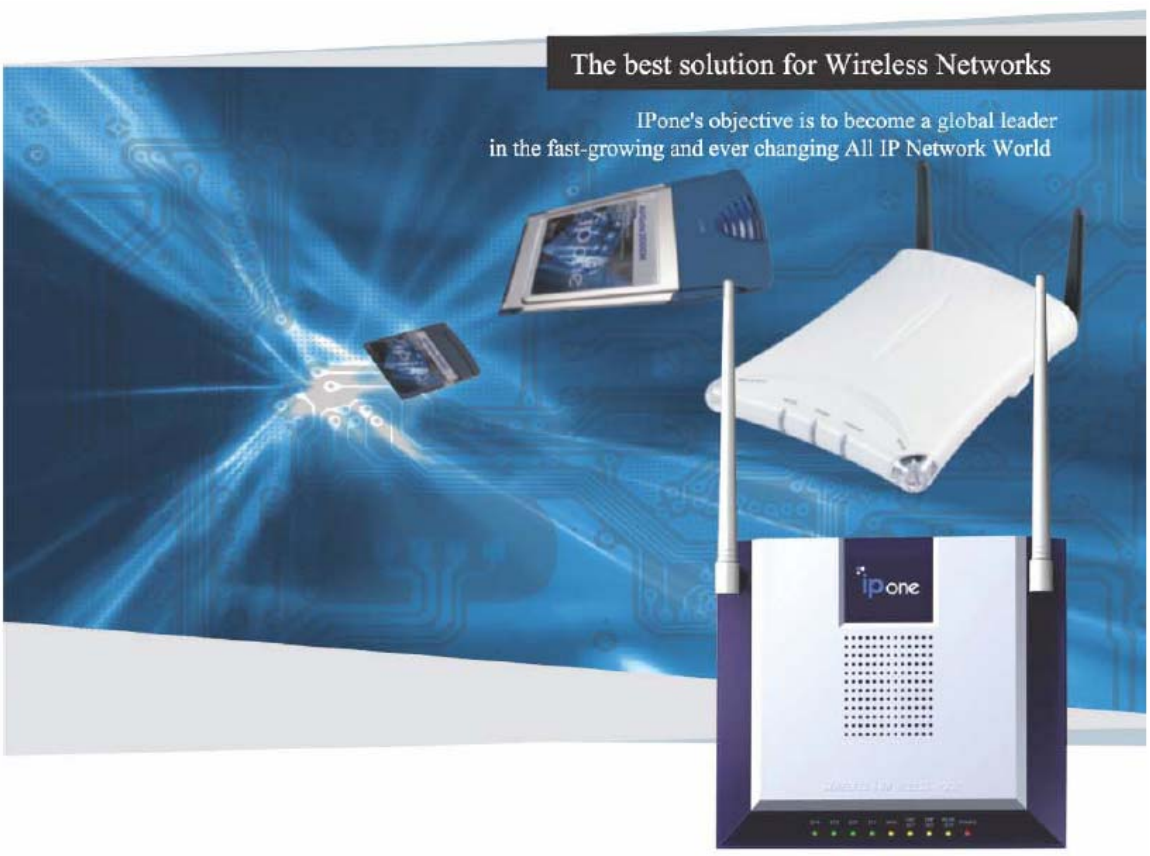



# IPOne 54Mbps Wireless LAN Access Point

## User's Manual ver. 1.1.4e

**IP ONE, Inc.**
Gusang Bldg. 2F, 1009-5, Daechi-dong, Gangnam-gu, Seoul, 135-280, Korea
http://www.ipone.co.kr
Tel: +82-2-3011-0947
E-mail: sales_marketing@ipone.co.kr



☞ Models subjected to this document: AG3000/5000/503X series.

**The instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual.**

## INFORMATION TO THE USER (Part 15.105(b))

**For Class B digital device**

**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 (Part 15.21)

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

"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."

"CAUTION: RF Exposure to Radio Frequency Radiation.

This equipment must be installed and provided minimum seperatiom distance of 20cm from the body of user and near by person. In addition to seperation distance, this device cannot be transmitted and operating in conjuction with any other transmitter or antenna.

# CONTENTS

# ABBREVIATION

| | |
|---|---|
| AAA : | Authentication, Authorization, Accounting |
| ADSL : | Asymmetric Digital Subscriber Line |
| AP : | Access Point |
| BSS : | Basic Service Set |
| CCK : | Complimentary Code Keying |
| CTS: | Clear To Send |
| DBPSK : | Differential Binary Phase Shift Keying |
| DC : | Direct Current |
| DHCP : | Dynamic Host Configuration Protocol |
| DNS : | Domain Name Service |
| DTIM : | Delivery Traffic Indication Map |
| DQPSK : | Differential Quadrature Phase Shift Keying |
| EAP : | Extensible Authentication Protocol |
| ESSID : | Extended Service Set Identity |
| FA: | Foreign Agent |
| GMT : | Greenwich Mean Time |
| HA: | Home Agent |
| HTTP: | Hypertext Transfer Protocol |
| IP : | Internet Protocol |
| IAPP : | Inter Access Point Protocol |
| ICMP: | Internet Control Message Protocol |
| ID: | Identity |
| IEEE : | Institute of Electrical and Electronics Engineers |
| LAN : | Local Area Network |
| LED: | Light Emitting Diode |
| MAC : | Media Access Control |
| MIP: | Mobile IP |
| MN: | Mobile Node |
| NAT : | Network Address Translation |
| NAS : | Network Access Server |
| PC : | Personal Computer |
| PCMCIA : | Personal Computer Memory Card International Association |
| POD : | Pull Out Detection |

| | |
|---|---|
| PoE : | Power over Ethernet |
| PPP : | Point-to-Point Protocol |
| PPPoE : | Point-to-Point Protocol over Ethernet |
| PS : | Power Save |
| RADIUS : | Remote Authentication Dial In User Service |
| RF : | Radio Frequency |
| RTS : | Request To Send |
| Rx : | Receive |
| SNMP : | Simple Network Management Protocol. |
| SNTP : | Simple Network Time Protocol |
| SSID : | Service Set Identity |
| TCP : | Transmission Control Protocol |
| TFTP : | Trivial File Transfer Protocol |
| Tx : | Transmit |
| UDP : | User Datagram Protocol |
| USB : | Universal Serial Bus |
| WAN : | Wide Area Network |
| WEP : | Wired Equivalent Privacy |
| WLAN : | Wireless Local Area Network |

# CHAPTER 1. Wireless LAN Overview

Wireless LAN (WLAN) refers to a LAN that uses high frequency radiowave instead of cables for inter-node communications. WLAN operation is specified in IEEE 802.11. Unlimited access to business applications is becoming essential. WLANs are increasingly being used to provide flexible network connectivity. WLAN solutions are typically deployed internally, usually within an office or factory environment, although they can be installed externally to provide short-range connectivity to mobile users.

WLAN benefits include:

- Increased mobility
- Fast deployment
- Network access where cabling is difficult
- Connectivity for temporary networks

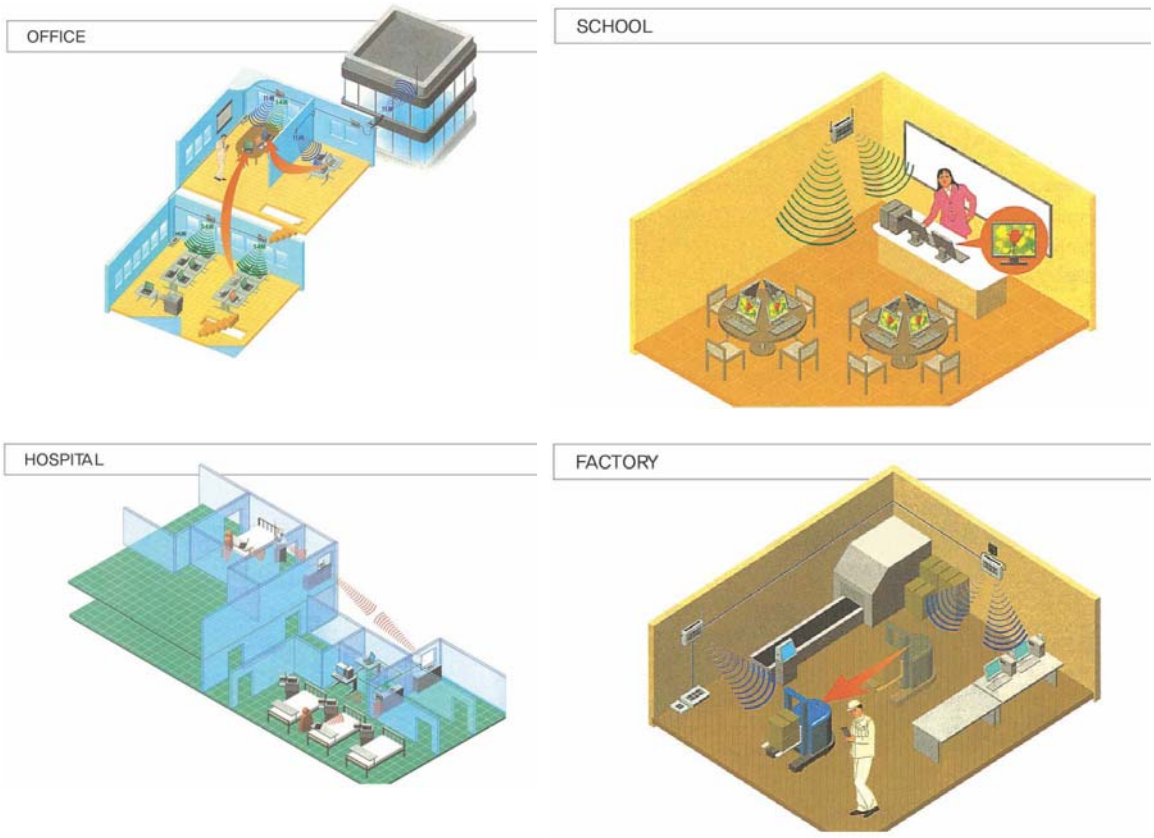



Fig. 1.1.1 Wireless LAN examples

# CHAPTER 2. AP Architecture and Installation

## 2.1 AP Components

Please check the following components before installation:

① Access Point

② Antenna

③ Power Adaptor

④ RS-232 Cable (option)

⑤ CD (User's Manual)

## 2.2 AP View

### 2.2.1 AP Front

Fig. 2.2.1 AP Front

| Num | LED Name | Color | Description |
|---|---|---|---|
| ① | PWR | Green | Power status |
| ② | WL1 | Green | Tx/Rx data to/from WLAN port |
| ③ | WL2 | Green | Tx/Rx data to/from WLAN port 2<br>(Internal for Dual-mode AP) |
| ④ | LAN | Green | Tx/Rx data to/from Ethernet LAN port<br>(Internal for 2 port Ethernet AP) |
| ⑤ | WAN | Green | Tx/Rx data to/from Ethernet WAN port |
| ⑥ | SEC | Green | Encryption status |

### 2.2.2 AP Rear


Fig. 2.2.2 AP Rear (Model dependent)

| Num | Name | Description |
|---|---|---|
| ① | WAN | RJ-45 Ethernet Connect |
| ② | CONSOLE | RS-232 Serial Port |
| ③ | LAN | RJ-45 Ethernet Connector (Internal for 2 port Ethernet AP) |
| ④ | RESET | Factory Reset Switch |
| ⑤ | S/W | Power ON/OFF Switch |
| ⑥ | POWER | DC Power Connector |

## 2.3 AP Installation

### 2.3.1 Notice before Installation

We recommend you to avoid these places where may be cause of performance decline or trouble:

① Places with high humidity or wet condition
② Places with extreme temperature (too hot or too cold)
③ Places where change of temperature is extreme
④ Places with a lot of dusts
⑤ Places sealed with thick walls or still structure which cause high interference

### 2.3.2 Installation

STEP 1 Attach UTP Ethernet Cable

Attach UTP Ethernet cable to AP's RJ-45 connector and connect the other side of the cable to network equipments such as Router or Hub.

STEP 2 Attach RS-232C Serial Cable

Attach RS-232C serial cable to the AP and PC. The parameters of AP can be configured through connection of RS-232C serial cable to the PC (Refer Chapter 3).

STEP 3 Supply Power

Plug in the DC output to AP's power port. Make sure that the "Power" LED is on. If the "Power" LED is not on, please check the connections of the power code.

☞ Notice: Use the supplied power adapter (DC 5V, 2A) only to prevent the permanent failure of AP.

☞ Notice: Don't use both DC power and PoE power at the same time.

☞ PoE usage: The PoE (Power over Ethernet) is the equipment that both power and data are supplied throughput Ethernet cable. Plug in the power adapter to DC in of PoE and the Ethernet cable to Data in of PoE. Attach UTP Ethernet cable to AP's RJ-45 connector and connect the other side of the cable to Data & Power Out of PoE (Internal for PoE supported models).

STEP 4 Confirm Installation

Change settings of AP referring User's Guide. Insert a wireless LAN card into your PC. Enter the same ESSID that you have set for the AP, using the wireless LAN card utility running on your PC. Check the signal strength of wireless link on the wireless LAN card utility.

### 2.3.3 Notice when you use

We recommend you to avoid the followings when you use:

① Do not disassemble on your own.

② Do not drop the product or give excessive impact.

③ Do not use any parts or components, which are not provided.

④ Use only the power adapter provided.

⑤ Use the PoE only for PoE supported models.

# CHAPTER 3. AP Software Configurations

☞ This software configuration guide describes how to configure AG5031DU-AN2 Access Points using web-based management system (WMS) or console-based management system (CMS). This guide can be subject to other 54Mbps Access Points if we don't comment specific notice.

☞ This software configuration guide is based on IPOne Access Point software, Wireless LAN Operating System (WOS) version 1.1.14. However, this guide can be subject to other higher WOS versions if we don't comment specific notice.



## Management Options

You can use the access point management system throughput the following interfaces:

- A web-browser interface
- A command-line interface (CLI)
- Simple Network Management Protocol (SNMP)

## 3.1 IPOne WOS Key Features

The key features of IPOne WOS are as follows:

| | |
|---|---|
| **Authentication, Security, Billing** | |
| Authentication | IEEE 802.1x based authentication/security<br>MAC address authentication<br>WPA |
| Security | 64/128/152 bit static WEP, 64/128 bit dynamic WEP, WPA |
| Billing and Local Services | RADIUS accounting<br>Session/Idle-timeout, Lost carrier detection<br>WEB-Redirection, white list support<br>Private IP allocation for guest uses<br>Notify user's IP address to server |
| **Networking and Control** | |
| IP sharing | NAT |
| Network Protocol | TCP/IP, IEEE 802.1d transparent bridge, 802.1x<br>DHCP server/client/relay, PPPoE |
| Access Control | MAC address filtering,<br>Control of the maximum number of association |
| Wireless Radio Control | Radio transmission power control,<br>Automatic change of transmit rate,<br>Automatic channel selection |
| **Roaming** | |
| L2 roaming | Seamless roaming between AP's, IEEE 802.11f IAPP support |
| L3 roaming<br>(Subnet roaming) | Mobile IP foreign agent support (RFC2002).<br>☞ This function is included only in Enterprise high-level AP product (AG5031DU series). |
| **Quality of Service** | |
| Downstream QoS | IEEE 802.1p based downstream QoS support |
| **Management** | |
| SNMP/MIB | SNMP MIB (MIB II, WLAN MIB, 802.1x MIB, 802.1d Bridge MIB, Enterprise MIB), Trap message |
| Local Configurations | ITU-T V.24 (EIA-RS232C), RJ-45 Port |
| Remote Configurations | Telnet, HTTP, SNMP, Web-based management |
| Firmware Upgrade | Upgrade via TFTP, FTP, HTTP |

## 3.2 AP Management System Access

### 3.2.1 AP Access and TCP/IP Setting using HyperTerminal

Attach RS-232C serial cable to the AP and PC. Execute "HypterTerminal" program on your MS-Windows by following the steps.

STEP1 Execute HyperTerminal program.

STEP2 After executing the HyperTerminal, the following window will be displayed on MS-Windows. As displayed above, type "IPOne WOS Configuration" in the name field, and click [OK] button. You can enter any name you wish for the connection.


Fig. 3.2.1 HypterTerminal Initial Screen

STEP 3 Select the modem port as shown in the window below, and click [OK] button. In most of the cases, select either "Direct to Com1" or "Direct to Com2.".


Fig. 3.2.2 HypterTerminal Select modem port

STEP 4 You will view the following window and must set the properties of the selected COM port as shown below. Click [OK] button.

