AirGate 2000K

2003. 09

IPone Inc

Contents

1. AP Overview

1.1 General

1.1.1 Overview of Wireless LAN (WLAN)

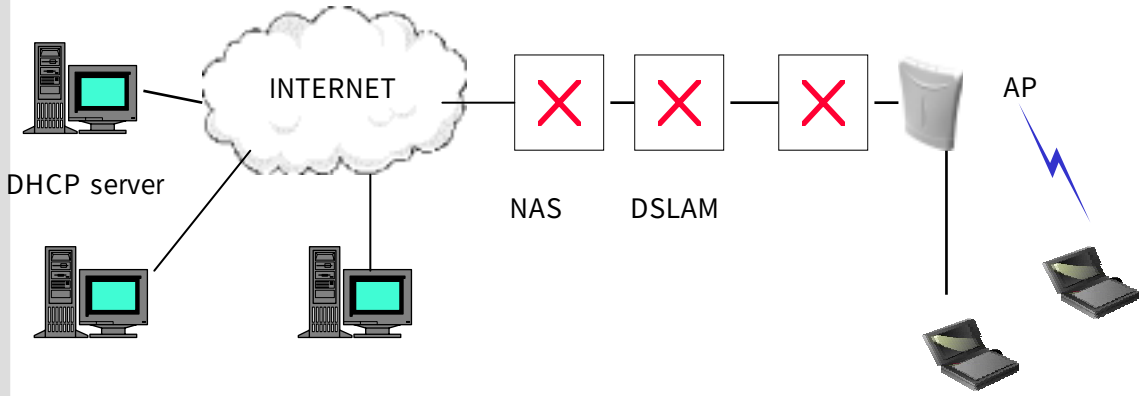
Wireless LAN(WLAN) refers to a LAN that uses high frequency radiowave instead of cables for inter-node communication. WLAN operation is defined in IEEE 802.11b. WLAN transmits high-speed data up to 11 Mbps. WLAN can keep high speed in rural environment (country area) as well as in buildings and campuses, and supports data communication with high reliability. In addition, it is easy and fast installs it. It is possible to install WLAN even in places where it is impossible to install wired LANs, and also possible to install it temperately. Currently connected to ADSL network used for companies or houses, it aims to provide the wireless LAN service through Access Point (Integrated Access Point: hereinafter referred to as “The integrated AP”) which combines ADSL with wireless LAN. The integrated AP, composed of ADSL Access device and 11M Wireless Access Point, is designed to provide the wireless LAN service over the high-speed Internet served via ADSL line.

The integrated AP, equipped with 10/T base wired port as 1 port, is designed to configure 10/T base wired LAN without the help of other equipments. In medical and education fields, WLAN has shown a rapid growth.

1.2 Configuration Diagram

1.2.2 Network Configuration Diagram

The configuration diagram illustrates how WIMS server (authentication server), DHCP server, NAS system and DSLAM system used by ISP can interwork with the integrated AP in order to provide the wireless LAN service.



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.

1.3 AP Structure

1.3.1 AP Structure

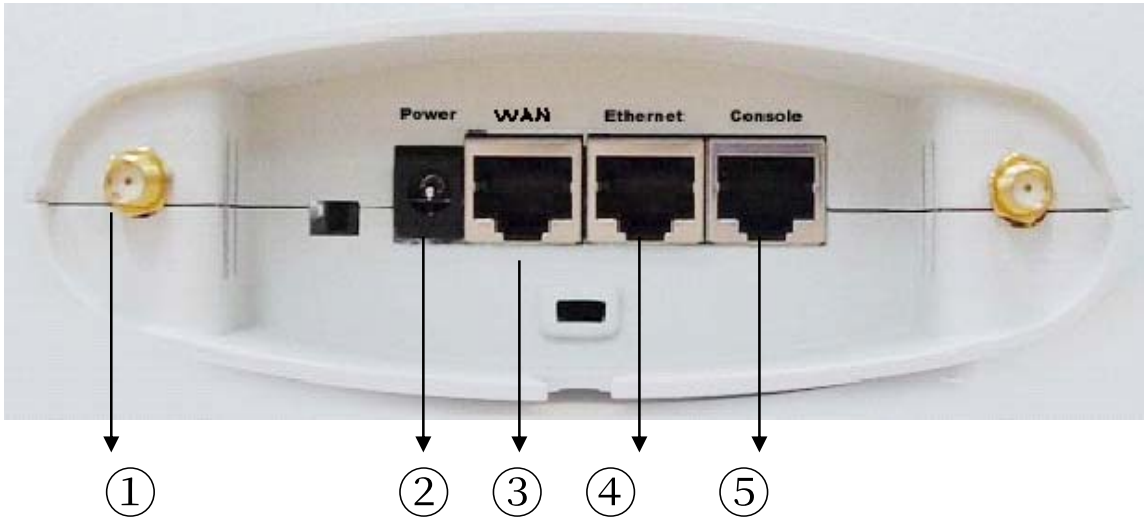
1.3.1.1 AP Front View

AP LED LAYOUT

No.	LED Name	Color	LED	Operation State
①	Wireless	Green	On	Wireless LAN is connected
			Off	Wireless LAN connection is stopped
②	WLAN	Green	On/Off Repeat	WLAN Data Communication
			Off	No WLAN Data Communication
③	Power	Green	On	Power is already supplied
			Off	Power is not supplied
④	Ethernet	Green	On/Off 반복	Ethernet data communication
			Off	Ethernet data communication is stopped
⑤	WLAN	Green	On	Ethernet is connected

			Off	Ethernet connection is stopped

1.3.1.2 AP Rear View



① Dipole Antenna Connector
② DC Power Connector
③ RJ-45 Ethernet Connector
④ RJ-45 Ethernet Connector
⑤ RJ-45 Serial Port

1.4 AP Components

1.4.1 AP Components

Check AP products components before installing the AP

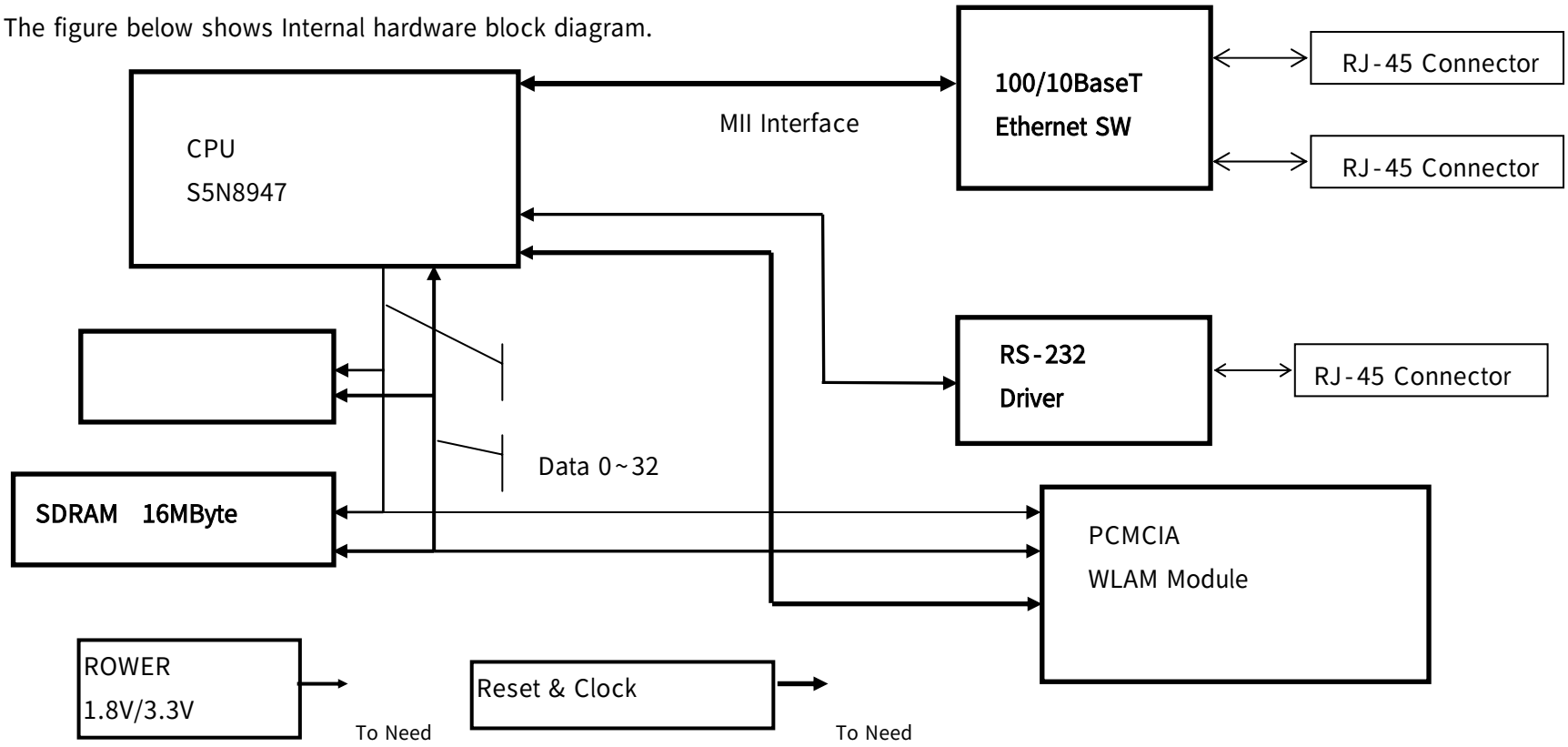
① Access Point Set
② Outer Antenna
③ Power Adaptor
④ RS- 232 Cable
⑤ Manual CD-ROM

2. H/W, S/W Structure

2.1 Internal Block Diagram

2.1 Internal Block Diagram

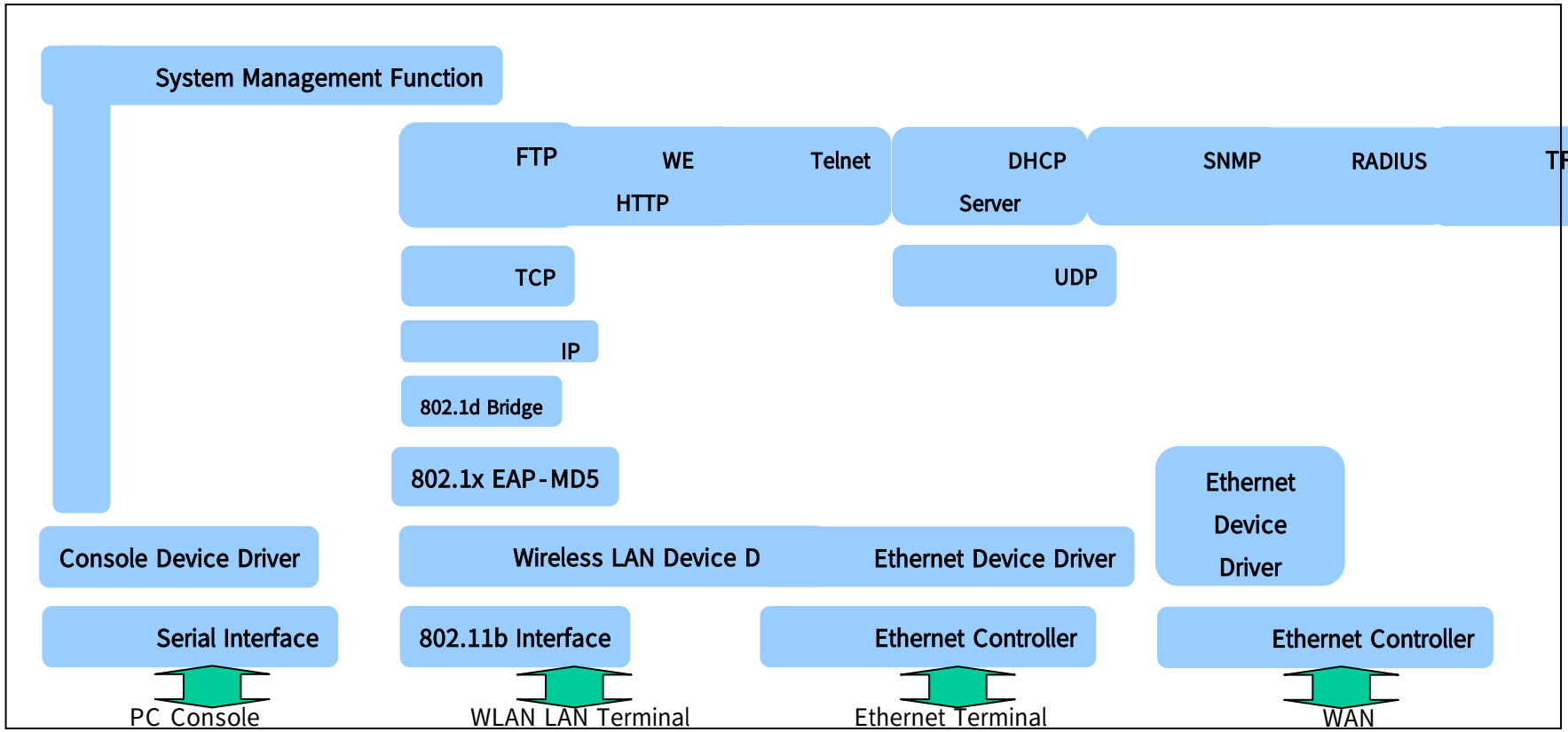
The figure below shows Internal hardware block diagram.



