APPENDIX G

: USER’S MANUAL

CMAX Stand-alone WLAN Module User Manual

Upgrade History

Date	Version	Comment
2010-04-13	1.0	Initial Release

Contents

1. General Description 6
1.1 Features 6
1.2 Applications 6
1.3 Product description 6
1.4 Specification 7
2. Installation 8
2.1 Fundamentals of wireless LAN 9
2.1.1 Infrastructure Mode 9
2.1.2 Ad-hoc Mode 10
2.1.3 Basic Requisites 10
2.1.4 Authentication and Security 10
2.2 Installation 11
2.2.1 Making Wireless LAN Network 11
3. Configuration 14
3.1 Configuration with WLAN Module Manager 14
3.1.1 Configuration via WLAN 15
3.1.2 Configuration via Serial 15
3.1.3 Printer Search 16
3.1.4 System 16
3.1.5 Protocol 17
3.1.6 BSS Info 18
3.1.7 Network 18
3.1.8 Authentication 19
3.1.9 Certification 21
3.1.10 Firmware 21
3.1.11 Information 22
3.2 Web Configuration 22
3.2.1 Web Connection 23
3.2.2 Home 24
3.2.3 System 24
3.2.4 Protocol 26

3.2.5 Network 26
3.2.6 Authentication 26
3.2.7 Wizard 27
3.2.8 Web Site 28
3.2.9 Contact 28
3.3 TELNET 29
3.3.1 TELNET Connection 29
3.3.2 System 30
3.3.3 Protocol 30
3.3.4 Network 31
3.3.5 Authentication 32
3.3.6 Save 36
3.3.7 Exit 36
3.4 FTP 36
3.4.1 FTP Connection 36
3.4.2 Config File list view 37
3.4.3 Config File download 37
3.4.4 Config File Upload 37
3.4.5 Config File Specification 38
3.5 SNMP 40
3.5.1 SNMP Connection 40
3.5.2 SNMP Manager operation test..41
4. Hardware Block Diagram 44
4.1 Hardware Pin Array 45
5. Demo and Test 45
5.1 Test environment 45
5.1.1 Hardware 45
5.1.2 Software 45
5.2 Start Test 46
5.2.1 STEP1. 46
5.2.2 STEP2. 46
5.2.3 STEP3. 46
6. Configuration Tool Command List 46
6.1 Configuration Tool Protocol 46
6.1.1 Serial Operation Specification 46
6.1.2 WLAN Operation Protocol & Port 47
6.2 Serial & WLAN Command 47

6.2.1 Serial Operation 47
6.2.2 Wireless LAN Operation 49
6.2.3 Serial & Wireless LAN Command Format 49
7. Technical Support, Warranty, and Precaution 55
7.1 Technical Support 55
7.2 Warranty 55
7.2.1 Refund 55
7.2.2 Free Repair Services 56
7.2.3 Charged Repair Services 56
7.3 Precaution 56
7.4 USA-Federal Communications Commission (FCC)..57
7.4.1 Labeling 57

1. General Description

CMAX stand-alone WLAN Module"supports stand-alone WLAN system which embeds MCU(Micro Controller Unit) with various configuration applications, monitoring functions and security protocols.

The stand-alone WLAN system, along with CMAX S/W package, can easily be adapted to target systems which have RS-232 serial interface to enable wireless network (IEEE802.11 b/g) functionality with no redesign of the system, thus making the system connected, controlled and maintained in WLAN network.

