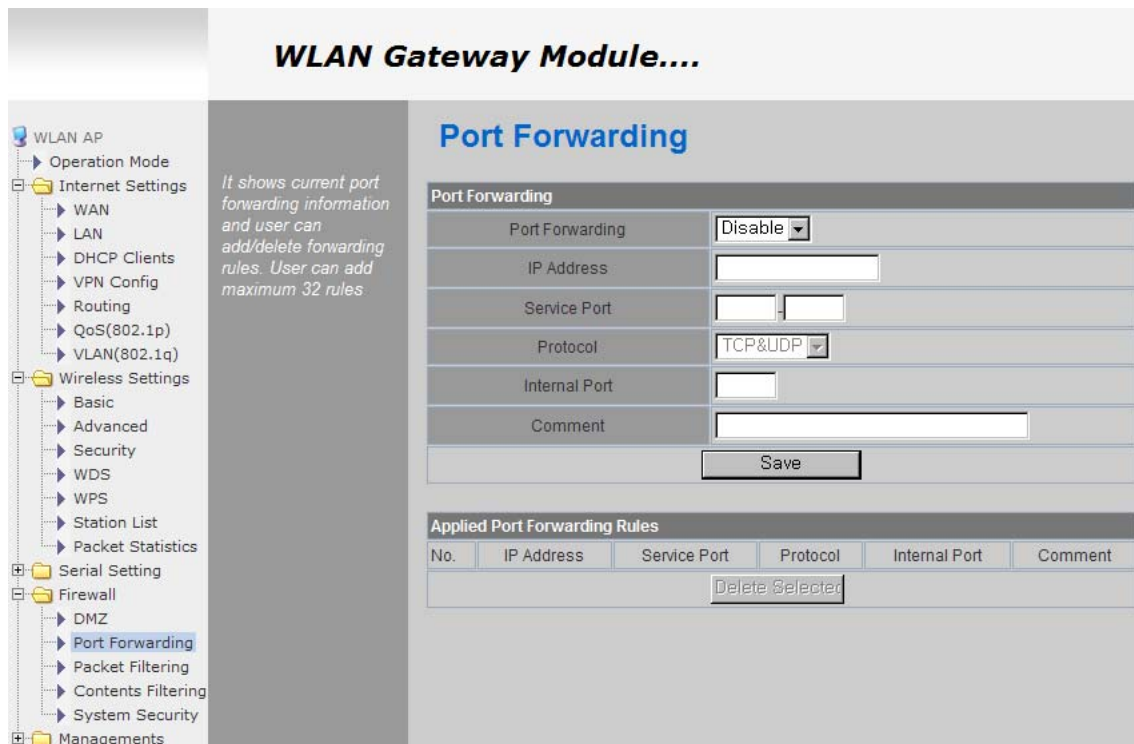
- ◆ Enable/Disable DMZ function.
- ◆ A DMZ allows a single computer on your LAN to expose ALL of its unused ports to the Internet. When doing this, the exposed computer is no longer behind the firewall.
- ◆ Sometimes TCP/IP applications require very specialized IP configurations that are difficult to set up or not supported by your router. In this case, placing your computer in the DMZ is the only way to get the application working.



Type	Description
<b>DMZ Settings</b>	Disable/Enable DMZ
<b>DMZ IP Address</b>	Input the IP address that you would like to expose all of its unused ports to the Internet

## 2.6.2. Port forwarding

When a computer on the internet sends data to the external IP address of the router (WizFi630), the router (WizFi630) needs to know what to do with the data. Port Forwarding simply tells the WizFi630 which computer on the local area network to send the data to. When you have port forwarding rules set up, your router takes the data off of the external IP address:port number and sends that data to an internal IP address:port number. Port Forwarding rules are created per port. Thus, a rule set up for port 53 will only work for port 53.



Type	Description
<b>Port Forwarding</b>	Disable/Enable Port Forwarding
<b>IP Address</b>	Internal IP address
<b>Service Port</b>	External ports range
<b>Protocol</b>	Supports TCP and UDP
<b>Internal Port</b>	Internal port

## 2.6.3. Packet filtering

- ◆ WizFi630 can accept or block Internet packets according to pre-defined MAC or IP address
- ◆ First, please do the basic settings

**WLAN Gateway Module....**

- WLAN AP
  - Operation Mode
  - Internet Settings
    - WAN
    - LAN
    - DHCP Clients
    - VPN Config
    - Routing
    - QoS(802.1p)
    - VLAN(802.1q)
  - Wireless Settings
    - Basic
    - Advanced
    - Security
    - WDS
    - WPS
    - Station List
    - Packet Statistics
  - Serial Setting
  - Firewall
    - DMZ
    - Port Forwarding
    - Packet Filtering**
    - Contents Filtering
    - System Security
  - Managements

