WIZ630wi User Manual

(Version 0.93)

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 WIZ630wi is in compliance with the essential requirements 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.

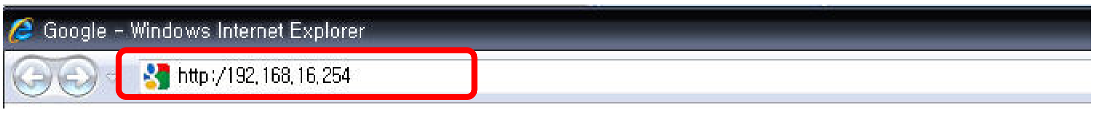
WARNING: This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change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

Connecting the Web page of WIZ610wi

- ◆ Some items may be not supported depending on the version.

Web address

- ◆ Open a web browser on user's PC. Input the default IP address of WIZ630wi, "192.168.16.254" and click Enter.

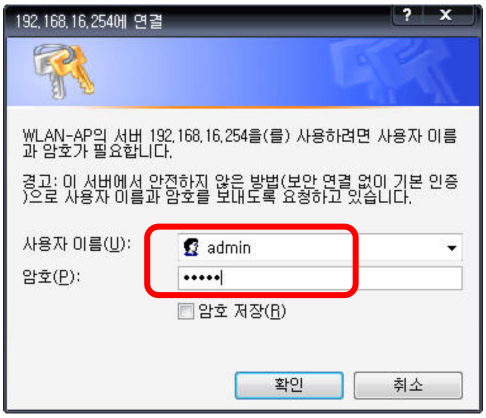


Google - Windows Internet Explorer

http://192.168.16.254

Web Login

- ◆ A pop up will request user to input User ID and Password
- ◆ User ID: admin / Password: admin



192.168.16.254에 연결

WLAN-AP의 서버 192.168.16.254을(를) 사용하려면 사용자 이름과 암호가 필요합니다.

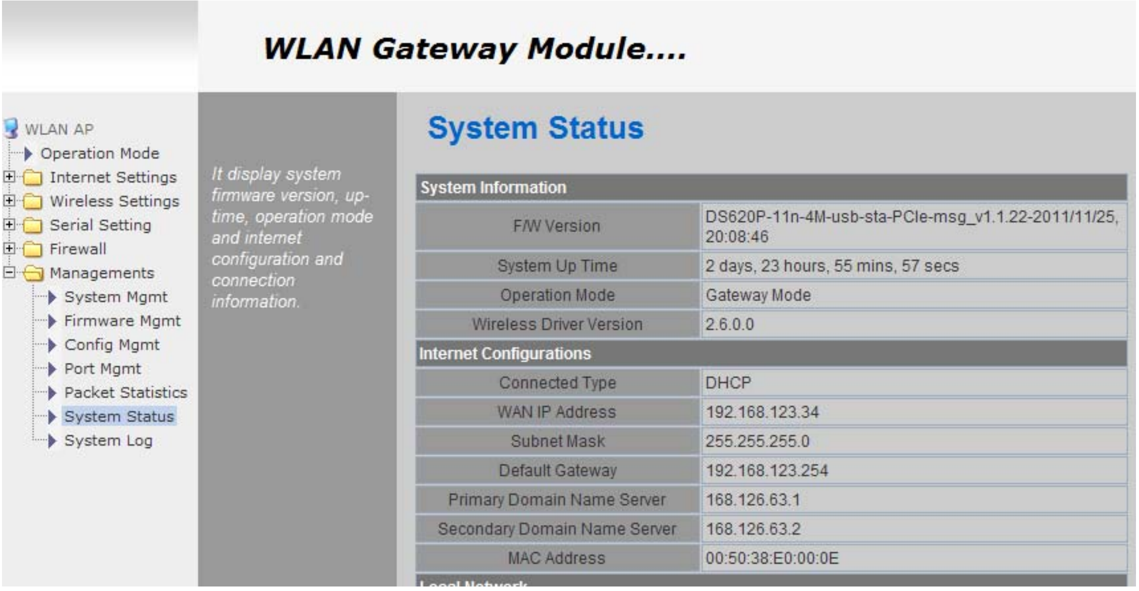
경고: 이 서버에서 안전하지 않은 방법(보안 연결 없이 기본 인증)으로 사용자 이름과 암호를 보내도록 요청하고 있습니다.

사용자 이름(U): admin

암호(P): •••••

□ 암호 저장(R)

- ◆ The system's basic information, as shown below, will appear if successfully authenticated.



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

System Status

System Information	
F/W Version	DS620P-11n-4M-usb-sta-PCIe-msg_v1.1.22-2011/11/25, 20:08:46
System Up Time	2 days, 23 hours, 55 mins, 57 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

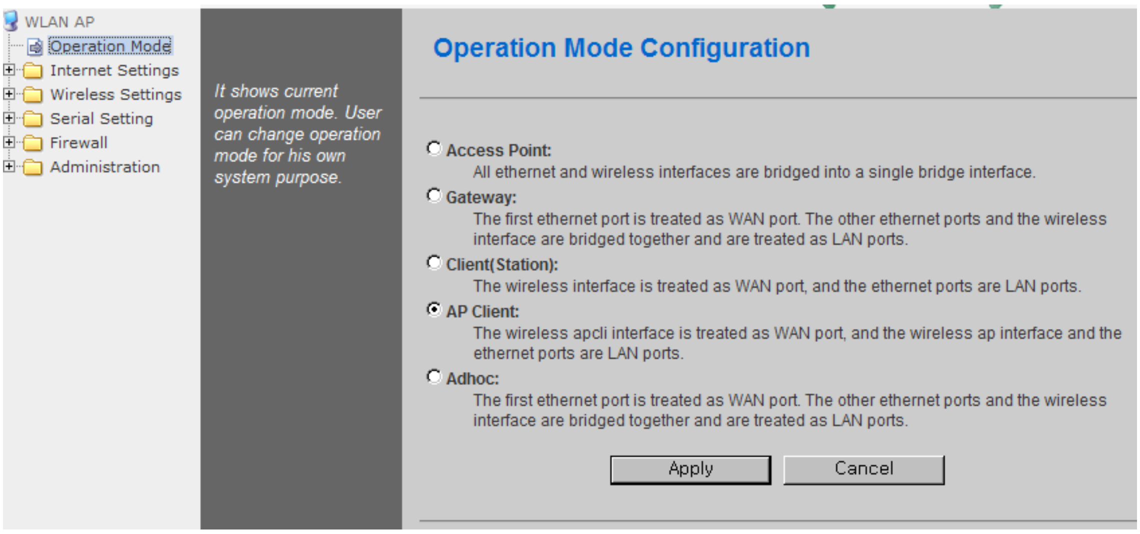
Type	Description
F/W Version	The firmware version of WIZ630wi is displayed.
System Up Time	System up time displayed.
Operation Mode	System operation mode displayed.
Internet Configuration	Information of the external network is displayed.
Local Network	Information of the Local network is displayed.
Ethernet Port Status	Link of LAN Port status is displayed.

Wireless Specifications

Type	Description
Wireless Standard	IEEE802.11b/g/n
Frequency Range	USA: 2.400 ~ 2.483GHz Europe: 2.400 ~ 2.483GHz Japan: 2.400 ~ 2.497GHz China: 2.400 ~ 2.483GHz
Operating Channels	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)
Output Power (Tolerance(+/-1dBm)	802.11b: 9.88dBm@11Mbps 802.11g: 7.44dBm@54Mbps 802.11n(20MHz): 8.08dBm@72Mbps 802.11n(40MHz): 4.83dBm@150Mbps
Receive Sensitivity	802.11b: -89dBm@11Mbps 802.11g: -74dBm@54Mbps 802.11n(20MHz): -70dBm@72Mbps 802.11n(40MHz): -66dBm@150Mbps
Data Rates	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
Modulation Type	11g: OFDM(64QAM, 16QAM, QPSK, BPSK) 11b: DSS(CCK, DQPSK, DBPSK)
Operation Distance	802.11b Outdoor: 150m@11Mbps, 300m@1Mbps Indoor: 30m@11Mbps, 100m@1Mbps 802.11g Outdoor: 50m@54Mbps, 300m@6Mbps Indoor: 30m@54Mbps, 100m@6Mbps 802.11n Outdoor: 30m@150Mbps, 250m@7Mbps Indoor: 20m@150mbps, 100m@7Mbps
Dimension	33mm X 43mm X 4.5mm

1. Operation mode

- ◆ User can select the operation mode.
- ◆ The default setting of WIZ630wi is AP Mode. (DHCP Server Enabled)



It shows current operation mode. User can change operation mode for his own system purpose.

Operation Mode Configuration

○ **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.

Access Point (Bridge)

In this mode, all Ethernet ports and wireless interface are bridged together. Wired/Wireless interface has the same IP address space with its top mesh. DHCP Server function is disabled and WIZ630wi does not assign an IP. Wireless (LAN Port included) sending periodic Broadcast Packet to Station and maintains a connection with Station.

Gateway (Router)

Operate in router mode. Interfaces are separated into WAN I/F (Top Internet Business Network), LAN I/F (Sub Private Network: 192.168.16.xxx), Wireless I/F (Sub Private Network: 192.168.16.xxx). Port # 0 will be assigned to the WAN Port. WIZ630wi periodically sends Broadcast Packet to Sub-LAN (LAN Port included) and maintains connection with Station.

Client (Station)

Wireless I/F is assigned as WAN Port and all Ethernet Ports are bound to LAN Port. Set the profile and the WIZ630wi 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. WIZ630wi periodically sends PING Packet to AP Gateway and maintains connection with AP.

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. WIZ630wi periodically sends Broadcast Packet to Sub-LAN (LAN Port included) and maintains connection with Station.

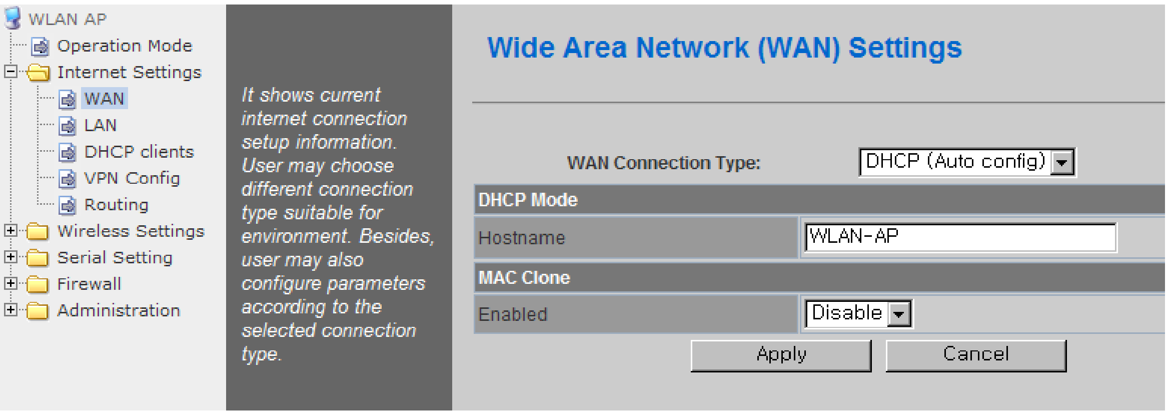
ad-hoc mode

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. Internet Setting

3.1 Internet connection setting

- Select the internet service type and WIZ630wi can connect to the internet
- If users would like to access to Internet, Gateway Mode should be selected.



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)

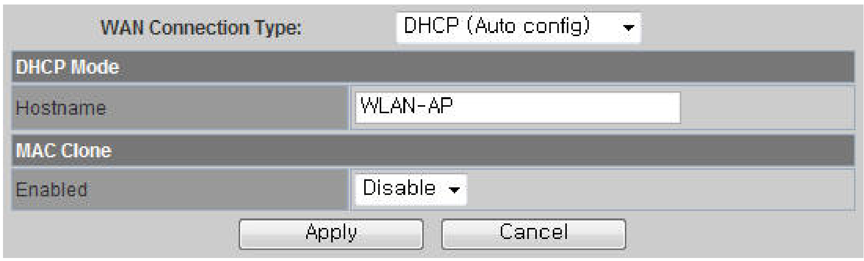
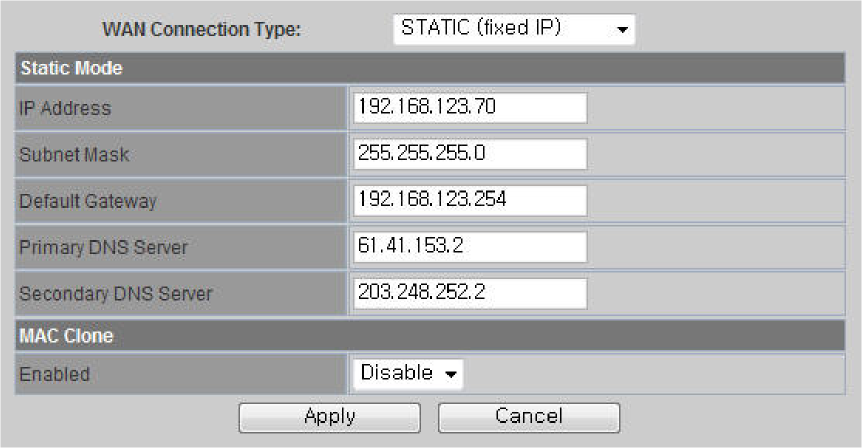
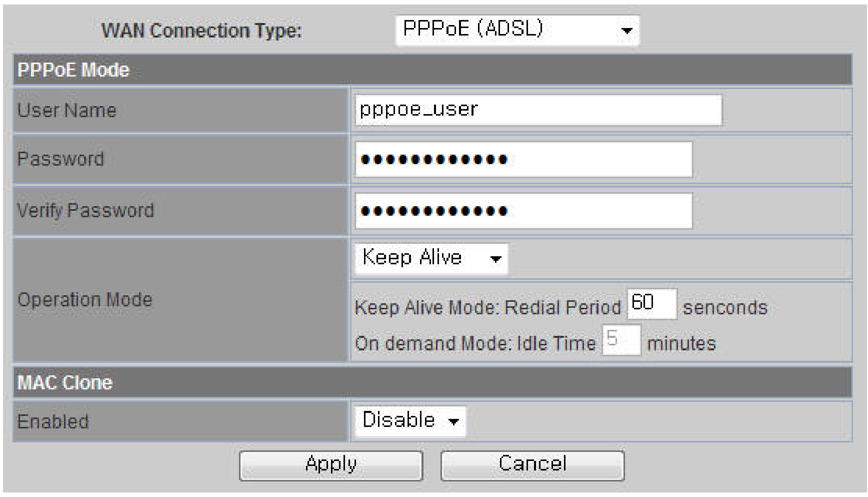
DHCP Mode