1.1 Features

- Embedded 802.11b/g Wireless Networking
- Supports Serial to WLAN, Infrastructure, Ad-hoc mode
- Supports network status indicator LEDs
- UART/SPI Interface
- Strong Security with WEP 64/128, WPA/WPA2 Personal, Enterprise
- Supports DHCP Client, HTTP, HTTPS, TELNET, FTP, ARP, SNMP, IPv4, TCP, UDP Protocol
- Compact design 30mm × 40mm × 4.8mm
- Distance Outdoor: approx. 100m

1.2 Applications

- POS Equipment
- Automotive Applications
- Medical Equipment
- Street Furniture
- Telematics
- Industrial Automation
- Metering Applications

1.3 Product description

CATEGORIES	IMPLEMENTATION

	CMAX Stand-alone WLAN Module
	Debugger board
	Serial Cable **(Serial Communication Cable)**
	Power **(DC 5V/200mA Adapter)**
	CD **(User Manual and H/W, S/W Doc Package)**

[Table 1.3.1] Product Description

1.4 Specifications

ITEM	SPECIFICATIONS
WIRELESS SPECIFICATION	
Wireless Standard	IEEE802.11b, IEEE802.11g
Frequency Range	2.412~2.484GHz (USA version: 2.412 ~ 2.462 GHz)
Channels	1 ~ 14 Channels (USA version: 1 ~ 11 Channel)
Baseband Processing	OFDM, CCK and DSSS
Modulation	BPSK, QPSK, 16-QAM, 64-QAM
Range	Up to 100m free space (Outdoor)
Connection Modes	Infrastructure and Ad-hoc (IBSS)
RF PERFORMANCE	
Transmit Power (Conducted)	Max 15 dBm (802.11g), Max 18 dBm(802.11 b)
Receive sensitivity(802.11g)	Receive sensitivity(6Mbps) : -89dBm
	Receive sensitivity(54Mbps) : -72dBm

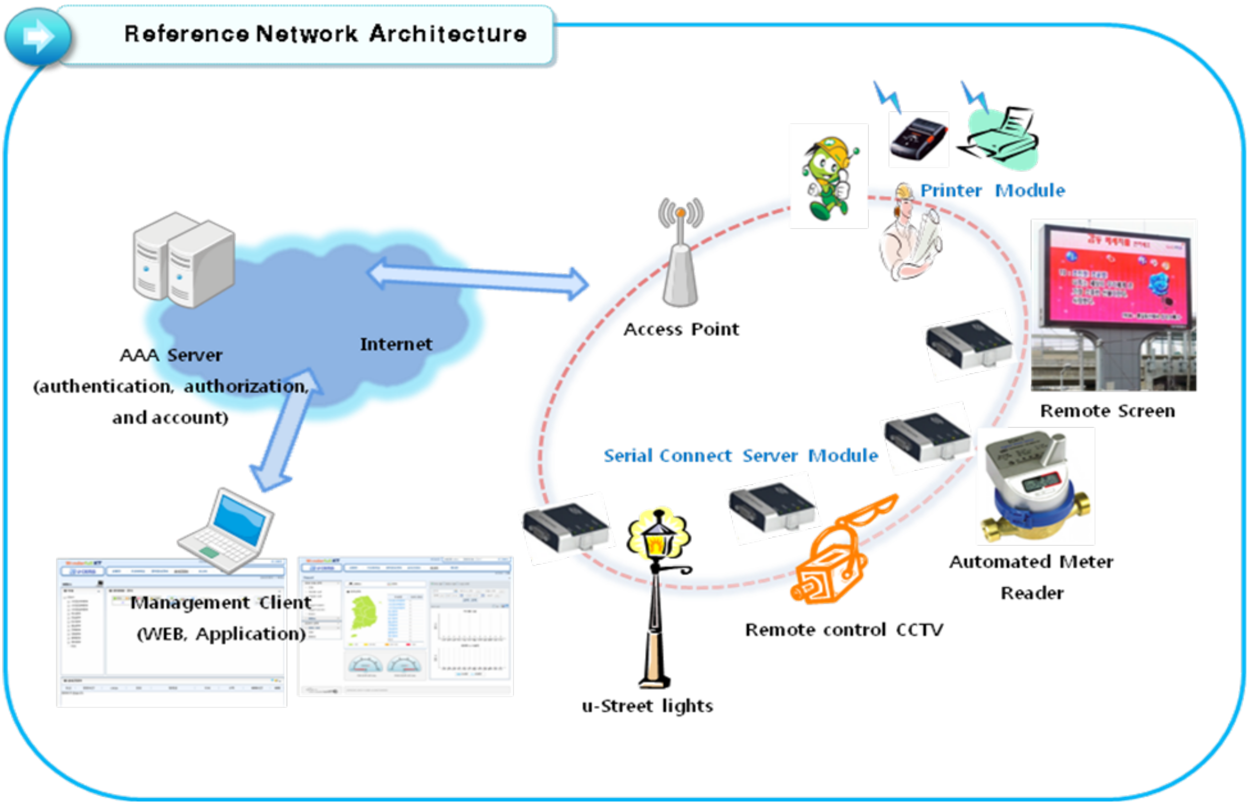
Antenna Gain	2dBi ± 0.5 dBi, (internal chip antenna)
Tx EVM	Min 25dB (54Mbps)
Tx Center Frequency Accuracy	20ppm
Tx Symbol Clock Frequency Tolerance	20ppm
Tx Spectrum Mask	-21dBr @ fc +/- 11MHz
	-29dBr @ fc +/- 20MHz
	-41dBr @ fc +/- 30MHz
Tx Spectral Flatness	2dB/ - 4dB
UART INTERFACE	
Baud Rate	115,200bps
Bits	8
Parity	None
Stop bits	1
Flow Control	CTS/RTS (Hardware)
PROTOCOL	
Internet	DHCP Client, HTTP, HTTPS, TELNET, FTP, ARP, ICMP, SNMP, IPv4, TCP, UDP
Security	Open Connection
	Shared Key (WEP encryption 64 and 128 bit options)
	WPA1/2-Personal (PSK)
	WPA1/2-Enterprise (EAP-TLS, EAP-TTLS, PEAP, LEAP, FAST)
	SSL2 / SSL3 / TLS1
OTHERS	
Management	Configuration Tool, HTTP, HTTPS, TELNET, FTP
Software Update	Firmware upgradeable via UART and Wireless LAN
PHYSICAL DIMENSION	
Power	80mA * 3.3V (Peak 90mA * 3.3V)
Dimensions	30mm × 40mm × 4.8mm
Weight	8g (Approx.)
Power Consumption	264mW (Peak 297mW)
MCU	200MHz ARM9 with SRAM 8M and Flash 8M
Environmental	-5℃ ~ 55℃
	-20℃ ~ 70℃
Humidity	Operation: 10% to 90%, Non-Condensing
	Storage: 5% to 90%, Non-Condensing