*it shows current mac/ip/port filtering information. User can change add and delete rules for special purpose. User can add maximum 32 rules*

### MAC/IP/Port filtering Settings

**Basic Settings**

MAC/IP/Port Filtering: Disable

Default Policy -- The packet that don't match with any rules would be: Accepted

**MAC/IP/Port Filter Settings**

Source MAC:

Dest IP:

Source IP:

Protocol: None

Dest Port Range:  -

Source Port Range:  -

Action: Drop

Comment:

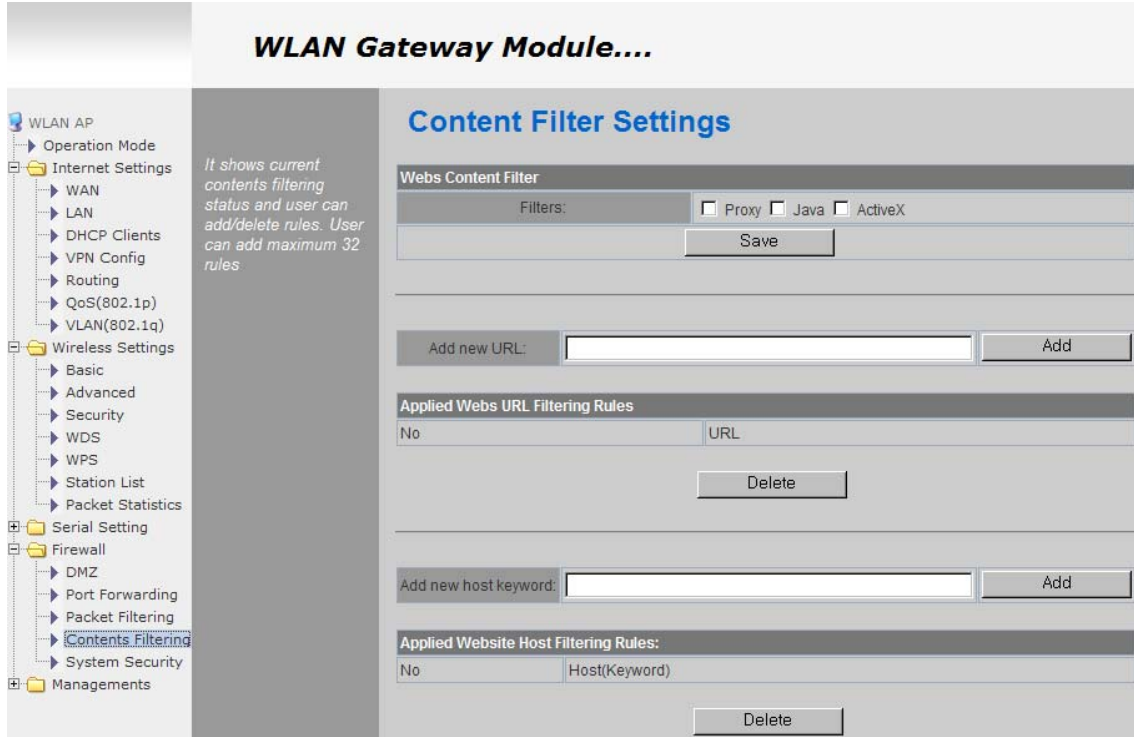
**Applied MAC/IP/Port Filtering Rules**

No.	Source MAC	Dest IP	Source IP	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be accepted									-

Type	Description
<b>Source MAC</b>	Pre-defined source MAC address for MAC filtering function
<b>Dest IP Address</b>	Destination IP address
<b>Source IP Address</b>	Source IP address
<b>Protocol</b>	Supports TCP, UDP, ICMP
<b>Dest Port Range</b>	Destination port range
<b>Source Port Range</b>	Source port range
<b>Action</b>	Enable/Disable MAC/IP/Port filtering function