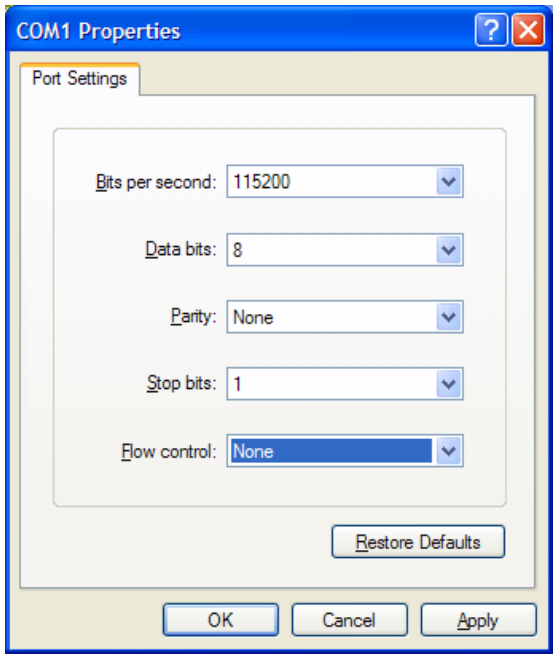



Fig. 3.2.3 HypterTerminal Port Settings

STEP 5 If all the steps above are executed correctly, then the following login prompt will be displayed on the HyperTerminal window. The default username and password is "admin" and "admin" respectively.

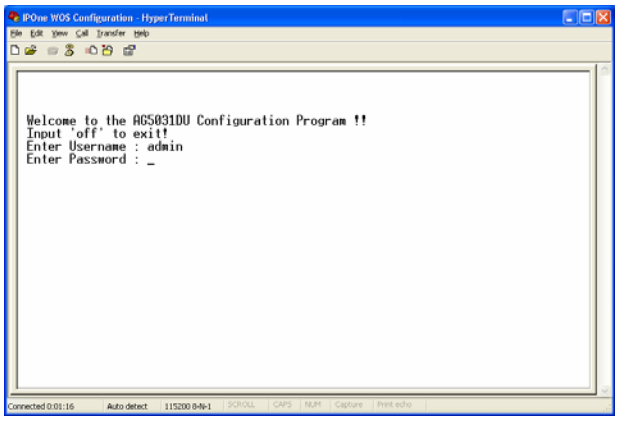



Fig. 3.2.4 HyperTerminal AP CMS Login

STEP 6 When username and password are correctly entered, the following [Status] menu of AP CMS (Console-based Management System) appears on the HyperTerminal window.

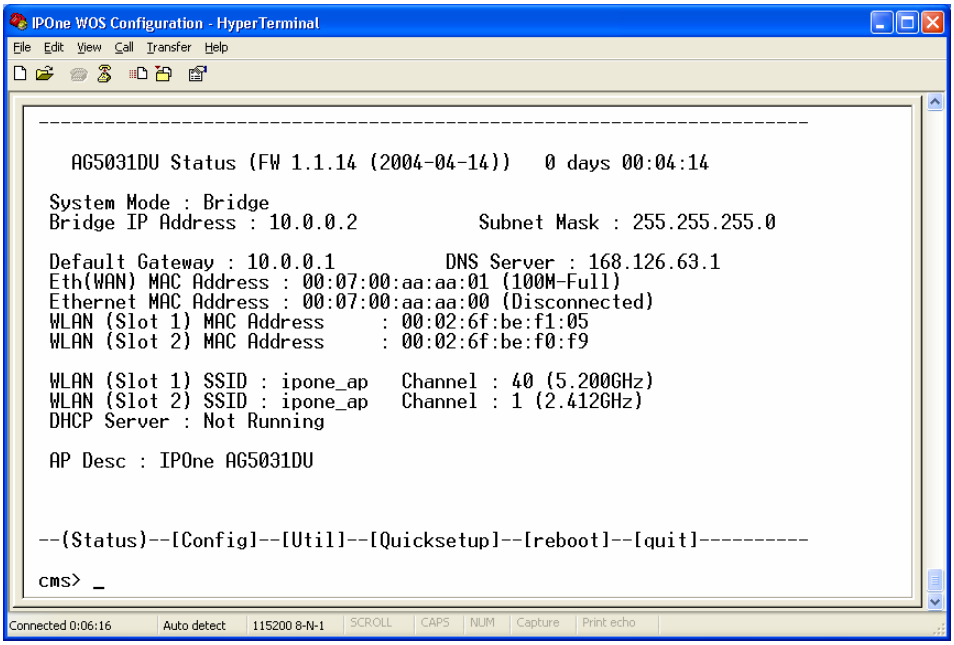



Fig. 3.2.5 HyperTerminal AP CMS Status

In AP CMS, the command is the follows:

| Command | Description |
|---|---|
| S <enter> | AP Status |
| C <enter> | AP Configurations |
| U <enter> | AP Management Functions |
| reboot <enter> | Reboot |
| quit <enter> | Logout |

STEP 7 In AP CMS, configure TCP/IP information by following the steps.

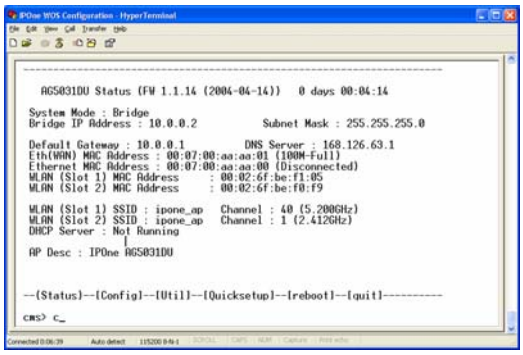
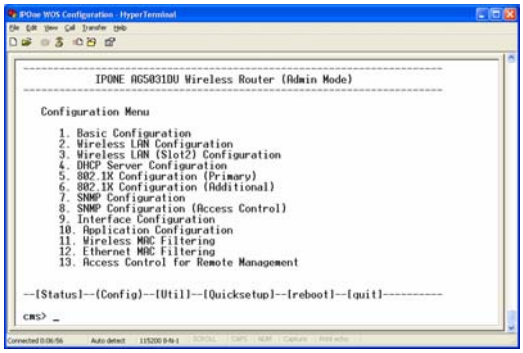
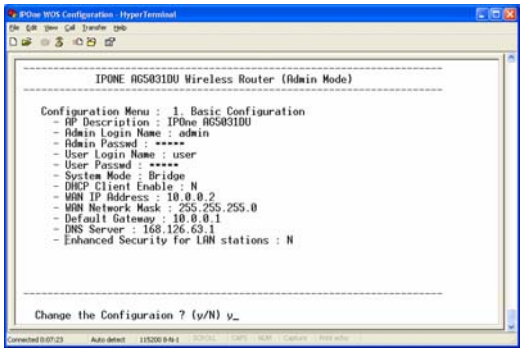
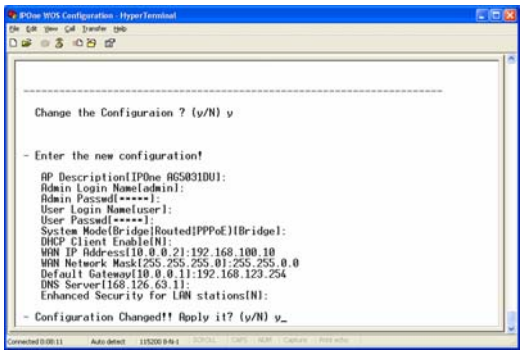
| | |
|---|---|
|  | ① Enter the command "C" to move [Config] menu of CMS. |
|  | ② Enter the command "1" to select the menu of [1. Basic Configuration]. |
|  | ③ Enter the command "y" to change configurations. |
|  | ④ Enter the proper values. Then, enter the command "y" to apply them. If you just enter without input of the proper value, the default value keeps. |

Fig. 3.2.6 HyperTermal TCP/IP Settings

### 3.2.2 AP Access using Web Browser

☞ Default IP address of the AP is "10.0.0.2." This example assumed that you change the IP address into "192.168.110.10" by using HyperTerminal.

STEP 1 Open Web Browser. We recommend beyond IE 5.0.

STEP 2 Enter AP's IP address and Port number on "Address" of the Web Browser to access AP's WMS (Web-based Management System). The default HTTP port number is 8899.

http://[AP's IP Address]:8899

STEP 3 Enter Username and Password. The default username and password is "admin" and "admin" respectively.

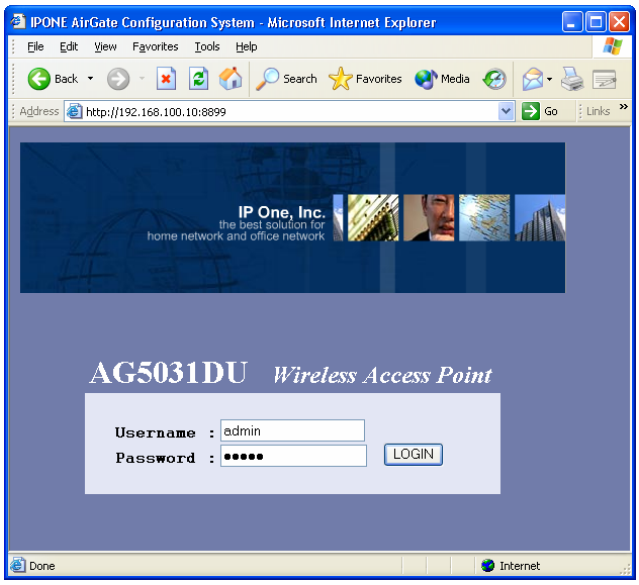



Fig. 3.2.7 AP WMS Login

STEP 4 When username and password are correctly entered, the following [Status] menu of AP WMS appears.

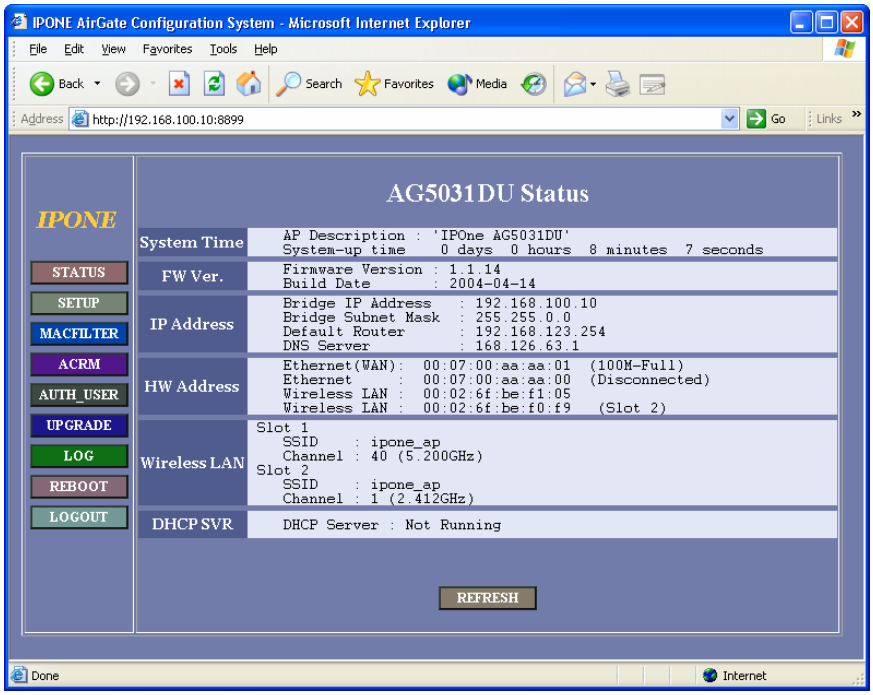



Fig. 3.2.8 AP WMS Status

### 3.2.4 AP Access using Telnet

| |
|---|
| ☞ Default IP address of the AP is "10.10.10.2." This example assumed that you change the IP address into "192.168.110.10" by using HyperTerminal. |

STEP 1 Open "Run" on [Start] menu of MS-Windows. Enter the IP address for Internet Connection as following Example. Click [OK] button.

| |
|---|
| telenet [AP's IP address] |

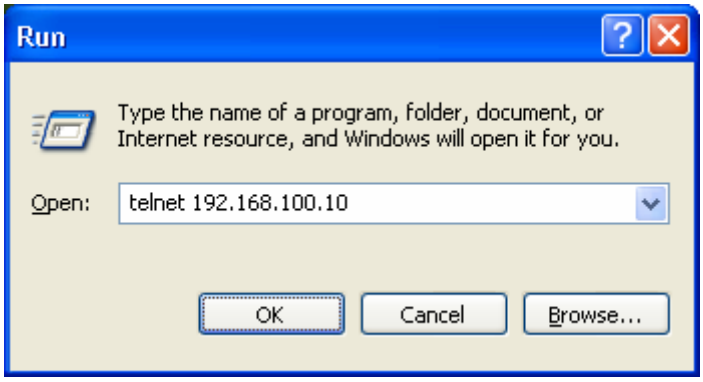



Fig. 3.2.9 AP access using Telnet

STEP 2 Telnet order window appears, and please refer to "AP Access using HyperTerminal."

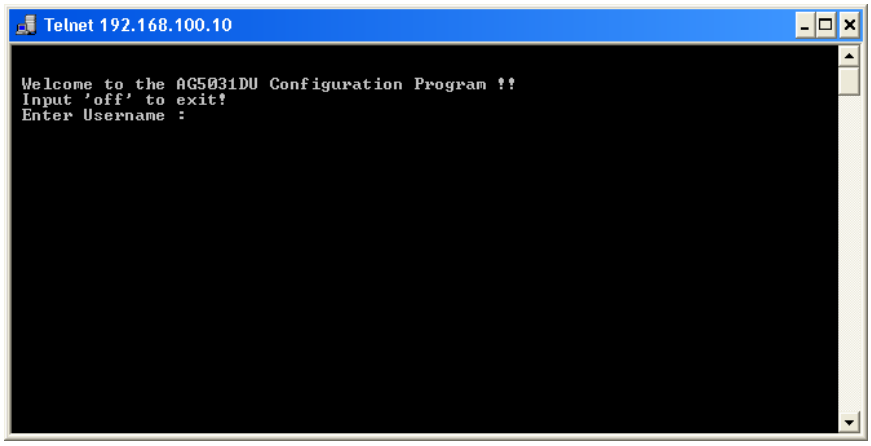
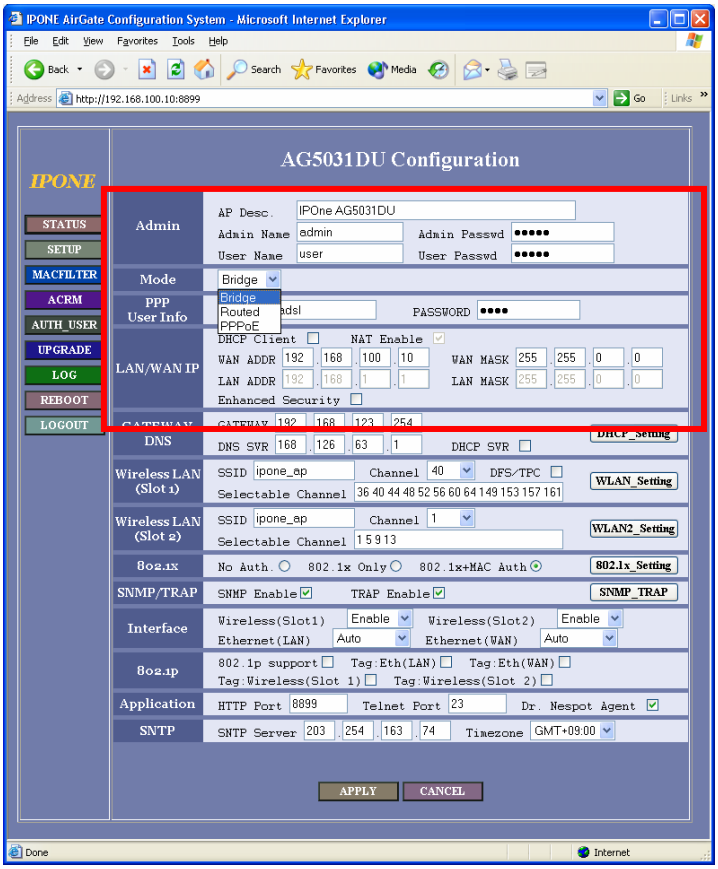