[Table 1.4.1] Specification

2. Installation

2.1 Fundamentals of wireless LAN

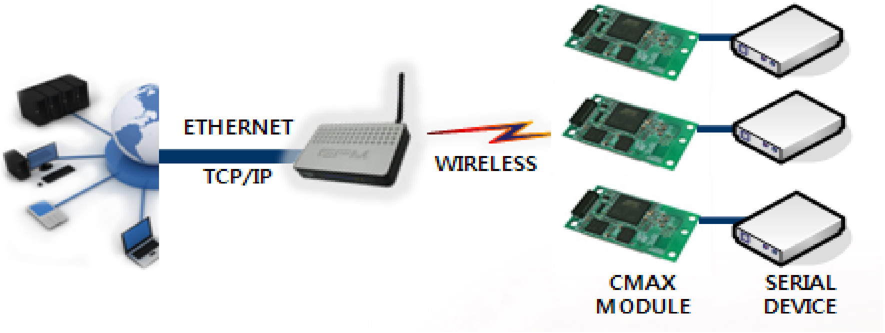
CMAX Module supports IEEE802.11b/g. The IEEE802.11b and IEEE802.11g support 11Mbps and 54Mbps transmission rate respectively. There are two types of wireless LAN networks – infrastructure and ad-hoc.