## 2.6.4. Contents filtering

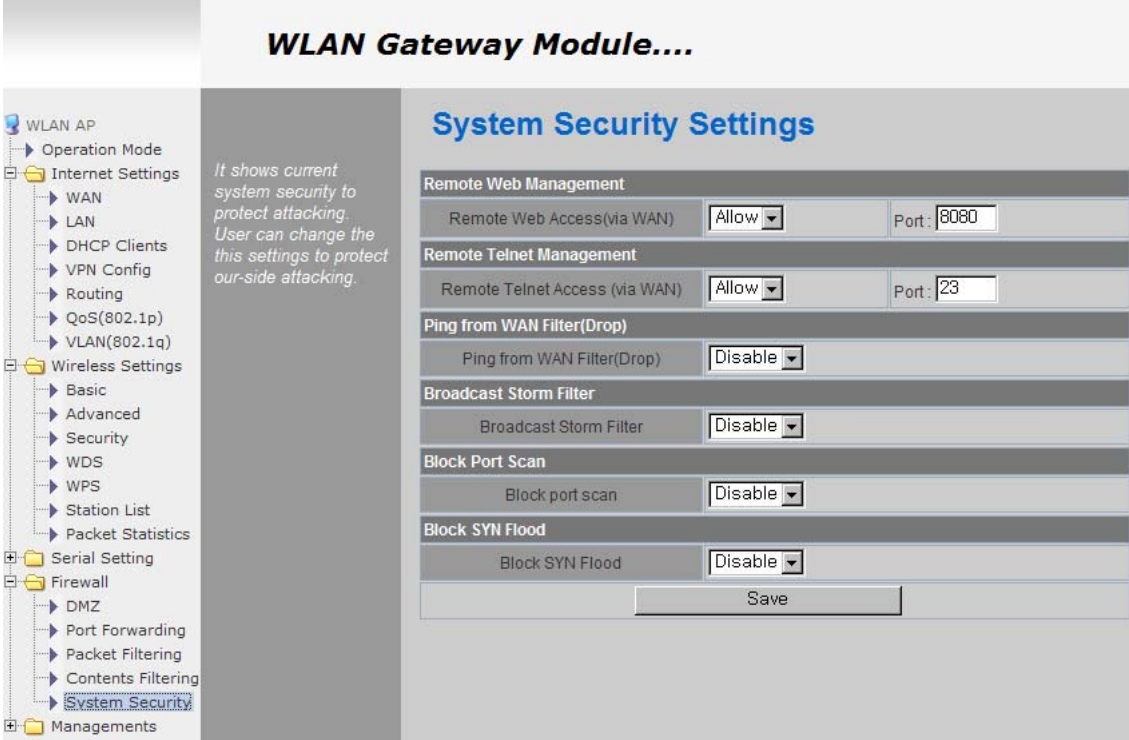
- ◆ Used to block certain websites (IP or domain names).



Type	Description
<b>URL Filter</b>	Block all the websites whose domain is the input text For example, if you input "sex", the websites like <a href="http://www.sex.com">www.sex.com</a> is blocked. But <a href="http://www.sexgood.com">www.sexgood.com</a> is not blocked. If you would like to block all the websites whose domain name contains the input text, please use Host Filter function
<b>Host Filter</b>	Block all the websites whose domain name contains the input text. For example, if you input "game", the websites like <a href="http://www.hangame.com">www.hangame.com</a> , <a href="http://www.hangame.co.kr">www.hangame.co.kr</a> are blocked

## 2.6.5. System Security

- ◆ Defense from external attack.



**WLAN Gateway Module...**

**System Security Settings**

It shows current system security to protect attacking. User can change the this settings to protect our-side attacking.

**Remote Web Management**

Remote Web Access(via WAN)  Port:

**Remote Telnet Management**

Remote Telnet Access (via WAN)  Port:

**Ping from WAN Filter(Drop)**

Ping from WAN Filter(Drop)

**Broadcast Storm Filter**

Broadcast Storm Filter

**Block Port Scan**

Block port scan

**Block SYN Flood**

Block SYN Flood

Type	Description
<b>Remote management</b>	Settings about accessing methods from WAN to WizFi630's embedded web server
<b>Telnet management</b>	Settings about accessing methods from WAN to WizFi630's telnet
<b>Ping from WAN Filter</b>	Disable/Enable the WizFi630's Ping response
<b>Broadcast Storm filter</b>	Block/Accept the Broadcast packets
<b>Block Port Scan</b>	Block WizFi630's port-scan function
<b>Block SYN Flood</b>	Block SYN flood



## 2.7. Managements

### 2.7.1. System Management

**WLAN Gateway Module....**

**System Management**

Configure lanaguage code for web sever, login account and password, NTP (system time zone), Green AP function for power save, Dynamic DNS.

WLAN AP

- Operation Mode
- Internet Settings
- Wireless Settings
- Serial Setting
- Firewall
- Managements
  - System Mgmt**
  - Firmware Mgmt
  - Config Mgmt
  - Port Mgmt
  - Packet Statistics
  - System Status
  - System Log

**Language Settings**

Select Language:  Save

**Module Name**

Name:  Save

**Administrator Settings**

Account:  Password:  Save

**Telnet Connection Count**

Count:  (default:5, 1-10) Save

**NTP Settings**

Current Time:  Sync with host

Time Zone:

NTP Server:   
ex: time.nist.gov , ntp0.broad.mit.edu , time.stdtime.gov.tw

NTP synchronization(hours):  Save

**Green AP**

Duration	Action
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>

Save

**DDNS Settings**

Dynamic DNS Provider:

Account:

Password:

DDNS:

Save

**System Status Report**

Status:

IP/Domain:Port #1:   0-65535

IP/Domain:Port #2:   0-65535

Interval:  (1-1440)Minutes

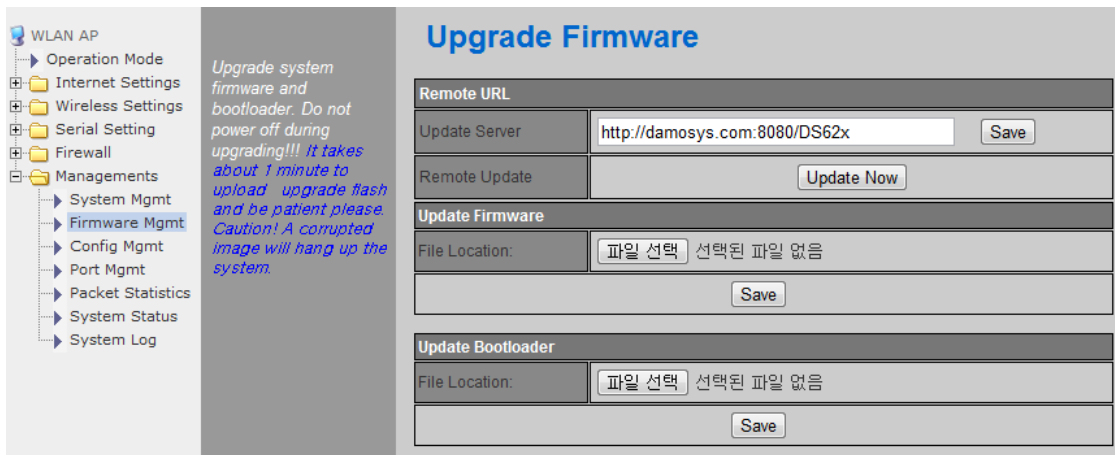
System Description:

Save

Type	Description
<b>Language</b>	Select language in the list
<b>Administrator</b>	Pre-defined ID/Password for webpage or Telnet login
<b>NTP (Network Time Protocol)</b>	Set NTP server
<b>Green AP</b>	Low power consumptive AP
<b>DDNS</b>	Once the DDNS server registers yours MAC address, your device can connect to the internet regardless of your address. DDNS service can be provided by DynDNS, freeDNS, zoneedit, no-ip. To use DynDNS, users should go to www.dyndns.org to create user name and domain name. And then, set related configurations by using WizFi630's webpage. Similarly, to use freeDNS zoneedit, or no-ip, users should go to their homepage first to create user name and domain name. And then, set related configurations by using WizFi630's webpage.
<b>DDNS Provider</b>	DynDNS, freeDNS, zoneedit, no-ip
<b>Account</b>	ID for DDNS.
<b>Password</b>	Password for DDNS
<b>DDNS</b>	Host name for DDNS

## 2.7.2. Firmware

- ◆ Upgrade firmware and bootloader.
- ◆ WizFi630 do not support upgrading by Remote URL..