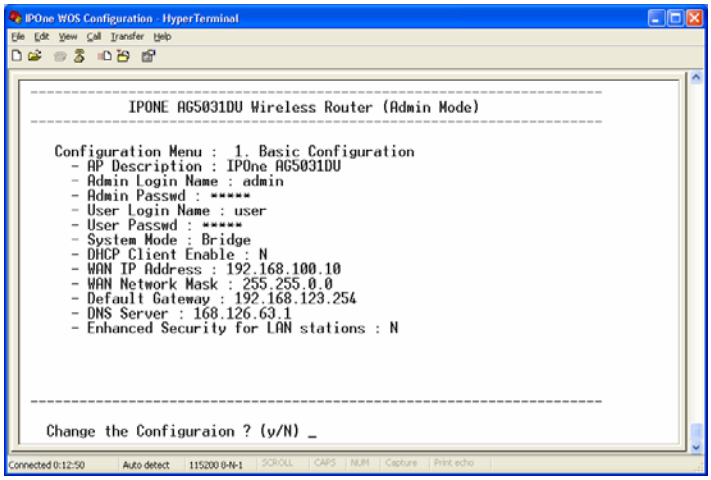

Fig. 3.2.10 Telnet AP CMS Login

## 3.3 Basic Settings

### 3.3.1 Configuring Operating Mode and TCP/IP




(a) WMS Screen




(b) CMS Screen

Fig. 3.3.1 Configuring Operating Mode and TCP/IP

- **Configurations**

| Item | Description |
|---|---|
| Admin | ➢ AP Desc.: Describe brief of AP.<br>➢ Admin User Name: Administrator's user name.<br>➢ Admin Passwd: Administrator's password.<br>➢ User Name: General user's user name. Access to AP settings is limited for general user.<br>➢ User Passwd: General user's password. |
| System Mode | System operation mode is selected one among Bridge, Routed, or PPPoE. General mode is Bridge.<br>The detail is described in the following sentence. |
| LAN/WAN IP | ➢ DHCP Client: IP address is automatically allocated from the network.<br>➢ WAN ADDR: IP address of WAN interface.<br>➢ WAN MASK: IP subnet mask of WAN interface.<br>➢ LAN ADDR: IP address of LAN interface in Routed mode.<br>➢ LAN Mask: IP subnet mask of LAN interface in Routed mode. |
| Enhanced Security for LAN stations | The function prohibits communications between wireless terminals and wired terminals directly connected with AP's Ethernet port. If this function is enabled, wireless terminals don't communicate with wired terminals.<br><br>☞ This function does not prohibit communications between wired terminals connected with switch or Hub. |
| GATEWAY<br>DNS | ➢ GATEWAY: Default gateway address.<br>➢ DNS SVR: DNS server address |

**(1) Bridge Mode**

| Item | Description |
|---|---|
| System Mode | In Bridge mode, all physical interfaces (wireless interface, Ethernet interface) use one IP address. |
| LAN/WAN IP | Just set one IP address of WAN interface because all physical interfaces use one IP address. If DHCP client function is enabled, the IP address is automatically allocated from the network.<br><br>☞ In Bridge mode, you cannot use NAT function. |

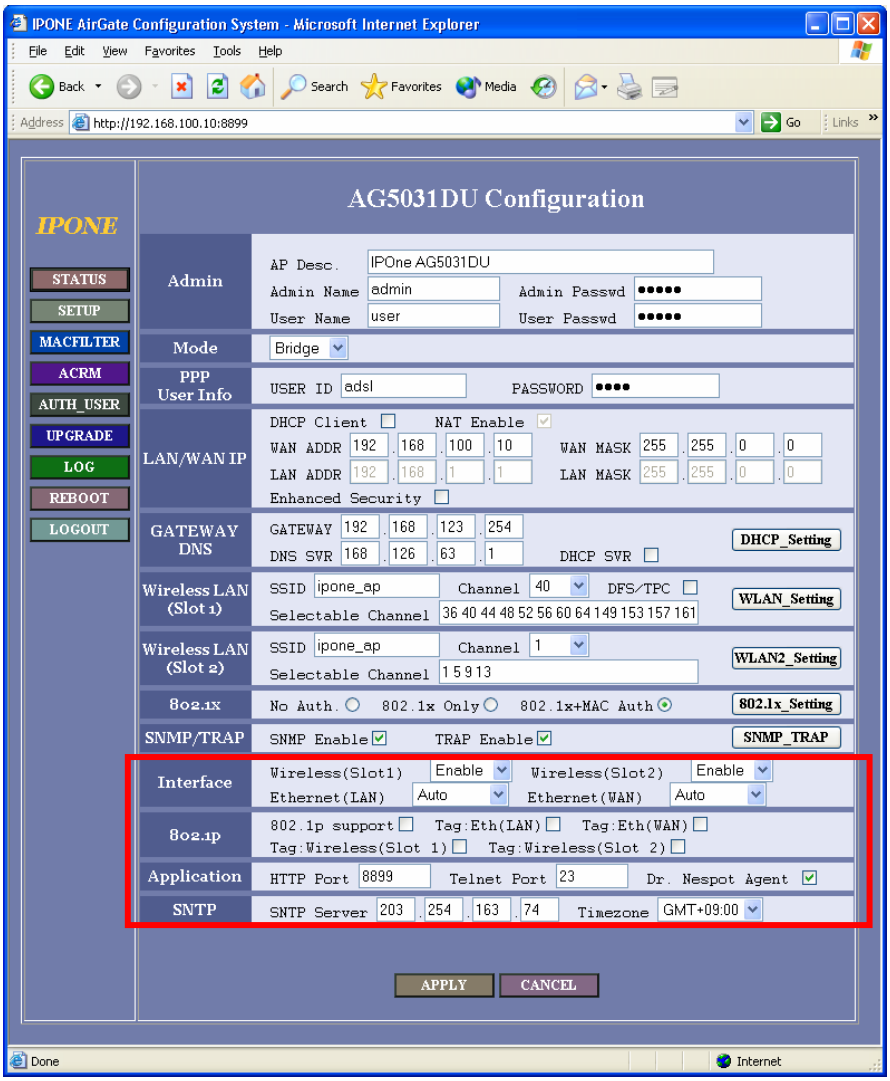
**(2) Routed Mode**

| Item | Description |
|---|---|
| System Mode | In Routed mode, the WAN interface and the other interfaces (wireless interface, local Ethernet) are differentiated as a different IP subnet. |
| LAN/WAN IP | Set two IP addresses for WAN interface and local LAN/wireless interface, respectively. If you want to use NAT function, enable the NAT function.<br><br>☞ In Bridge mode, you can use NAT function. |

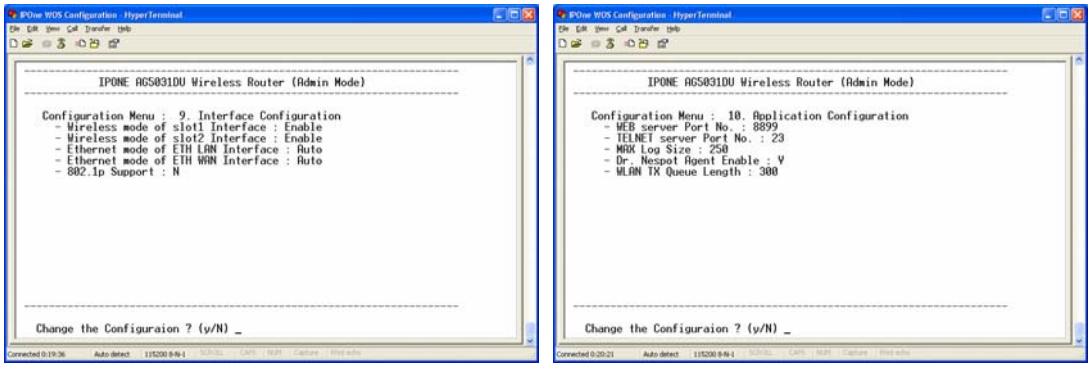
**(3) PPPoE Mode**

| Item | Description |
|---|---|
| System Mode | You must set the PPPoE mode when the AP is directly connected with ADSL modem. |
| PPP User Info | Set "User ID" and "Password" of ADSL modem. |
| LAN/WAN IP | Set private IP address for local LAN/wireless interface.<br><br>☞ In PPPoE mode, you can use NAT function. |

### 3.3.2 Configuring Interface and Application Port




(a) WMS Screen




(b) CMS Screen

Fig. 3.3.2 Configuring Interface and Application Port

- **Configurations**

| Item | Description |
|---|---|
| Interface | ➢ Wireless: Enable or disable the wireless LAN operation.<br>➢ Ethernet: Enable or disable the Ethernet port. Moreover, configure Ethernet link speed and duplex.<br><br>☞ Be careful when changing the settings for the Ethernet ports. Incorrectly forcing a specific speed or duplex mode may result in poor performance and data loss, or disconnection. Consult your LAN administrator before forcing a speed or duplex mode or if you don't know the capabilities of the attached device. |
| Application | ➢ HTTP Port: Configure HTTP port number.<br>➢ Telnet Port: Configure Telnet port number.<br><br>☞ Enter AP's IP address and port number on "Address" of the Web Browser to access AP's WMS (Web-based Management System). The default HTTP port number is 8899. Ex) http://10.0.0.2:8899 |
| SNTP | ➢ Set IP address of SNTP(Simple Network Time Protocol) time server. |

### 3.3.3 QoS Configurations

AP supports 802.1p based simplified downstream priority service. AP firstly transmits high priority packets, and then transmits low priority packets on downlink wireless channel. The value of MOS (Mean Opinion Score) will be improved when the QoS function is enabled.

**(1) 802.1p Overview**

The IEEE 802.1p signaling technique is an OSI Layer 2 standard for prioritizing network traffic at the data link/MAC sublayer. It can also be defined as best-effort QoS at Layer 2. 802.1p traffic is simply classified and sent to the destination; no bandwidth reservations are established. The 802.1p standard is derived from the 802.1Q Virtual Local Area Networks (VLANs) standard, which specifies a tag appended to a MAC frame. According to 802.1Q, the tag carrying VLAN information has two parts: the VLAN ID (12 bits) and Prioritization (3 bits). Because the Prioritization field was never defined in the VLAN standard, the 802.1p implementation defines this Prioritization field.

The 3-bit Prioritization field in 802.1P establishes eight levels of priority, similar to the IP Precedence bits. Network adapters and switches route traffic based on the priority level. Using Layer 3 switches allows you to map 802.1p prioritization to IP Precedence before forwarding to routers.

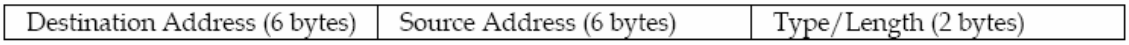



Fig. 3.3.3 Ethernet Layer 2 Header without 802.1p/Q information

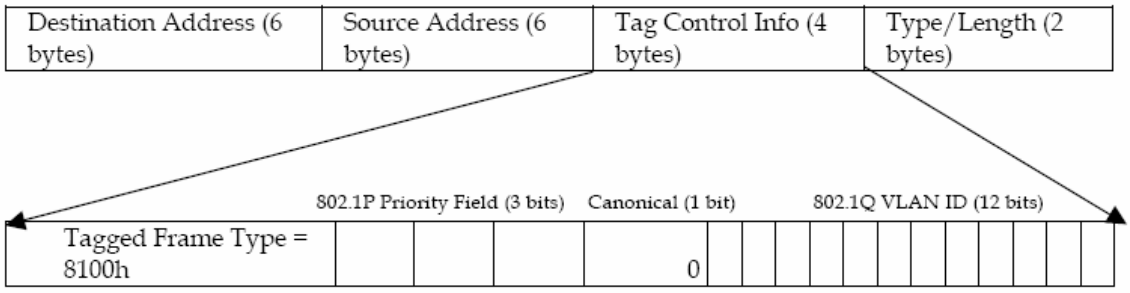



Fig. 3.3.4 Ethernet Layer 2 Header with 802.1p/Q information

802.1p QoS is sometimes referred to as QoS for the LAN since PC NIC cards mark the packets, and newer switches can prioritize the traffic in a switched network segment based on these markings. 802.1p has received a lot of interest lately because many IP Phones are

marking voice streams with an 802.1P bit setting of 5. For example, many Cisco IP phones set 802.1p and IP TOS to 5 for voice data streams.

**(2) 802.1p QoS Application**

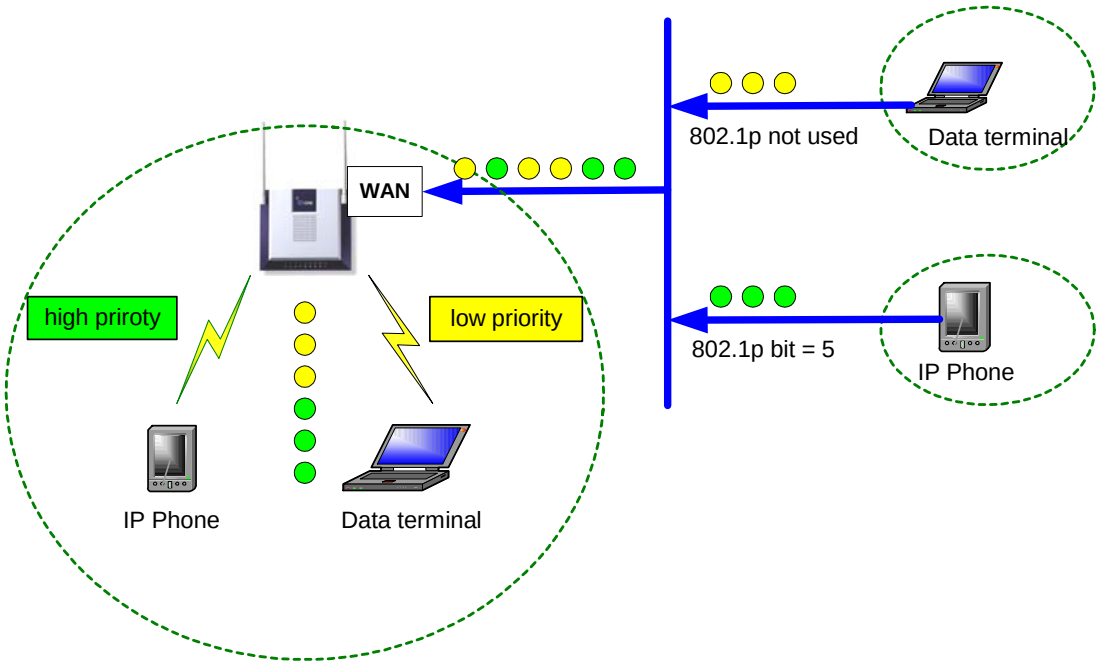



Fig. 3.3.5 802.1p Application

① Priority of traffic

AP supports 802.1p based downstream QoS. AP classifies incoming packets into 3 group according into their 802.p tag. Each packet is queued in AP. After serving all packets in the high priority queue, AP transmits packets in the low priority queue.

Table 3.3.1 802.1p priority bit and priority class in AP

| 802.1p priority bit | Priority class in AP |
|---|---|
| 7 (highest priority) | High priority |
| 6 | |
| 5 (Voice data stream) | Middle priority |
| 4 | |
| 3 | Low priority |
| 2 | |
| 1 | |
| 0 (lowest priority) | |

② Ingress Packet

AP classifies incoming packets into 3 group according into their 802.p priority bit. If there is no 802.1p tag in the packet, it is queued in the lowest priority queue.

③ Egress Packet

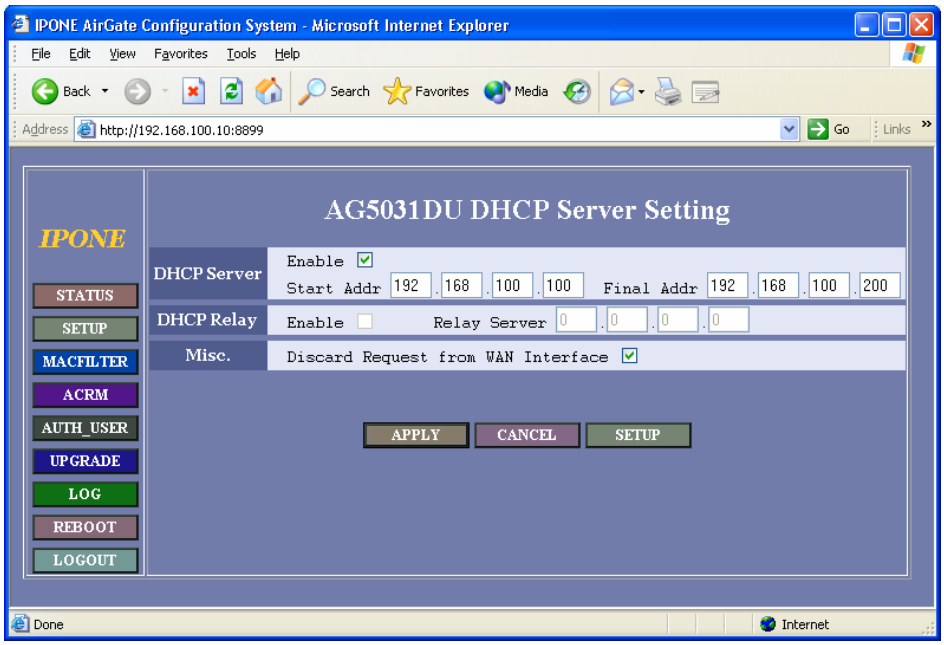
AP adds or removes the 802.1p/Q tag in packets outgoing to Ethernet or wireless port.