2.2 S/W Hierarchical Structure

2.2.1 S/W Hierarchical Structure

The figure blow shows software hierarchical structure of our AP.



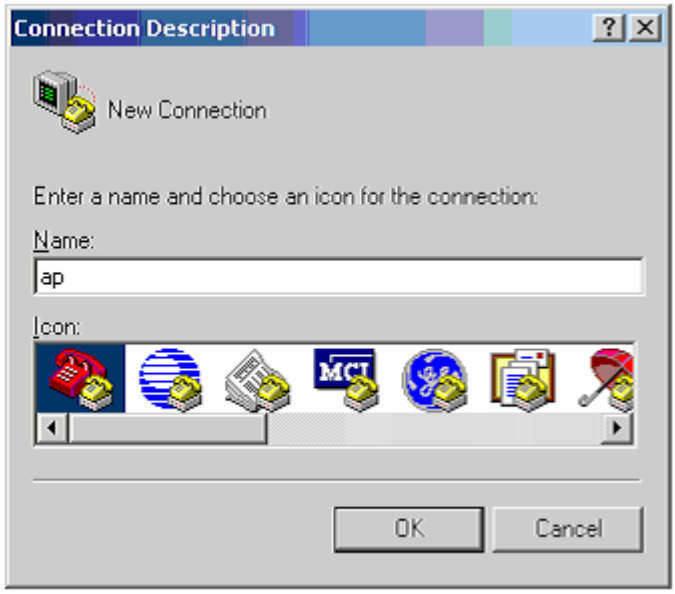
3. Console, Telnet Setup

3.1 : Setting Terminal Emulator for Console

There are various terminal emulators as commercial products. Among them, this chapter describes 'Hyper Terminal' embedded in Window that is the most widely used.
If you want to execute Hyper Terminal, click 'Start' -> 'Program'-> 'Auxiliary Program'-> 'Communication'->'Hyper Terminal' in order.

3.1.1 Hyper Terminal Execution Screen

: If you execute hyper terminal, name dialog box for 'Connection' appears as shown in the figure below. At this time, set a desired name.



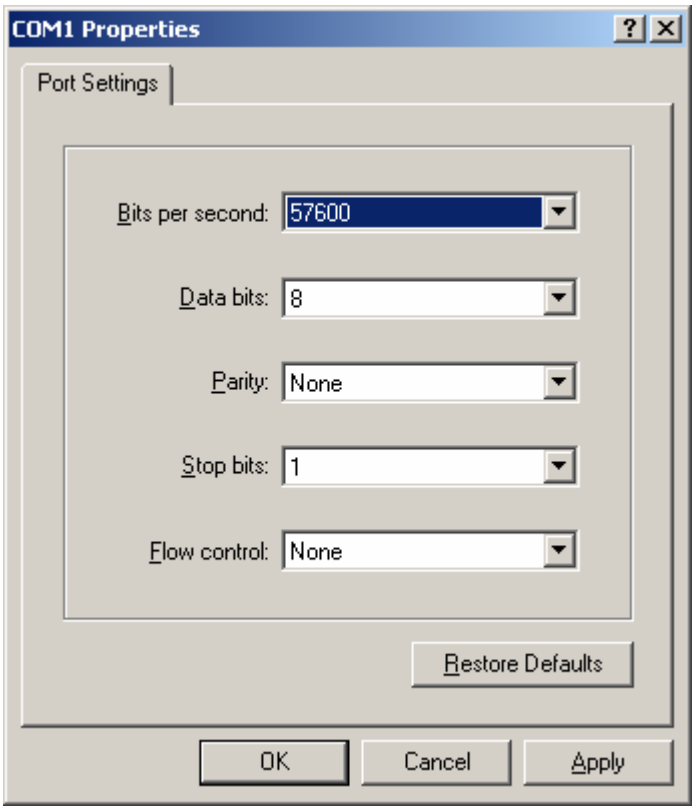
3.1.2 Connection Target

: In Connection Target dialog box, enter Serial port to be connected. In general, Com1/Com2 are used, and Com1 is used in most cases.

3.1.2 Entry Information Dialog Box

: After Entry Information Dialog box appears, fill out the following items.

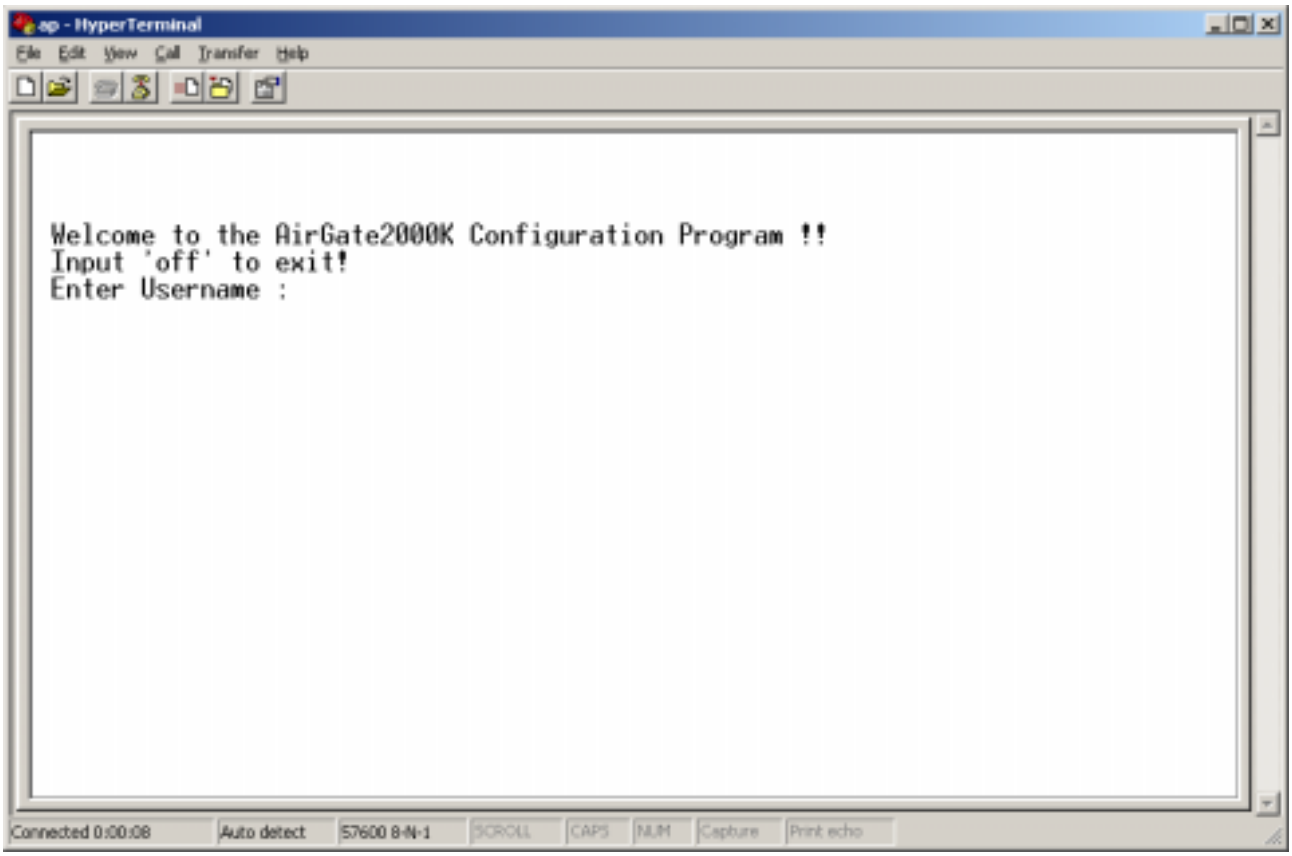
- Bit/Sec : 57600
- Databit : 8
- Parity : None
- Stopbit : 1
- Flow Control : None



3.1.4 Login

: After setting, login screen appears as shown below. An initial Username/Password are as follows.

- Initial Username : admin
- Initial Password : admin



3.2 : Connecting Telnet

• If you want to connect to AP through Telnet for the purpose of management, be sure to know AP IP address. AP's default IP Address is 10.0.0.2 and default port number is No. 23 (Telnet default port). Example of connection is as follows.

Example) Enter the following command in Command Prompt.

```
C: \ >telnet 10.0.0.2
```

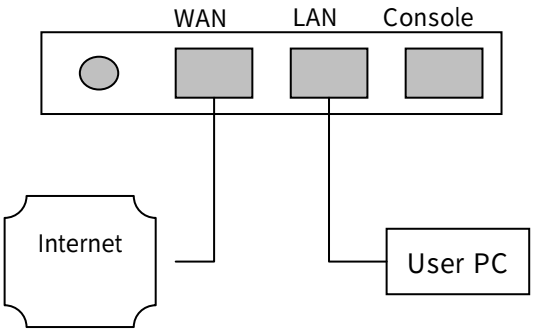
To Provide wireless LAN service by installing APs, you have to be provided with the following items by the network manager.

① AP Operation Mode: Bridge mode, Routed mode, PPPoE mode
② External Network Connection Mode: Fixed IP, DHCP, or ADSL(PPPoE)
③ AP IP address and network mask address
④ Basic gateway address of AP, and DNS server address
⑤ Wireless LAN SSID, channels used, and encryption status
⑥ Authentication/billing Information, radius server address, port, and secret key
Network management server address

3.3 : AirGate 2000K Setup

AirGate2000K has physical interface such as one wireless interface and two Ethernet interfaces. One of the two Ethernet interfaces is 'WAN' interface, and the other is 'LAN' interface. When installing AirGate2000K, connect backbone network coming from the outside to 'WAN' port. If 'WAN' port and 'LAN' port are changed when installed, it might cause serious effects on some functions. Thus, be sure to check 'WAN' port and 'LAN' port before installation.

Example) If there is an UTP cable connected through Kornet network, connect it to 'WAN' port, and connect internal LAN user's (wired) PC to 'LAN' port.



3.4 : Status

In ‘Status’, you can view system setup information. If you normally log on through Console and Telnet, the page below appears first. If you want to see ‘Status’, enter ‘s’ or ‘status’.

Ex : cms>s or cms>status

```
------------------------------------------------------------------
            IPONE AirGate2000K Wireless Router (Admin Mode)
------------------------------------------------------------------

   AirGate2000K Status (FW 1.2.4 (2003-03-28))   0 days 00:00:26

 System Mode : Bridge
 Bridge IP Address : 192.168.77.110     Subnet Mask : 255.255.0.0

 Default Gateway : 192.168.123.254   DNS Server : 168.126.63.1
 Eth(WAN) MAC Address : 00:07:13:ff:00:00 (100M-Full)
 Ethernet MAC Address : 00:07:13:ff:00:01 (Disconnected)
 WLAN MAC Address     : 00:07:13:61:01:24

 WLAN  SSID : NESPOT   Channel : 9
 DHCP Server : Not Running




--(Status)--[Config]--[Util]--[reboot]--[quit]-----------------------

cms>
```

In ‘Status’ as shown in the figure below, you can search firmware version (ex: FW 1.2.4), system uptime, ADSL, network setup, wireless LAN setup, interface information and the status of DHCP Server. After setting to subscriber’s environment, you can check the results in ‘Status’. For further information on setup, refer to 3.5 ‘Config’.

3.5 : Config

In ‘Config’, you can set up all AP functions. If you want to set up AP in ‘Config’, enter ‘c’ or ‘config’.

Ex: cms>c or cms>config

If you want to set the appropriate menu in ‘Config’, enter the appropriate menu number, and enter ‘Y’ if current setup status for ‘Change Setup’ appears, and then set according to each step. If you enter wrong number by mistake, enter ‘n’ if ‘Change Setup’ is shown.

Note! Before you set up AP in ‘Config’ menu, be sure to be familiar to this manual. If you change a part of settings without permission, the system might be in malfunction.

```
------------------------------------------------------------------------
            IPONE AirGate2000K Wireless Router (Admin Mode)
------------------------------------------------------------------------

   Configuration Menu

      1. Basic Configuration
      2. Wireless LAN Configuration
      3. DHCP Server Configuration
      4. 802.1X Configuration (Primary)
      5. 802.1X Configuration (Additional)
      6. SNMP Configuration
      7. SNMP Configuration (Access Control)
      8. Interface Configuration
      9. Application Configuration
      10. Wireless MAC Filtering
      11. Ethernet MAC Filtering
      12. Access Control for Remote Management
      13. Selectable Channels in AutoCh mode



--[Status]--(Config)--[Util]--[reboot]--[quit]-----------------------

cms>
```

3.5.1 Basic Configuration

: If you want to set Basic Configuration, enter '1'(the appropriate menu), and enter 'Y' if you are asked whether to change the current setup.

When setting, value in brace ([ ]) means current set value, and press Enter key if you want to maintain it without changing.

```
- Enter the new configuration!

   Admin Login Name[ admin ]:
   Admin Passwd[***** ]:
   User Login Name[user]:
   User Passwd[*****]:
   System Mode(Bridge|Routed|PPPoE)[Bridge]:
   DHCP Client Enable[N]:
   WAN IP Address[192.168.77.110]:
   WAN Network Mask[255.255.0.0]:
   Default Gateway[192.168.123.254]:
   DNS Server[168.126.63.1]:
   Enhanced Security for LAN stations[N]:
```

• Admin Login Name[admin] : AP Admin login name. Default is 'admin' (value in the brace ([ ]), and if you log in Admin, you can execute AP setting, setup change, setup inquiry and other functions.

• Admin Password[*****] : Password for AP Admin login. Default is 'admin'. Do not change.