Hostname: WLAN-AP

MAC Clone

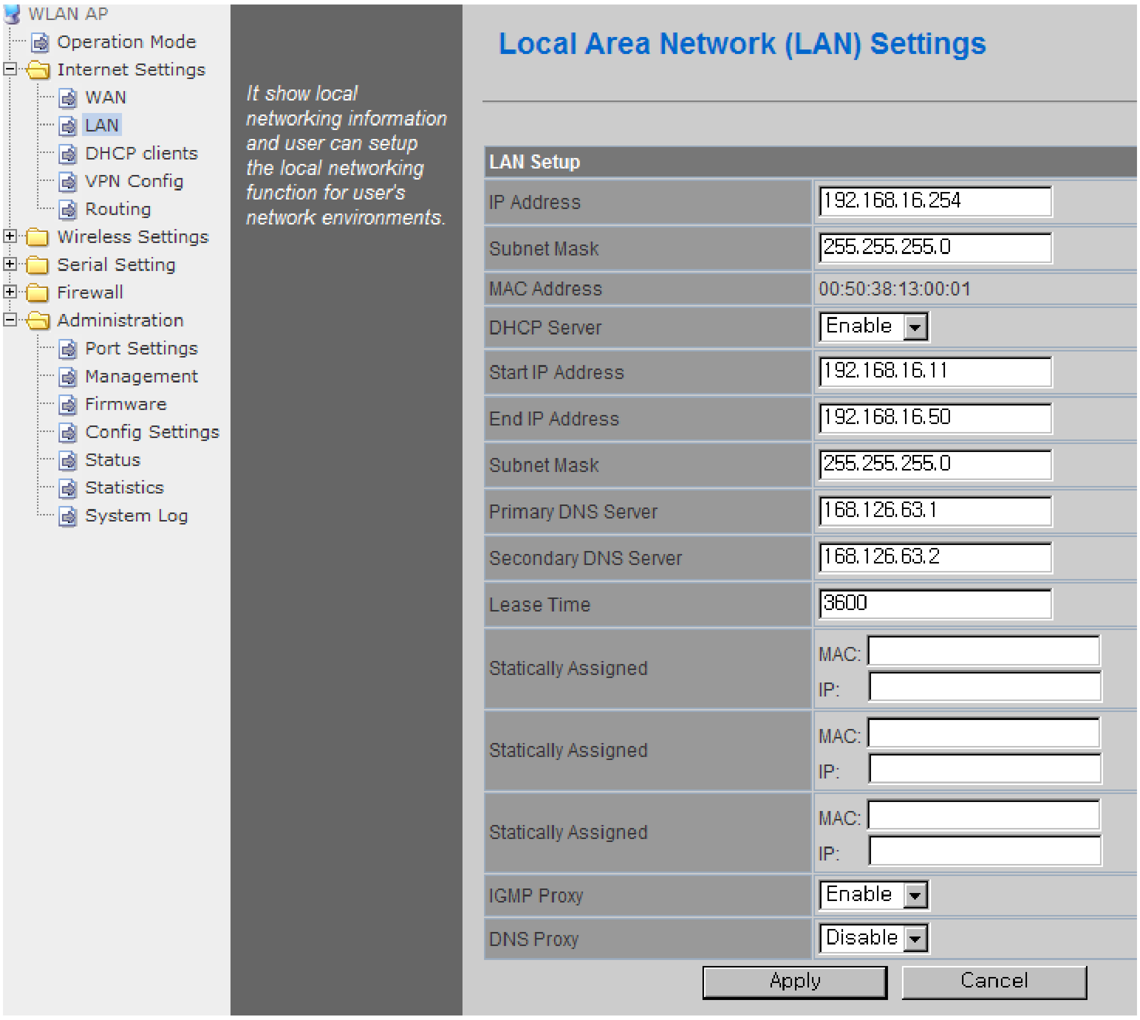
Enabled: Disable

Type	Description
WAN Connection Type	Select the communication ways for Internet's connection - Static(Fixed IP) - DHCP (Auto config) - PPPoE
Host Name	Settings about module's host name
Mac Clone	Some ISPs require that you register a MAC address. Users can directly enter MAC address or use the MAC Clone function.

Type	Description
DHCP(Auto config)	User should choose DHCP Mode when the user connects to the internet service such as FTTH, cable modems, VDSL, IP-ADSL.  WAN Connection Type: DHCP (Auto config) DHCP Mode Hostname: WLAN-AP MAC Clone Enabled: Disable
Static(Fixed IP)	Static IP setting window. If user receives static IP from ISP, user should set the Fixed IP .  WAN Connection Type: STATIC (fixed IP) Static Mode 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 MAC Clone Enabled: Disable Input the network information that got from ISP (such as IP, Subnet, Gateway, DNS)
PPPoE(ADSL)	 WAN Connection Type: PPPoE (ADSL) PPPoE Mode User Name: pppoe_user Password: ●●●●●●●●●●●● Verify Password: ●●●●●●●●●●●● Operation Mode: Keep Alive Keep Alive Mode: Redial Period 60 senconds On demand Mode: Idle Time 5 minutes MAC Clone Enabled: Disable -. User Name: Setting the User Name received from ISP -. Password: Password assigned by the internet service company -. Operation Mode: This mode is used for re-connecting when connection is bad.

3.2 Local network setting

◆ WIZ630wi internal IP setting, DHCP server setting and DHCP.



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

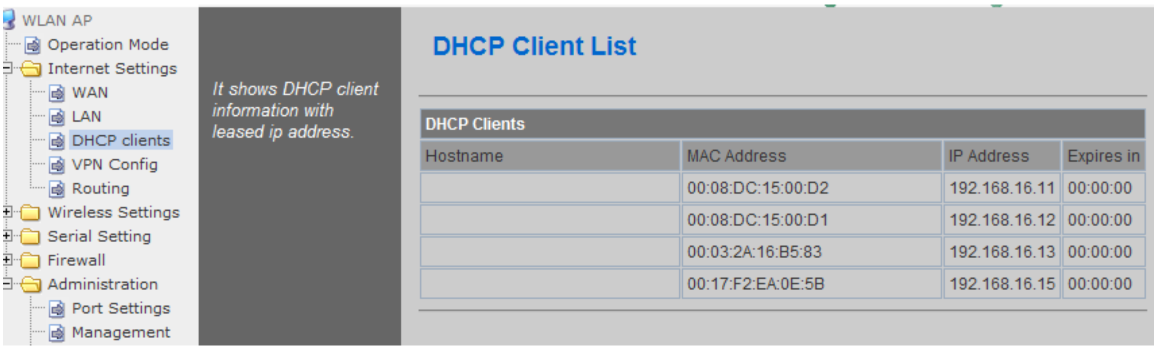
Local Area Network (LAN) Settings

LAN Setup	
IP Address	192.168.16.254
Subnet Mask	255.255.255.0
MAC Address	00:50:38:13:00:01
DHCP Server	Enable
Start IP Address	192.168.16.11
End IP Address	192.168.16.50
Subnet Mask	255.255.255.0
Primary DNS Server	168.126.63.1
Secondary DNS Server	168.126.63.2
Lease Time	3600
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
IGMP Proxy	Enable
DNS Proxy	Disable

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

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.

DHCP Client List

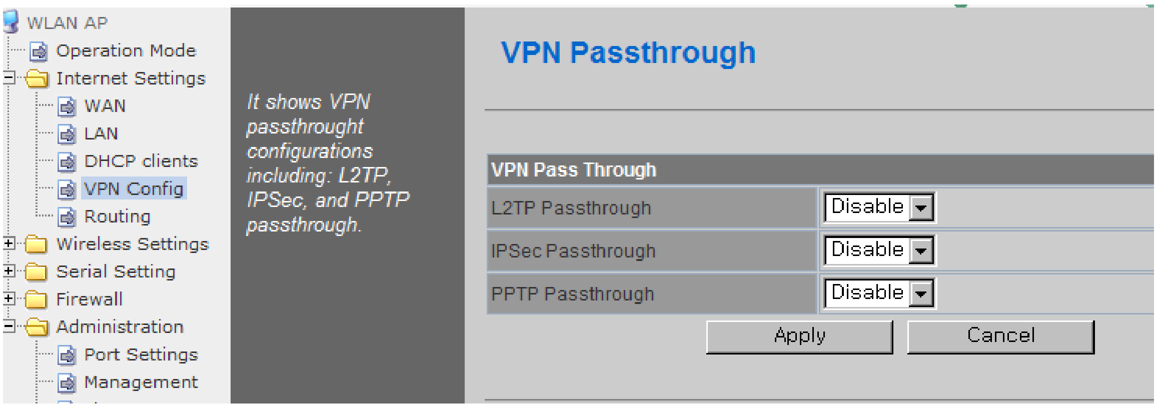
DHCP Clients

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
Host name	Client's host name is shown
Mac Address	Client's MAC address is shown.
IP Address	Client's IP address is shown.
Expires in	The usable time of client's IP address is shown.

3.4 VPN setting

◆ This section will explain on VPN packet settings.



It shows VPN passthrought configurations including: L2TP, IPSec, and PPTP passthrough.

VPN Passthrough

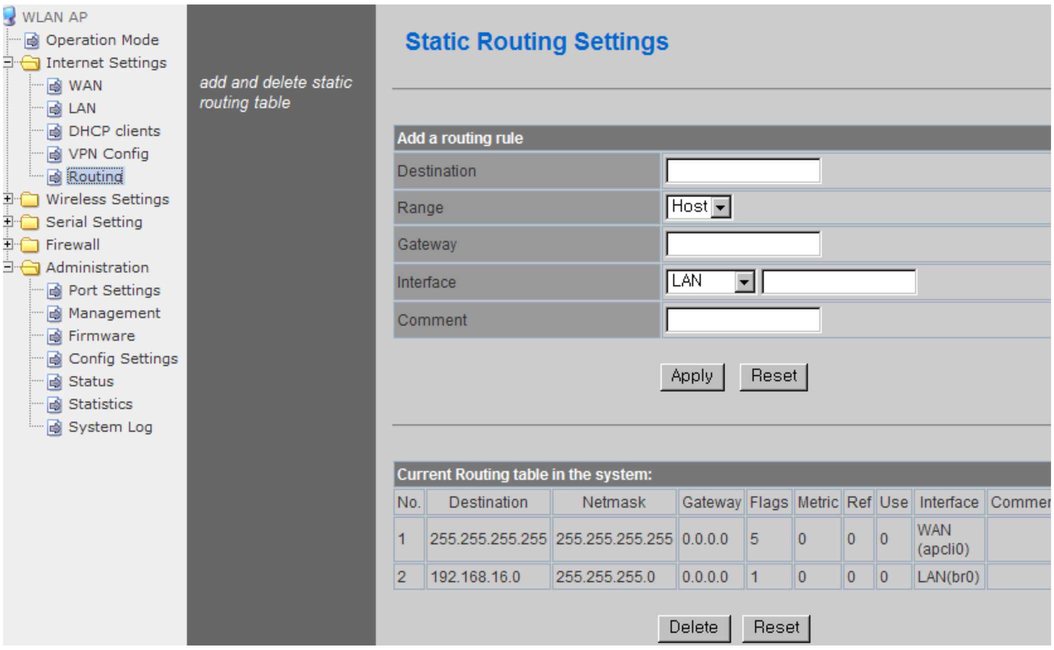
VPN Pass Through

L2TP Passthrough	Disable
IPSec Passthrough	Disable
PPTP Passthrough	Disable

Type	Description
L2TP Pass-through	Enable : VPN L2TP packet is passed through WAN. Disable : VPN L2TP packet is not passed through WAN. (Default value)
IPSec Pass-through	Enable : VPN IPSec packet is passed though WAN. Disable : VPN IPSec packet is not passed through WAN. (Default value)
PPTP Pass-through	Enable : VPN PPTP packet is passed through WAN. Disable : VPN PPTP packet is not passed through WAN. (Default value)

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	Host
Gateway	
Interface	LAN
Comment	

Current Routing table in the system:

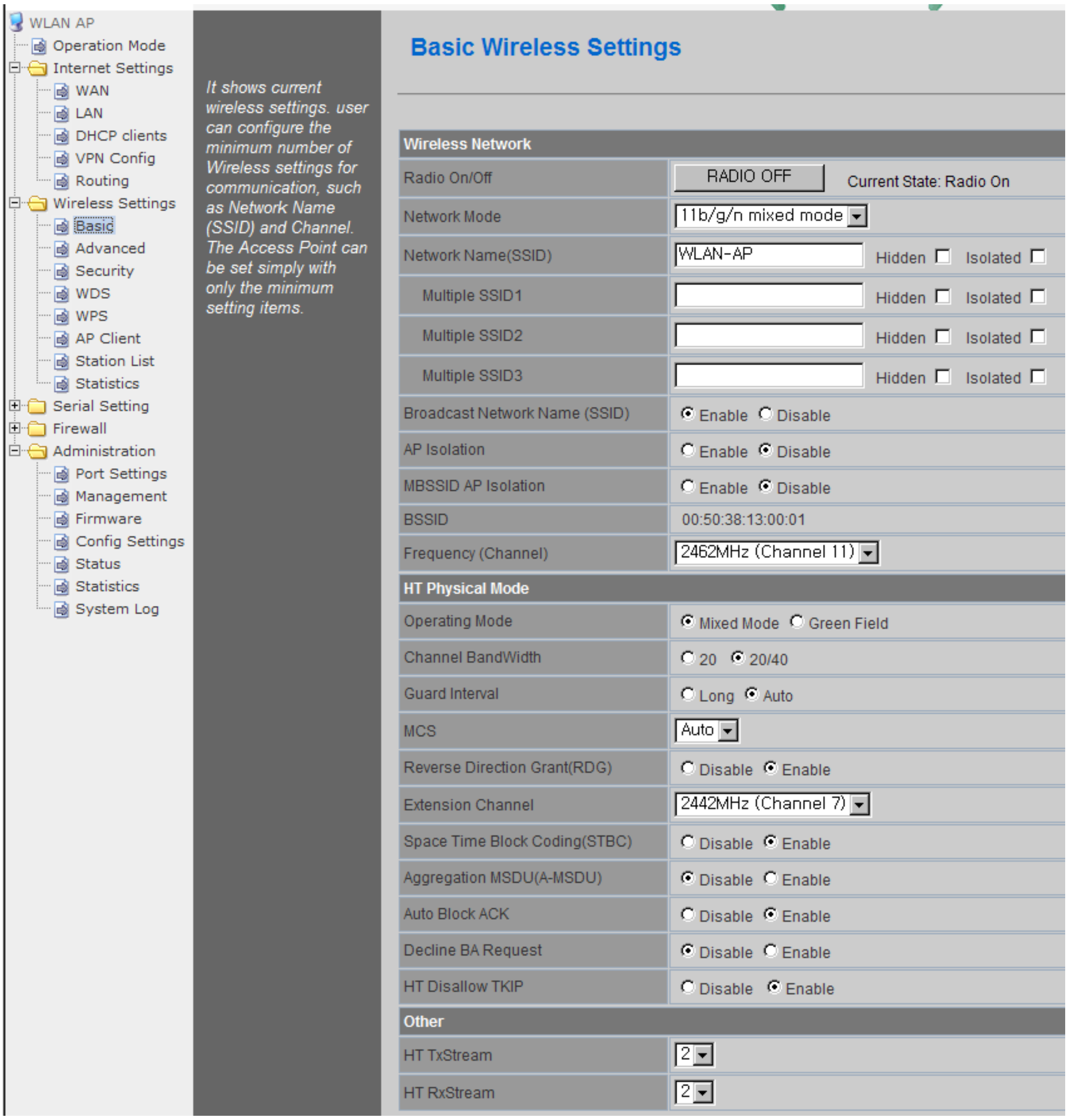
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Commer
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	WAN (apcli0)	
2	192.168.16.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	

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

3. Wireless setting

Basic settings

◆ This chapter is about basic setting for wireless LAN.