☞ Refer "Testing 802.1P QoS with Chariot Application Note," December 20, 2001.

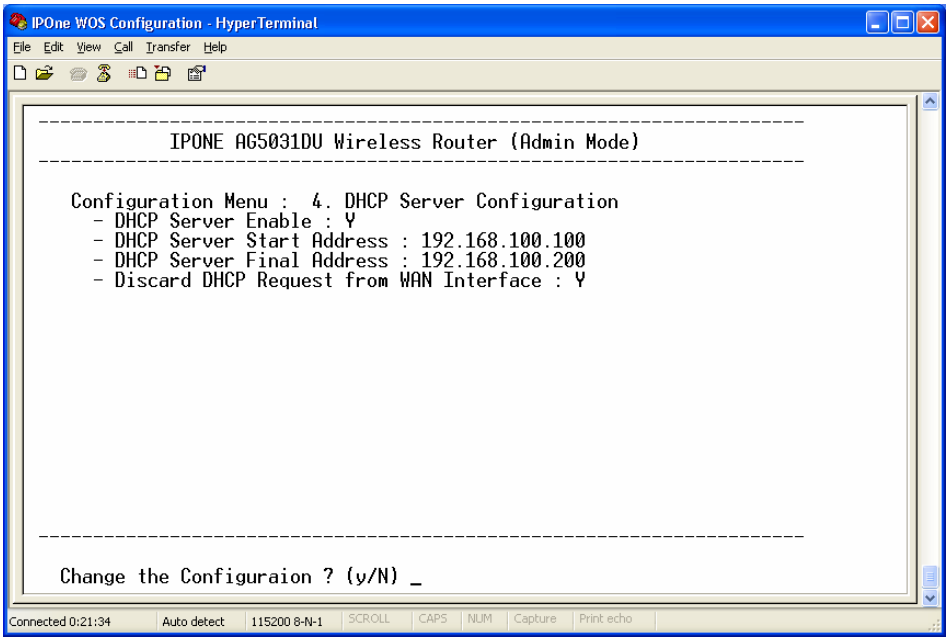
**(3) QoS Configurations**

| Item | Description |
|---|---|
| QoS | ➢ Downstream QoS (802.1p)<br>Enable or disable downstream QoS function.<br>➢ Tag: Ethernet<br>Enable: Add or keep 802.1p/Q tag in all packets outgoing to Ethernet port.<br>Disable: Remove 802.1p/Q tag of all packets outgoing to Ethernet port.<br>➢ Tag: Wireless<br>Enable: Add or keep 802.1p/Q tag in all packets outgoing to wireless port.<br>Disable: Remove 802.1p/Q tag of all packets outgoing to wireless port. |

## 3.4 Configuring DHCP Server




(a) WMS Screen




(b) CMS Screen

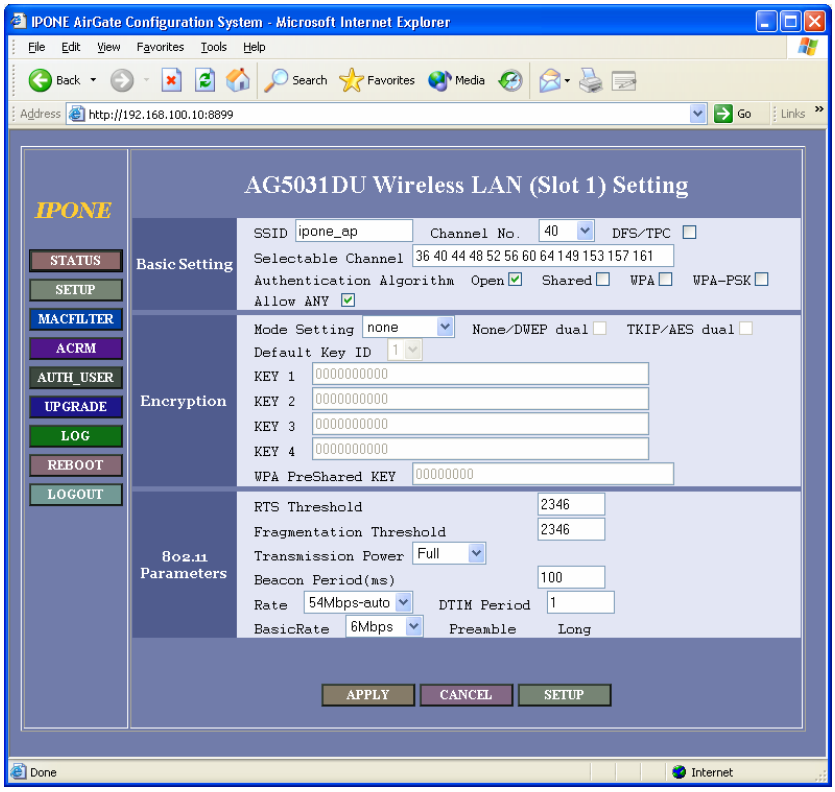
Fig. 3.4.1 Configuring DHCP server

- **Configurations**

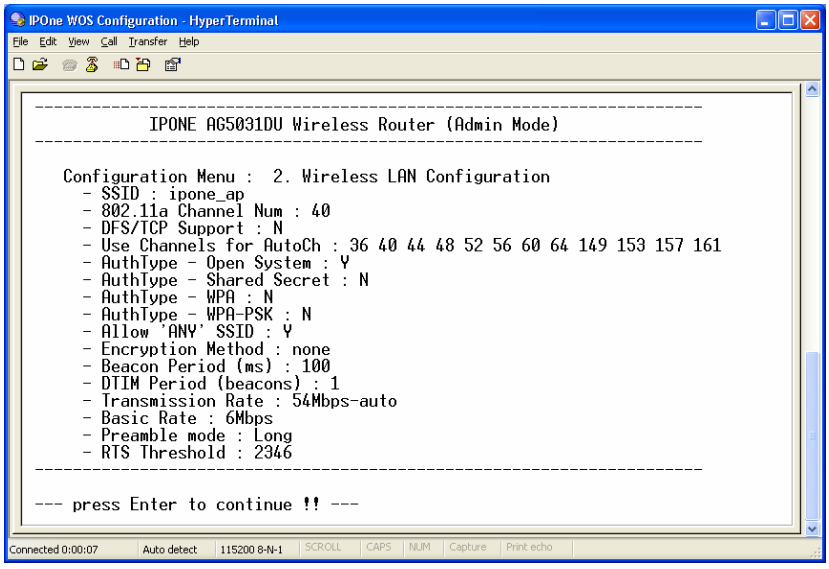
| Item | Description |
|---|---|
| DHCP Server | ➢ Enable: Enable or disable DHCP server function.<br>➢ Set the scope of assignable IP address. Enter the beginning value in "Start Addr.", and ending value in "Final Addr.". |
| DHCP Relay | ➢ Enable: Enable or disable DHCP relay function.<br>➢ Relay Server: Set the IP address of DHCP relay server.<br><br>☞ Cannot use both DHCP server and DHCP relay at the same time. |
| Misc. | ➢ Discard Request from WAN Interface: AP does not reply for the DHCP request packet from the network. |

## 3.5 Configuring Wireless LAN

### 3.5.1 5GHz IEEE 802.11a Radio Configuration




(a) WMS Screen




(b) CMS Screen

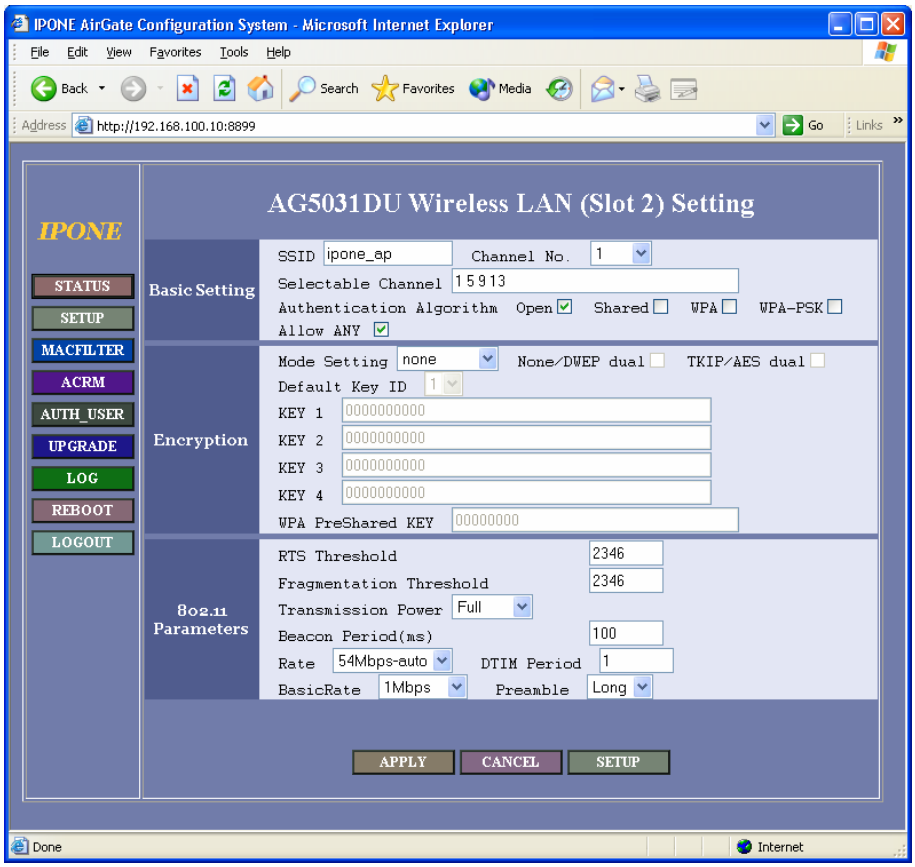
Fig. 3.5.1 Configuring Wireless LAN

- **Configurations**

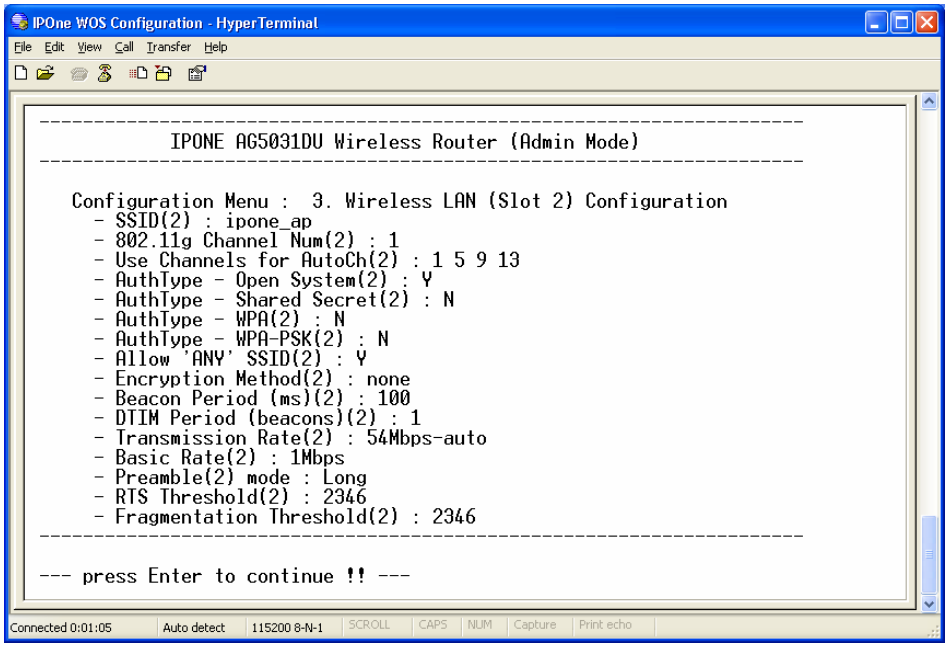
| Item | Description |
|---|---|
| SSID | An SSID is a unique identifier that wireless clients use to associate with the AP. Set an SSID by using any alphanumeric, case-sensitive entry from 1 to 32. |
| Channel | Set the default channel for AP radio. If you select "Auto," the channel number is automatically selected among the selectable channel considering channels used by neighbor's APs.<br>If you enable the "DFS/TPC" function, the AP's channel will be automatically changed when the radar signal is detected according to the IEEE 802.11h.<br><br>☞ Too many APs in the same vicinity creates radio congestion that can reduce throughput. |
| Selectable Channel | Set the channel list allowable to search. |
| Association Algorithm | Set the 802.11 authentication algorithm among Open System, Shared Secret, WPA, and WPA-PSK. Please, reboot the AP after changing the association algorithm between WAP (or WPA-PSK) and Open System (or Shared Secret). |
| Allow ANY | Disable this setting to prevent wireless client, which SSID is "ANY," from associating with the AP. If this function is disabled, wireless client cannot survey AP's SSID |
| Encryption | ➢ Mode Setting:<br>▪ **None**: Don't use encryption algorithm<br>▪ **WEP64/WEP128/WEP152**: Set the static 64/128/152 bit WEP (Wired Equivalent Privacy). The static WEP is an encryption protocol specified in IEEE 802.11 standard. One default key is used for encrypting or decrypting the data. Set the WEP key by using alphanumeric, 1~10 or A~F.<br>▪ **DWEP64/DWEP128**: Set the dynamic 64/128 bit WEP. In the dynamic WEP mode, the WEP key for a client is dynamically allocated from the AP after the AP receives the session key from the RADIUS server. Therefore, the dynamic WEP function must be used with IEEE 802.1x EAP-TTLS/PEAP authentication protocol. |

| | |
|---|---|
| | ■ **TKIP/AES**: Set the encryption algorithm when the WAP authentication is used.<br><br>➢ **None/DWEP dual**: Service all users using WEP as well as not using WEP at the same time.<br><br>➢ **TKIP/AES dual**: Service all users using TKIP as well as using AES. |
| Beacon Period | The amount of time between beacons in milliseconds. |
| DTIM Period | The setting, a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power save clients that a packet is waiting for them. |
| Transmission Rate | Choose the data rates the radio uses for data transmission. |
| Basic Rate | Choose the data rates the radio use for control data transmission. |
| Preamble mode | Choose the preamble mode, Long or Short. |
| RTS Threshold | This setting determines the packet size at which the AP issues a request to send (RTS) before sending the packet. |
| Fragmentation Threshold | This setting determines the size at which packets are fragmented (sent as several pieces instead of as one block). |
| Tx Power | This setting determines the power level of radio transmission. |

### 3.5.2 2.4GHz IEEE 802.11g Radio Configuration




(a) WMS Screen




(b) CMS Screen

Fig. 3.5.1 Configuring Wireless LAN

- **Configurations**

| Item | Description |
|---|---|
| SSID | An SSID is a unique identifier that wireless clients use to associate with the AP. Set an SSID by using any alphanumeric, case-sensitive entry from 1 to 32. |
| Channel | Set the default channel for AP radio. If you select "Auto," the channel number is automatically selected among the selectable channel considering channels used by neighbor's APs.<br>If you enable the "DFS/TPC" function, the AP's channel will be automatically changed when the radar signal is detected according to the IEEE 802.11h.<br><br>☞ Too many APs in the same vicinity creates radio congestion that can reduce throughput. |
| Selectable Channel | Set the channel list allowable to search. |
| Association Algorithm | Set the 802.11 authentication algorithm among Open System, Shared Secret, WPA, and WPA-PSK. Please, reboot the AP after changing the association algorithm between WAP (or WPA-PSK) and Open System (or Shared Secret). |
| Allow ANY | Disable this setting to prevent wireless client, which SSID is "ANY," from associating with the AP. If this function is disabled, wireless client cannot survey AP's SSID |
| Encryption | ➢ Mode Setting:<br>▪ **None**: Don't use encryption algorithm<br>▪ **WEP64/WEP128/WEP152**: Set the static 64/128/152 bit WEP (Wired Equivalent Privacy). The static WEP is an encryption protocol specified in IEEE 802.11 standard. One default key is used for encrypting or decrypting the data. Set the WEP key by using alphanumeric, 1~10 or A~F.<br>▪ **DWEP64/DWEP128**: Set the dynamic 64/128 bit WEP. In the dynamic WEP mode, the WEP key for a client is dynamically allocated from the AP after the AP receives the session key from the RADIUS server. Therefore, the dynamic WEP function must be used with IEEE 802.1x EAP-TTLS/PEAP authentication protocol. |

| | |
|---|---|
| | ■ **TKIP/AES**: Set the encryption algorithm when the WAP authentication is used.<br><br>➢ **None/DWEP dual**: Service all users using WEP as well as not using WEP at the same time.<br><br>➢ **TKIP/AES dual**: Service all users using TKIP as well as using AES. |
| Beacon Period | The amount of time between beacons in milliseconds. |
| DTIM Period | The setting, a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power save clients that a packet is waiting for them. |
| Transmission Rate | Choose the data rates the radio uses for data transmission. |
| Basic Rate | Choose the data rates the radio use for control data transmission.<br><br>☞ In an 802.11g AP, the basic rate must be set as a one of 1, 2, 5.5, and 11Mbps of 802.11b standard. |
| Preamble mode | Choose the preamble mode, Long or Short. |
| RTS Threshold | This setting determines the packet size at which the AP issues a request to send (RTS) before sending the packet. |
| Fragmentation Threshold | This setting determines the size at which packets are fragmented (sent as several pieces instead of as one block). |
| Tx Power | This setting determines the power level of radio transmission. |