• User Login Name[user] : User Login Name [user]: AP user login name. Default is 'user', and if you log in user, you can search AP setup information and reboot the system only.

- User passwd[******] : Password for AP user login. Default is 'ipone'.
- System Mode(Bridge|Routed|PPPoE)[Bridge] : System mode setting
  - Bridge : Bridge all physical interfaces.
  - Routed : Routing mode between ADSL interface and wireless& Ethernet interface.
  - PPPoE : AP closes PPPoE session, and IP Address is assigned to AP. Set ID and Password for PPPoE session.
- DHCP Client Enable[N] : DHCP Client Enable [N]: Used to assign AP IP address as flexible IP. Default is 'N'. If it is set to 'Y', you do not have to execute IP setting. If you install AP through authentication mode, be sure to set to 'N' and set IP in the next item.
- WAN IP Address[10.0.0.2] : WAN interface IP address. Enter IP address assigned to AP. If you do not know IP address, contact with administrator and then enter correct IP address. Default is '10.0.0.2'.
- WAN Network Mask[255.255.255.0] : Subnet mask by WAN interface IP address. If you do not know Subnet mask, contact with administrator and then enter correct subnet mask. Default is '255.255.255.0 (24bit)'.
- Default Gateway[10.0.0.1] : Default Gateway setting. If you do not know Gateway, contact with administrator and then enter correct Gateway. Default is '10.0.0.1'.
- DNS Server[168.126.63.1] : DNS server setting. Default is '168.126.63.1'.
- Enhanced Security for LAN station[N] : Separation between LAN users (wired/wireless). If you set this function to 'Y', communication between LAN users is no performed. Default is 'N'.

3.5.2 Wireless LAN Configuration

: In Wireless LAN Configuration', you can execute wireless LAN-related setting.

If you want to set Wireless LAN Configuration, enter '2', and enter 'Y' if you are asked whether to change the current setup, and go on according to each step.

```
- Enter the new configuration!

   SSID[IPONE] :
   802.11b Channel Num(Auto|1|2|3|4|5|6|7|8|9|10|11)[AUTO] :
   AuthType – Open System[Y] :
   AuthType – Shared Secret[N] :
   Allow 'ANY' SSID[Y] :
   Encryption Method(non|wep64|wep128|Dynamic64|Dynamic128)[none]:
   Beacon Period (ms)(1-10000)[100]:
   Basic Rate of 1 Mb/s[Y]:
   Basic Rate of 2 Mb/s[Y]:
   Basic Rate of 5.5 Mb/s[Y]:
   Basic Rate of 11 Mb/s[Y]:
   Operation Rate of 1 Mb/s[Y]:
   Operation Rate of 2 Mb/s[Y]:
```

```
Operation Rate of 5.5 Mb/s[Y]:
Operation Rate of 11 Mb/s[Y]:
RTS Threshold(0-3000)[2432]:
Fragmentation Threshold (256-2346)[2346]:
Transmission Power(Default=70mW)(Default|10mW|30mW|50mW|100mW)[100mW]:
```

- SSID[IPONE]: Set ESSID. Set to 'IPONE'. Default is 'IPONE'.

! Note: Enter an SSID value, discriminating between large and small letters. If you set to 'ipone', thus, IPONE wireless terminal is not connected.

- 802.11b Channel Num(Auto|1|2|3|4|5|6|7|8|9|10|11|)[Auto]:
  Set wireless LAN channel. If you want to fix channel, enter a desired channel number, and enter 'auto' if you use 'Auto Setting' function through which AP can search optimal channel by itself. Default is IPONE.
- AuthType - Open System[Y]: Set 802.11b authentication method. Default is 'Y'.
- AuthType - Shared Secret[N]: Set 802.11b authentication method. Default is 'N'.
- Allow 'ANY' SSID[Y]: Set terminal 'ANY' SSID allowance. If you set to 'Y', it allows the terminal to search AP or enables wireless connection of the terminal set to 'ANY'. If you set to 'N', it is possible to connect the terminal wirelessly if you enter SSID identical to AP in the terminal. Default is 'Y'.
- Encryption Method(none|wep64|wep128|Dynamic64|Dynamic128)[none]: Setting data encryption in wireless section. For data encryption in wireless section, be sure to set encryption key value and key index. If it is not Dynamic WEP Encryption, in addition, communication is in normal status if AP is the same as terminal encryption key and key index. Default is 'none' (unused).
  - wep64 : Set to 64bit data encryption mode. When using wep64, set encryption key and key index, and also AP should have the same encryption key and key index.
  - wep128 : Set to 128bit data encryption mode. When using wep128, set encryption key and key index, and also AP should have the same encryption key and key index.
  - Dynamic64 : The terminal is assigned with session key through authentication, and performs 64bit data encryption. For Dynamic64, do not set encryption key and key index.
  - Dynamic128 : The terminal is assigned with session key through authentication, and performs 128bit data encryption. For Dynamic128, do not set encryption key and key index.
- Beacon Period (ms)(1-10000)[100]: Beacon Set transmission period of Beacon packet. Default is '100'.
- Basic Rate & Operation Rate : Indicates transmission rate in wireless LAN section. In case of

802.11b wireless LAN, it is possible to automatically adjust transmission rate according to signal strength, environment and noise. Transmission rate such as 11Mbps, 5.5Mbps, 2Mbps and 1Mbps is supported. Under the environment of good signal strength and less noise, communication is performed at a rate of 11Mbps, however, if not, communication is carried out at a different rate of transmission according to the environment. Basic Rate means transmission rate of communication not through negotiation with terminal like Broadcast; Operation Rate does transmission rate through negotiation with terminal like Unicast. For basic rate, default (1Mbps/2Mbps) is set to 'Y', and for Operation Rate, it is set to 'Y'. Do not change setting but wireless LAN technician.

- RTS Threshold(0-3000)[2432]: Set RTS Threshold value. Default is '2432'.
- Fragmentation Threshold(256-2346)[2346]: Set Fragmentation Threshold value. Default is '2346'.
- Transmission Power(Defalut=70mW)(Default|10mW|30mW|50mW|100mW)[100mW]: Set output power. Default is '100mW'.

3.5.3 DHCP Server Configuration

: In 'DHCP Server Configuration', you can set DHCP Server and Relay. If you want to set DHCP Server and Relay, enter '4', and enter 'Y' if current setup status for 'Change Setup' appears, and then set according to each step.

```
- Enter the new configuration!

   DHCP Server Enable[N]:
   DHCP Relay Enable[N]:
```

- DHCP Server Enable[N] : Start and set DHCP Server. When running DHCP Server, enter the first IP address and last IP address. Default is 'N (unused)'.
- DHCP Relay Enable[N] : Start and set DHCP Relay. When running DHCP Relay, enter Relay Server IP address. Default is 'N (not used)'.

3.5.4 802.1x Configuration (Primary)

: In '802.1x Configuration (Primary)', you can execute major setting related to authentication. If you want to set 802.1x Configuration (Primary), enter '5', and enter 'Y' if current setup status for 'Change Setup' appears, and then set according to each step.

```
- Enter the new configuration!

   802.1x Authentication(none|e8021x|mac8021x)[mac8021x]:
   Primary Auth Server[61.78.54.2]:
   Primary Auth Port(1-65535)[1812]:
   Primary Auth Shared Key[megapass]:
   Secondary Auth Server[0.0.0.0]:
   Secondary Auth Port(1-65535)[1812]:
   Secondary Auth Shared Key[megapass]:
   Radius Auth Request Retrans. Interval(ms)(10-65535)[15000]:
   Radius Auth Request Retrans. Number(1-65535)[3]:
   Primary Acct Server[61.78.54.2]:
   Primary Acct Port(1-65535)[1813]:
   Primary Acct Shared Key[megapass]:
   Secondary Acct Server[0.0.0.0]:
   Secondary Acct Port(1-65535)[1813]:
   Secondary Acct Shared Key[megapass]:
   Radius Acct Request Retrans. Interval(ms)(10-65535)[15000]:
   Radius Acct Request Retrans. Number(1-65535)[3]:
```

- 802.1x Authentication(none|e8021x|mac8021x)[mac8021x]:Setting for 802.1x authentication method.
  - e8021x : If 802.1x EAP-MD5 only is authenticated.
  - mac8021x : If MAC/802.1x EAP-MD5 are all authenticated.
- Primary Auth Server[61.78.54.2] :
  Set up Primary Auth Server IP address. Default is '61.78.54.2'.
- Primary Auth Port(1-65535)[1812]:
  Set up Primary Auth. Server Auth. Server. Default is '1812'.
- Primary Auth Shared Key[megapass]:
  Secret key for authentication between Primary Auth. Server and AP. Default is 'megapass'.
- Secondary Auth Server[0.0.0.0]:
  Set up Secondary Auth Server IP address. Default is '0.0.0.0'.
- Secondary Auth Port(1-65535)[1812]:
  Set up Secondary Auth Port IP address. Default is '1812'.
- Secondary Auth Shared Key[megapass]:
  Secret key for authentication between Secondary Auth Server and AP. Default is 'megapass'.
- Radius Auth Request Retrans. Interval(ms)(10-65535)[15000]:
  If authentication packet transmission fails, set retransmission interval. Default is '15000'.
- Radius Auth Request Retrans. Number(1-65535)[3]:
  If authentication packet transmission fails, set the number of retransmission. Default is '3'.
- Primary Acct Server[61.78.54.2]:
  Set Primary Acct Server IP address. Default is '61.78.54.2'.
- Primary Acct Port(1-65535)[1813]:
  Set up Primary Acct Server Auth port. Default is '1813'.
- Primary Acct Shared Key[megapass]:

Secret key for authentication between Primary Acct Server and AP. Default is ‘megapass’.

- Secondary Acct Server[0.0.0.0]:
  Set Secondary Acct Server IP address. Default is ‘0.0.0.0’.
- Secondary Acct Port(1-65535)[1813]:
  Set up Secondary Acct Server Auth port. Default is ‘1813’.
- Secondary Acct Shared Key[megapass]:
  Secret key for authentication between Secondary Acct server and AP. Default is ‘megapass’.
- Radius Acct Request Retrans. Interval(ms)(10-65535)[15000]:
  If authentication packet transmission fails, set retransmission interval. Default is ‘15000’.
- Radius Acct Request Retrans. Number(1-65535)[3]:
  If authentication packet transmission fails, set the number of retransmission. Default is ‘3’.

3.5.5 802.1x Configuration (Additional)

: In ‘8021x Configuration (Additional)’, you can execute additional setting related to authentication. If you want to set 8021x Configuration (Additional), enter ‘5’, and enter ‘Y’ if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   802.1x Authentication(none|e8021x|mac8021x)[mac8021x]:
   Authentication to Ethernet Interface(None|Equal|New)[None]:
   Web Redirection Enable[Y]:
   Private Network for Unauthencticated Users[N]:
   Web Redirection Page[first.nespot.com]:
   Web Redirection Open Page 1[]:
   Web Redirection Open Page 2[]:
   Web Redirection Open Page 3[]:
   Web Redirection Open Page 4[]:
   IAPP Enable[N]:
   Lost-Carrier Detection[Y]:
   Lost-Carrier Detection Check Period (sec)(5-1000)[10]:
   Lost-Carrier Detection Expiry Time (sec)(10-10000)[60]:
   Reauthentication[N]:
   Default Session Time (sec)(0-1879048192)[0]:
   Default Idle Time (sec)(0-1879048192)[0]:
   MAC Auth Period (sec)(0-1879048192)[300]:
   NAS ID for Radius Server[IPONE_AG2500_KT]:
   802.1x Wecome Message[]:
```

- 802.1x Authentication (none|e8021x|mac8021x)[mac8021x] :
  Setting for 802.1x authentication method. Default is ‘mac8021x’.
- Authentication to Ethernet Interface(None|Equal|New)[None] :
  Set 8021x authentication of a wired terminal. Default is ‘none’.
  - Equal: Authentication of a wired terminal is performed the same as wireless terminal.
  - New: Wired and wireless terminals are classified for authentication.
- Web Redirection Enable[Y] : If an unauthenticated terminal attempts to access the Internet through Web browser, it is connected to the Web Page that is designated by force. Default is ‘Y’.

- Private Network for Unauthenticated Users[N] : If Web Redirection is enabled, IP address is assigned to the unauthenticated terminal to redirect to the designated Web Page. At this time, Private IP is assigned to the terminal Default is 'N'.
- Web Redirection Page[www.ipone.co.kr]: Web page address to be redirected. Default is 'www.ipone.co.kr'. This item can be set only if Web Redirection is enabled.
- Web Redirection Open Page 1~ 4: Used if a specific Web Page is assigned to an unauthenticated terminal. Default is 'blank'.
- IAPP Enable[N]: IAPP (Inter AccessPoint Protocol) enables authenticated terminal roaming in the policy where overlapped login is not allowed.
- Lost-Carrier Detection[Y]: Lost-Carrier Detection[Y]: Used to detect that a wireless signal is not transmitted from the authenticated terminal. After detecting it, AP sends session termination packet because a wireless signal is not transmitted to the Auth Server.
- Lost-Carrier Detection Check Period (sec)(5-1000)[10]: Set Lost-Carrier Detection period. Default is '10'.
- Lost-Carrier Detection Expiry Time (sec)(10-10000)[60]:
  When performing Lost-Carrier Detection, set expiry time. If there is no response to AP Lost-Carrier Detection during the time, AP ends session because wireless terminal does not transmit a wireless signal.
- Reauthentication[N]:
  Set whether to re-authenticate the authenticated terminal (session). Default is 'N'.
- Default Session Time (sec)(0-1879048192)[0]:
  Set session time of the authenticated terminal (session). Default is '0'.
- Default Idle Time (sec)(0-1879048192)[0]: Set idle time of the authenticated terminal (session). If there is no User packet from the authenticated terminal during the time, AP sends session-end packet to Auth Server because of Idle timeout. Default is '0'.
- MAC Auth Period (sec)(0-1879048192)[300]: Indicate authentication period of MAC-authenticated terminal. Default is '300'.
- NAS ID for Radius Server[IPONE_AG2500]: NAS ID used to send authentication packet to the Radius Server.
- 802.1x Welcome Message[]: Message to be sent if authentication is successful. Default is 'blank'.

3.5.6 SNMP Configuration

: In 'SNMP Configuration', you can perform SNMP-related setting. If you want to set SNMP-related setting, enter '6', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   SNMP Agent Enable[Y]:
   SNMP Port No.(1-65535)[161]:
   SNMP Get Community[nesp-pub]:
   SNMP Set Community[apms-prv]:
   TRAP Enable[Y]:
   TRAP Server[211.216.50.215]:
   TRAP Port No.(1-65535)[162]:
   Trap Community[nesp-pub]:
```

- SNMP Agent Enable[Y] : Set whether or not SNMP Agent is in operation. Default is 'Y'.
- SNMP Port No.(1-65535)[161] : Set SNMP port. Default is '161'.
- SNMP Get Community[nesp-pub]: Set community to be used for Get. Default is 'nesp-pub'.
- SNMP Set Community[apms-prv] : Set community to be used for Set. Default is 'apms-prv'.
- TRAP Enable[Y] : Set whether to send SNMP Trap message. Default is 'Y'.
- TRAP Server[211.216.50.215]: Set IP address of the server that sends SNMP Trap message. Default is '211.216.50.215'.
- TRAP Port No.(1-65535)[162] : Set Trap message transmission port. Default is '162'.
- Trap Community[nesp-pub] : Set community to be used for Trap. Default is 'nesp-pub'.