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

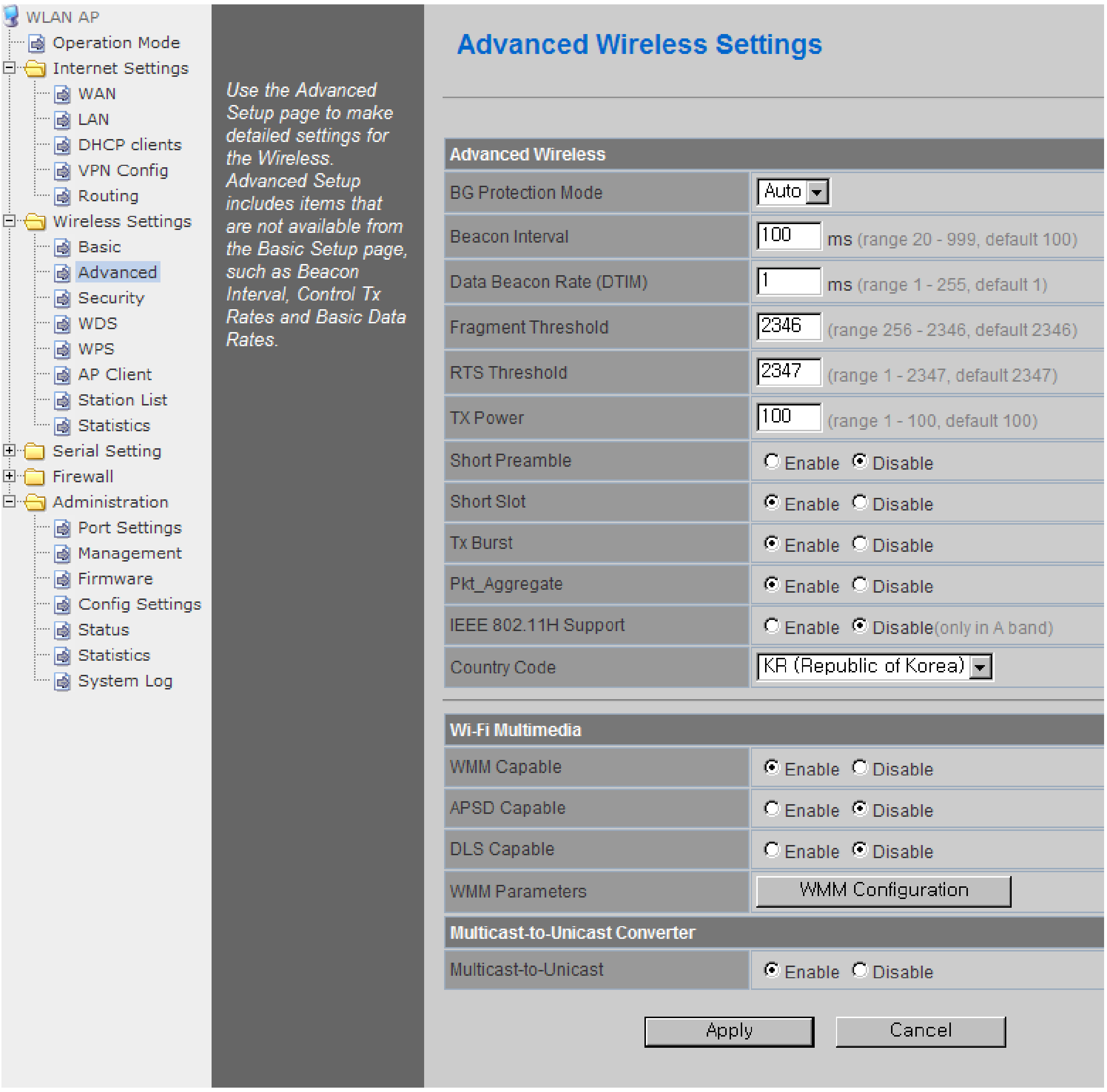
Wireless Network	
Radio On/Off	RADIO OFF Current State: Radio On
Network Mode	11b/g/n mixed mode
Network Name(SSID)	WLAN-AP Hidden ☐ Isolated ☐
Multiple SSID1	Hidden ☐ Isolated ☐
Multiple SSID2	Hidden ☐ Isolated ☐
Multiple SSID3	Hidden ☐ Isolated ☐
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:50:38:13:00:01
Frequency (Channel)	2462MHz (Channel 11)
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2442MHz (Channel 7)
Space Time Block Coding(STBC)	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
Other	
HT TxStream	2
HT RxStream	2

Type	Description
Radio On/Off	Decide radio on/off of wireless AP function.
Network Mode	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
SSID	Enter the name of the wireless network.
Channel	Select the channel that composes the wireless network.
Broadcast Network Name	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.
AP Isolation	The communication between stations that are connected to the identical SSID is blocked.
MBSSID AP Isolation	The communication between stations that are connected to different SSID is blocked.

Type	Description
Operation Mode	Decide whether the PHY mode is going to be Mixed Mode or Green Field Mode.
Channel Bandwidth	Fix bandwidth channel to 20MHz. . Use 40MHz as bandwidth in case connection with wireless station that supports 11n channel bonding.
Guard Interval	Long: 800nsec, Short: 400nsec
MCS	Control link rate. Set link rate to auto considering any interruptions.
RDG	The wireless performance can be improved using Reverse Direct Grant, 11n's RDG technology.
Extension Channel	Setting for the other 20MHz area when channel bandwidth is set to 40MHz.
STBC	STBC is supported when the value of MCS is 0-7.
A-MSDU	Decide whether numerous MSDUs inside one MPDU will transmit.
Auto Block ACK	Decide whether Block ACK will be transmitted automatically.
Decline BA Request	Decide whether user wants to decline Block ACK request.
HT Disallow TKIP	Decide whether to operate in 802.11g, if using TKIP.
HT TxStream	Setting for number of Tx antennas of 2T2R system.
HT RxStream	Setting for number of Rx antennas of 2T2R system.

4.1 Advanced Wireless Settings

◆ This chapter is about higher-level setting for wireless LAN



Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless Settings

Advanced Wireless	
BG Protection Mode	Auto ▾
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable(only in A band)
Country Code	KR (Republic of Korea) ▾

Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
DLS Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration

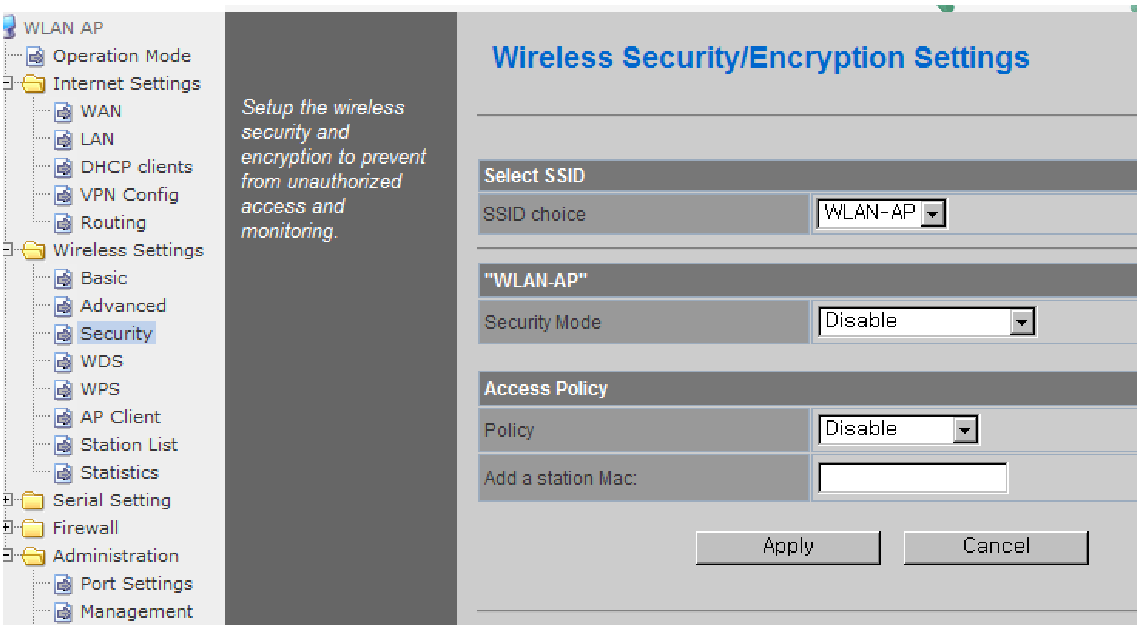
Multicast-to-Unicast Converter	
Multicast-to-Unicast	● Enable ○ Disable

Type	Description
BG Protection	Setting for wireless communication when using both 11b and 11g LAN cards. Recommended for automatic settings in general.
Beacon Interval	Controls the interval of sending beacon. The setting range is 20~999 and 100ms is usually used
DTIM	Controls the data rate of beacon being sent. The setting range is 1~255 and 1ms is usually used.
Fragmentation Threshold	When a data that is larger than the threshold size, it is fragmented and sent. Smaller 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.

RTS Threshold	When a data that 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.
Tx Power	Controls the range of wireless radio being sent. The range of wireless radio being sent gets larger as the value is larger.
Short Preamble	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.
Short Slot	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.
Tx Burst	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.
Pkt_Aggregate	Numerous packets can be transmitted in one MPDU by enabling this function.
Country Code	Setting for country code. Example: KR(Republic of Korea), US(United State), FCC(Europe), JP(Japan), FR(France), ES(Spain)
WMM	Decide to whether or not use WMM function.
APSD	Decide to whether or not use Power Saving Mode.
DLS	Decide whether or not use DLS (Direct Link Setup) function.
WMM Parameter	If WMM is enabled, set the value for WMM Parameter.
Multicast-to-Unicast	Decide whether or not use Multicast function.

4.2 Wireless Security

◆ This chapter is about settings for wireless network security.



Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Wireless Security/Encryption Settings

Select SSID

SSID choice: WLAN-AP

"WLAN-AP"

Security Mode: Disable

Access Policy

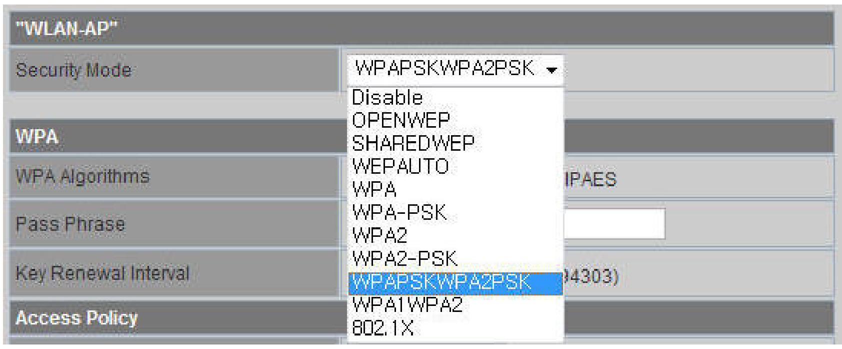
Policy: Disable

Add a station Mac:

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

4.3.1. Wireless Security setting

◆ Authentication settings



"WLAN-AP"

Security Mode: WPAPSKWPA2PSK

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

4.3.2. Wireless Authentication Setting

Encryption	Type	Description
WEP64	SHARED/ WEPAUTO/802.1x	WEP encryption algorithm is used with 64bit key.
WEP128		WEP encryption algorithm is used with 128 bit key.
TKIP	WPA/WPA2/ WPA-PSK/ WPA2-PSK/ WPA1WPA2/ WPAPSKWPA2PSK	More complex encryption algorithm than WEP Is used.
AES		New encryption algorithm is used.
TKIP/AES		Support TKIP/AES simultaneously

5.3.2.1. WEP

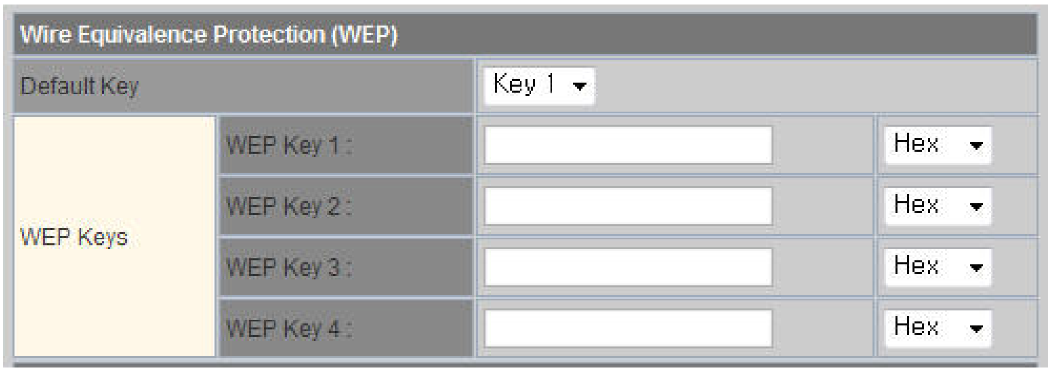
◆ Enter key for WEP64 or WEP128 network.