[Figure 2.1.1] Reference Network Architecture

2.1.1 Infrastructure Mode

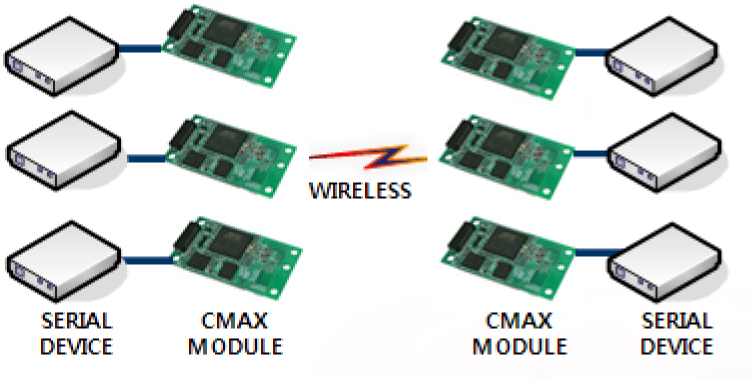
The wireless LAN stations communicate through an Access Point (AP). So, at least one AP is needed to make the infrastructure network. The wireless LAN station can talk to wired network hosts because AP relays between wireless LAN stations as well as between wireless LAN station and wired LAN (Ethernet) host.



[Figure 2.1.1.1] Infrastructure

2.1.2 Ad-hoc Mode

Wireless stations communicate each other without the AP. So user can make a system more simply. It is proper if there's no wired LAN requirement and it is a small network. Some people call it peer-to-peer mode.



[Figure 2.1.2.1] Ad-Hoc

2.1.3 Basic Requisites

- SSID

It is an identifier to identify the particular wireless LAN. So the same SSID should be configured to all stations to communicate in the same wireless network. In case of infrastructure mode, user has to set his station's SSID as same as AP's.

- Channel

IEEE802.11b/g wireless LAN stations communicate through the ISM (Industrial, Scientific, and Medical) band whose frequency is about 2.4GHz. IEEE802.11 specification divides this band into 14 channels every 5MHz. If user installs more than one wireless LAN networks in the same area, the channels should be apart more than 4 channels to avoid interferences.

2.1.4 Authentication and Security

- Authentication

A wireless LAN station should get authentication from the AP in the infrastructure mode. There are the Open system and the Shared key for the authentication methods.

- WEP (Wired Equivalent Privacy)

The WEP is a secure protocol for wireless LAN. There are two kinds of WEP method - 64 bits and 128 bits key.

- WPA (Wi-Fi Protected Access)

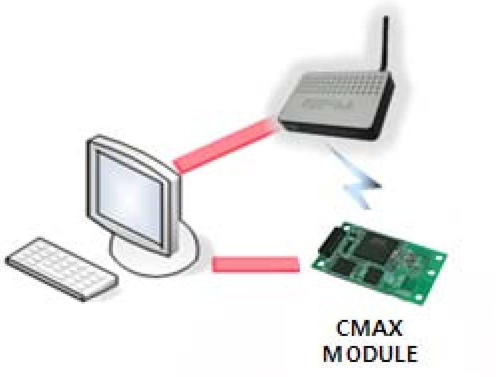
WPA is a security standard for users of device equipped with Wi-Fi wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). There are two modes about the user authentication in WPA security. The one is Enterprise which has authentication server and the other one is PSK (Pre-Shared Key) which doesn't have any server. CMAX Module supports both Enterprise mode and Personal mode (WPA-PSK).

- WPA 2

To final security of Wireless LAN, IEEE 802.11i, a standard about Wireless LAN, has suggested the Counter Mode with Cipher Block Changing Message Authentication Code Protocol (CCMP) for replacing the TKIP. CCMP uses Advanced Encryption Standard (AES), it is the WPA 2 that adopts the using the method. WPA 2 has also both Enterprise and PSK mode. CMAX Module supports also both them.

2.2 Installation

Before testing, users should connect the CMAX Module. There are two methods for connecting. The first method is to connect a target device with the serial port and the other method is to connect by wireless LAN card on your PC.