3.5.7 SNMP Configuration (Access Control)

: In 'SNMP Configuration (Access Control)', you can set access authority of SNMP Client. If you want to set access authority of SNMP Client, enter '7', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   SNMP Client Access Control Enable[N]:
```

In this menu, you can set Get/Set/Both authority of access to Client by using SNMP Client IP address and Netmask.

예) SNMP Client IP Address 1[0.0.0.0] : 10.0.0.5
SNMP Client Netmask 1 [255.255.255.255] : 255.255.255.255
SNMP Client Mode 1 (Both|Get|Set)[Both] : Get

If set as shown in the table above, Get authority only is allowed to SNMP Client 10.0.0.5 (since Subnet is 24bit, set only one host).

3.5.8 Interface Configuration

: In 'Interface Configuration', you can perform physical setting for wireless and wired interface. If you want to physically set wireless and wired interface, enter '8', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
Configuration Menu :  9. Interface Configuration
  - Wireless Mode : Enable
  - Mode of ETH Interface(Link speed,Duplex mode) : Auto
```

• Wireless Mode : Set whether wireless module is in operation. Default is 'Enable'.

• Mode of ETH LAN Interface(Link speed , Duplex mode) : You can set wired interface speed and Duplex method. You can select one of 10M Half, 10M Full, 100M Half and 100M Full.

• Mode of ETH WAN Interface(Link speed , Duplex mode) : You can set wired interface speed and Duplex method. You can select one of 10M Half, 10M Full, 100M Half and 100M Full.

3.5.9 Application Configuration

: In 'Application Configuration', you can set Http, Console port and log size. For setting, enter '10', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   WEB server Port No.(1-65535)[8899]:
   TELNET server Port No.(1-65535)[23]:
   MAX Log Size(20-65535)[80]:
```

• WEB server Port No.(1-65535)[8899] : Set WEB server Port. Default is '8899'.

• TELNET server Port No.(1-65535)[23]: Set Telnet Server Port. Default is '23'.

• MAX Log Size(20-65535)[80]: Set maximum log size. Default is '20'.

3.5.10 Wireless MAC Filtering Configuration

: In 'Wireless MAC Filtering Configuration', you can set not only filtering (Allow/Deny) by using adapter MAC address of a wireless terminal but also the number of restricted access of a wireless terminal. For setting, enter '10', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   MAC Filtering Mode(No|Allow|Deny|Num)[No]:
```

• MAC Filtering Mode(No|Allow|Deny|Num)[No]:
  - No : MAC filtering is not performed.
  - Allow : Wireless link for the entered MAC address only is allowed.
  - Deny : Wireless link for the entered MAC address only is denied.
  - Num : Set the number of maximum connector.

3.5.11 Ethernet MAC Filtering

: In 'Ethernet MAC Filtering', you can set not only filtering (Allow/Deny) by using adapter MAC

address of a wired terminal but also the maximum number of allowed access host of a wired terminal. For setting, enter '11', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   Ethernet MAC Filtering Mode(No|Allow|Deny|Num)[No]:
```

- Ethernet MAC Filtering Mode(No|Allow|Deny|Num)[No]:
  - No : MAC filtering is not performed
  - Num : Set the number of maximum connector.
- Expiry timeout in Ethernet MAC Filtering Number Mode (sec) : Set Idle timeout of a wired terminal.

3.5.12 Access Control for Remote Management

: In 'Access Control for Remote Management', you can restrict host accessible for the purpose of setting in AP. For setting, enter '11', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   Access Control for Remote Management[N]:
```

In this menu, you can set access to the Client by using HOST IP address and Netmask, and total number of settable Netmask is 4.

Ex) Network ID of ACRM List 1 [0.0.0.0]:10.0.0.5
Network Mask of ACRM List 1[255.255.255.255]: 255.255.255.0

If set as shown in the table above, all the hosts (254) included in the same subnet are allowed to access for the purpose of management since Host IP 10.0.0.5/ Subnet is 24bit, set only one host).

3.5.13 Selectable Channels in AutoCh mode

: In 'Selectable Channels in AutoCh mode', you can set the usage of channel when selecting an auto channel. For setting, enter '11', and enter 'Y' if you are asked whether to change the current setup, and then go on according to each step.

```
- Enter the new configuration!

   Use Channel 1 for AutoCh[Y]:
   Use Channel 2 for AutoCh[N]:
   Use Channel 3 for AutoCh[N]:
   Use Channel 4 for AutoCh[N]:
   Use Channel 5 for AutoCh[Y]:
```

```
Use Channel 6 for AutoCh[N]:
Use Channel 7 for AutoCh[N]:
Use Channel 8 for AutoCh[N]:
Use Channel 9 for AutoCh[Y]:
Use Channel 10 for AutoCh[N]:
Use Channel 11 for AutoCh[N]:
```

The figure above shows default. If you use Auto Channel Select function when set to 'default', select one of 1, 5, and 9 channels.

3.6 : Util

You can access util with the following command.

Ex : cms>u or cms>util

3.6.1 Firmware Upgrade

: It is to upgrade AP Firmware. To upgrade AP firmware, enter '1' and set the required items in the order of protocol, server, file name and user account (only for FTP).

```
------------------------------------------------------------------
            IPONE AirGate2000K Wireless Router (Admin Mode)
------------------------------------------------------------------



Firmware Upgrade !!

   Firmware Upgrade Protocol(FTP|TFTP|HTTP)[FTP]:
   Firmware Upgrade Server Address[192.168.123.5]:
   Firmware Upgrade File name[image.cramfs.img]:
   FTP Username for Firmware Upgrade[ipone]:
   FTP Password for Firmware Upgrade[*****]:

Upgrade The Firmware Really ? (y/N)
```

3.6.2 Configuration Upgrade

: It is to upgrade AP configuration. For this purpose, enter '2' and set the required items in the order of protocol, server, file name and user account (only for FTP).

```
------------------------------------------------------------------
            IPONE AirGate2000K Wireless Router (Admin Mode)
------------------------------------------------------------------



Configuration Upgrade !!

   Configuration File Upgrade Protocol(FTP|TFTP|HTTP)[HTTP]:
```

3.6.3 Default Config

: It is to initialize the AP configuration. For this purpose, enter '3' and then 'Y' if asked whether to initialize the configuration.

! Note! Make sure to contact administrator before you initialize the configuration of AP under operation.

3.6.4 Authenticated Users Display

: This function is used to display information on authenticated or non-authenticated users when AP is in the authentication mode. The displayed information includes MAC address, IP address, authentication method, status of wire/wireless and used packet of user. The display is available only when AP is in authentication mode. For using this function, enter '4'.

3.6.5 Force State of User

: It is to perform forced authentication or forced termination for terminal (session). Enter '5' and execute it. This function is also available only when AP is in authentication mode.

3.6.6 Log Message

: It is to display system logs. The corresponding number is '6'.

3.7 : Reboot

This menu is used to reboot the AP. Enter 'reboot' in prompt of console or Telnet.

```
Ex : cms>reboot
```

3.8 : quit

It is to log off after completing AP configuration in console or Telnet.

```
Ex : cms>quit
```

4. Web-based Management

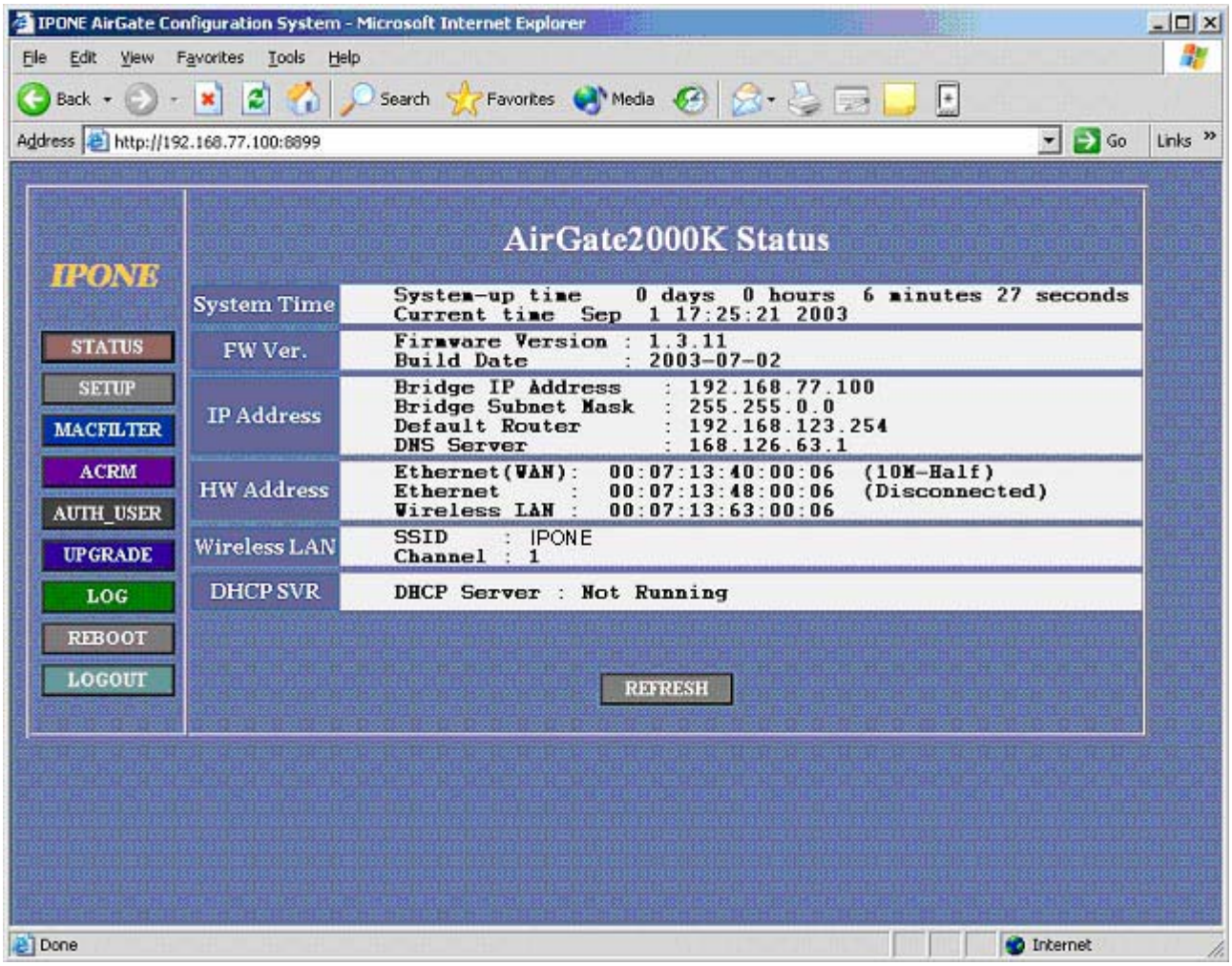
4.1 : Web-based Management

Web-based (HTTP) management system enables user to easily perform configuration setting, system operation and error handling that include equipment status check, configuration management and firmware upgrade. In the chapter for console and Telnet,

you have learned the basic concept and how to use this management system. This chapter describes how to set the system on Web.

4.2 : Status

This menu is used to view AP configuration. For more information on items, refer to the section 3.