◆ Use either character string or hex character when entering key.

◆ Select 1~4 for 'Default Key..

◆ Enter at least one WEP Key.

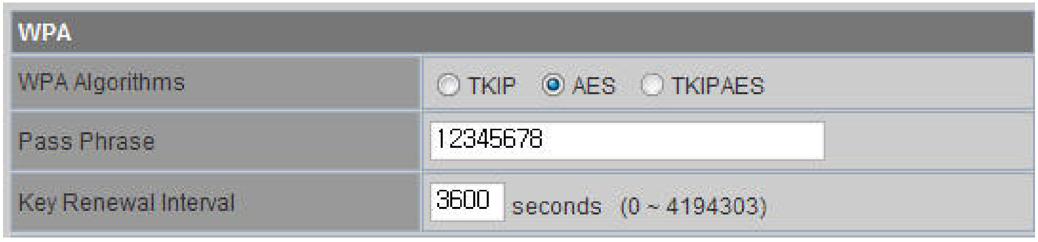
◆ The entered WEP key is used for connection from wireless terminal



Wire Equivalence Protection (WEP)			
Default Key		Key 1 ▾	
WEP Keys	WEP Key 1 :		Hex ▾
	WEP Key 2 :		Hex ▾
	WEP Key 3 :		Hex ▾
	WEP Key 4 :		Hex ▾

5.3.2.2. TKIP/AES authentication

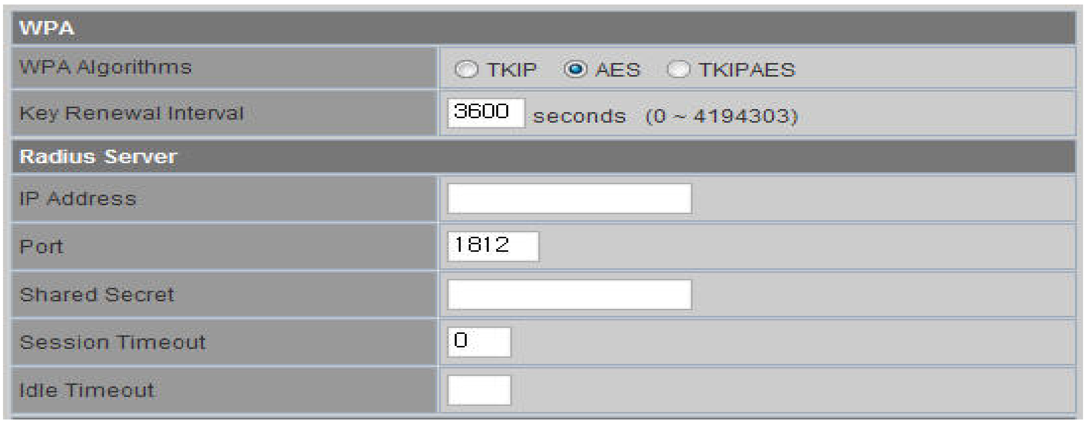
- ◆ Enter at least 8 characters of character string for the network key value.



WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)

5.3.2.3. Wireless 802.1x authentication

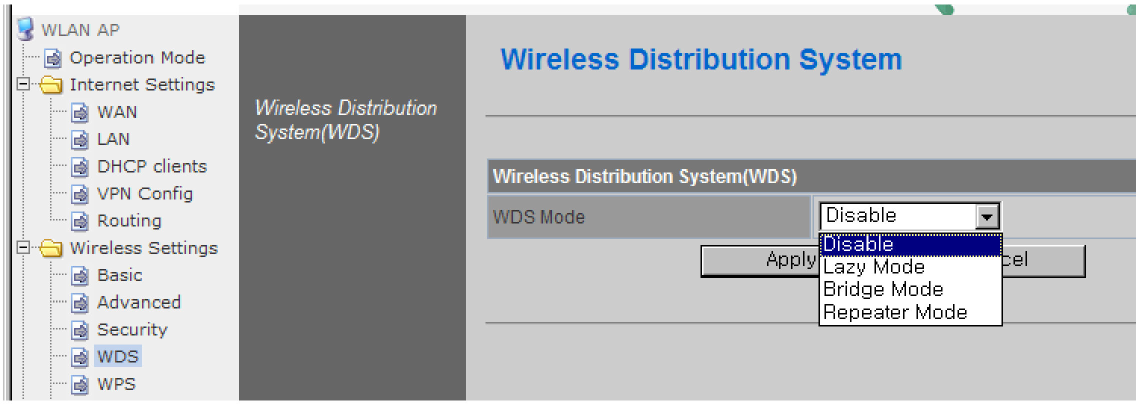
- ◆ Enter the value for linking with the Radius Server.
- ◆ The values related to the Radius Server are provided by the internet service company.



WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Key Renewal Interval	3600 seconds (0 ~ 4194303)
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

4.3 WDS 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.



Wireless Distribution System

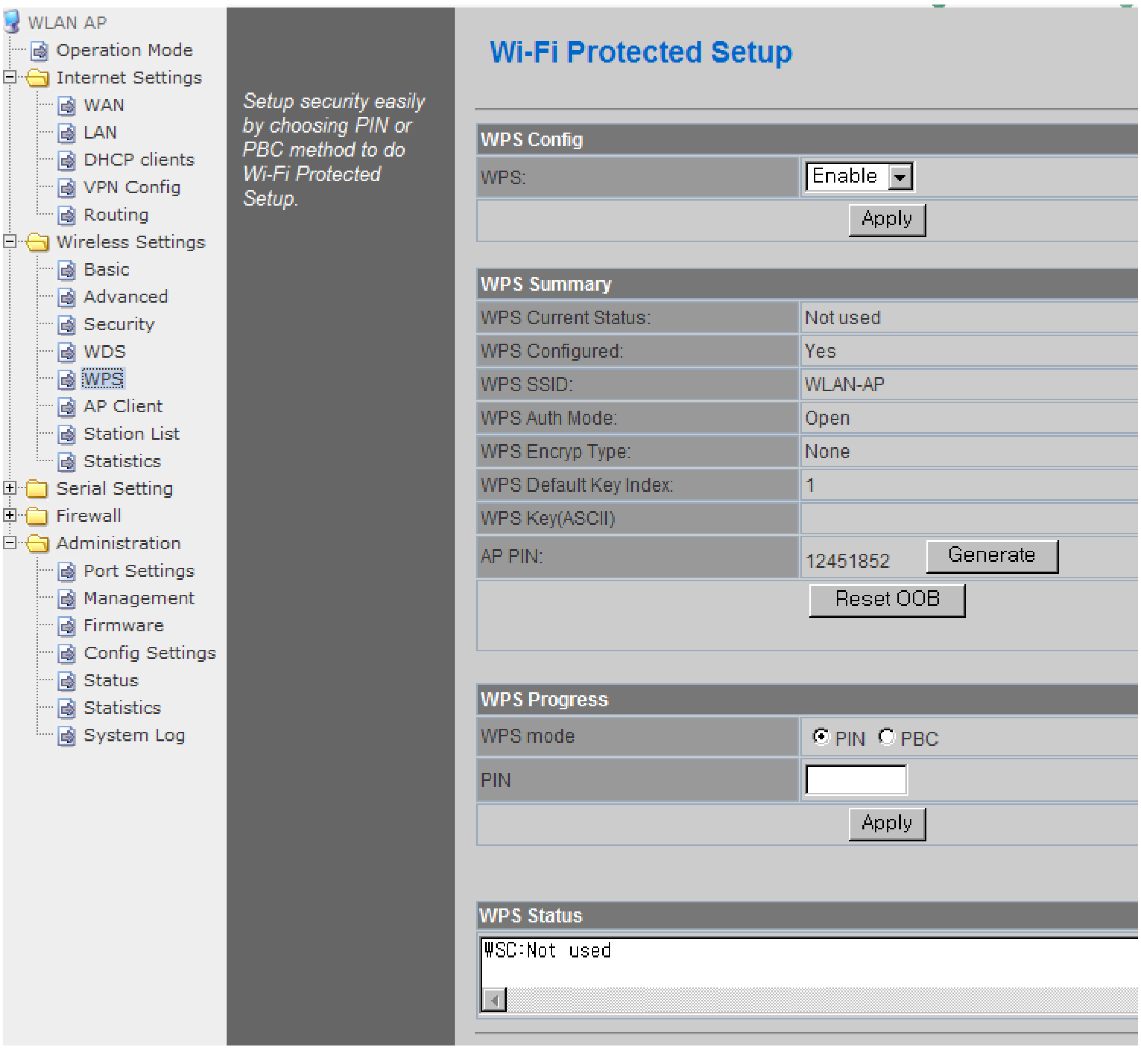
Wireless Distribution System(WDS)

WDS Mode: Disable

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

4.4 WPS Setting

◆ The WDS function enables easier wireless network setting..



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

Wi-Fi Protected Setup

WPS Config

WPS: Enable

WPS Summary

WPS Current Status:	Not used
WPS Configured:	Yes
WPS SSID:	WLAN-AP
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	12451852

WPS Progress

WPS mode ● PIN ○ PBC

PIN

WPS Status

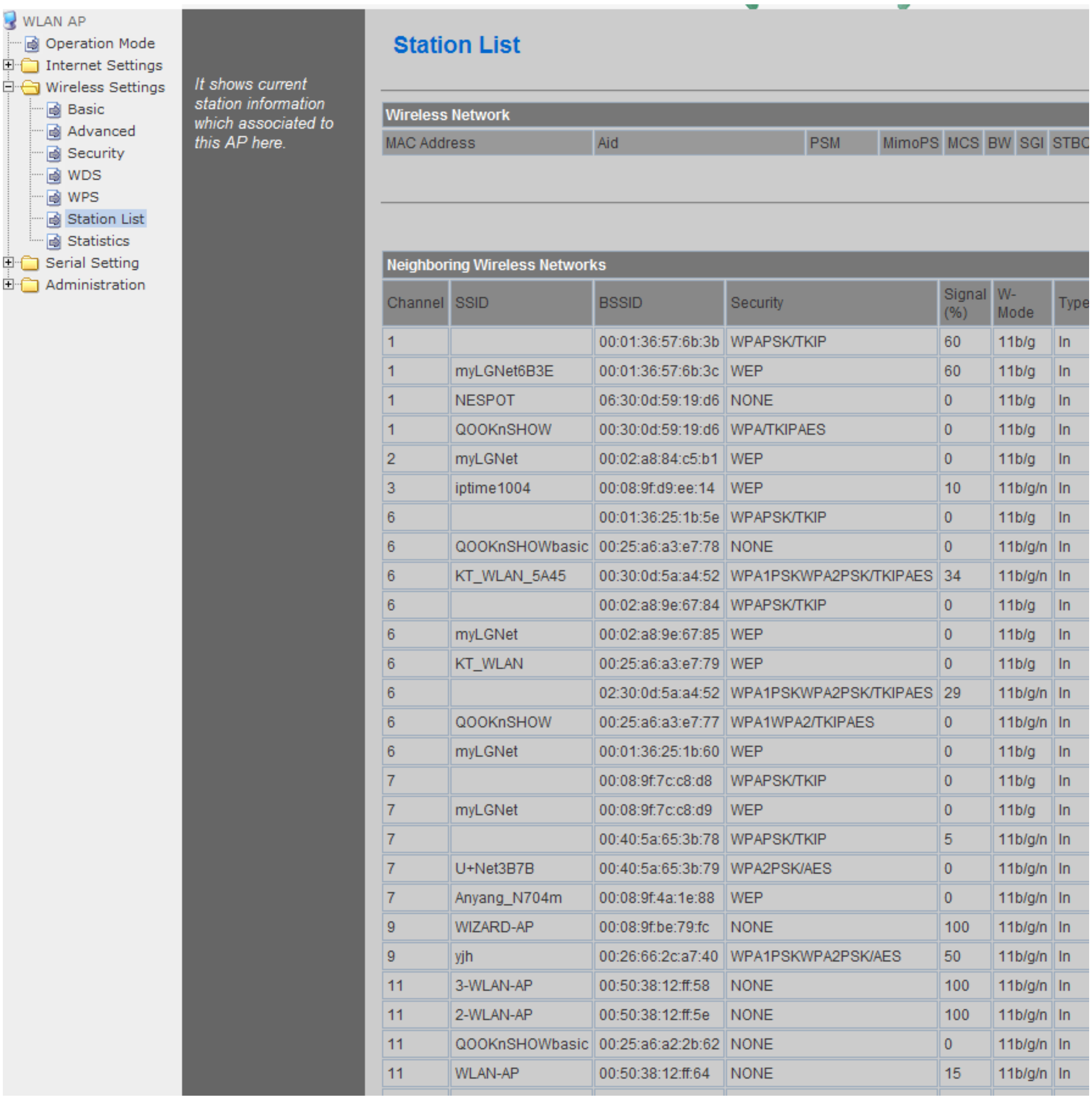
```
WSC:Not used
```

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

4.5 Wireless network status

◆ The status of the station that is connected to WIZ630wi is shown.

◆ The surrounding wireless AP's status are shown..