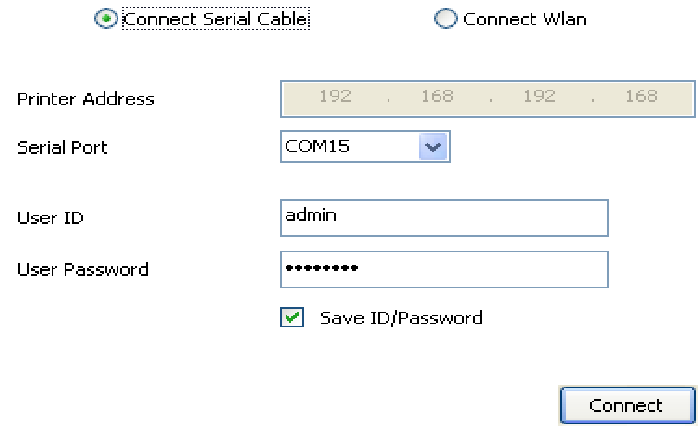
[Figure 2.2.1] Connect between CMAX Module and a PC

2.2.1 Making Wireless LAN Network

Even though you connect an AP on your network, wireless LAN network could not be made automatically. You should configure values of items which related with wireless network. Please follow the below steps.

- Connect the CMAX Module through serial port

Start the WLAN Module Manager on your PC. Push the “Connect” button after Selecting a COM port, User ID and User Password as the same values with the your COM port.



● Connect Serial Cable ○ Connect Wlan

Printer Address: 192 . 168 . 192 . 168

Serial Port: COM15

User ID: admin

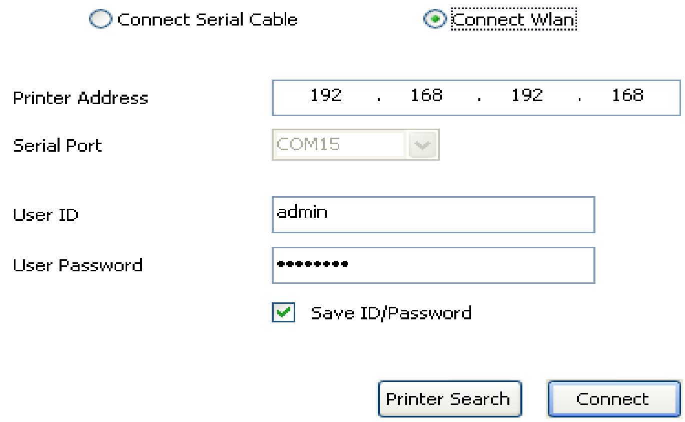
User Password: ••••••••

☑ Save ID/Password

[Figure 2.2.1.1] Connect through serial port

- Connect the CMAX Module through WLAN

Start the WLAN Module Manager on your PC. Click the “Connect” button after inserting IP Address, User ID and User Password as the same values with the CMAX Module.