4.3 : Network Settings

4.3.1 Operation-as-Bridge Stage

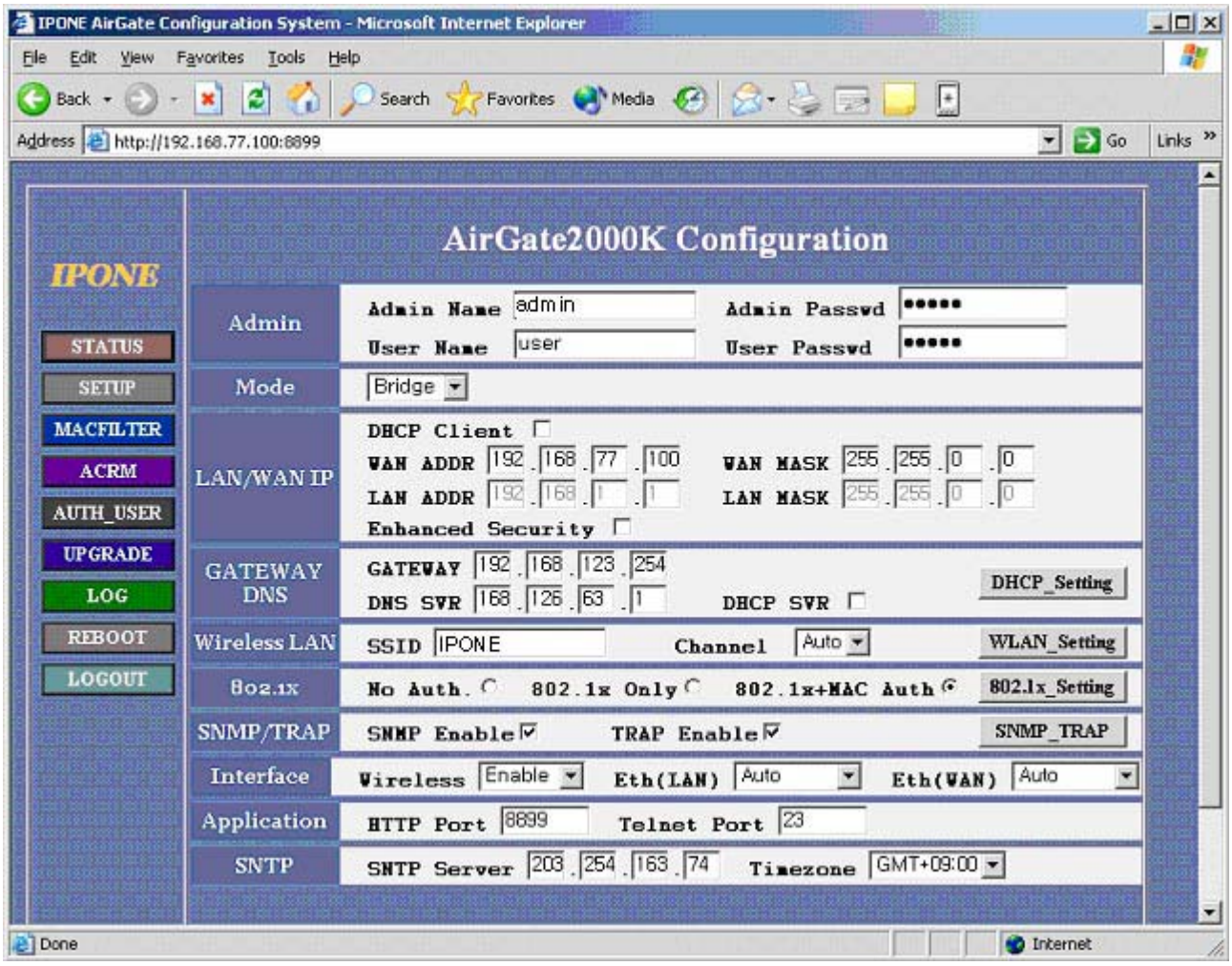
: When you provide wireless LAN services in bridge mode, you have to set one IP address for all physical interfaces in AP as a whole. To set AP to bridge mode, install the AP as shown below.

In [Default Setting] window, set the [Mode] to [Bridge].

If you check [DHCP Client] in [LAN/WAN IP], an IP address is assigned from the network. If network administrator has assigned a fixed IP address for AP to you, enter the IP address in WAN address and WAN MASK. Set [GATEWAY, DNS] with the basic gateway and the DNS server addresses provided by

the network manager.

When all settings are completed, click[Apply] to apply the settings. The settings in [Network Settings] are applied when the system restarts, so restarts the system by clicking [Restart]. Once the system restarts, you have to access WMS with the new IP address of the AP.

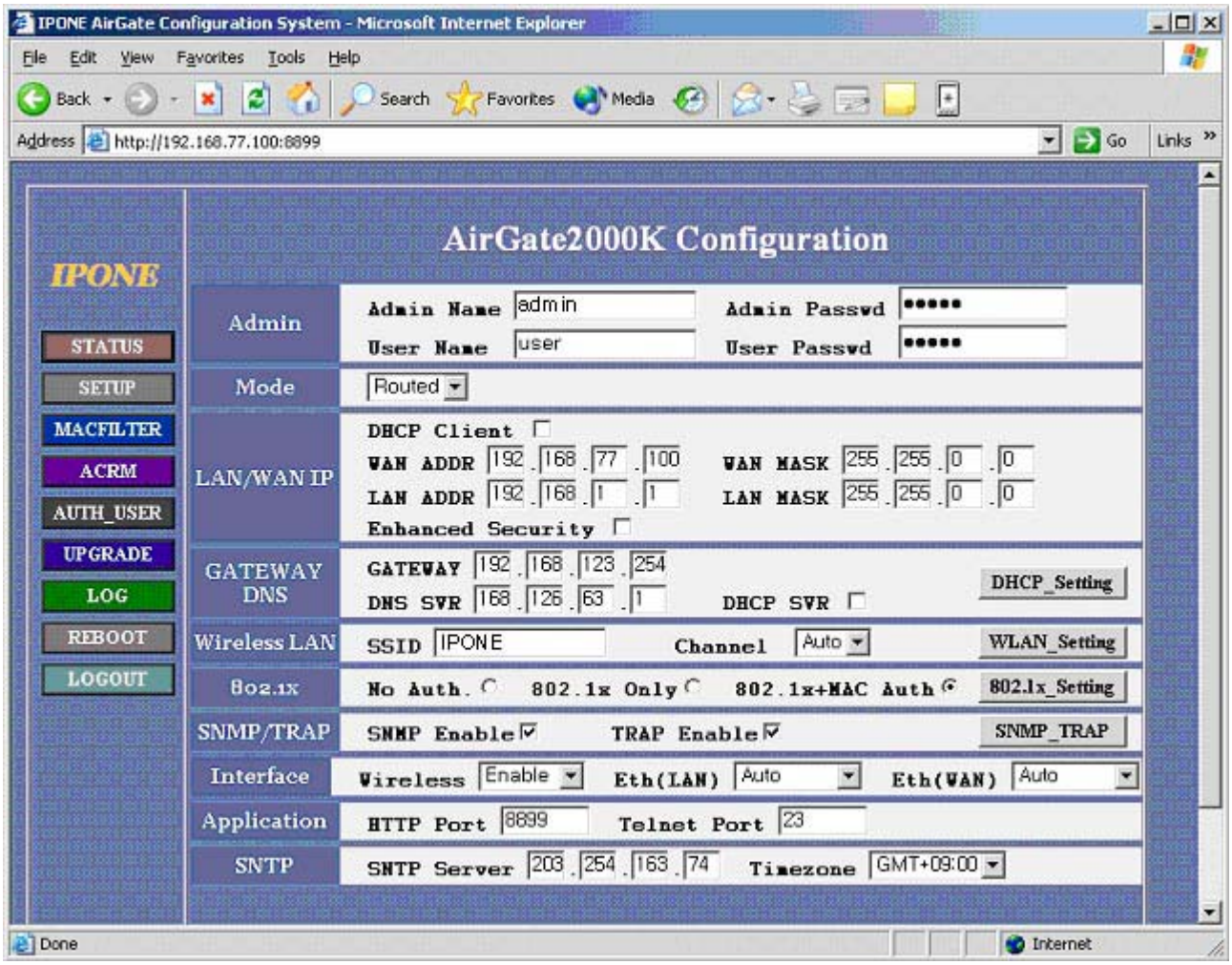


4.3.2 Operation-as-Router Stage

Set the [Mode] of [Basic Setting] to [Routed]. Uncheck [DHCP Client] and then, set [WAN Address], [WAN MASK], [LAN Address] and [LAN MASK] with IP address and network mask assigned by the network administrator.

Likewise, set [GATEWAY], [DNS Server] with the basic gateway and the DNS server addresses provided by the network manager.

When all settings are completed, click[Apply] to apply the settings. The settings are applied when the system restarts, so restarts the system by clicking [Restart].



4.4 : WLAN Setting

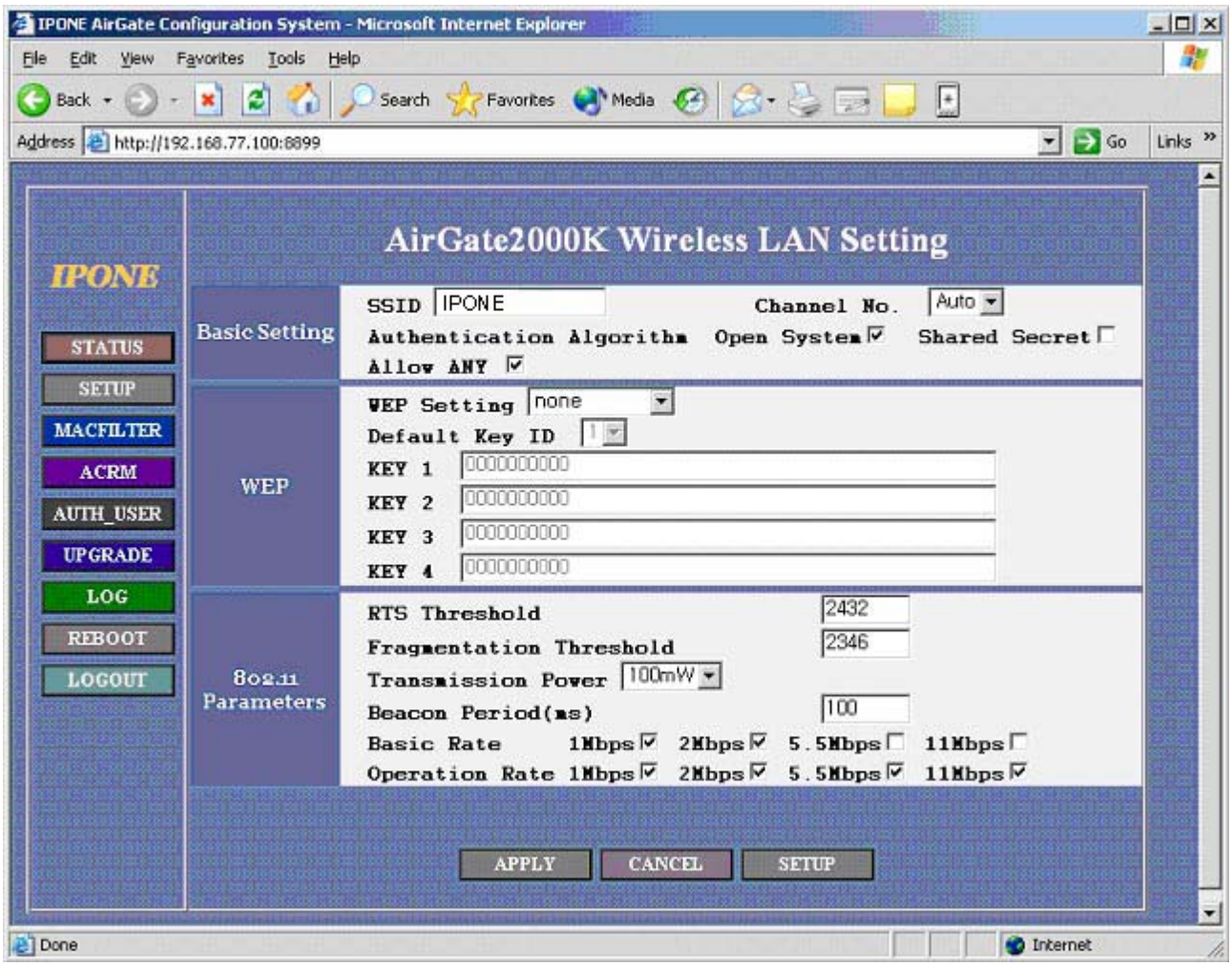
4.4.1 SSID and Channel Setting

Click the [Basic Setting] tab and enter [SSID] and [Channel] in [Wireless LAN].

Enter an SSID value, discriminating between large and small letters.

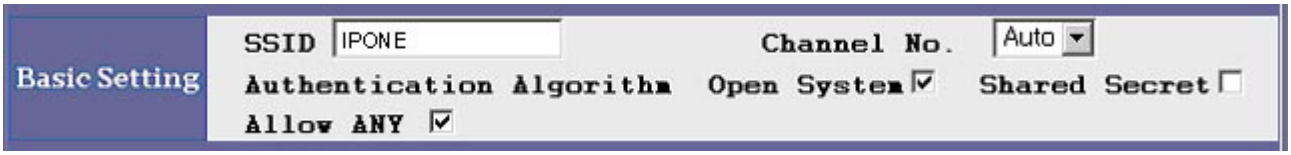
If you are assigned any channel, set the [Channel] of [Wireless LAN] to the channel (one of 1~11). If you have no assigned channel, set it to [Auto].

(Note: If another AP uses the channel that the AP is using or other channels around it, the AP performance may be degraded. In this case, click [Scan] to check whether the corresponding frequency is in use, and then change the channel to be used by the AP through consultation with the network manager.)