**Upgrade Firmware**

Remote URL

Update Server:  Save

Remote Update: Update Now

Update Firmware

File Location:  선택된 파일 없음 Save

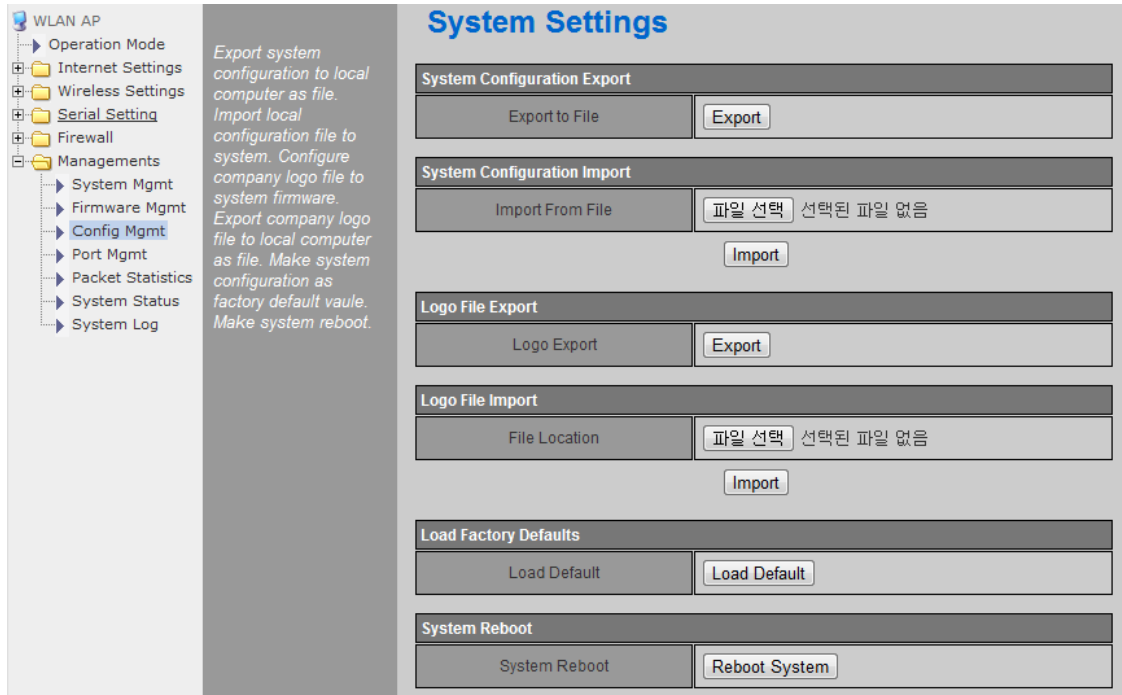
Update Bootloader

File Location:  선택된 파일 없음 Save

*Upgrade system firmware and bootloader. Do not power off during upgrading!!! It takes about 1 minute to upload upgrade flash and be patient please. Caution! A corrupted image will hang up the system.*

## 2.7.3. Config Settings

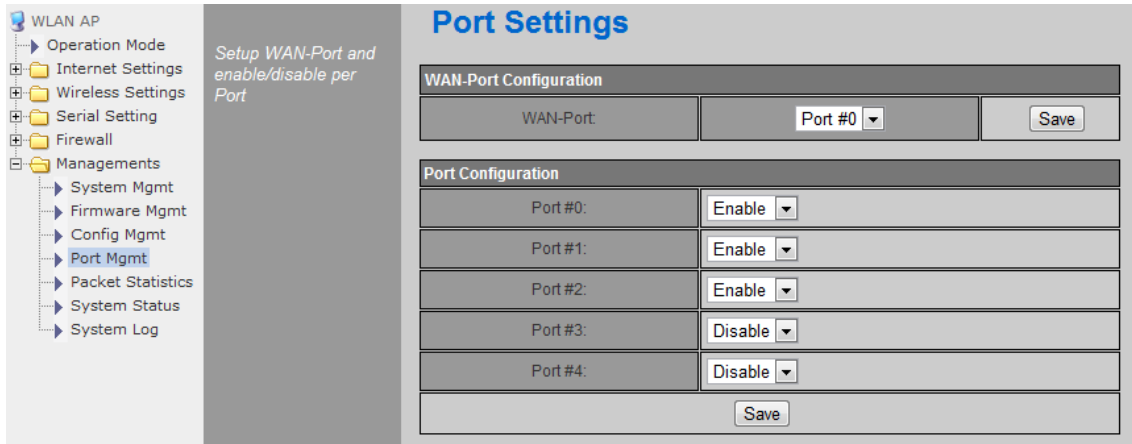
- ◆ Save the setting value of WizFi630 to the PC.



Type	Description
<b>Export Settings</b>	The setting files from the PC file are applied to the module.
<b>Import Settings</b>	The system's setting information is saved as a file in the PC.
<b>Logo Export Settings</b>	User's company logo file is saved in the PC.
<b>Logo Import Settings</b>	User's company logo from the PC is applied to the system. ( GIF file size : 10K , 126x42)
<b>Load Factory Defaults</b>	Change the module's setting to default setting.
<b>Reboot</b>	Reboots the system.

## 2.7.4. Port Setting

- ◆ Settings about wired port. In case of Gateway Mode, WAN port is set here
- ◆ In case of Gateway Mode, it is better to use the default WAN port number (Port #0)
- ◆ If you are not the administrator, we do not recommend changing this.



Type	Description
<b>WAN Port</b>	Select the WAN Port in case of Gateway Mode.
<b>Port #0</b>	Enable / Disable Port #0.
<b>Port #1</b>	Enable / Disable Port #1.
<b>Port #2</b>	Enable / Disable Port #2.
<b>Port #3</b>	Enable / Disable Port #3.
<b>Port #4</b>	Enable / Disable Port #4.

## 2.7.5. Packet Statistics

- ◆ System Statistics shows the system's memory information and system's data transmission size.

WLAN AP

- ▶ Operation Mode
- ▶ Internet Settings
- ▶ Wireless Settings
- ▶ Serial Setting
- ▶ Firewall
- ▶ Managements
  - ▶ System Mgmt
  - ▶ Firmware Mgmt
  - ▶ Config Mgmt
  - ▶ Port Mgmt
  - ▶ Packet Statistics
  - ▶ System Status
  - ▶ System Log

*it displays packet information per interfaces.*

### Statistics

Memory				
Memory total:	29656 kB			
Memory left:	12576 kB			
WAN/LAN				
Name	Rx Packet	Rx Byte	Tx Packet	Tx Byte
WAN	0	0	21	10404
LAN	677	86932	316	133105
All interfaces				
Name	Rx Packet	Rx Byte	Tx Packet	Tx Byte
eth2	26992	3633422	21619	14706595
lo	16	2387	16	2387
ra0	5063	1357905	117	0
wds0	0	0	0	0
wds1	0	0	0	0
wds2	0	0	0	0
wds3	0	0	0	0
eth2.1	684	90322	316	134369
eth2.2	0	0	21	10404
br0	677	86932	316	133105