## 3.6 Configuring Authentication and Accounting

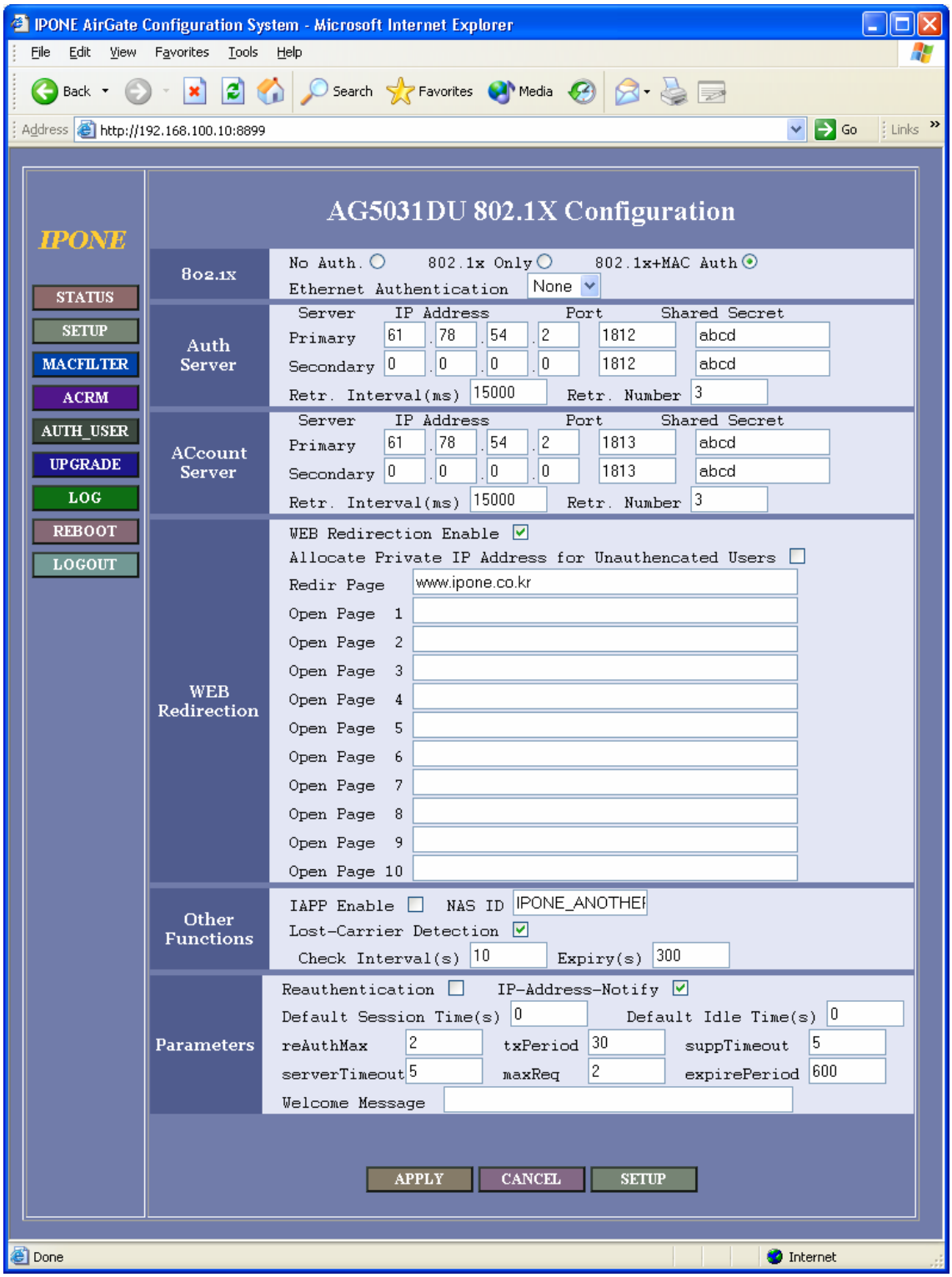
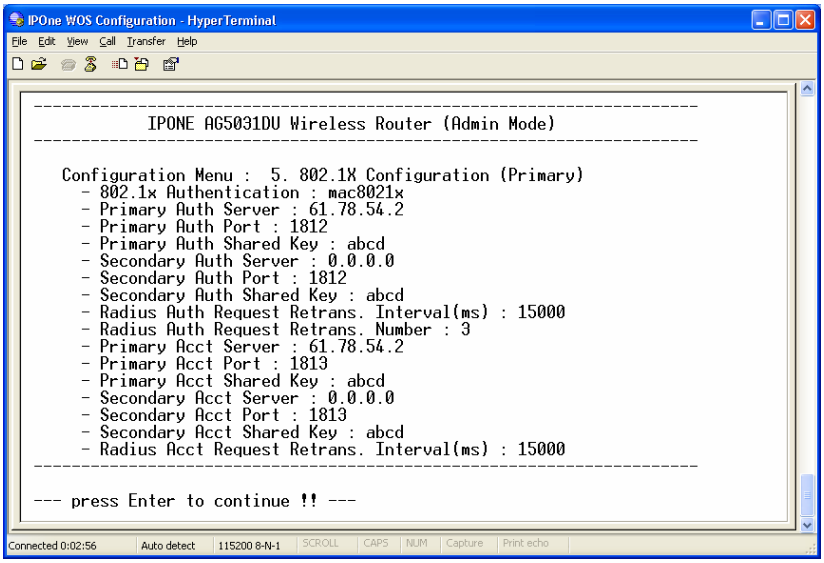
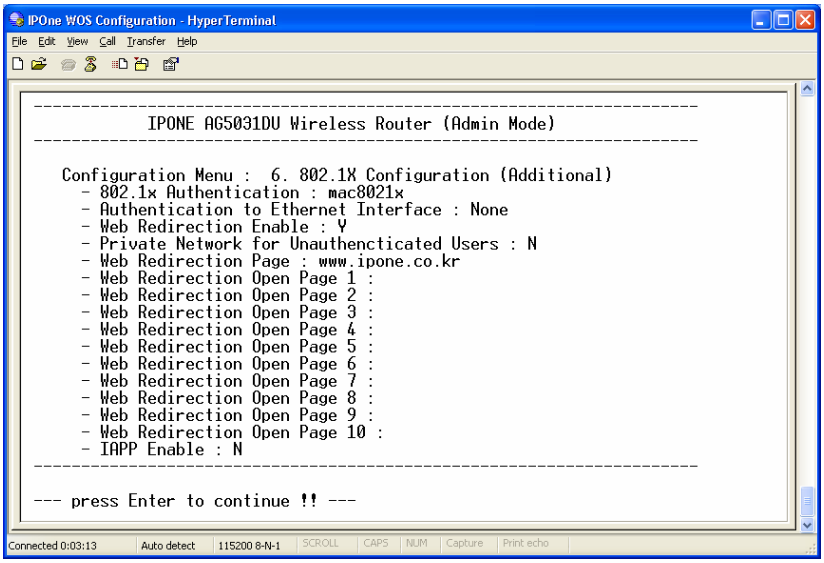



Fig. 3.6.1 Configuring Authentication and Accounting (WMS)



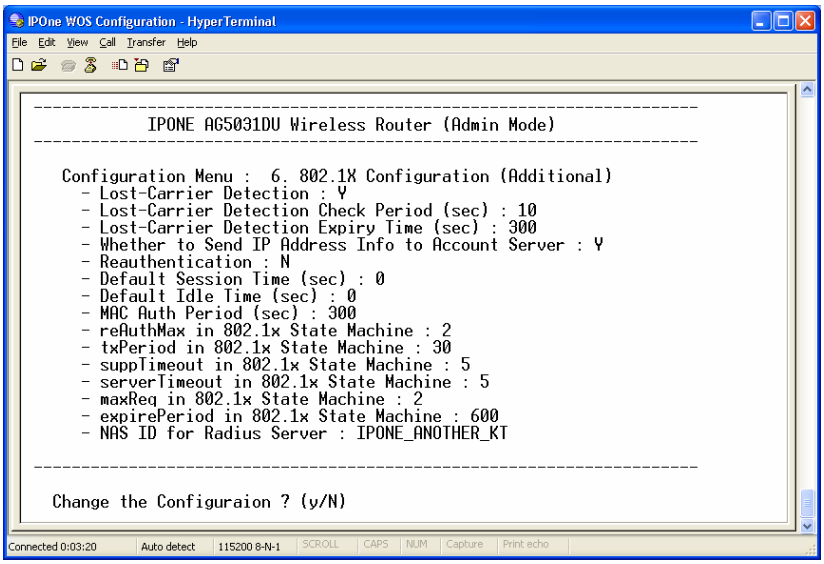




Fig. 3.6.2 Configuring Authentication and Accounting (CMS)

- **Configurations**

| Item | Description |
|---|---|
| 802.1x | ➢ Choose one IEEE 802.1x authentication mode among [No Auth], [802.1x Auth], or [802.1x+MAC Auth].<br>➢ [No Auth]: The 802.1x authentication is not used.<br>➢ [802.1x Auth]: The 802.1x authentication is used.<br>➢ [802.1x+MAC Auth]: Both 802.1x authentication and MAC authentication are all used.<br><br>☞ For MAC authentication, the MAC address of an client must be registered in the authentication server. The method of registering it is the same as that of registering 802.1x users. |
| Auth Server | ➢ Set IP address, Port number, and Shared Secret of primary authentication server and secondary authentication server.<br>➢ The AP retransmits a request until a certain number (Retr. Number) after waiting for answer for a time (Retr. Interval) if it does not receive any reply after requesting. |
| Account Server | ➢ Set IP address, Port number, and Shared Secret of primary accounting server and secondary accounting server.<br>➢ The AP retransmits a request until a certain number (Retr. Number) after waiting for answer for a time (Retr. Interval) if it does not receive any reply after requesting. |
| WEB Redirection | ➢ When a guest user (unauthenticated user) accesses the Internet by using Web browser, his Web page request is redirected the designated Web page. Here, the AP allocates a private or public IP address to the guest user.<br>➢ Set the site of the designated Web page in "Redir Page." And set the site of the Web pages, which the guest user can access, in "Open Page 1~10."<br><br>☞ To allocate a private IP address to the guest user, the NAT mode must not be enabled. Moreover, the IP address of AP must not be 10.10.10.x. |

- **Advanced Configurations**

| Item | Description |
|---|---|
| IAPP | This setting determines the usage of IEEE 802.1f IAPP function. |
| NAS ID | Set the NAS ID when the AP sends a packet to an authentication server. |
| Lost Carrier Detection (*Note 1*) | The function of LCD (Lost Carrier Detection) is sometimes called by POD (Pull Out Detection). This setting is used to detect wireless clients which were moved away or detached wireless adapter without logout. If the AP detects a wireless client moved away, it sends accounting information of the wireless client to an accounting server and closes the session of the client.<br><br>☞ This function of LCD help to accumulating accurate accounting information of an client. Moreover, this prevent from managing the unnecessary associations of clients.<br>☞ This setting can be enabled only when 802.1x authentication is enabled. |
| Reauthentication | This setting determines whether the client will be reauthenticated or not after session-timeout or idle-timeout. |
| Session Timeout | This setting determines the timer value for session timeout. The value of '0' means no usage of this function.<br><br>☞ The value will be replaced with the value received from the authentication server. |
| Idle Timeout | This setting determines the timer value for idle timeout. The value of '0' means no usage of this function.<br><br>☞ The value will be replaced with the value received from the authentication server. |
| reAuthMax | In 802.1x module, the number of reauthentication attempts that are permitted before the Port becomes Unauthorized. The default value is 2. |
| txPeriod | In 802.1x module, the timer value to wait for reply from the wireless client when the AP transmits an authentication request packet to the client. |
| suppTimeout | In 802.1x module, the timer value to wait for reply from the wireless client when the AP transmits a request packet received from an authentication server to the client. |

| | |
|---|---|
| serverTimeout | In 802.1x module, the timer value to wait for replay from the authentication server when the AP transmits an authentication packet to the server. |
| maxReq | In 802.1x module, the maximum number of times that the AP request an authentication of a wireless client before it times out the authentication session. |
| expirePeriod | The timer value when the AP manages the 802.1x state of an unauthenticated client. |
| Welcome Messages | The notification message to be sent to a client when it was authenticated successfully.<br><br>☞ This message will be replaced the message received from the authentication server. |

☞ (Note 1) LCD Algorithm

When the function of LCD is enabled, the AP periodically monitors the wireless link of a client every the time of "Check Interval." The AP decides the client to be disassociated when the client doesn't answer for a time of "Expiry."

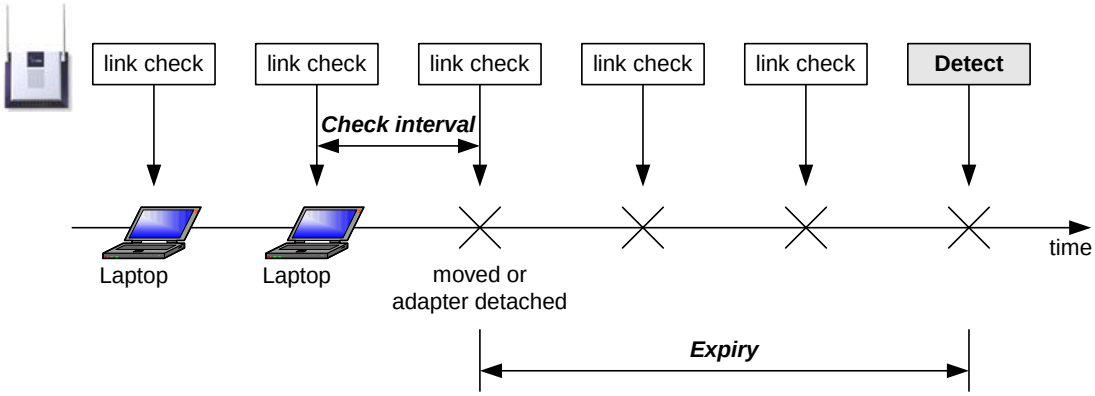
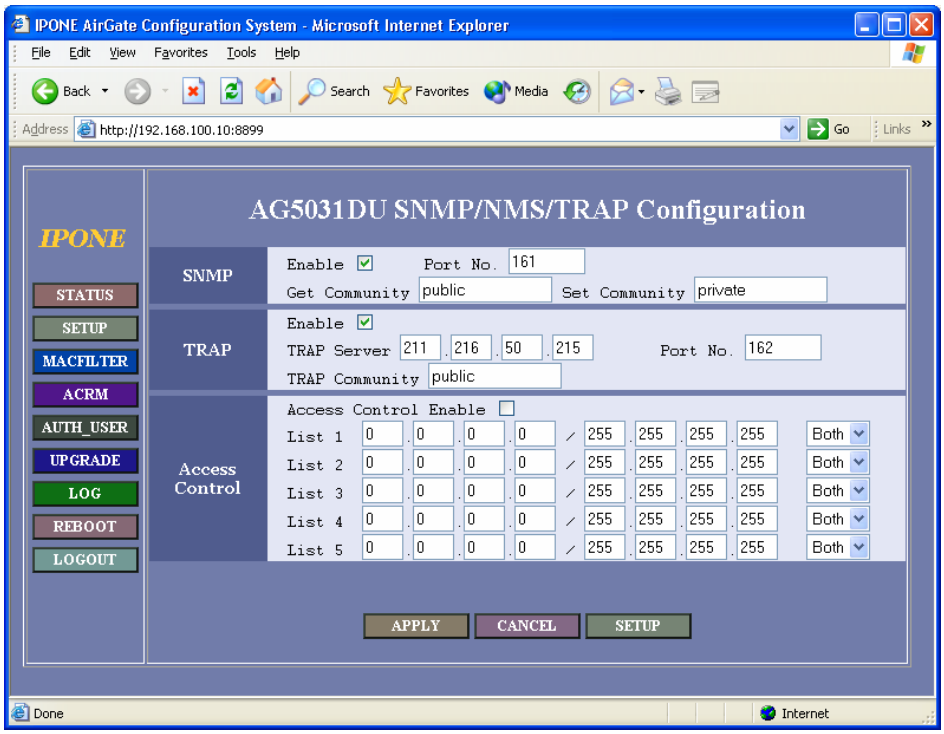
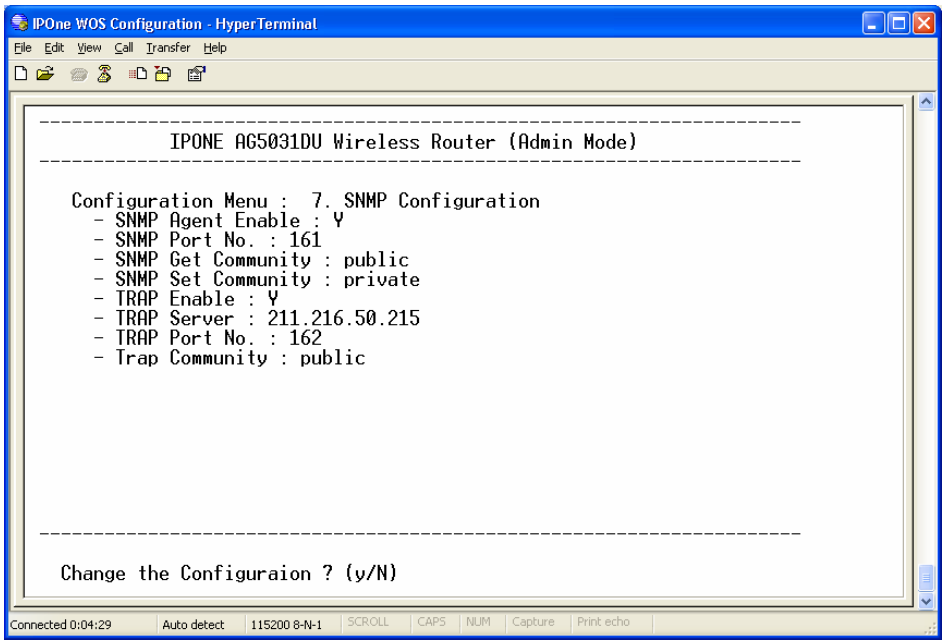