4.4.2 SSID ANY Allowed Mode Setting

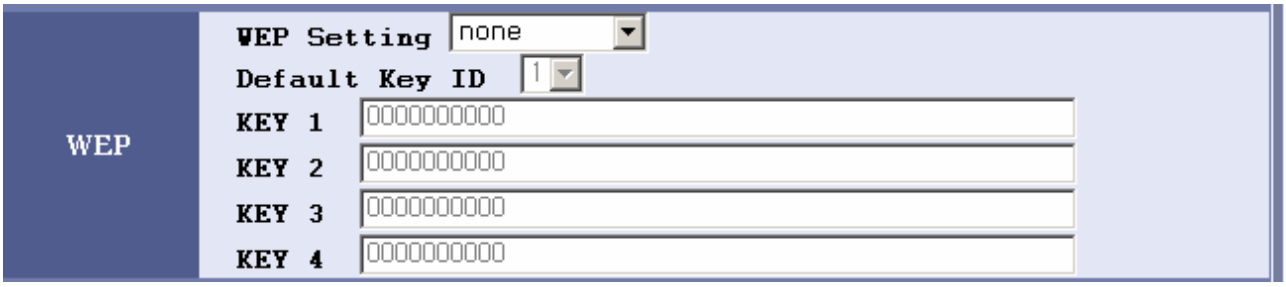
Select [Basic Setting] and then, [Wireless LAN]. If you check [ANY Allowed], you can see SSID and MAC address of AP through channel scanning in LAN card.



4.4.3 Wireless LAN Encryption

If you want to encrypt AP WLAN, select [Basic Setting] and then, [Wireless LAN]. Set [Default Key

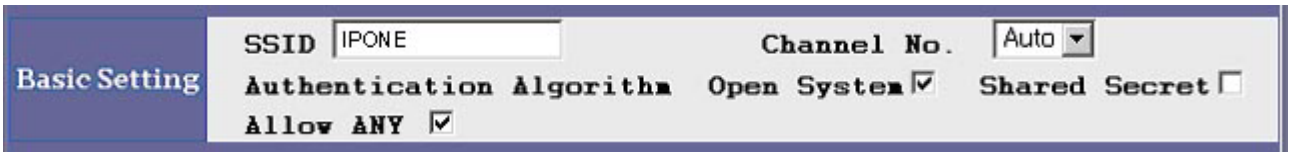
ID] and [Default Key] with WEP Key ID and WEP Key assigned by network administrator and then, [WEP Setting].



For details on WEP (Wired Equivalent Privacy), refer to the section 3.

4.4.4 WLAN Authentication

The section 3 describes WLAN authentication.

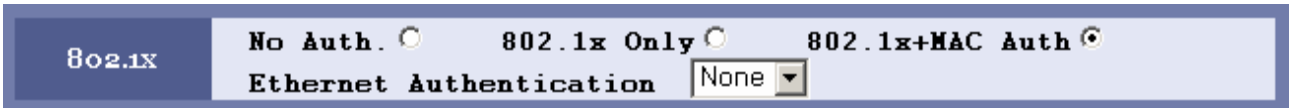


4.5 : Authentication and Billing Configuration

4.5.1 Authentication and Billing Basin Setting

Select [Basic Setting] and then, [Authentication Setting]. First, ask network administrator authentication/billing method. Second, select one of [No Auth], [802.1x Auth] and [802.1x + Mac Auth]. Third, set the details in [Authentication Setting].

Provided that authentication and billing are performed on IEEE 802.1x protocol, select [802.1x Auth]. If they are based on MAC address confirmation as well as IEEE 802.1x protocol, select [802.1x + Mac Auth].



4.5.2 802.1X Authentication

Select either [802.1x Auth] or [802.1x + Mac Auth]. After selecting [802.1x_Setting], ask administrator the registered radius server IP and enter IP address, port number and secret key in [Default Server] in [Authentication Server].

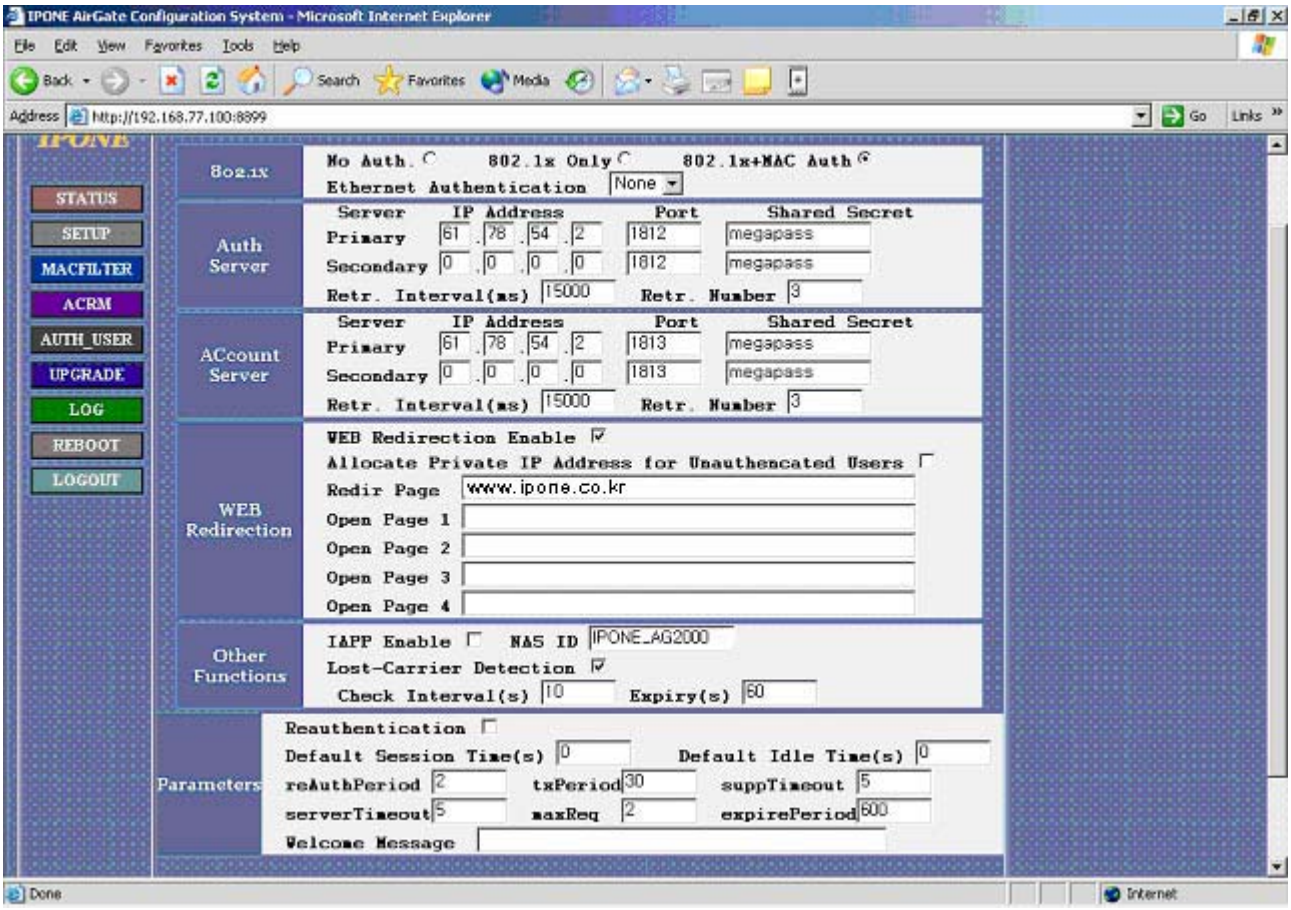
If there is a secondary billing sever, enter its IP address and secret key too. Press[Apply]button.

4.5.3 MAC Authentication

Select the [802.1x + Mac Authentication]. To enable MAC authentication, MAC address of the current user PC should be registered to the radius server.

Setting of radius server is same as that of 802.1x authentication.

When all settings are completed, press [Apply] button to apply the settings.



4.6 : Other Setting for Authentication and Billing

When required by the network manager, you have to set authentication-related service.

Other settings for authentication include web redirection, IAPP, lost carrier detection and parameters.

4.6.1 Web Redirection

This item sets whether to open a certain web page for unauthenticated terminals when they access with the web browser.

With the authentication applied, select [Use Web Redirection] in [Web Redirection]. Enter an initial web redirection page in [Redir Page] and then, pages to open in [Open Page 1~4]. Press [Apply] button.

4.6.2 IAPP

For 802.1x authentication, select whether to enable roaming function between same

subnets.

4.6.3 Lost Carrier Detection

This function determines whether to terminate 802.1x authentication when no radio signal is sent from terminal.

4.6.4 Reauthentication

This item sets reauthentication status for the case when the terminal is not informed of reauthentication status by the radius server at the time of 802.1x or MAC authentication. For example, if this flag is not set, the terminal terminals the session without reauthentication at the time of session timeout. When reauthentication status is informed by the radius server, this value is ignored.

4.5.5 Welcome message

Set a message to be delivered to terminal by using EAP-notification when 802.1x access succeeded. This message is ignored when reply-message is received from radius server.

4.7 : SNMP Setting

4.7.1 SNMP Agent Setting

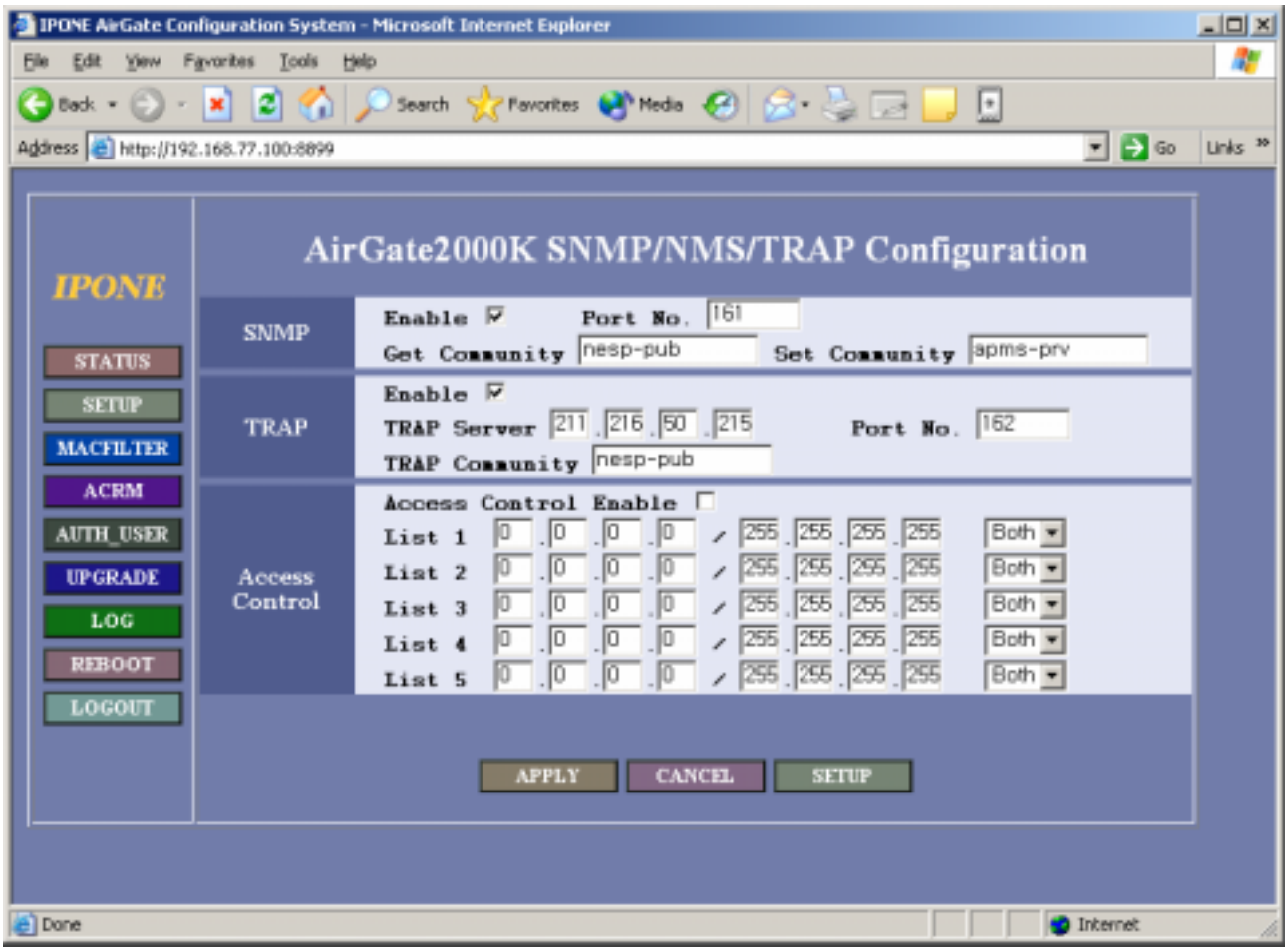
When the network manager wants to manage Aps outside, you have to set the system accordingly. Set [SNMP Community setting] table according to what is required by the network manager, in [SNMP Setting] in [System Setting].

Select [Use TRAP] and [Enable] in [SNMP]. If the network administrator has designated Get Community and Set Community, check [Get Community] and [Set Community]. Press [Apply] button to change the settings.

To control traffic attempting to access SNMP, designate network address and network mask which have right to access [Access Control] and then, select either Deny or Allow for access control mode.