Type	Description
<b>Memory Total</b>	System Memory Size
<b>Memory left</b>	System Free Memory
<b>Rx Packet</b>	Rx Packets counts
<b>Rx Byte</b>	Rx Bytes Counts
<b>Tx Packet</b>	Tx Packet Counts
<b>Tx Byte</b>	Tx Bytes Counts

## 2.7.6. System Status

System Status shows the status of the system, status of the system's network information, and the link status of LAN port.

WLAN Gateway Module....

- WLAN AP
- ▶ Operation Mode
- ▶ Internet Settings
- ▶ Wireless Settings
- ▶ Serial Setting
- ▶ Firewall
- ▶ Managements
  - ▶ System Mgmt
  - ▶ Firmware Mgmt
  - ▶ Config Mgmt
  - ▶ Port Mgmt
  - ▶ Packet Statistics
  - ▶ System Status
  - ▶ System Log

*It display system firmware version, up-time, operation mode and internet configuration and connection information.*

### System Status

System Information	
FW Version	DS620P-11n-4M-usb-sta-PCle-msg_v1.1.22-2011/11/25, 20:08:46
System Up Time	2 days, 19 hours, 47 mins, 25 secs
Operation Mode	Gateway Mode
Wireless Driver Version	2.6.0.0
Internet Configurations	
Connected Type	DHCP
WAN IP Address	192.168.123.34
Subnet Mask	255.255.255.0
Default Gateway	192.168.123.254
Primary Domain Name Server	168.126.63.1
Secondary Domain Name Server	168.126.63.2
MAC Address	00:50:38:E0:00:0E
Local Network	
Local IP Address	192.168.16.254
Local Netmask	255.255.255.0
MAC Address	00:50:38:E0:00:0C

Ethernet Port Status

W
L
L
L
L

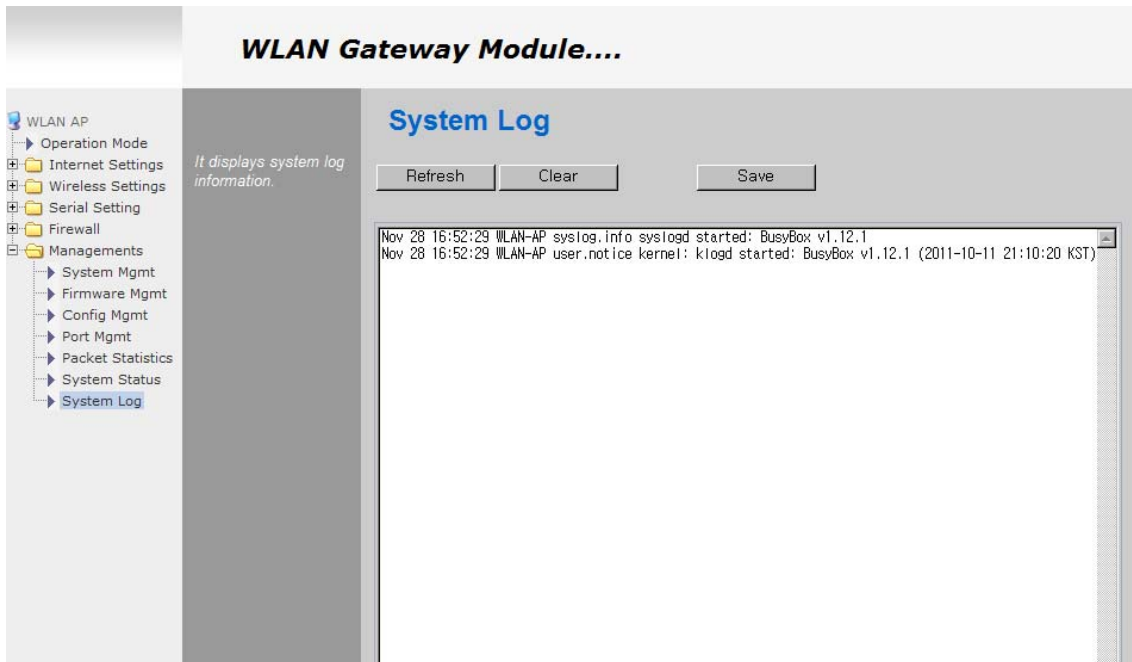
Type	Description
<b>F/W Version</b>	Shows the firmware version.
<b>System Up Time</b>	Shows the system up time.
<b>Operation Mode</b>	Shows the operation mode currently being used.
<b>Internet Configuration</b>	Shows the internet configuration information.
<b>Local Network</b>	Shows the local network information.