Fig. 3.6.3 LCD operation

## 3.7 Configuring SNMP




(a) WMS Screen




(b) CMS Screen

Fig. 3.7.1 Configuring SNMP

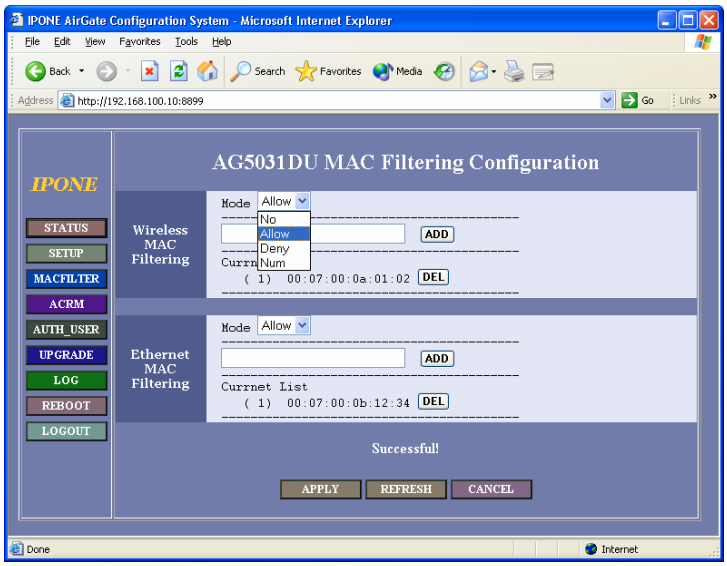
- **Configurations**

| Item | Description |
|---|---|
| SNMP | ➢ Enable: Enable or disable the SNMP function.<br>➢ Port No: SNMP port number.<br>➢ Get Community: SNMP Get Community.<br>➢ Set Community: SNMP Set Community. |
| TRAP | ➢ Enable: Enable or disable the TRAP function.<br>➢ TRAP Server: IP address of TRAP server.<br>➢ Port No: TRAP port number.<br>➢ TRAP Community: TRAP Community. |
| Access Control | ➢ Enable: This setting allows the specific clients to access the SNMP server of the AP.<br>➢ List 1~5: Set IP addresses of clients which can access the SNMP server of the AP. |

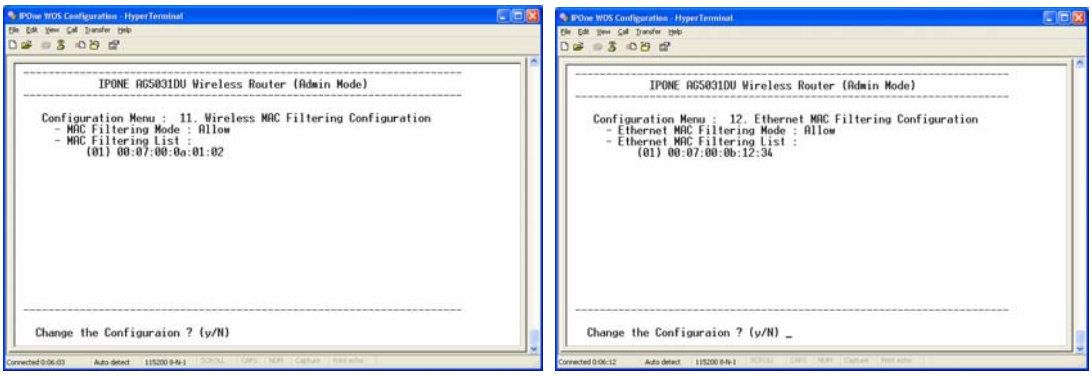
## 3.8 Configuring MAC Filtering and ACRM

### 3.8.1 MAC Filtering

MAC address filtering allows or disallows the forwarding of packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify.




(a) WMS Screen




(b) CMS Screen

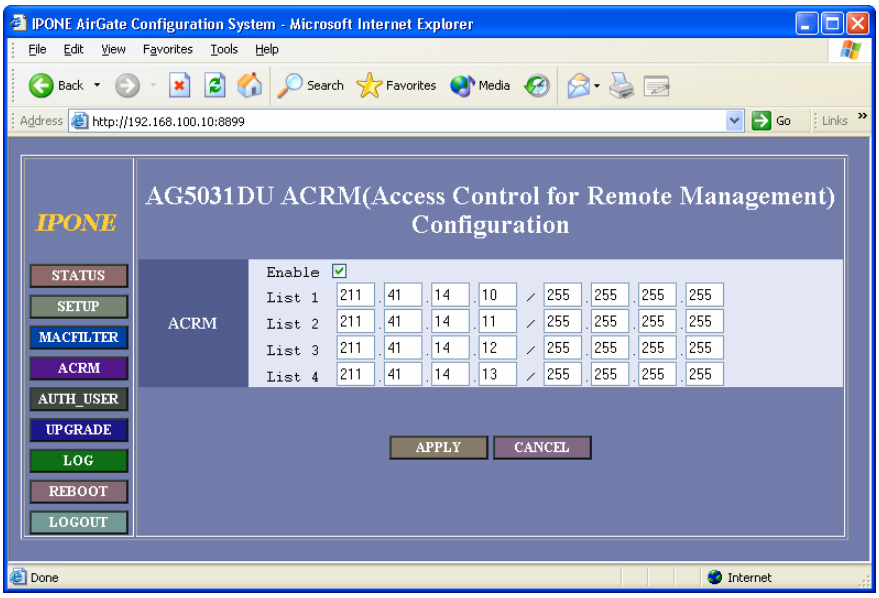
Fig. 3.8.1 Configuring MAC Filtering

- **Configurations**

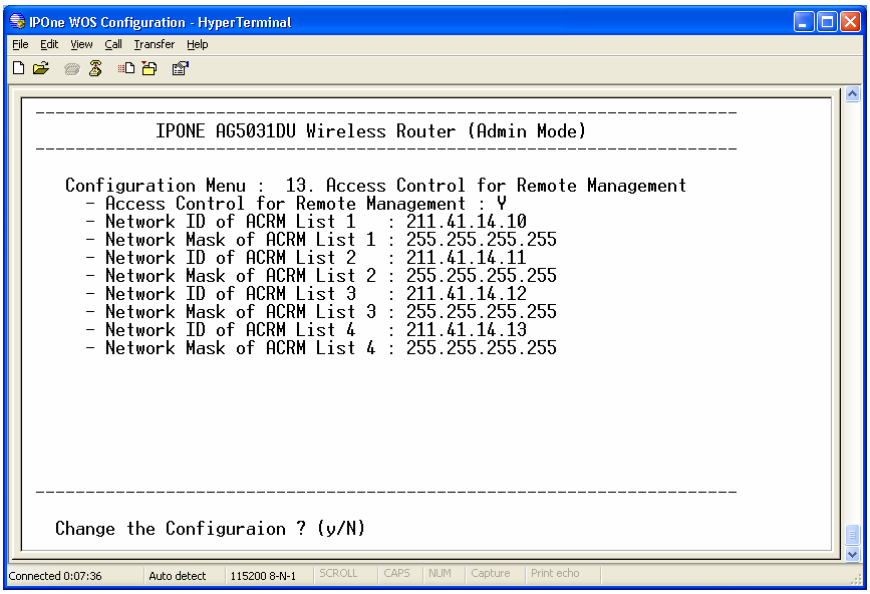
| Item | Description |
|---|---|
| MAC Filtering | Mode: Choose one among [No], [Allow], [Deny], or [Num].<br><br>➢ No: Don't use this function.<br>➢ Allow: Choose this to allow the forwarding of packets either sent from or addressed to registering MAC addresses.<br>➢ Deny: Choose this to disallow the forwarding of packets either sent from or addressed to registering MAC addresses.<br>➢ Num: Set the maximum number of MAC addresses allowed to forward packets. If there is no packet either sent from or addressed to a MAC address during a time, "Expiry Timeout", the MAC address will be removed in the registered list.<br><br>☞ MAC filtering of Ethernet interface may be different from that of wireless interface according into models. |

### 3.8.2 ACRM (Access Control for Remote Management)

ACRM (Access Control for Remote Management) function allows only specific clients to access AP's management system by using Web browser or Telnet.




(a) WMS Screen




(b) CMS Screen

Fig. 3.8.1 Configuring ACRM

- **Configurations**

| Item | Description |
|---|---|
| ACRM | ➢ Enable: Enable or disable ACRM function.<br>➢ List 1 ~ List 4: Set IP addresses of clients who can access AP's management system by using Web browser or Telnet. |

## 3.9 Configuring Mobile IP Foreign Agent

☞ Mobile IP Foreign Agent function is only supported in high Enterprise high-level AP product such as AG5031DU plus model.

**(1) Introduction to Mobile IP**

The wireless technologies such as IEEE 802.11 wireless LAN enables mobile devices such as laptops or handheld computers not to be restricted to access provided by Ethernet wiring. As the reach of wireless coverage expands beyond the campus to metropolitan, national, and global levels, it is more important that maintaining connectivity with a client's home network and seamless roaming between different subnets.

However, the IP address of a mobile device should be changed whenever it moves from one network to another. Hence, a mobile user experiences a disconnection of Internet whenever roaming across subnets. As a result, the Internet Engineering Task Force (IETF) has standardized Mobile IP to allow mobile users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between different IP networks.

The Mobile IP standard is based on a few components described below:

- Mobile Node (MN): A mobile node is a device such as a laptop or PDA that has Mobile IP client software to change its location without changing its IP address.
- Home Agent (HA): A home agent is a router on a mobile node's home network that tunnels datagram for delivery to the mobile.
- Foreign Agent (FA): A foreign agent is a router on a mobile node's visited network that provides routing services to the mobile node while registered.

**(2) Mobile IP operations**

A clear understanding of Mobile IP requires a foundation knowledge of Mobile IP standard, IETF RFC 2002 document. Figure 3.9.1 shows an example of Mobile IP applications. In order for an MN successfully roam across subnets its home IP address must be registered in the HA. The HA contains a list of all MNs' IP addresses. After the MN roams to a new network (foreign network), it registers with the HA as being away from home through the FA. The FA includes a care-of-address (CoA) in the registration it sends to the HA. A tunnel is then build between the HA and the FA which has the CoA for all traffic destined for the MN.

There are two tunneling methods, triangle tunneling and reverse tunneling. The triangle tunneling is firstly explained. When an MN sends traffic to the target device such as a web server using its home IP address, the outbound traffic are routed directly to the target

destination device. The destination device replies to the source IP address, resulting in the traffic being routed the home agent. The HA then forwards the traffic through the tunnel to the FA, which forwards it to the MN.

However, in the reverse tunnel, the outbound traffic from the MN are sent to the target device through the HA not sent directly to the target device.