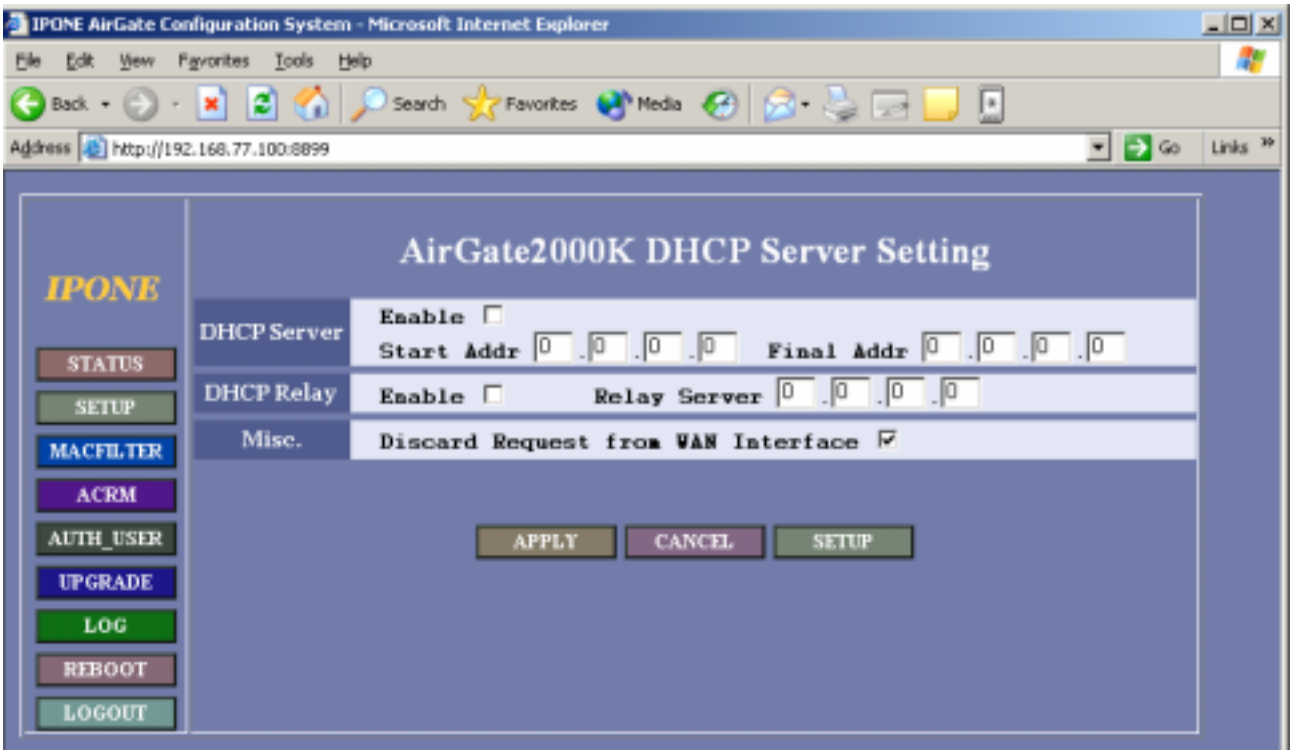
4.7.2 SNMP Trap Setting

In [SNMP/TRAP] of [Basic Setting] menu, select [Use TRAP] according to requirements of the network administrator. After selecting [SNMP/TRP], select [Enable] in [TRAP] menu, and select TRAP IP Address Port number and Community if network administrator sets TRAP Server and Port number. Press [Apply] to change setting.

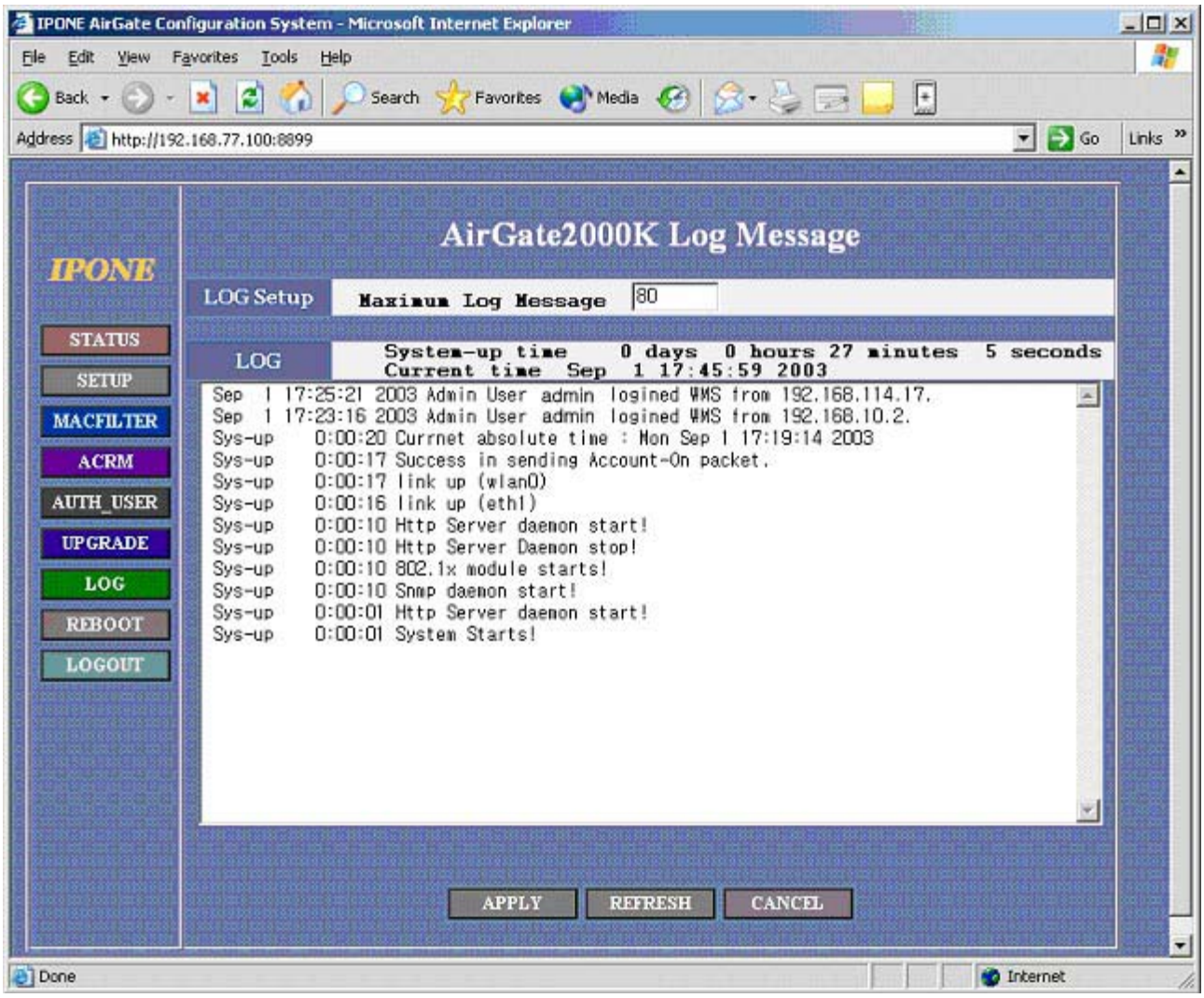


4.8 : DHCP Setting

Select [DHCP Setting] in [GATEWAY DNS]

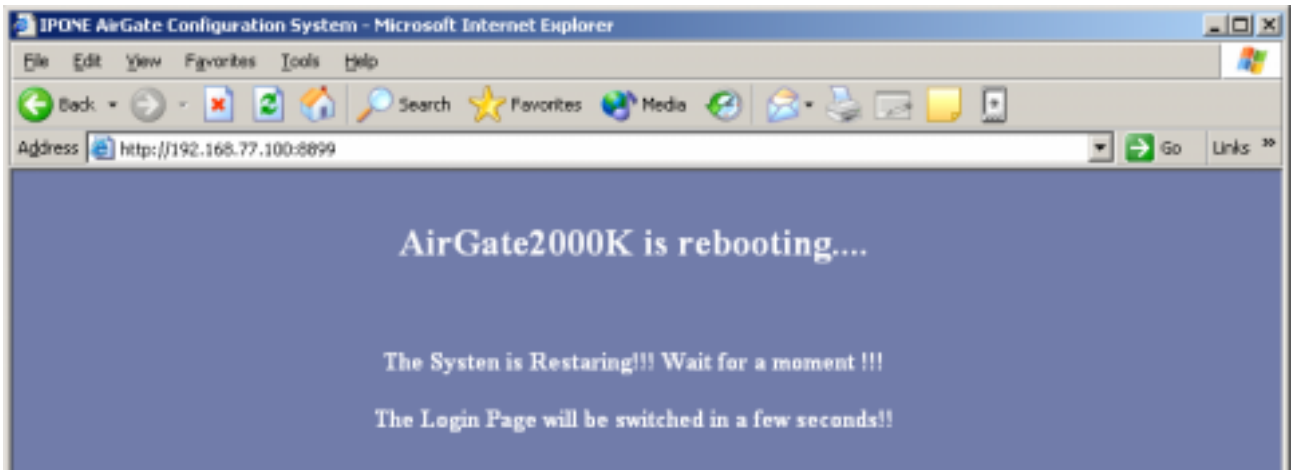

IPONE AirGate Configuration System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.77.100:8899
Go Links
IPONE
STATUS
SETUP
MACFILTER
ACRM
AUTH_USER
UPGRADE
LOG
REBOOT
LOGOUT
AirGate2000K DHCP Server Setting
DHCP Server
Enable
Start Addr 0 . 0 . 0 . 0 Final Addr 0 . 0 . 0 . 0
DHCP Relay
Enable
Relay Server 0 . 0 . 0 . 0
Misc.
Discard Request from WAN Interface
APPLY
CANCEL
SETUP

4.9 : LOG

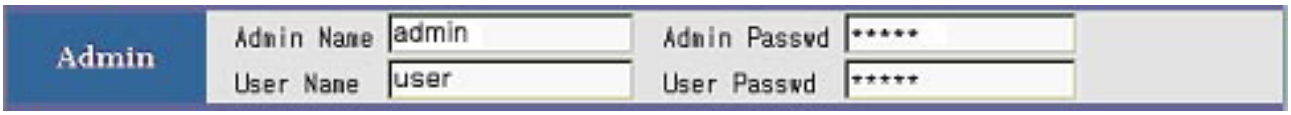


4.10 : System Reboot

Change system setting or reboot the system if required. If you select [Reboot], the screen below is displayed and you can connect to the original screen after about 1 minute.



4.11 : AP Management Tool Login Password Change

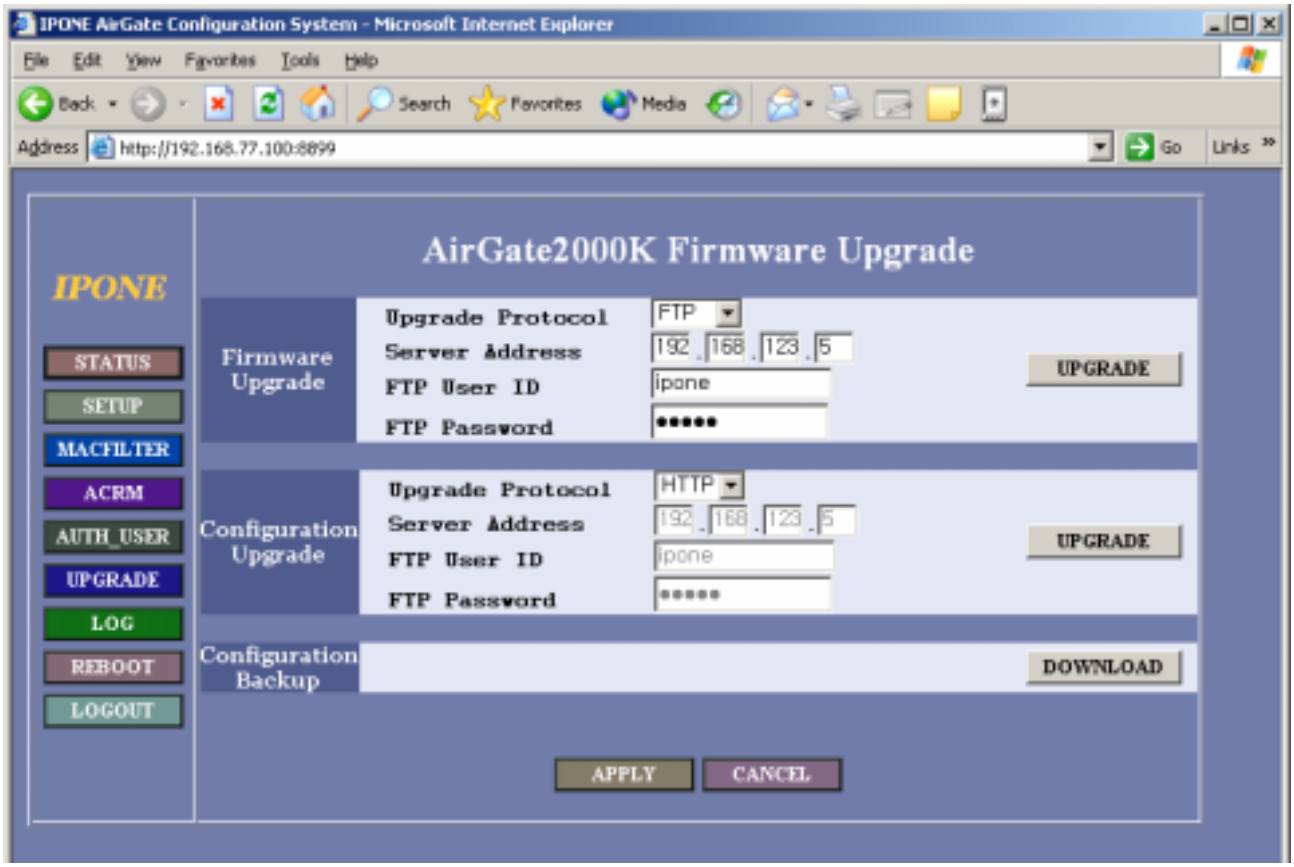


This item is used for changing the management password. Enter the current password and new password and confirm the new password. Unless you are a system administrator, do not change the management password.