○ Connect Serial Cable ● Connect Wlan

Printer Address: 192 . 168 . 192 . 168

Serial Port: COM15

User ID: admin

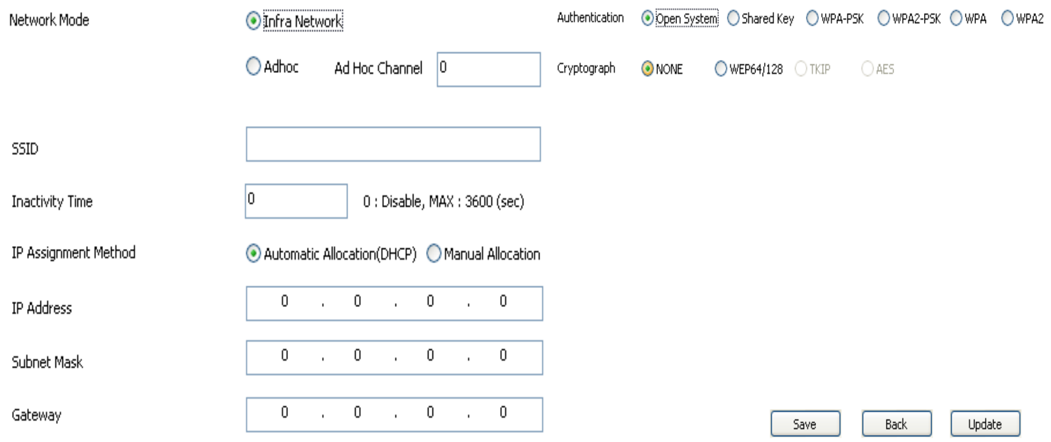
User Password: ••••••••

☑ Save ID/Password

[Figure 2.2.1.2] Connect through WLAN

- Configuring Wireless LAN Parameters

Move to the [Network] menu and setting SSID as the same values with the AP's. Then, move to the [Authenticaton] menu and setting security options. Finaly, Click the "Update" button. Please ask the manufacturer of the AP, when you want to know about setting the AP's value.



Network Mode ● Infra Network ○ Adhoc Ad Hoc Channel 0

Authentication ● Open System ○ Shared Key ○ WPA-PSK ○ WPA2-PSK ○ WPA ○ WPA2

Cryptograph ● NONE ○ WEP64/128 ○ TKIP ○ AES

SSID

Inactivity Time 0 0 : Disable, MAX : 3600 (sec)

IP Assignment Method ● Automatic Allocation(DHCP) ○ Manual Allocation

IP Address 0 . 0 . 0 . 0

Subnet Mask 0 . 0 . 0 . 0

Gateway 0 . 0 . 0 . 0

[Figure 2.2.1.3] Configuring Wireless LAN Parameters

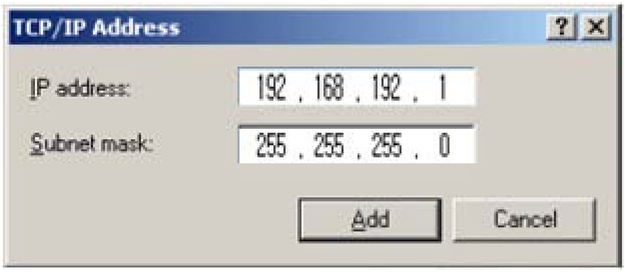
If you want to make an Ad-hoc network, choose the [Ad-hoc] as the value of [WLAN Topology] and set a value of [SSID]. Then, try to connect your PC to the network.

2.2.2 Setting Network Aera

This step is for setting both CMAX Module and your PC to be located the same network. If only they are, the TCP connection between them can be established.

- Setting of the PC

Add or change the IP address of the network adapter on your PC like following. Get into the menu of [Windows Control Panel] >> [Network Connections] >> [Properties of the Network Adapter - with right click of your mouse]. Then, you can show the properties of [Internet Protocol (TCP/IP). In there, press the [Advanced] button for adding an IP Address like the below figure.