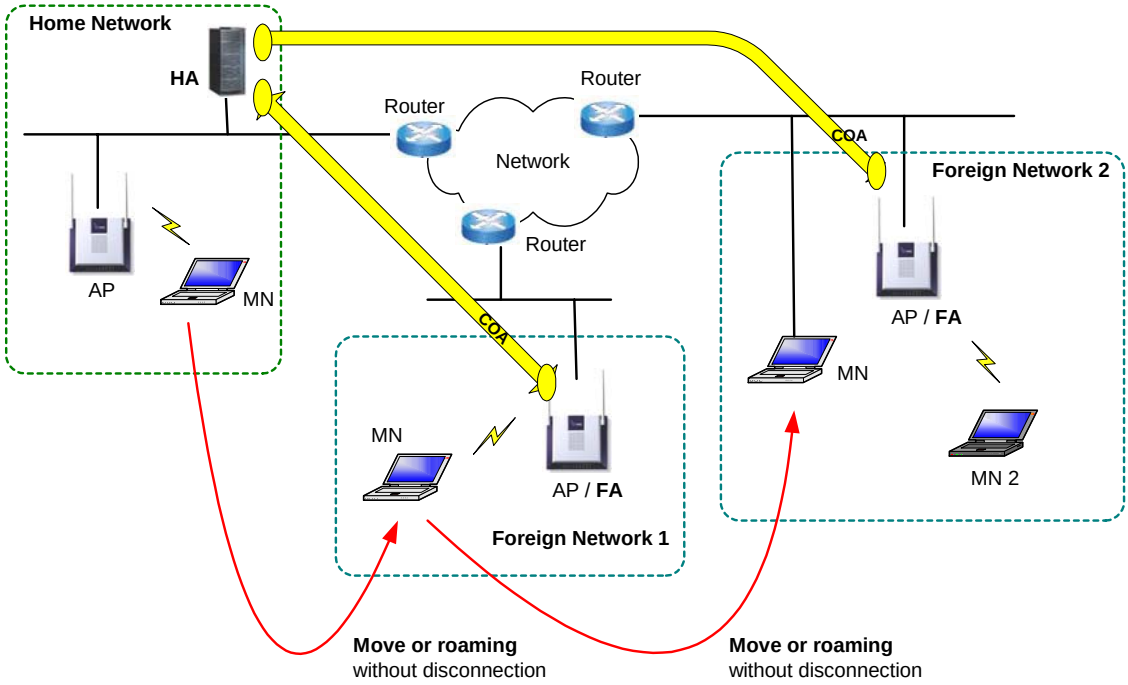
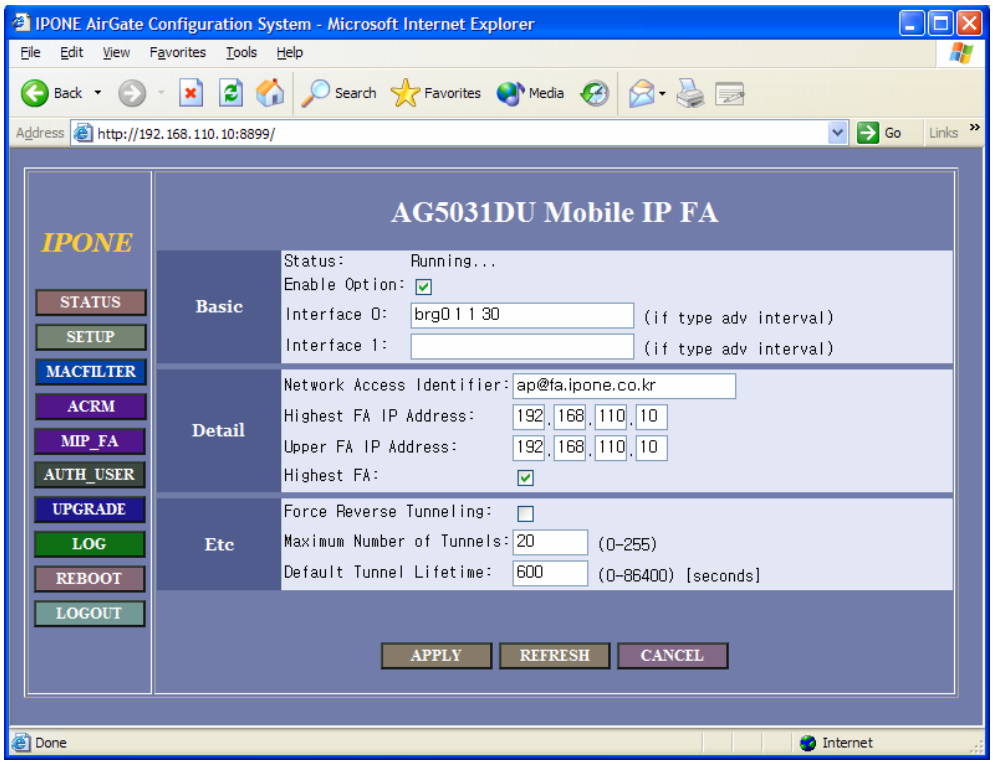
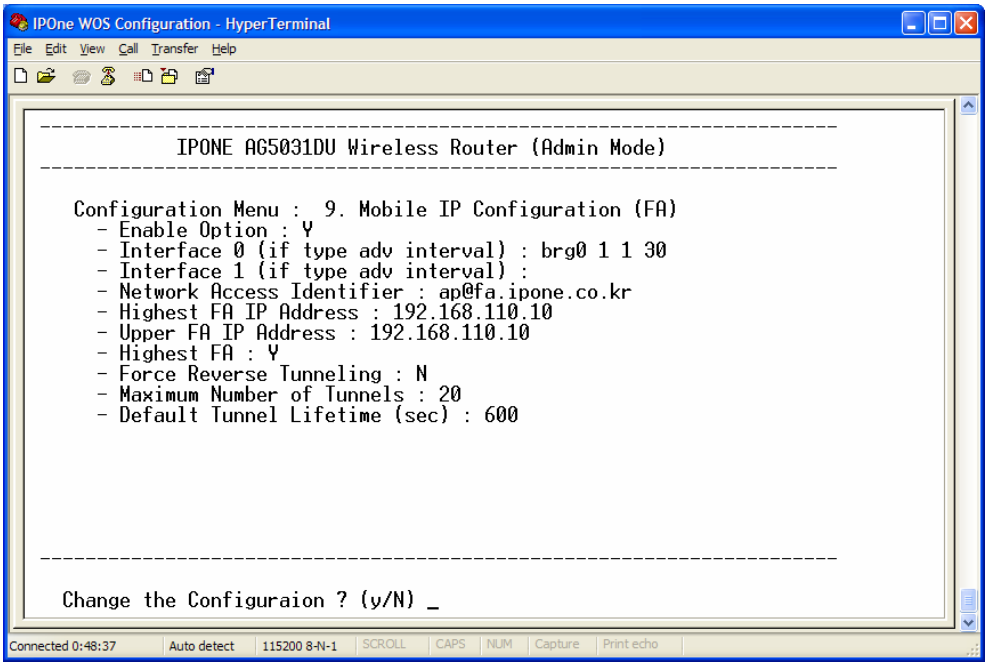



Fig. 3.9.1 Mobile IP operation

### (3) Mobile IP Foreign Agent Configurations




(a) WMS Screen




(b) CMS Screen

Fig. 3.9.2 Configuring Mobile IP Foreign Agent

- **Configurations**

| Item | Description |
|---|---|
| Status | Display the status of running. |
| Enable | Run the Mobile IP foreign agent. |
| Interface | You can set two interfaces to be used for Mobile IP services. You must set one interface at least.<br>The interface is configured as the follows:<br>interface type agentadv interval force_IP_addr<br>ex) brg0 1 1 30<br>➢ [interfaces] name of the interface, e.g., brg0 (recommend), eth0, eth1<br>➢ [type] direction for Mobile IP services, e.g, 1, 2, 3.<br>• 1 = both upper and lower direction (recommend)<br>• 2 = only upper direction<br>• 3 = only lower direction<br>➢ [agentadv] send agent advertisement message or not, e.g, 0, 1, -1.<br>• 0 = do not send agent advertisements without agent solicitation<br>• 1 = send agent advertisements regularly<br>• -1 = do not send any (even solicited) agent advertisements<br>➢ [interval] number of seconds to wait between two agentadvs.<br>➢ [force_IP_addr] local address to be forced for this interface. If not entered, the primary address of the interface is used. |
| NAI | ➢ Network Address Identifier (NAI) of this FA. |
| Highest FA IP Address | ➢ Address of the highest FA in hierarchical architecture. This address is used in the communication with the HA and it is advertised in agent advertisement messages as a CoA (Care-of-Address).<br>☞ If the address of the AP is private address allocated from NAT, this "Highest FA IP Address" should be from the "public side" interface of the NAT router. Mobile IP may not be operated well in NAT configurations. It depends on the operation of NAT. |
| Upper FA IP Address | ➢ Address of the upper FA in hierarchical architecture. This is the address of the FA to which the requests are forwarded on they way to the Home Agent. If this is the same as FA's own IP address, then this FA is really the highest FA and the requests are forwarded directly to the Home Agent. |

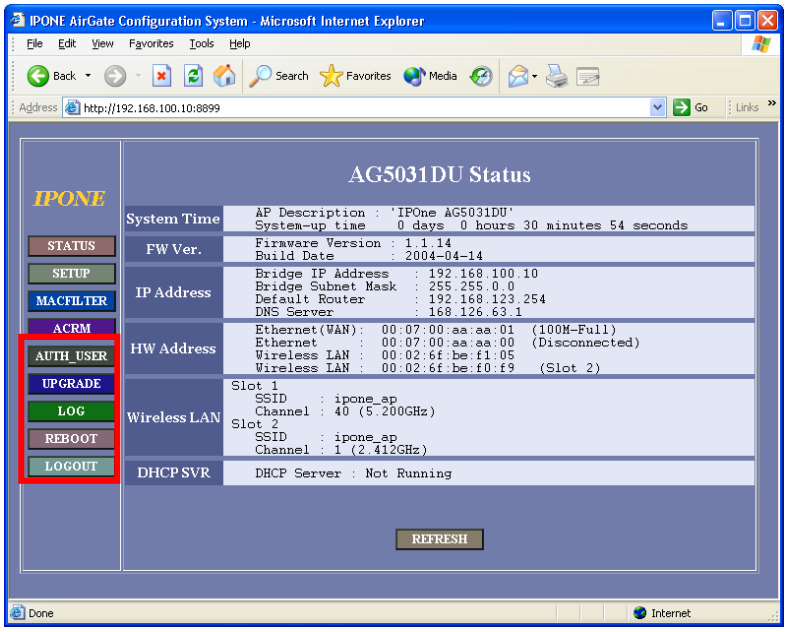
| | |
|---|---|
| Highest FA | ➢ Where this FA is the highest FA or not [TRUE \| FALSE]. The highest FA does not have any upper FAs. |
| Force Reverse Tunneling | ➢ Force FA to use reverse tunneling even if triangle tunneling is requested. |
| Max. Number of Tunneling | ➢ The maximum number of tunnels (bindings) going through this FA. If more than this number Mobile Nodes try to register, the new registrations are refused. |
| Default Tunnel Lifetime | ➢ Default Tunnel Lifetime is the maximum lifetime advertised for this FA. This should not be greater than any of the maximum lifetime configured for upper FAs.<br><br>☞ 65535 (or more) seconds mean unlimited time (the binding will not expire). |

## 3.10 Configuring Management Functions

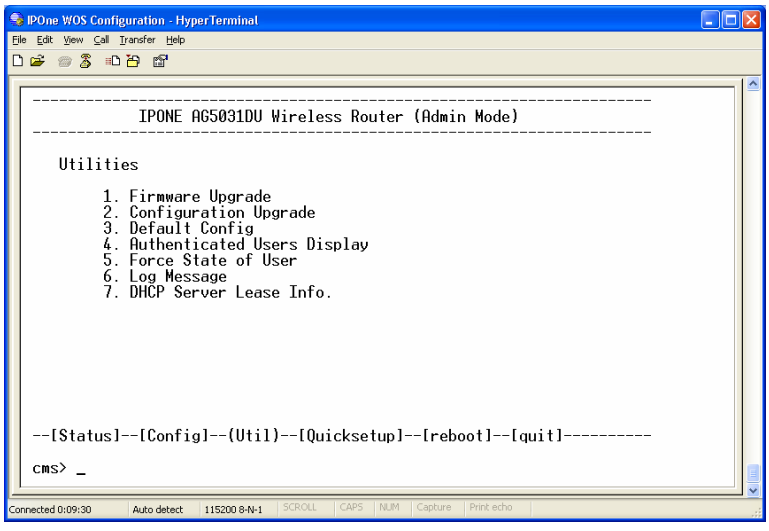
There are several functions for management as follows:

- Display Authenticated User's Information
- Updating Firmware
- Showing System Log
- Restarting System
- Logout

In CMS, the management functions are located at [Utility] menu.




(a) WMS Screen

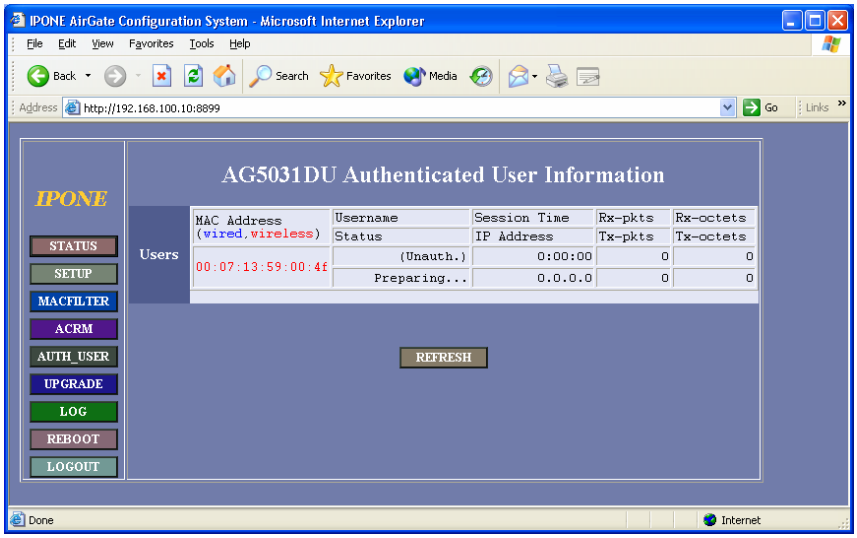



(b) CMS Screen

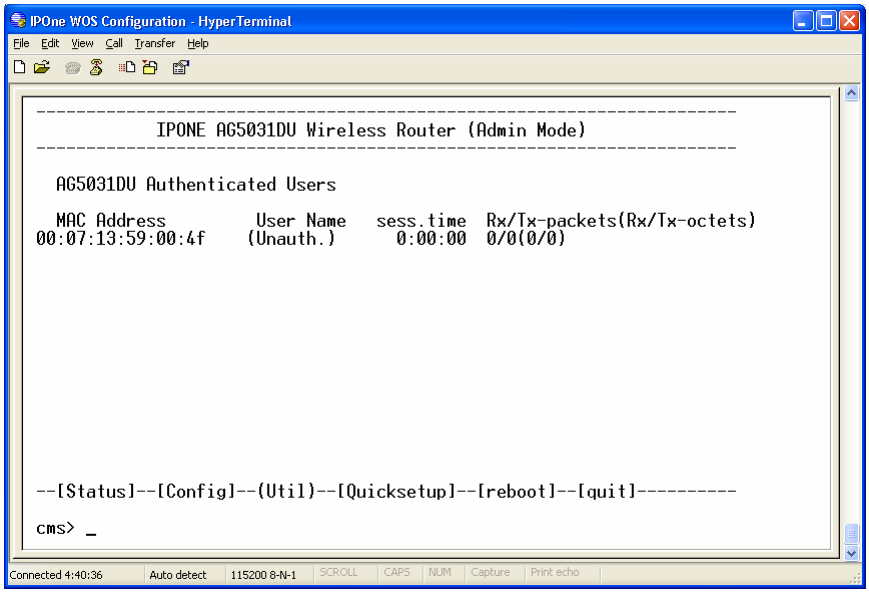
Fig. 3.10.1 Configuring Management Functions

### 3.10.1 Authenticated Users Information

The management system's Authenticated Users Information page lists all the authenticated users which the AP is aware.




(a) WMS Screen




(b) CMS Screen

Fig. 3.10.2 Authenticated User Information

- **Configurations**

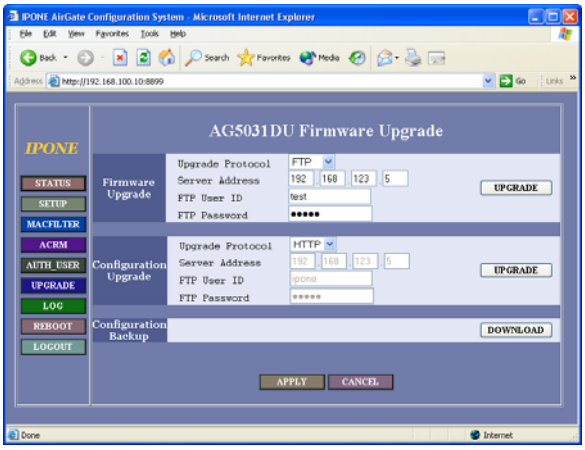
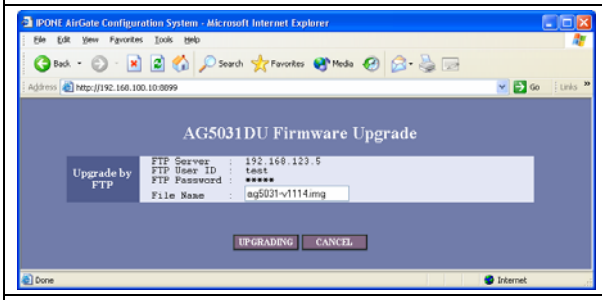
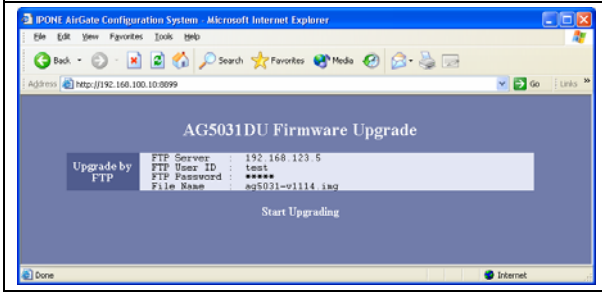
| Item | Description |
|---|---|
| Username | User name used to authenticate. |
| Status | Current status of a client:<br>➢ Preparing: The client didn't request for authenticating<br>➢ Authenticating: The client is being authenticated by using an 802.1x protocol.<br>➢ Authenticated: The client was authenticated by using an 802.1x protocol.<br>➢ MAC Authenticating: The client is now authenticated by using a MAC address authentication method.<br>➢ MAC Authenticated: The client was authenticated by using a MAC address authentication method.<br>➢ forced_auth: The AP forced the client to be authenticated.<br>➢ forced_unauth: The AP forced the client to be unauthenticated. |
| Session Time | Service time from authentication. |
| IP Address | IP address of the client. |
| Rx-pkts | The number of packets received at the client. |
| Tx-pkts | The number of packets transmitted from the client. |
| Rx-octets | The number of bytes received at the client. |
| Tx-octets | The number of packets transmitted from the client. |

### 3.10.2 Updating Firmware

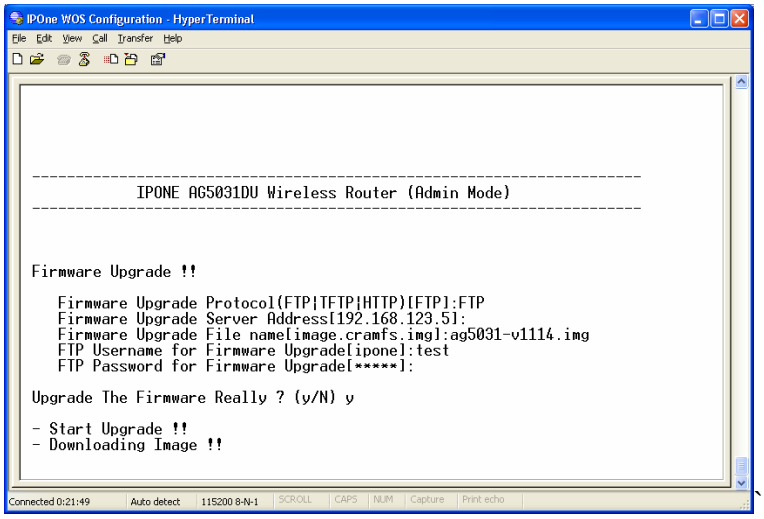
You can perform the update the AP's firmware, WOS version, by using several protocols, FTP, TFTP, or HTTP. Moreover, you can update or back up the AP's configuration file.