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

Station List

Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC

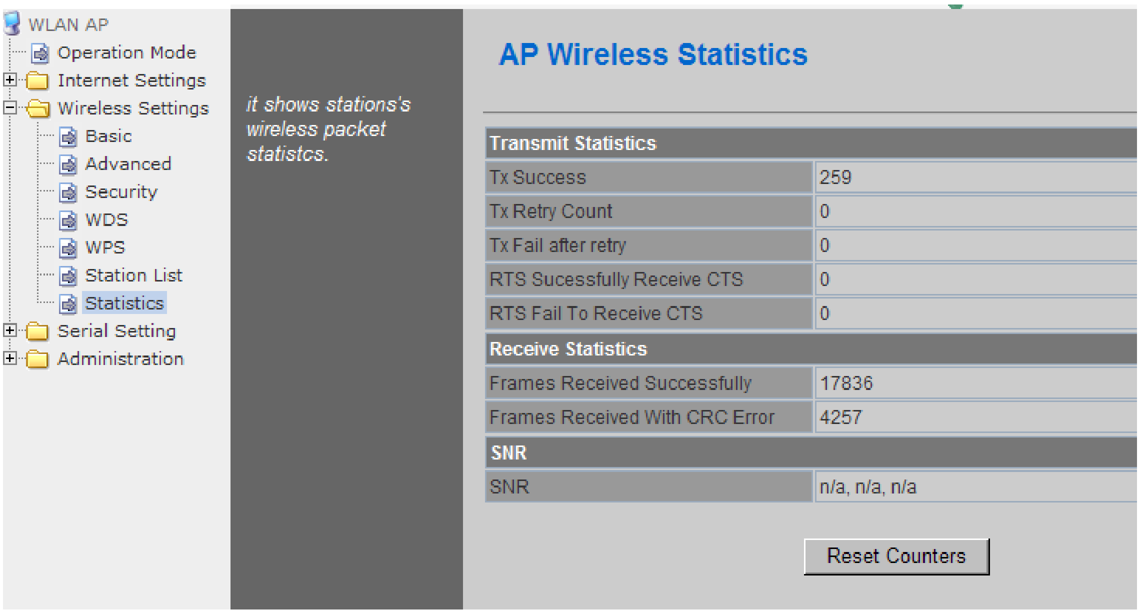
Neighboring Wireless Networks

Channel	SSID	BSSID	Security	Signal (%)	W-Mode	Type
1		00:01:36:57:6b:3b	WPAPSK/TKIP	60	11b/g	In
1	myLGNet6B3E	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	myLGNet	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	myLGNet	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	myLGNet	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	myLGNet	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
Channel	Channel information of AP
SSID	SSID of AP
BSSID	MAC address of AP
Security	Encryption method of AP
Signal	Signal strength with AP
W-Mode	Wireless mode of AP
Type	Network Type of finding AP In: Infrastructure, Ad: ad-hoc

4.6 AP Wireless Statistics

◆ The Statistics of wireless communication is shown.



it shows stations's wireless packet statistcs.

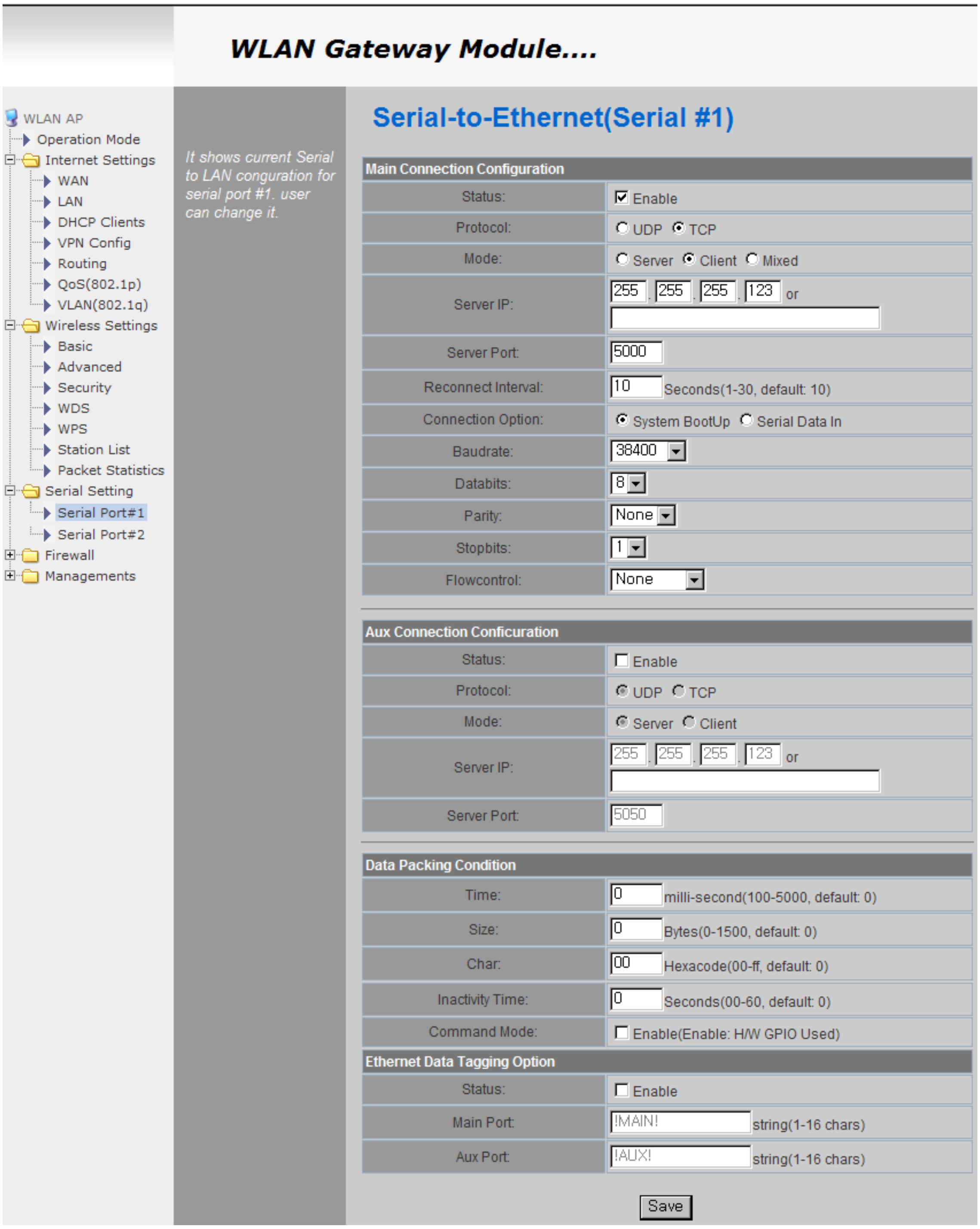
AP Wireless Statistics

Transmit Statistics	
Tx Success	259
Tx Retry Count	0
Tx Fail after retry	0
RTS Sucessfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	17836
Frames Received With CRC Error	4257
SNR	
SNR	n/a, n/a, n/a

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

4. Serial to LAN(Wired and Wireless)

- ◆ Individual settings for serial #1 / 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)



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

Serial-to-Ethernet(Serial #1)

Main Connection Configuration	
Status:	☑ Enable
Protocol:	○ UDP ● TCP
Mode:	○ Server ● Client ○ Mixed
Server IP:	255 . 255 . 255 . 123 or
Server Port:	5000
Reconnect Interval:	10 Seconds(1-30, default: 10)
Connection Option:	● System BootUp ○ Serial Data In
Baudrate:	38400
Databits:	8
Parity:	None
Stopbits:	1
Flowcontrol:	None

Aux Connection Conficuration	
Status:	□ Enable
Protocol:	● UDP ○ TCP
Mode:	● Server ○ Client
Server IP:	255 . 255 . 255 . 123 or
Server Port:	5050

Data Packing Condition	
Time:	0 milli-second(100-5000, default: 0)
Size:	0 Bytes(0-1500, default: 0)
Char:	00 Hexacode(00-ff, default: 0)
Inactivity Time:	0 Seconds(00-60, default: 0)
Command Mode:	□ Enable(Enable: H/W GPIO Used)

Ethernet Data Tagging Option	
Status:	□ Enable
Main Port:	!MAIN! string(1-16 chars)
Aux Port:	!AUX! string(1-16 chars)

5.1 Main Connection settings

Type	Description
Status	Enable checked : Serial to LAN is used. Enable un-check: Serial to LAN is not used.
Protocol	Protocol used in Serial to LAN communication -TCP -UDP
Mode	Serial to LAN operation mode. (Client Mode recommended) - Server : waits for connection. - Client : connected to the remote server of WIZ630wi - Mixed : not recommended
Server IP	Enter the IP address for WIZ630wi setting.
Server Port	Enter the port number for remote serial data server host PC.
Reconnect Interval	Interval of TCP reconnection.
Connection	WIZ630wi의 Serial LAN의 connection Type(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)
Baud rate	Select the serial communication speed.
Databits	Select the databits.
Parity	Select the method for parity check.
Stopbits	Select the stopbits.
FlowControl	Select the method for flow control. (Option: none, Xon/Xoff, RTS/CTS)

5.2 Aux Connection Settings

Type	Description
Status	Select whether to enable serial port or not.
Protocol	Protocol used in Serial to LAN communication.
Mode	Select Server or Client Mode.
Server IP	Enter the IP address for WIZ630wi setting.
Server Port	Enter the port number for remote serial data server host PC.

5.3 Packing Condition (Incoming serial data packing condition)

Type	Description
Time	Data packing until the set time and then sent to server after the set time.
Size	Data packing until the set size and then sent to the server.
Character	Data packing until the set character and then sent to the server.
Inactivity Time:	TCP/IP connection is discontinued if there is neither serial data nor network data during the set time.
H/W CMD switch	-. Enable/Disable the H/W CMD switch pin. -. H/W CMD switch pin is the switch for sending commands from CPU to WIZ630wi.

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
Status	Enable or disable this option (Checked : Enable, Un-Check : Disable)
Main Port	Before sending data from Main port to serial port, WIZ630wi added a TAG in the front of payload. For example: In-come LAN Data : "abcdegf" Output data to Serial Port : "!MAIN!abcdegf"
Aux Port	Before sending data from Aux port to serial port, WIZ630wi added a TAG in the front of payload. For example: In-come LAN Data : "abcdegf" Output data to Serial Port : "!AUX!abcdegf"

5. Firewall settings

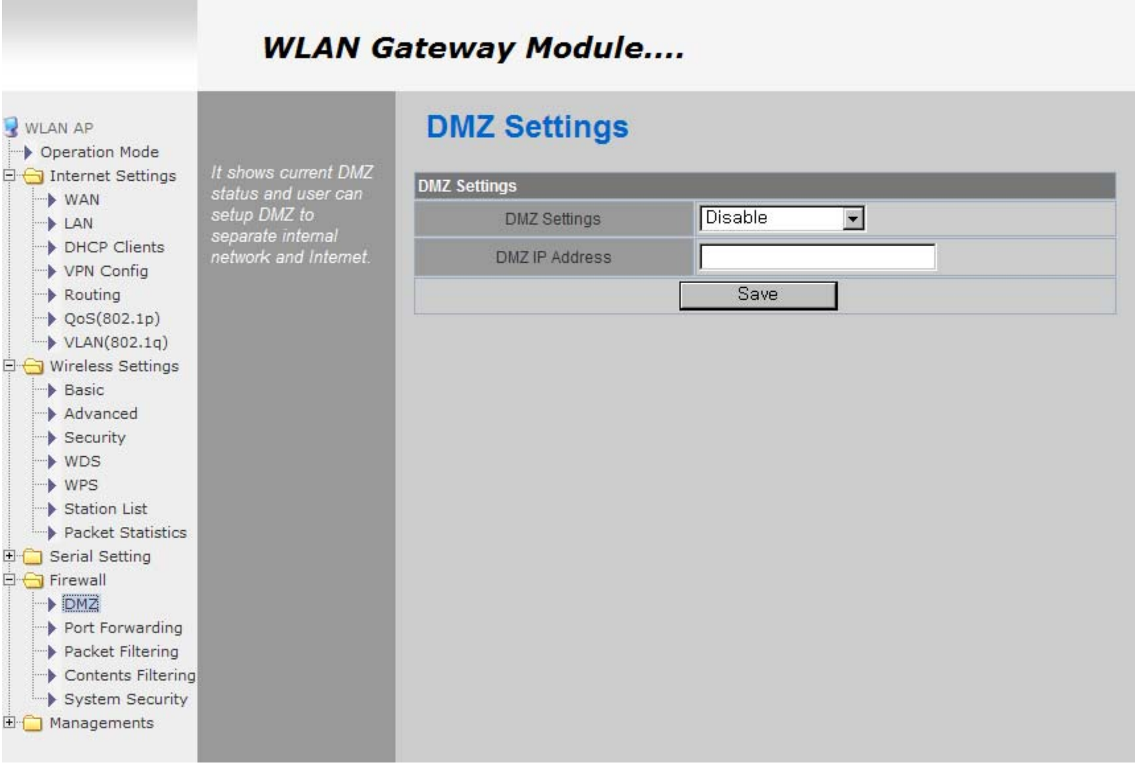
◆ Only work at the Gateway Mode

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 are not supported by your router. In this case, placing your computer in the DMZ is the only way to get the application working.



WLAN Gateway Module....

It shows current DMZ status and user can setup DMZ to separate internal network and Internet.