TCP/IP Address

IP address: 192 . 168 . 192 . 1

Subnet mask: 255 . 255 . 255 . 0

[Figure 2.2.2.1] adding / changing the IP address of users' PC

- Setting of CMAX Module

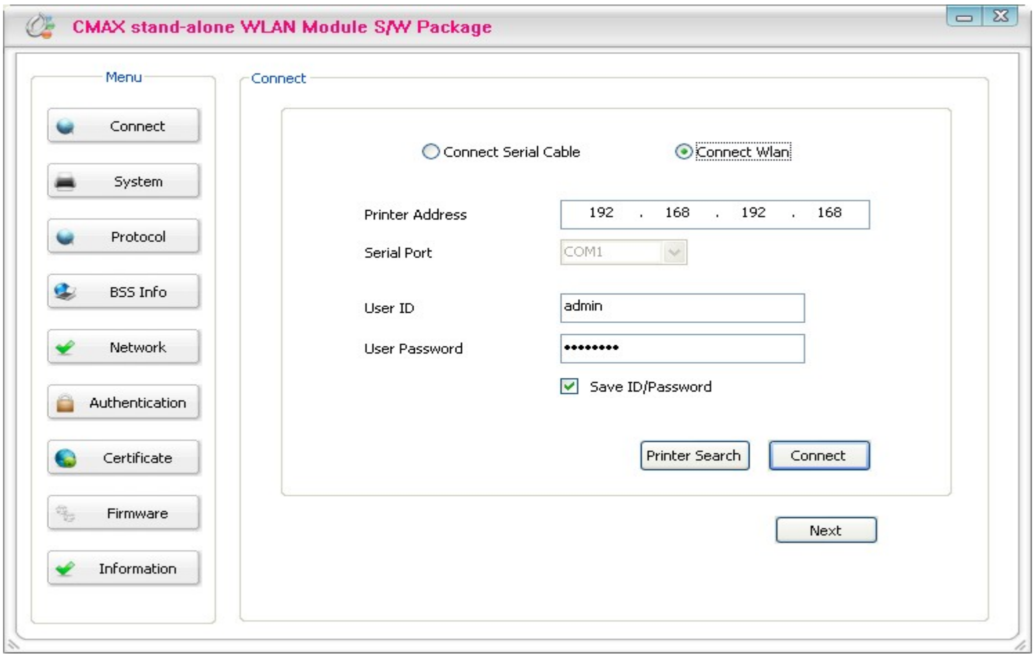
CMAX Module uses WLAN Module Manager as it's a configuration program. WLAN Module Manager is for MS Windows, and this is comfortable to use because it doesn't need installation. First, search your WLAN Module via network. All the values of parameters are set the default values in the factory. To apply it to your system, proper values should be set via WLAN Module Manager. Major parameter's default values are listed on below table. To implement this simple test, keep these values without any changes.

DISTRIBUTION	FUNCTION	VALUE
System	User ID	admin
	User Password	password
Protocol	FTP	Disable
	TELNET	Disable
	HTTP	Enable / HTTPS is disable
	SNMP	Disable
		Community Name (Read) : Public
		Community Name (Write) : Private
		Trap Destination IP Address : 0.0.0.0
		Trap Destination Community Name : Public
		Trap Mode : 1 (Enable), 0 (Disable)
Network	Locality	Disable
	Network Mode	Ad-hoc, channel 1
	SSID	CMAX_adhoc
	IP Assignment Method	Manual Allocation
	IP, Subnet, Gateway	IP : 192.168.192.168
		Subnet : 255.255.255.0
		Gateway : 192.168.192.1
Authentication	Open System	None
	Shared key	None

[Table 2.2.2.1] Default values of Major parameters

3 Configuration

3.1 Configuration with WLAN Module Manager



CMAX stand-alone WLAN Module S/W Package

○ Connect Serial Cable ● Connect Wlan

Printer Address: 192 . 168 . 192 . 168

Serial Port: COM1

User ID: admin

User Password: ••••••••

☑ Save ID/Password

[Figure 3.1.1] initial appearance of WLAN Module

3.1.1 Configuration via WLAN

- Checklists

Make sure the WLAN connection between your PC and WLAN Module Manager. If they are the same network, [search] button can be used. If they aren't, [IP Address] should be inserted to use.

- Procedures

1) Printer Address : Set the values of the CMAX Module's IP Address properly
2) User ID : Set the values of the User ID
3) User Password : Set the values of the Password
4) Connect : Connect through Wireless LAN to CMAX Module
5) Next : Move to System Configuration page.

Note : If you want to save [ID/Password], it choose the checkbox.

3.1.2 Configuration via Serial

- Checklists

Make sure the connection between your PC and WLAN Module Manager using RS232 direct cable. To use this, WLAN Module Manager has to be operating in the [Serial Configuration] mode. You press the “Connect” button after Selecting a COM port, User ID and User Password as the same values with the your COM port. Then, You can enter the [Serial Configuration] mode.