© Copyright 2012 WIZnet Co., Ltd. All rights reserved.

62

## 2.7.7. System Log

- ◆ The operation history of WizFi630 can be checked by using System Log.
- ◆ If the system log exceeds 24Kbyte, more recent log record is added.



## 3. Hardware Information

### 3.1. WizFi630 Pin Map

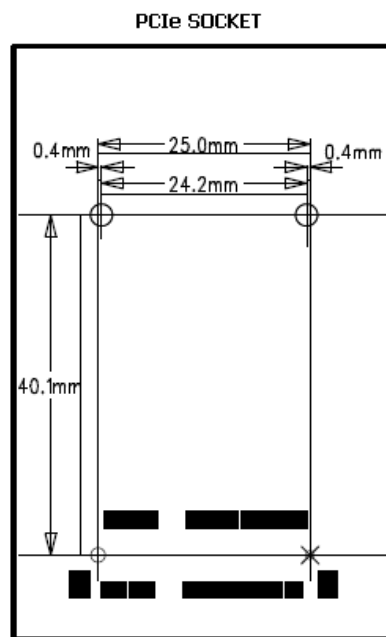
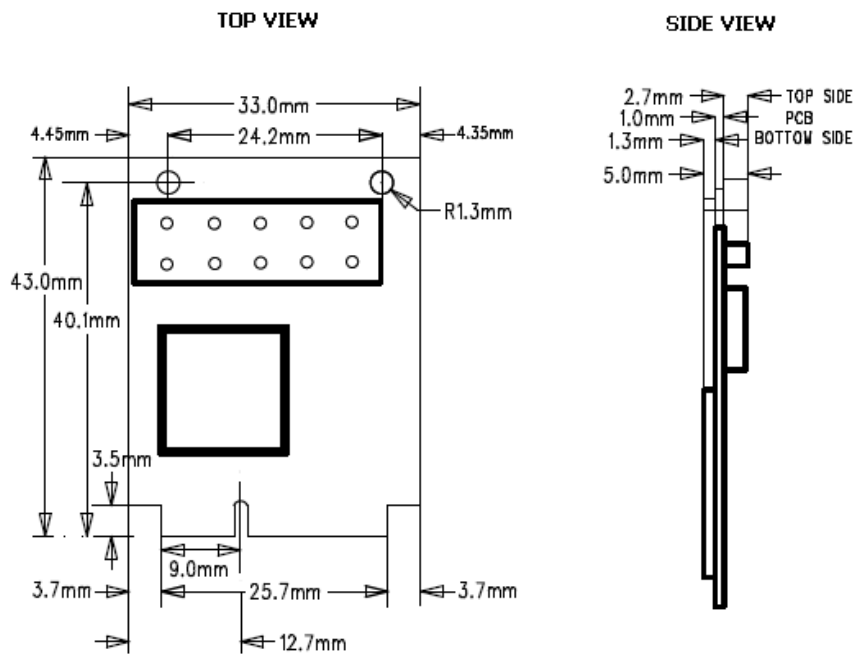
No	T	Name	Shared	Description
1		GND		
2		3.3V		
3		GND		
4		3.3V		
5	I/O, IPD	CTS_N	GPIO9	UART1 CTS-N
6	I/O, IPD	RTS_N	GPIO7	UART1 RTS-N
7	I/O, IPD	RIN	GPIO14	UART1 RIN
8	I/O, IPD	DTR_N	GPIO11	UART1 DTR-N
9	I/O, IPD	RxD	GPIO10	UART1 RXD
10	I/O, IPD	TxD	GPIO8	UART1 TXD
11	I/O, IPD	DSR_N	GPIO13	UART1 DSR-N
12	I/O, IPD	DCD_N	GPIO12	UART1 DCD-N
13	O	WLAN_LED		Wireless Init On/ Active Data:blinking
14		NC		
15	I/O	VBUS		USB OTG VBUS pin;Connect VBUS pin of the USB
16		NC		
17	I/O	PADP		USB OTG data pin Data+
18	I/O, IPD	UART_RX		UART2 RxD
19	I/O	PADM		USB OTG data pin Data-
20	I/O, IPD	UART_TX		UART2 TxD
21	O	TXOP0		10/100 PHY Port #0 TXP
22	I	RXIM0		10/100 PHY Port #0 RXN
23	O	TXOM0		10/100 PHY Port #0 TXN
24	I	RXIP0		10/100 PHY Port #0 RXP
25	I	RXIM1		10/100 PHY Port #1 RXN
26	O	TXOP1		10/100 PHY Port #1 TXP
27	I	RXIP1		10/100 PHY Port #1 RXP
28	O	TXOM1		10/100 PHY Port #1 TXN
29	I	RXIP2		10/100 PHY Port #2 RXP
30	O	TXOM2		10/100 PHY Port #2 TXN
31	I	RXIM2		10/100 PHY Port #2 RXN
32	O	TXOP2		10/100 PHY Port #2 TXP
33	O	LINK_LED_0		LAN port 0 Link LED
34	O	LINK_LED_2		LAN port 2 Link LED
35	O	LINK_LED_1		LAN port 1 Link LED
36	I/O, IPD	GPIO0		WPS Button Push
37	I, IPU	CPURST_N		
38	I/O, IPD	EJT_TDO		Reset Button Push(GPIO17)