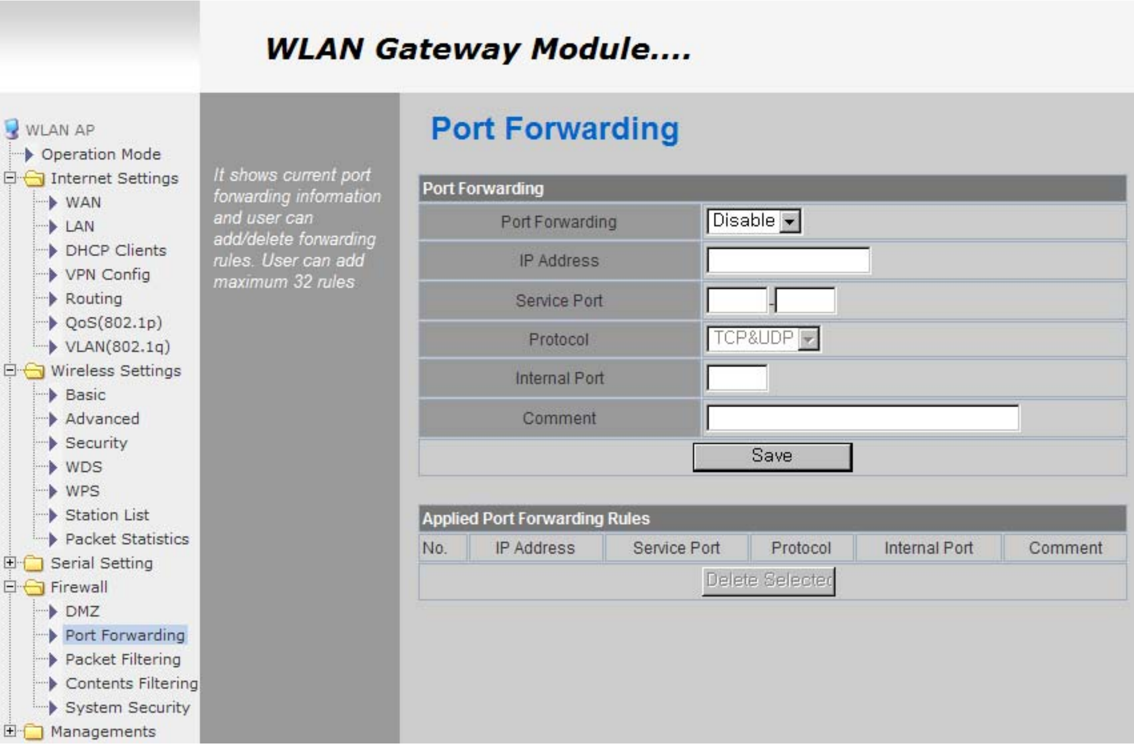
DMZ Settings

DMZ Settings	
DMZ Settings	Disable
DMZ IP Address	

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

6.2 Port forwarding

When a computer on the internet sends data to the external IP address of the router (WIZ630wi), the router (WIZ630wi) needs to know what to do with the data. Port Forwarding simply tells the WIZ630wi 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. So a rule set up for port 53 will only work for port 53.



Port Forwarding

It shows current port forwarding information and user can add/delete forwarding rules. User can add maximum 32 rules

Port Forwarding	
Port Forwarding	Disable
IP Address	
Service Port	-
Protocol	TCP&UDP
Internal Port	
Comment	

Applied Port Forwarding Rules

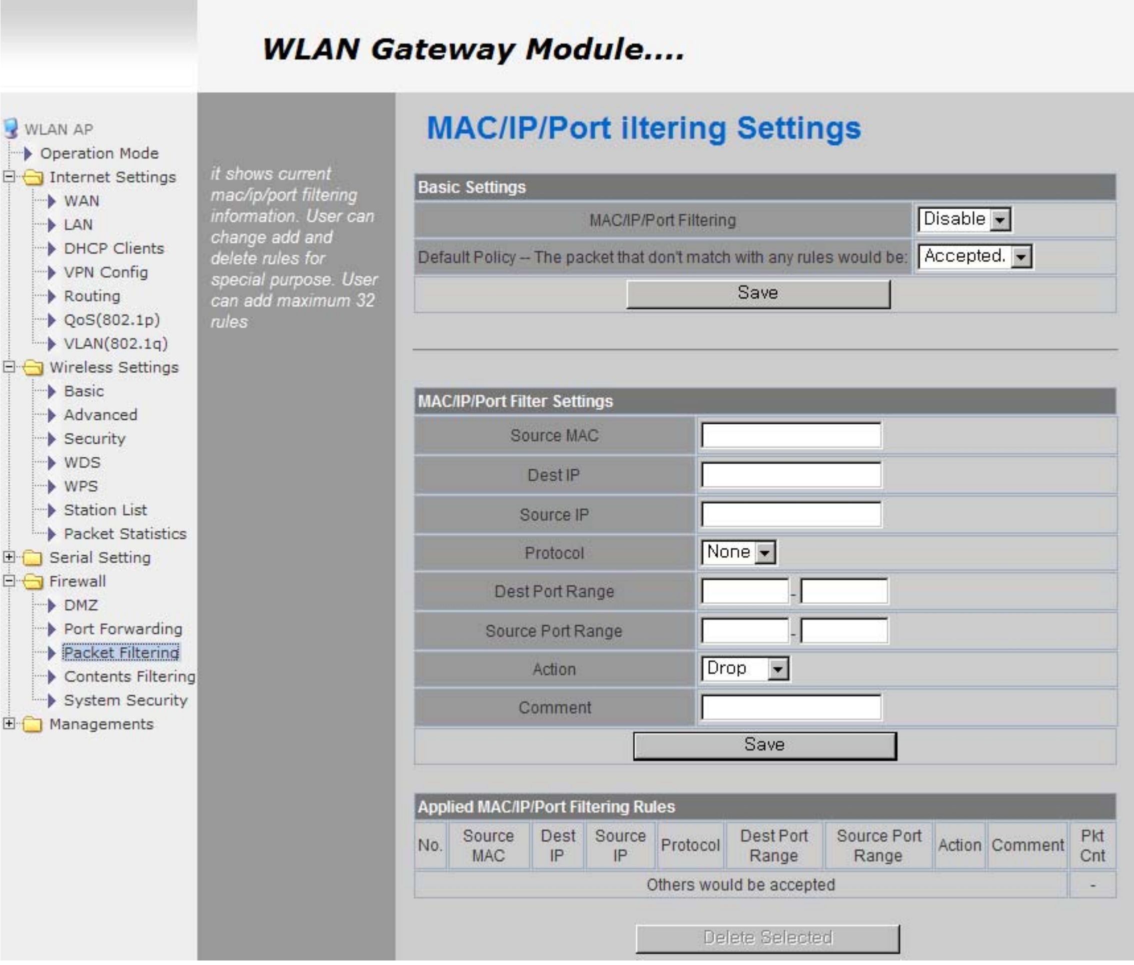
No.	IP Address	Service Port	Protocol	Internal Port	Comment

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

6.3 Packet filtering

◆ WIZ630wi can accept or block Internet packets according to pre-defined MAC or IP address

◆ First, please do basic settings



WLAN Gateway Module....

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 iltering Settings

Basic Settings	
MAC/IP/Port Filtering	Disable
Default Policy -- The packet that don't match with any rules would be:	Accepted.

Save

MAC/IP/Port Filter Settings	
Source MAC	
Dest IP	
Source IP	
Protocol	None
Dest Port Range	-
Source Port Range	-
Action	Drop
Comment	

Save

Applied MAC/IP/Port Filtering Rules

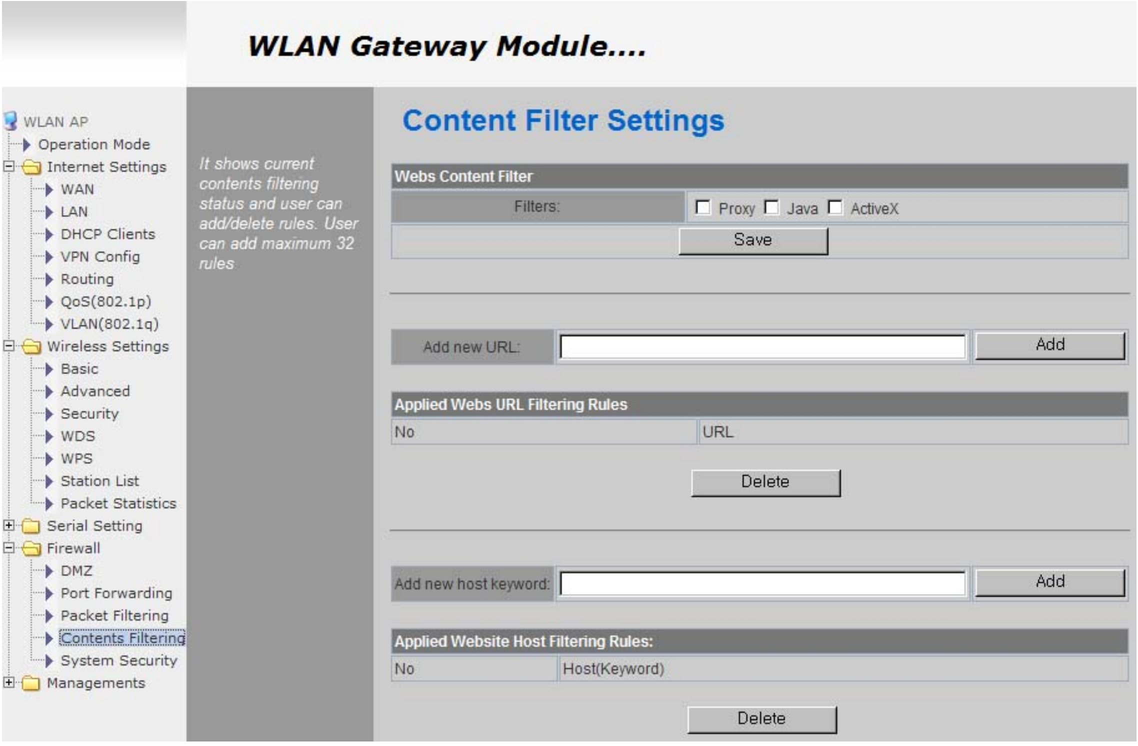
No.	Source MAC	Dest IP	Source IP	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be accepted									-

Delete Selected

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

6.4 Contents filtering

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



It shows current contents filtering status and user can add/delete rules. User can add maximum 32 rules

Content Filter Settings

Webs Content Filter

Filters: □ Proxy □ Java □ ActiveX

Add new URL:

Applied Webs URL Filtering Rules

No	URL

Add new host keyword:

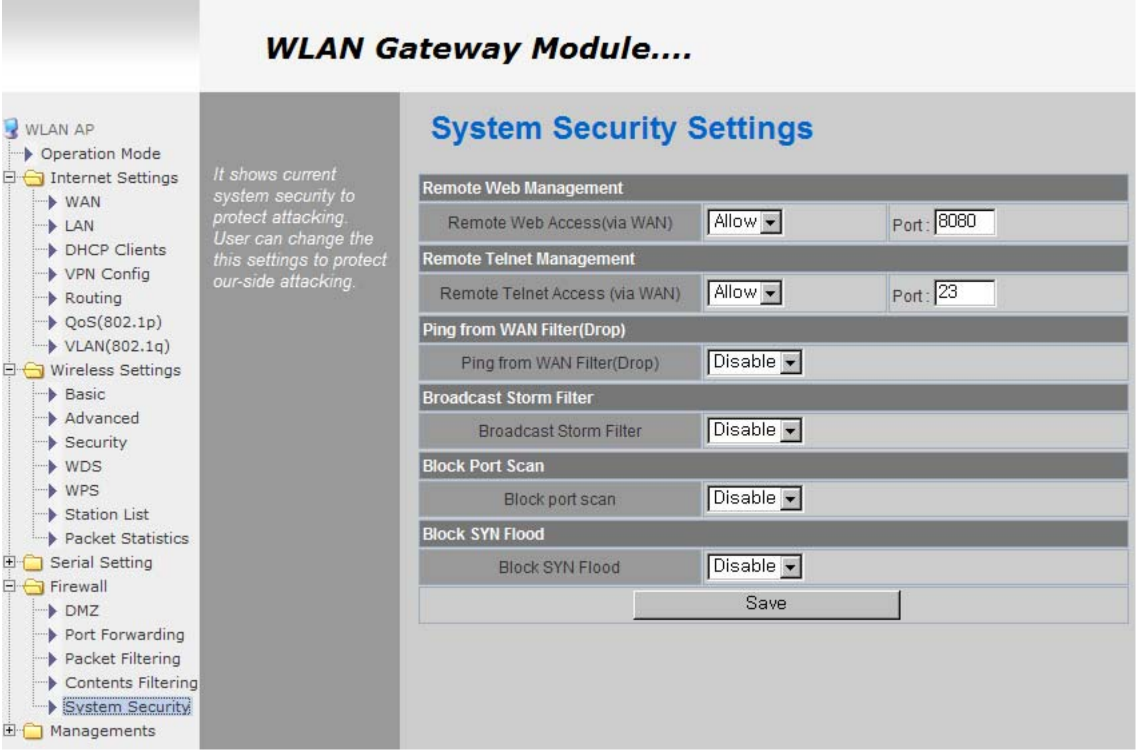
Applied Website Host Filtering Rules:

No	Host(Keyword)

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

6.5 System Security

◆ Defense of external attack.



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

System Security Settings

Remote Web Management
Remote Web Access(via WAN) Allow Port : 8080

Remote Telnet Management
Remote Telnet Access (via WAN) Allow Port : 23

Ping from WAN Filter(Drop)
Ping from WAN Filter(Drop) Disable

Broadcast Storm Filter
Broadcast Storm Filter Disable

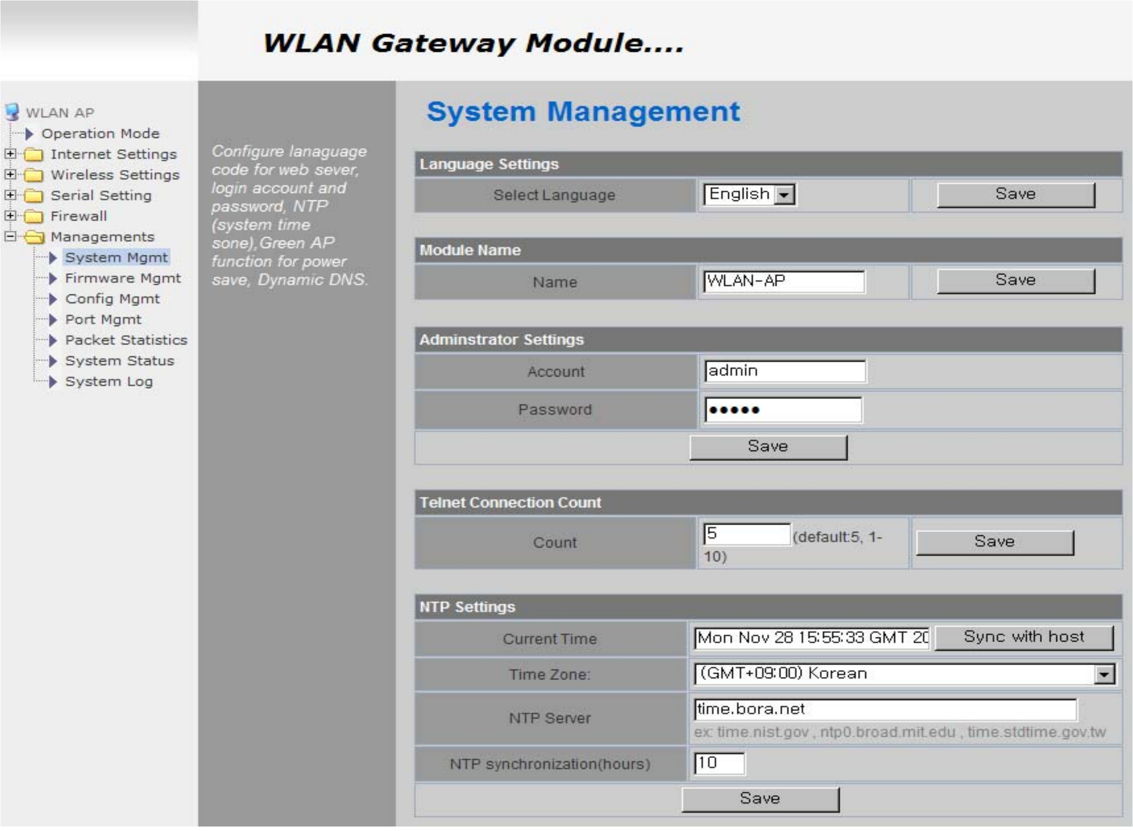
Block Port Scan
Block port scan Disable

Block SYN Flood
Block SYN Flood Disable

Type	Description
Remote management	Settings about accessing methods from WAN to WIZ630wi's embedded web server
Telnet management	Settings about accessing methods from WAN to WIZ630wi's telnet
Ping from WAN Filter	Disable/Enable the WIZ630wi's Ping response
Broadcast Storm filter	Block/Accept the Broadcast packets
Block Port Scan	Block WIZ630wi's port-scan function
Block SYN Flood	Block SYN flood