4.12 : Firmware Upgrade

<Notice> Do not power off the system or disconnect network while upgrading software image or configuration. It may cause a critical problem in the system.

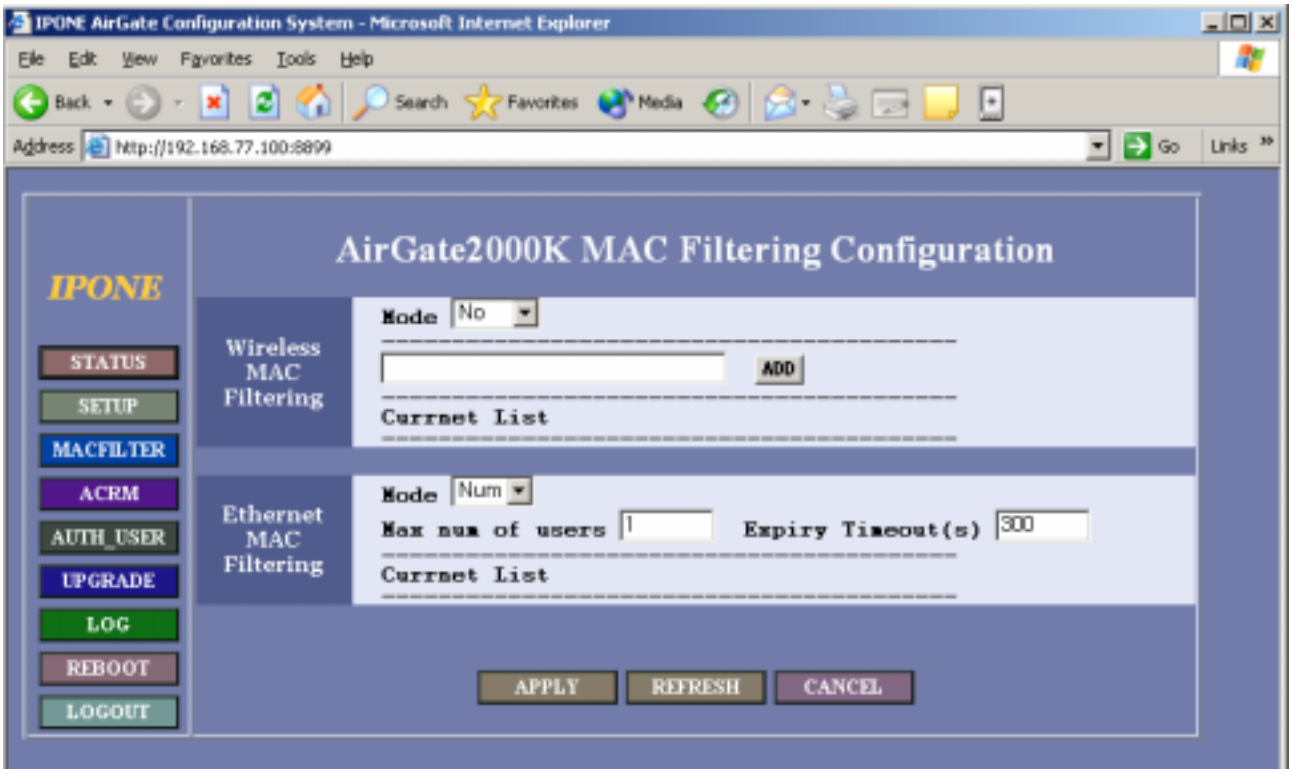
Click the [UPGRADE]. You can upgrade firmware image through network. Enter IP address to the upgrade server. Select the upgrade operation as [Image Upgrade]. Enter IP address to the upgrade server. Select the protocol used by the upgrade server, HTTP, FTP or TFTP. Enter the FTP account and password of the upgrade server in order, and press [UPGRADE_NOW] button.



4.13 : Other Setting

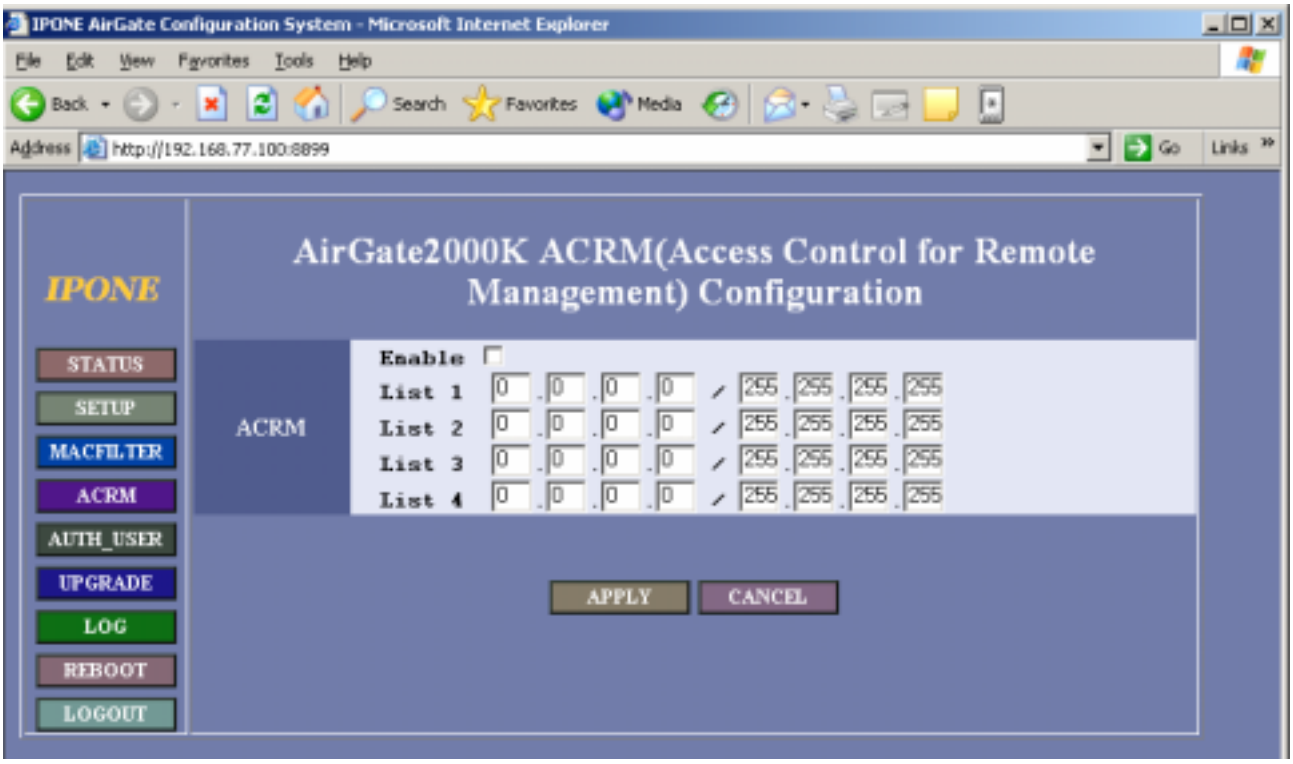
4.13.1 MAC FILTERING

With [MAC FILTER] function, you can perform 'Deny' or 'Allow' by entering terminal's MAC Address. In addition, you can restrict the number of user on Ethernet side through Ethernet MAC filtering, and figure out information on Ethernet user.



4.13.2 Access Control

If you click [ACRM], you can allow or deny terminal access for managing AP according to Subnet.



4.14 : Quick Installation

4.14.1. AP default is set according to ISP's environment. Items to be changed are as follows. (Note: Do not change other than the following items).

- IP address, Subnet mask, Gateway

4.14.2. How to change IP, Subnet mask, Gateway

1) Basic commands in Console terminal (Hyper Terminal) are as follows:

```
* AP status information check: S
* AP setting : C
* Firmware Upgrade/other command: U
* AP reboot : reboot
* Logout : quit
```

2) If you want to change IP, Subnet mask and Gateway, log in and enter 'C' -> 'I' in order. Enter 'Y' if you are asked whether to change the setup, and go on according to each step.

Example of input: Initial screen ->'C'-> '1' -> 'Y'-> Set according to the step.

! Note: Do not change other than IP, Subnet and Gateway.

· The table below shows examples of item set when shipped from the factory.

· Item marked '#' in the table below is used for AG2500 only.

```
------------------------------------------------------------
            IPONE AirGate 2000K Wireless Router <Admin mode>
------------------------------------------------------------
   Configuration Menu :   1. Basic Configuration
      - Admin Login Name : admin
      - Admin Passwd : *****
      - User Login Name : user
      - User Passwd : ******
      - System Mode : Bridge
      - DHCP Client Enable : N
      - WAN IP Address : 10.0.0.2  -> Item to be changed
      - WAN Network Mask : 255.255.255.0  -> Item to be changed
      - Default Gateway : 10.0.0.1  -> Item to be changed
      - DNS Server : 168.126.63.1
      - Enhanced Security for LAN Station : N
------------------------------------------------------------
 Change the Configuration ? <y/N>
```

* The table below shows examples when changing setting.

: When changing setting, value in brace ([ ]) means currently set value, and just press

'enter' in items other than IP, Netmask and Gateway, and enter value in the item to be changed.

```
- Enter the new configuration!

        - Admin Login Name[admin] : Enter
        - Admin Passwd[*****] : Enter
        - User Login Name[user] : Enter
        - User Passwd[*****] : Enter
        - System Mode(Bridge|Routed|PPPoE)[Bridge] : Enter
        - DHCP Client Enable[N] : Enter
        - WAN IP Address[10.0.0.2] : -> Enter IP address
        - WAN Network Mask[255.255.255.0] : -> Enter Subnet mask
        - Default Gateway[10.0.0.1] : -> Enter Gateway
        - DNS Server[168.126.63.1] : Enter
        - Enhanced Security for LAN station[N] : Enter
```

After entering values, a question about Save and Reboot appears, enter 'Y' (Yes).

5. Service Opening Method

5.1 Checkpoints before Installation

5.1.1 Places to Be Avoided for Installation

① Moist or humid places

② Too cold or hot places

③ Places where interference may occur, such as around thick walls or steel structures

5.1.2 AP Components

Refer to 1.4.1

5.2 Installation

5.2.1 Installation overview

Install AP -> Install wireless LAN card -> Install one clock program.

5.3 Work Procedures

5.3.1 AP Installation Steps

① Set power switch to “OFF”.

② Connect power supply adapter to “DC IN” connector of the system, and connect the opposite side to the outlet.

③ Connect “LAN” connector to PC Ethernet port (Ethernet card is already installed in PC) with Ethernet cable (UTP).

④ Connect phone access terminal in-house installed to “LINE” connector of the system with phone cable-A.

⑤ Connect desired phone to “PHONE” connector of the system with phone cable-B.

⑥ If required, connect external ground wire to “F.G” connector in order to protect the product.

⑦ For connecting monitor cable, connect serial cable (that DB-9 port and RJ-45 port are connected in serial) to serial port for PC, and Console port for AP. Connect serial cable to PC directly with hyper terminal, and use it when setting AP.

5.4 Configuration Method

5.4.1 AP Set Up

Set up the AP, referring to the Guide. After connecting AP through the console cable and executing hyper terminal, set its address, connect to web and then set ssid and channels.

5.4.2 Wireless LAN Card Insertion

Insert a wireless LAN card to the terminal. According to how to use the wireless LAN card, set Essid the same as that of AP to be connected and then check the link. With this, AP installation is completed.

5.4.3 Precautions

Use the designated power adaptor. Do not disassemble the product unless you are an authorized technician.

Do not drop or apply any impact to the AP.

5.5 Considerations

5.5.1 Considerations

Open service in reference to the following items:

- AP installation location

Install AP at a place where radio wave is less attenuated. Radio wave is attenuated because of distance, obstacle, etc. In particular, do not install AP around concrete wall, metal and microwave oven.

- Wireless LAN Card

Check Link status of the terminal in which wireless LAN card is inserted.

- Channel

Channels 1~11 are used in U.S.A. Check to see if channels 1~11 are available for wireless LAN card.

- Authentication server

Check Auth Server secret key and AP secret key.

6. Maintenance and Fault Handling

6.1 If authentication is not performed.

Check to see if communication is performed to Auth Server

- Check Ping from AP to Auth Server.

6.2 If Auth Server IP address is set abnormally

- Check to see if Auth Server IP address is normally entered when setting AP.

6.3 If Auth Server secret key is set abnormally

- Check Auth Server secret key when setting AP.

6.4 If authentication is overlapped

- Check to see if authentication is performed through another ID. If authentication is possible through another ID, contact with a person in charge of Auth Server to cancel authentication. This is generated if subscriber does not log off after authentication and turn off AP power by force.