39	I/O, IPD	EJT_TRSTN	GPIO21	UART2 Tx/Rx LED
40	I/O, IPD	EJT_TMS		Serial Command Mode #1(GPIO19)
41	I/O, IPD	EJT_TDI	GPIO18	UART1 Tx/Rx LED
42	I/O, IPD	EJT_TCK		WPS LED(GPIO20)
43		NC		
44		NC		
45		NC		
46		NC		
47	I/O, IPD	I2C_SCLK		Serial Command Mode #2(GPIO2)
48	I/O, IPD	I2C_SD		RUN LED(GPIO1)
49		GND		
50		3.3V		
51		GND		
52		3.3V		

Table 1. WizFi630 Pin Map

### 3.2. Dimensions



## 4. Important Notice

WIZnet reserves the right to make corrections, modifications, enhancements, improvements and other changes to its products and services at any time, and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders, and should verify that such information is current and complete. All products are sold subject to WIZnet's terms and conditions of sale, supplied at the time of order acknowledgment. Information relating to device applications, and the like, is intended as suggestion only and may be superseded by updates. It is the customer's responsibility to ensure that their application meets their own specifications. WIZnet makes no representation and gives no warranty relating to advice, support or customer product design.

WIZnet assumes no responsibilities or liabilities for the use of any of its products, conveys no license or title under any patent, copyright or mask work rights to these products, and makes no representations or warranties that these products are free from patent, copyright or mask work infringement, unless otherwise specified.

WIZnet products are not intended for use in life support systems/appliances or any systems where product malfunction can reasonably be expected to result in personal injury, death, severe property damage or environmental damage. WIZnet customers using or selling WIZnet products for use in such applications do so at their own risk and agree to fully indemnify WIZnet for any damages resulting from such use.

All trademarks are the property of their respective owners.

### FCC Certification Requirements

**Caution:** Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

**NOTE:** The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

**NOTE:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**WARNING:** This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

This device complies with Part 15 of the FCC rules. Operation is subject to following two conditions: 1. this device may not cause harmful interference and 2. This device must accept any interference received including interference that may cause undesired Operation of this device.

The changes or modifications not expressly approved by the party responsible for Compliance could void the user's authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter, except if installed in compliance with FCC Multi Transmitter procedures.

To inherit the modular approval, the antennas for this transmitter must be installed to provide a separation distance of 20cm from all persons and must not be co-located or operating in Conjunction with any other antenna or transmitter.

**Note:** This equipment has been tested and found to comply with the limits for a Class B digital device, Pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable Protection against harmful interference in a residential installation. This equipment generates Uses and can radiate radio frequency energy and, if not installed and used in accordance With the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference, Will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an Outlet on a circuit different from that to which the receiver is connected.

## To OEM Installer

1. FCC ID on the final system must be labeled with "Contains FCC ID: XR2WIZ630WI" and "Contains transmitter Module FCC ID: XR2WIZ630WI "
2. In the user manual, final system integrator must ensure that there is no instruction provided in the user Manual to install or remove the transmitter module.
3. Transmitter module must be installed used in strict accordance with the Manufacturer's instructions as described in the user documentation that comes with the product. The user manual of the final host system must contain the following statements: This device complies with Part 15 of the FCC rules. Operation is subject to following

Two conditions: 1. this device may not cause harmful interference and 2. This device Must accept any interference received including interference that may cause undesired operation of this device.

The changes or modifications not expressly approved by the party responsible for

Compliance could void the user's authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter, except if installed In compliance with FCC Multi Transmitter procedures.

To inherit the modular approval, the antennas for this transmitter must be installed to provide a Separation distance of at least 20cm from all persons and must not be co-located or operating in Conjunction with any other antenna or transmitter.

### **Note:**

The buyer of the module who will incorporate this module into his host must submit the final product to the Manufacturer of the module and the MANUFACTURER OF THE MODULE WILL VERIFY that the product is incorporated in host equipment in a way that is represented by the testing as shown in the test report.

### **Note:**

The module is used AP, Gateway, Household. (except PC.)

## **FCC RF Radiation Exposure Statement**

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

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

## **Manual Information to the End User**

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module. The end user manual shall include all required regulatory information/warning as show in this manual.