6. Managements

7.1 System Management



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

System Management

Language Settings

Select Language	English	Save

Module Name

Name	WLAN-AP	Save

Adminstrator Settings

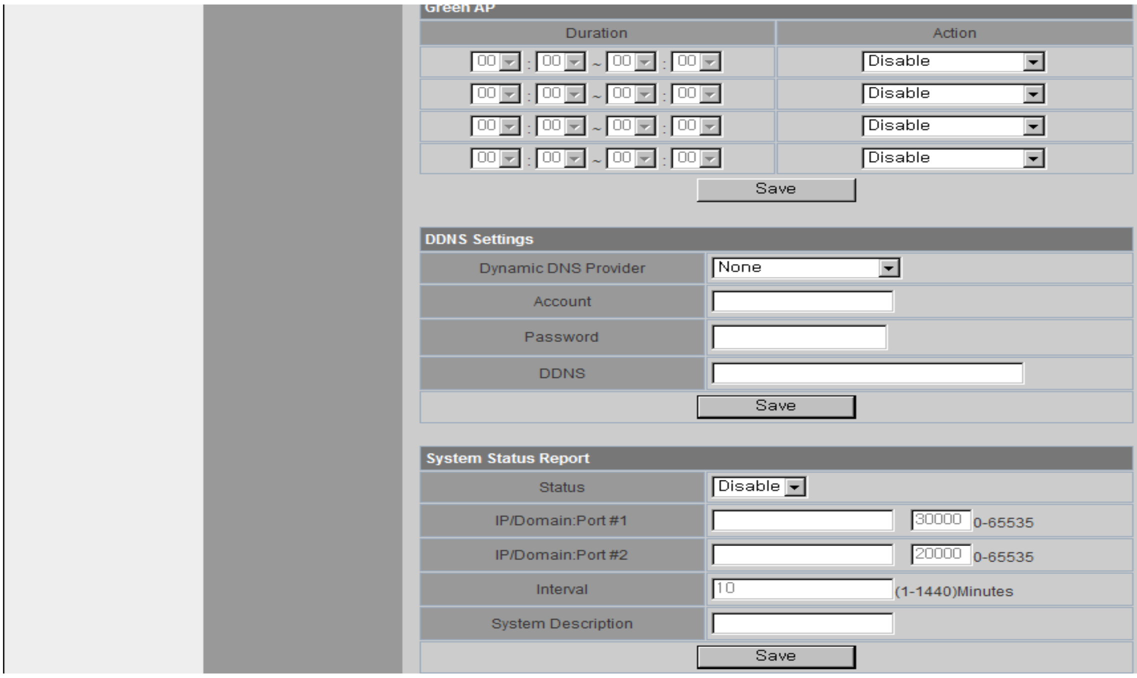
Account	admin
Password	●●●●●
	Save

Telnet Connection Count

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

NTP Settings

Current Time	Mon Nov 28 15:55:33 GMT 2(Sync with host
Time Zone:	(GMT+09:00) Korean
NTP Server	time.bora.net ex: time.nist.gov , ntp0.broad.mit.edu , time.stdtime.gov.tw
NTP synchronization(hours)	10
	Save



Green AP

Duration	Action
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable
Save	

DDNS Settings

Dynamic DNS Provider	None
Account	
Password	
DDNS	
	Save

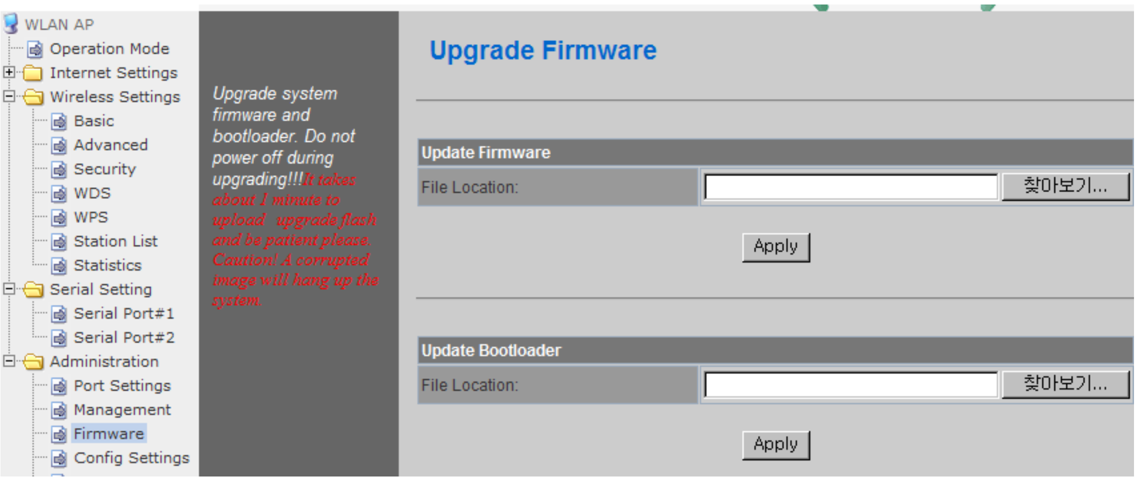
System Status Report

Status	Disable
IP/Domain:Port #1	30000 0-65535
IP/Domain:Port #2	20000 0-65535
Interval	10 (1-1440)Minutes
System Description	
	Save

Type	Description
Language	Select language in the list
Administrator	Pre-defined ID/Password for webpage or Telnet login
NTP	Set NTP server
Green AP	Low power consumptive AP
DDNS	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 WIZ630wi'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 WIZ630wi's webpage.
DDNS Provider	DynDNS, freeDNS, zoneedit, no-ip
Account	ID for DDNS.
Password	Password for DDNS
DDNS	Host name for DDNS

7.2 Firmware

◆ Upgrade firmware and bootloader. Now WIZ630wi doesn't support upgrading by Remote URL.



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.

Upgrade Firmware

Update Firmware

File Location: [ ] 찾아보기...

Apply

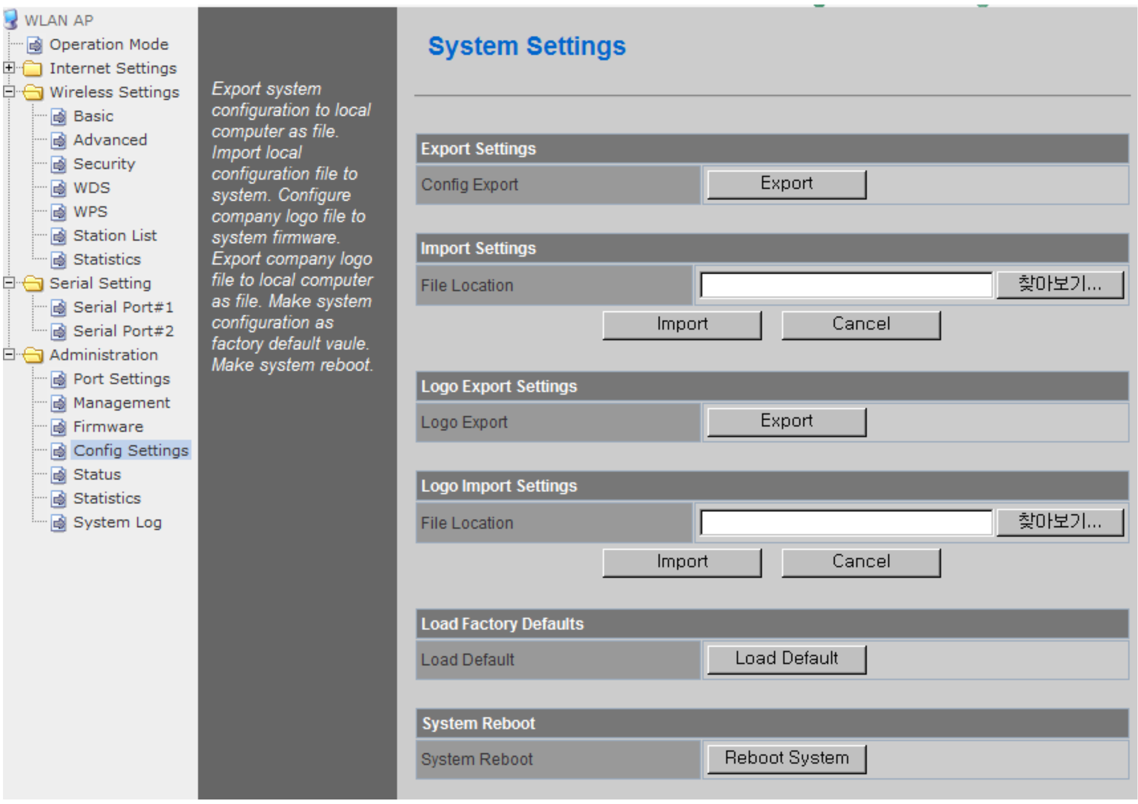
Update Bootloader

File Location: [ ] 찾아보기...

Apply

7.3 Config Settings

◆ Save the setting value of WIZ630wi to the PC,



Export system configuration to local computer as file. Import local configuration file to system. Configure company logo file to system firmware. Export company logo file to local computer as file. Make system configuration as factory default vaule. Make system reboot.

System Settings

Export Settings

Config Export — Export

Import Settings

File Location — 찾아보기...

Import — Cancel

Logo Export Settings

Logo Export — Export

Logo Import Settings

File Location — 찾아보기...

Import — Cancel

Load Factory Defaults

Load Default — Load Default

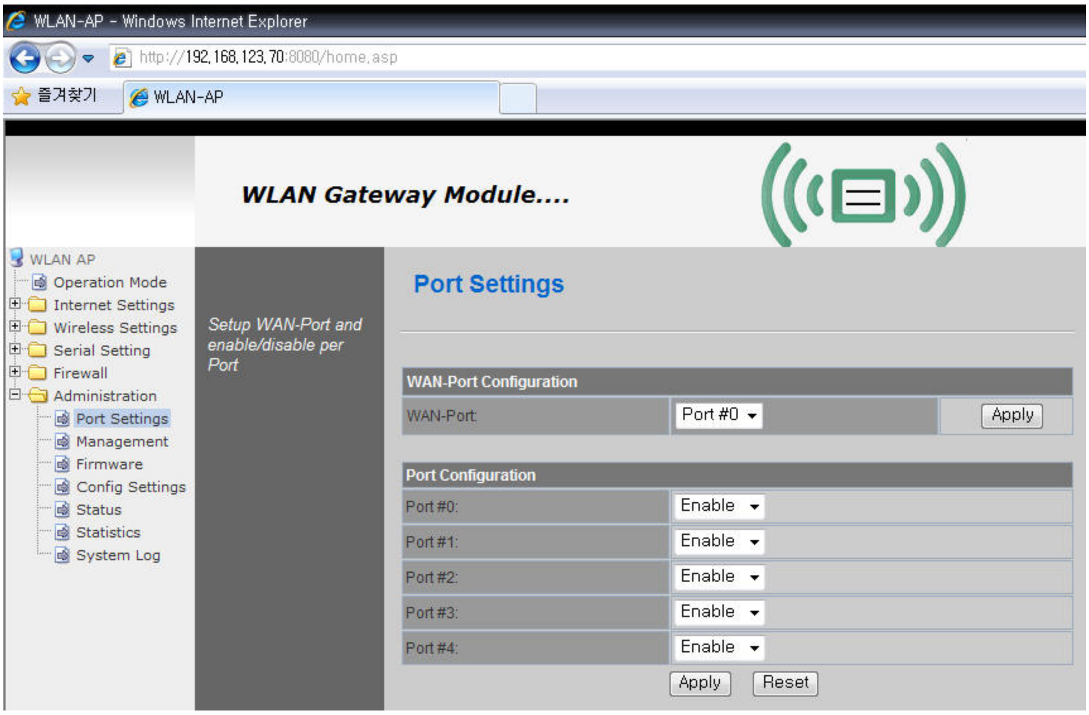
System Reboot

System Reboot — Reboot System

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

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 administrator, we do not recommend you do this change.