#### (1) Updating Firmware by using FTP

To update the AP's firmware or configuration file by using FTP, you set the IP address of FTP server, id and password for FTP. Moreover, you must know the name of the firmware or the configuration which you want to update.

| | |
|---|---|
|  | STEP 1: Select the "Upgrade Protocol" as "FTP." After configuring the following items, click "UPGRAD" button.<br>- FTP Server Address<br>- FTP User ID<br>- FTP Password |
|  | STEP 2: Input the firmware file name and then click "UPGRADING" button. |
|  | STEP 3: The updating will be started. After downloading, the AP will be restarted. |

(a) WMS Screen




(b) CMS Screen

Fig. 3.10.2(a) Updating Firmware by using FTP

**(2) Updating Firmware by using HTTP**

To update the AP's firmware or configuration file by using HTTP, there is the firmware or configuration in your PC.

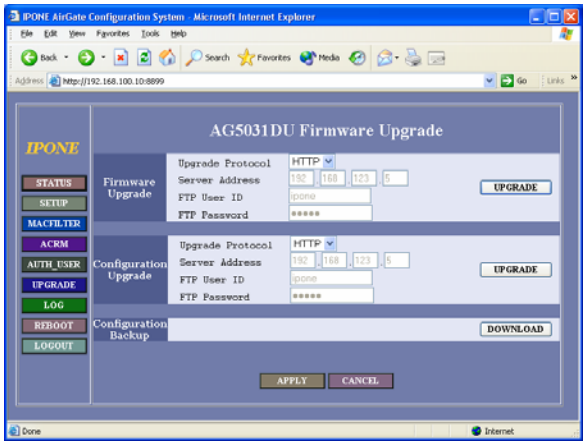
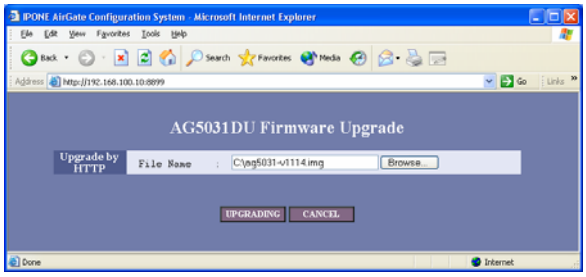
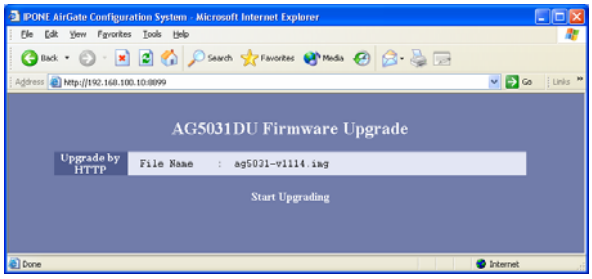
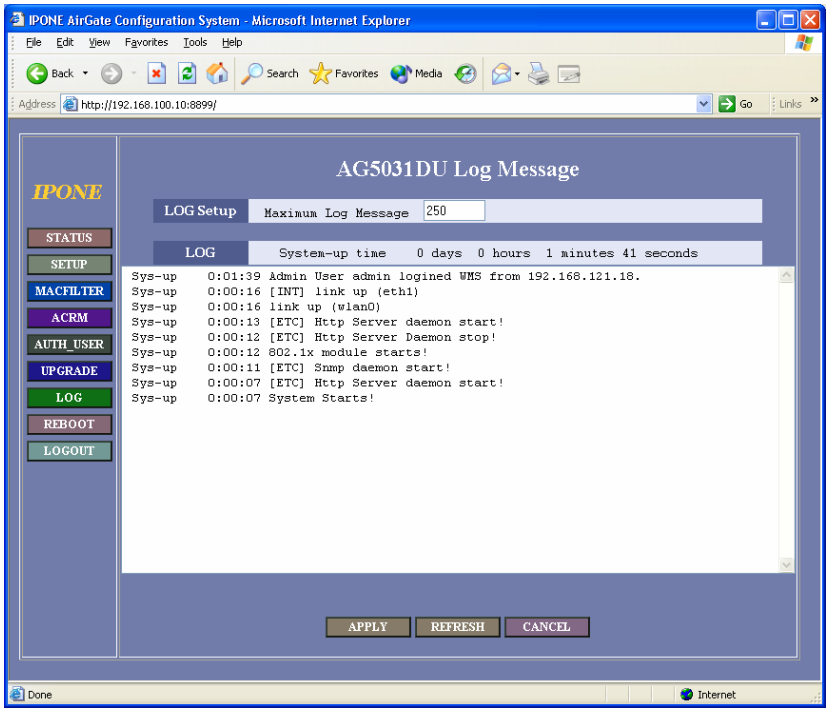
| | |
|---|---|
|  | STEP 1: Select the "Upgrade Protocol" as "HTTP." After then, click "UPGRAD" button. |
|  | STEP 2: Input the firmware file name by clicking the "Browse" button. |
|  | STEP 3: The updating will be started. After downloading, the AP will be restarted. |

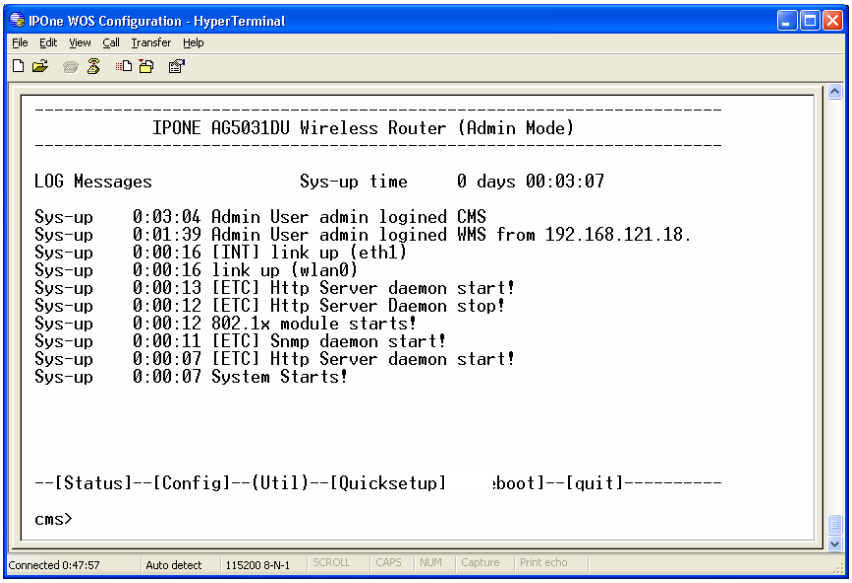
Fig. 3.10.2(b) Updating Firmware by using HTTP

### 3.10.3 System Log

You can see the list logged by the AP. The default value of the number of logs is 80. The log is listed by system time.




(a) WMS Screen




(b) CMS Screen

Fig. 3.10.4 System Log.

### 3.10.4 System Reboot and Logout

You can restart the AP by clicking the "REBOOT" button in WMS, or by entering "reboot" in CMS.

You can log off the AP's management system by clicking the "LOGOUT" button in WMS, or by entering "quit" in CMS.

# CHAPTER 4. AP Configurations According to Operation Mode

## 4.1 AP Configurations in Bridge mode

All physical interfaces of the AP in the Bridge mode use one IP address. In this mode, you must set the following configurations.

| Step | Item |
|---|---|
| 1 | Configure system mode as a Bridge mode. |
| 2 | Configure TCP/IP settings. |
| 3 | Configure Wireless LAN settings. |
| 4 | Configure Authentication and Accounting. |

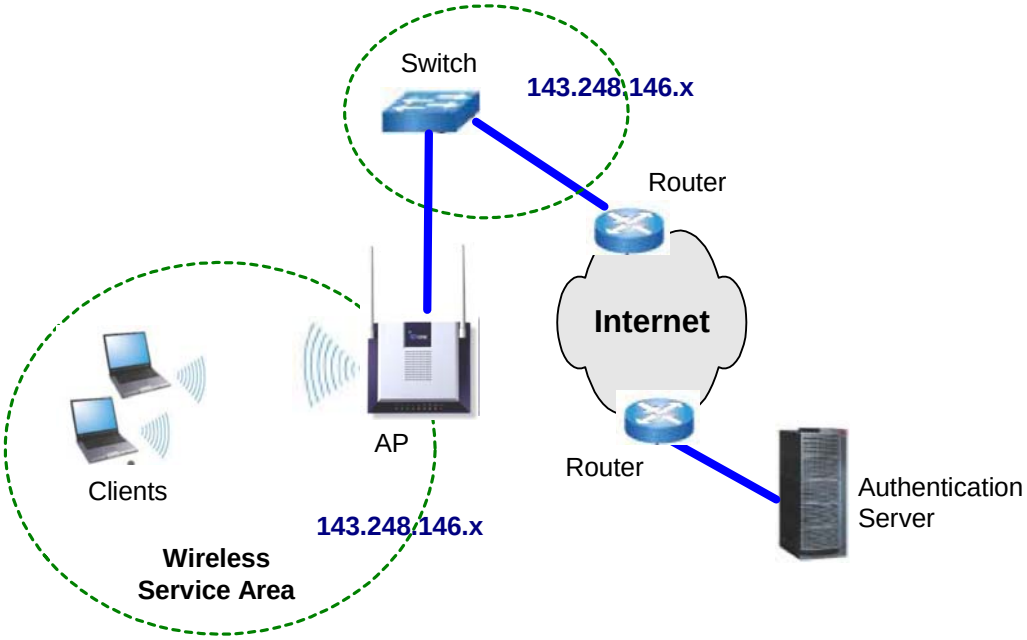



Fig. 4.1.1 Application example when the AP is used as a Bridge.

## 4.2 AP Configurations in Routed mode

In the Routed mode, the WAN interface and the other interfaces (wireless interface, local Ethernet) are set as a different IP address. In this mode, you must set the following configurations.

| Step | Item |
|---|---|
| 1 | Configure system mode as a Routed mode. |
| 2 | Configure TCP/IP settings. |
| 3 | Configure Wireless LAN settings. |
| 4 | Configure Authentication and Accounting. |

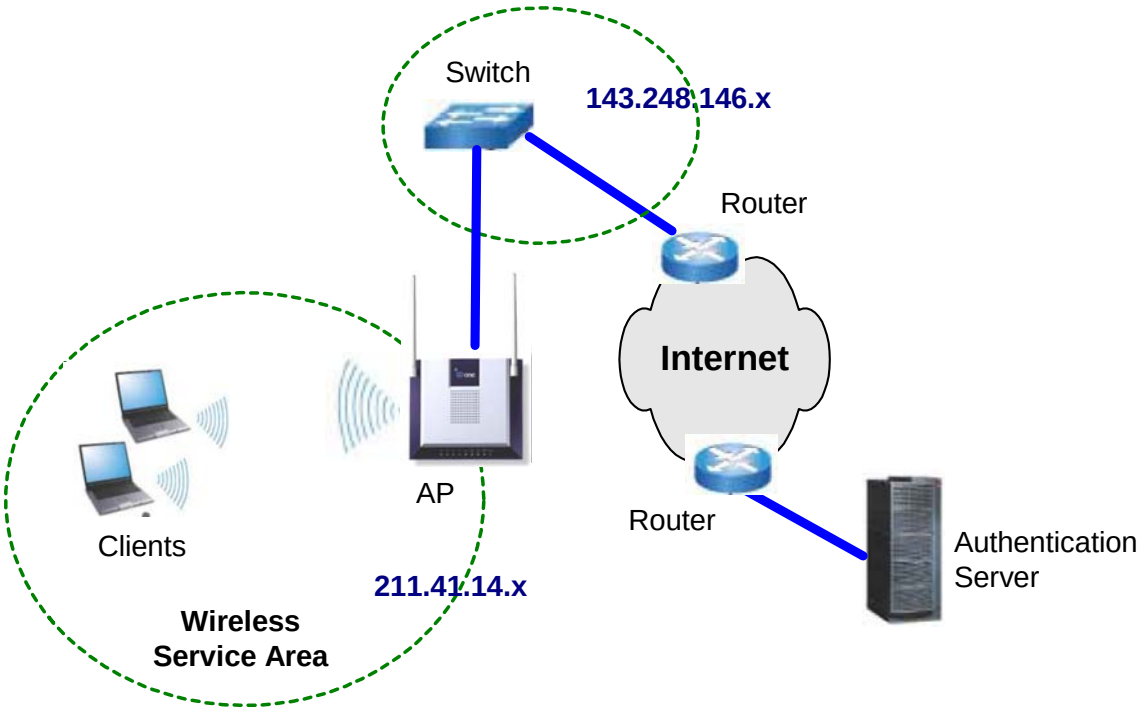



Fig. 4.2.1 Application example when the AP is used as a Router.

## 4.3 AP Configurations in NAT mode

In the NAT mode, you can allocate private addresses to local terminals. In this mode, you must configure the AP as a Routed mode. You must set the following configurations.

| Step | Item |
|---|---|
| 1 | Configure system mode as a Bridge mode. |
| 2 | Configure TCP/IP settings. Here, enable the NAT function. |
| 3 | Enable DHCP server function. |
| 4 | Configure Wireless LAN settings. |
| 5 | Configure Authentication and Accounting. |

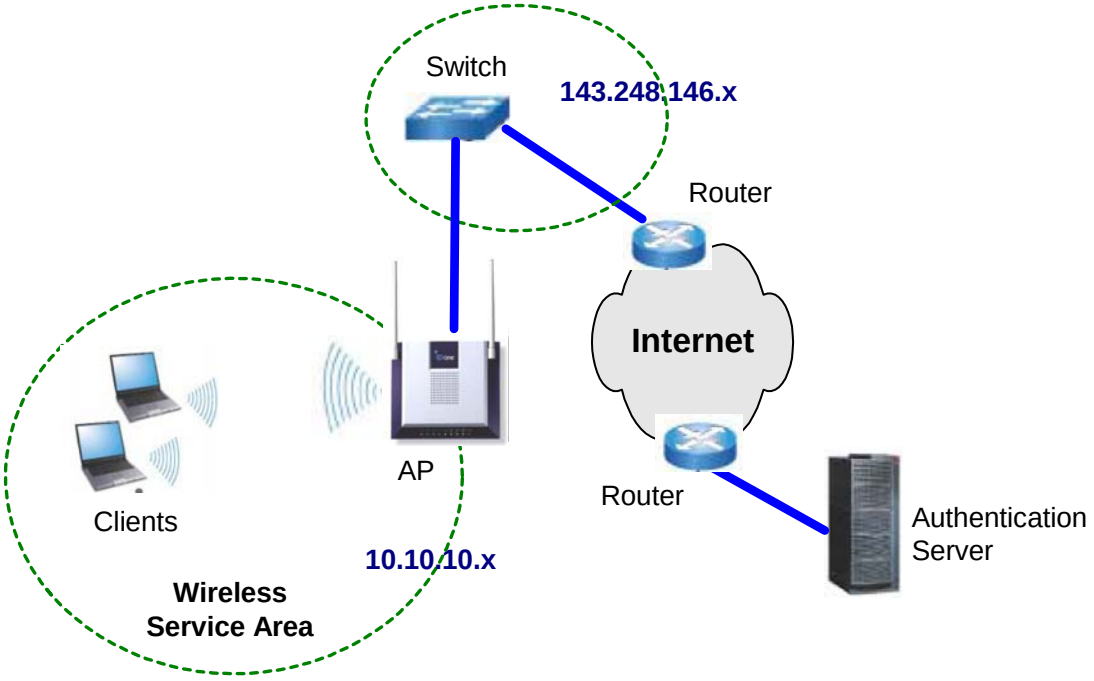



Fig. 4.3.1 Application example when the AP is used as a NAT.