WAN-Port Configuration

WAN-Port: Port #0 Apply

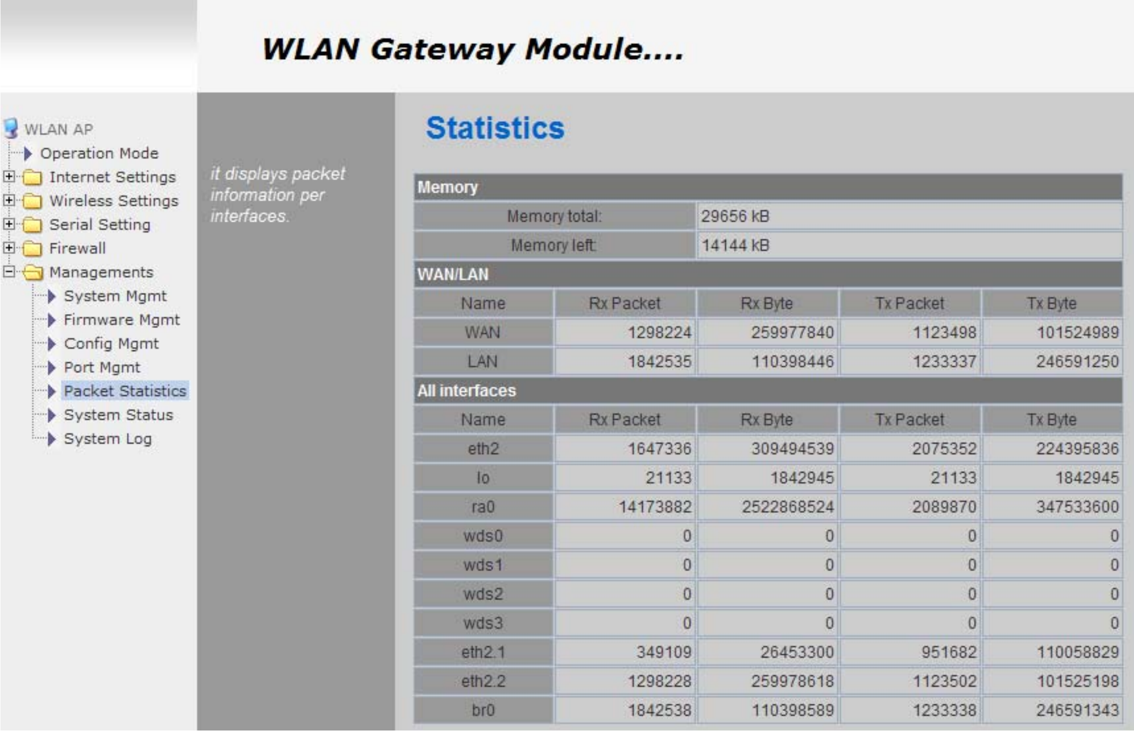
Port Configuration

Port #0:	Enable
Port #1:	Enable
Port #2:	Enable
Port #3:	Enable
Port #4:	Enable

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

7.5 Packet Statistics

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



WLAN Gateway Module....

it displays packet information per interfaces.

Statistics

Memory	
Memory total:	29656 kB
Memory left:	14144 kB

WAN/LAN

Name	Rx Packet	Rx Byte	Tx Packet	Tx Byte
WAN	1298224	259977840	1123498	101524989
LAN	1842535	110398446	1233337	246591250

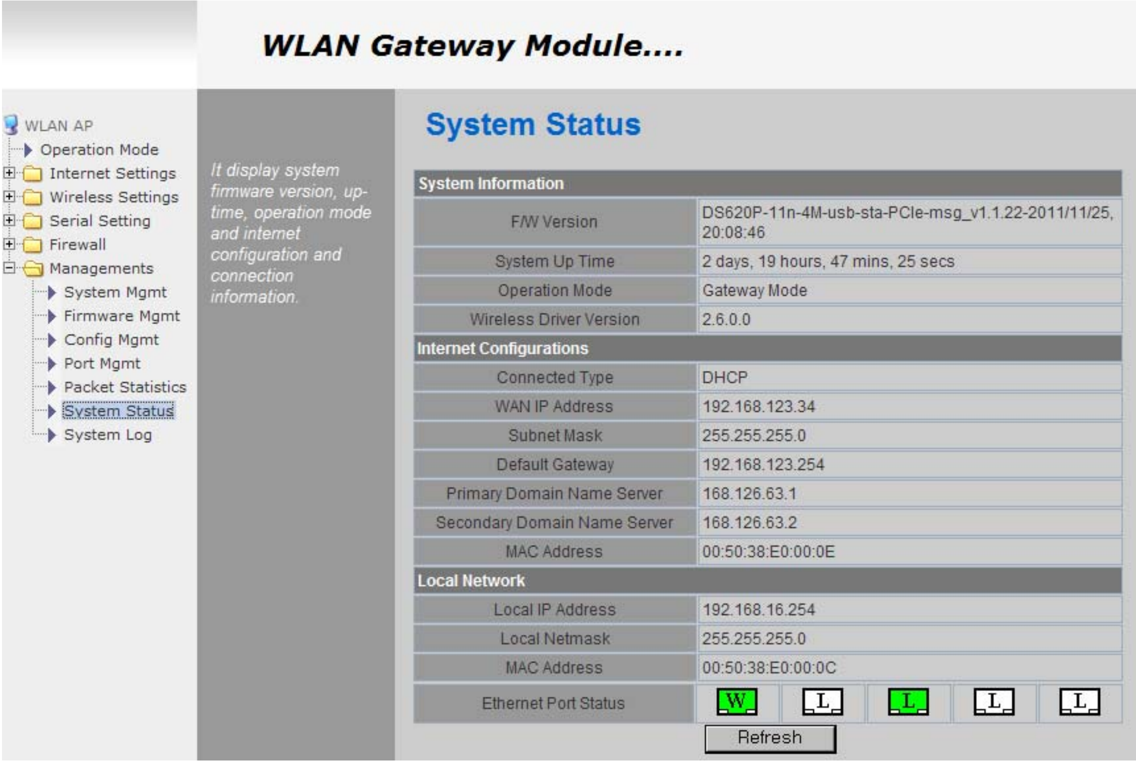
All interfaces

Name	Rx Packet	Rx Byte	Tx Packet	Tx Byte
eth2	1647336	309494539	2075352	224395836
lo	21133	1842945	21133	1842945
ra0	14173882	2522868524	2089870	347533600
wds0	0	0	0	0
wds1	0	0	0	0
wds2	0	0	0	0
wds3	0	0	0	0
eth2.1	349109	26453300	951682	110058829
eth2.2	1298228	259978618	1123502	101525198
br0	1842538	110398589	1233338	246591343

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

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.



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

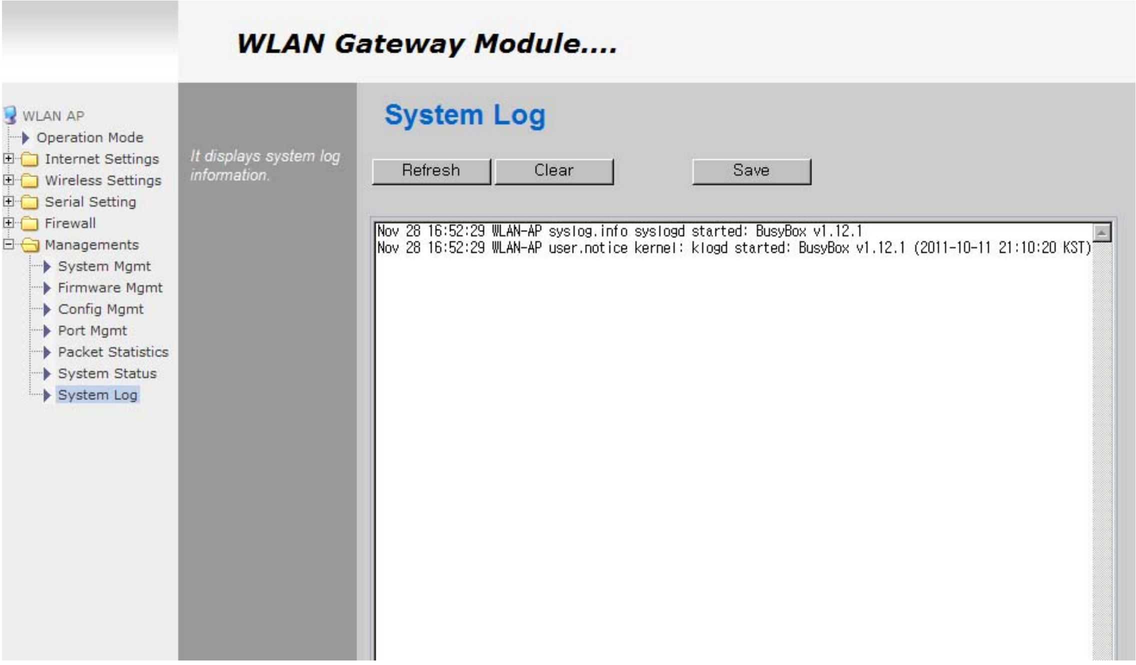
System Status

System Information	
F/W Version	DS620P-11n-4M-usb-sta-PCIe-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
F/W Version	Shows the firmware version.
System Up Time	Shows the system up time.
Operation Mode	Shows the operation mode currently being used.
Internet Configuration	Shows the internet configuration information.
Local Network	Shows the local network information.

7.7 System Log

- ◆ The operation history of WIZ630wi can be checked by using System Log.
- ◆ If the system log exceeds 24Kbyte, more recent log record are added..



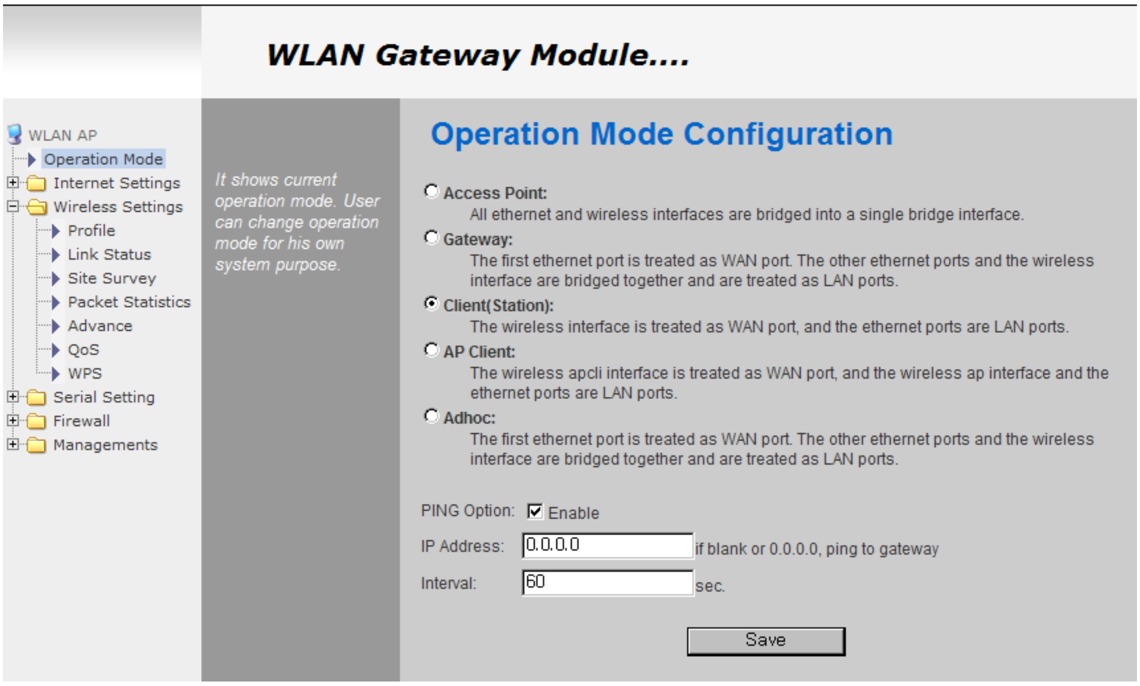
```
Nov 28 16:52:29 WLAN-AP syslog.info syslogd started: BusyBox v1.12.1
Nov 28 16:52:29 WLAN-AP user.notice kernel: klogd started: BusyBox v1.12.1 (2011-10-11 21:10:20 KST)
```

7. Client(Station) Mode setting

◆ WIZ630wi works as a WiFi client(station) which is always paired with a WiFi AP.

◆ Users can take Client Mode as an opposite of Gateway Mode

8.1 Client Mode Setting



WLAN Gateway Module....

It shows current operation mode. User can change operation mode for his own system purpose.

Operation Mode Configuration

○ **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.

PING Option: ☑ Enable

IP Address: 0.0.0.0 if blank or 0.0.0.0, ping to gateway

Interval: 60 sec.

Save

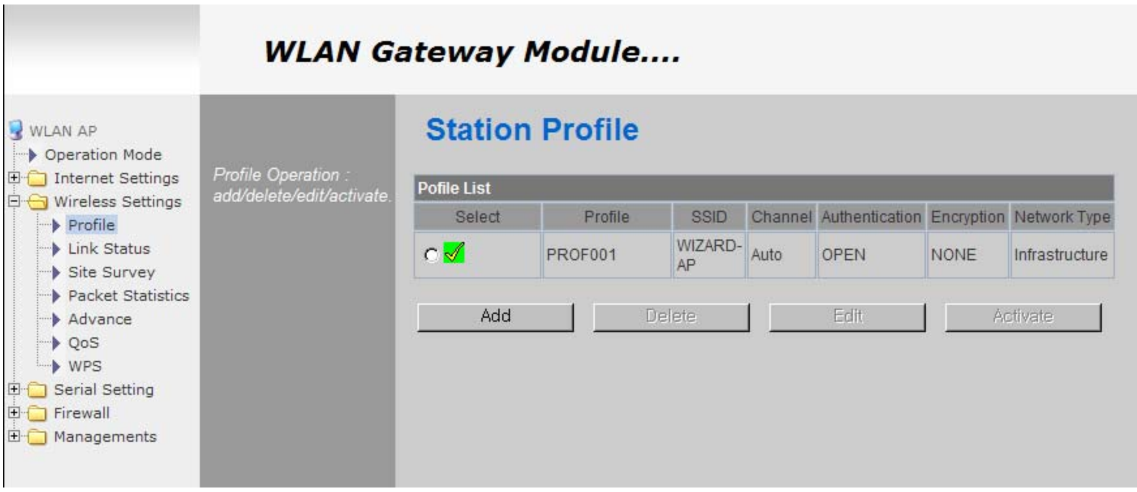
Type	Description
Client(Station)	Client mode setting
Ping Option	Send Ping data to top connected AP by using any time unit
IP Address	If IP is 0.0.0.0, send Ping data to top connected AP.
Interval	Ping Interval setting (time unit: second)

8.2 Profile

◆ Shows the profile of the connected AP. The profile information can be manually input. 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



Station Profile

Pofile List

Select	Profile	SSID	Channel	Authentication	Encryption	Network Type
○ ✓	PROF001	WIZARD-AP	Auto	OPEN	NONE	Infrastructure

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

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.