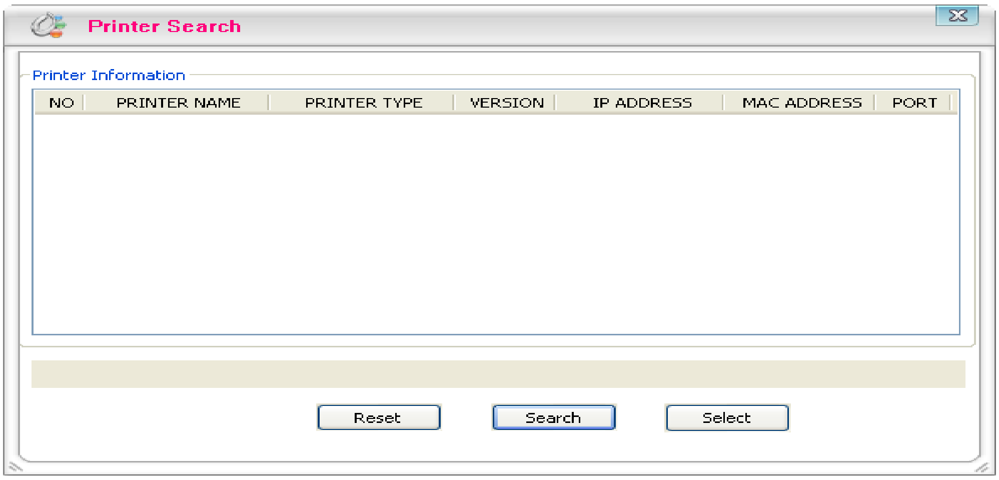
- Procedures

1) Serial Port : Select a COM port as the same values with the your COM port.
2) User ID : Set the User ID
3) User Password : Set the User Password
4) Connect : Connect through Serial communication to CMAX Module
5) Next : Move to the configuration page of system

Note : If you want to save [ID/Password], it choose the checkbox. After changing the configuration, you must be rebooted CMAX Module.

3.1.3 Printer Search

: Provide information of CMAX Module in the network.



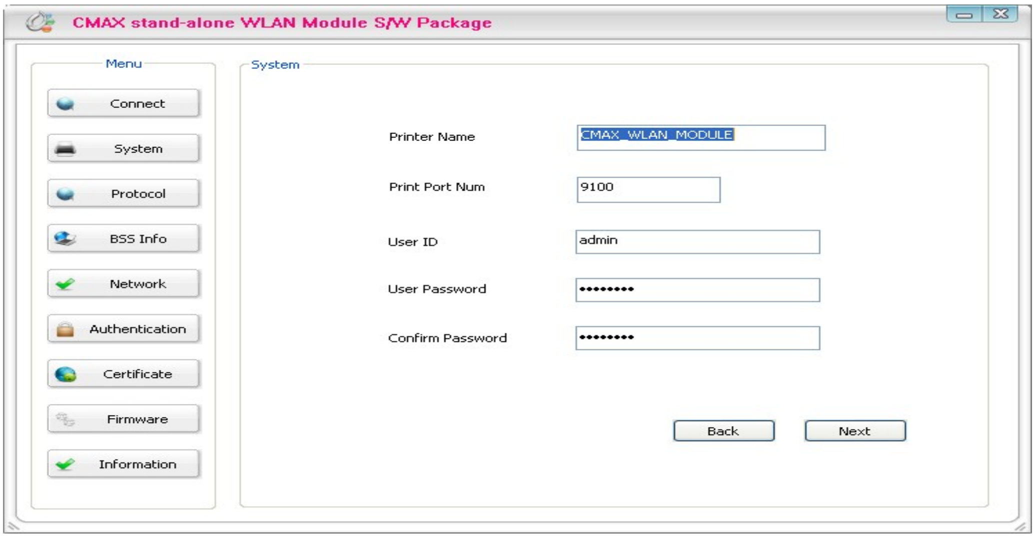
NO	PRINTER NAME	PRINTER TYPE	VERSION	IP ADDRESS	MAC ADDRESS	PORT

[Figure 3.1.3.1] Printer Search

- Reset : Delete the printer information
- Search : Search active printers in the network. If a network problem occurs, the printers will not scan. Then, you press the [Search] button again.
- Select : After selecting a printer to connect, you should press [Select] button.

3.1.4 System

: Set the Printer Name, Printer Port Num, User ID and User Password. User ID and password will be used to set the configuration.



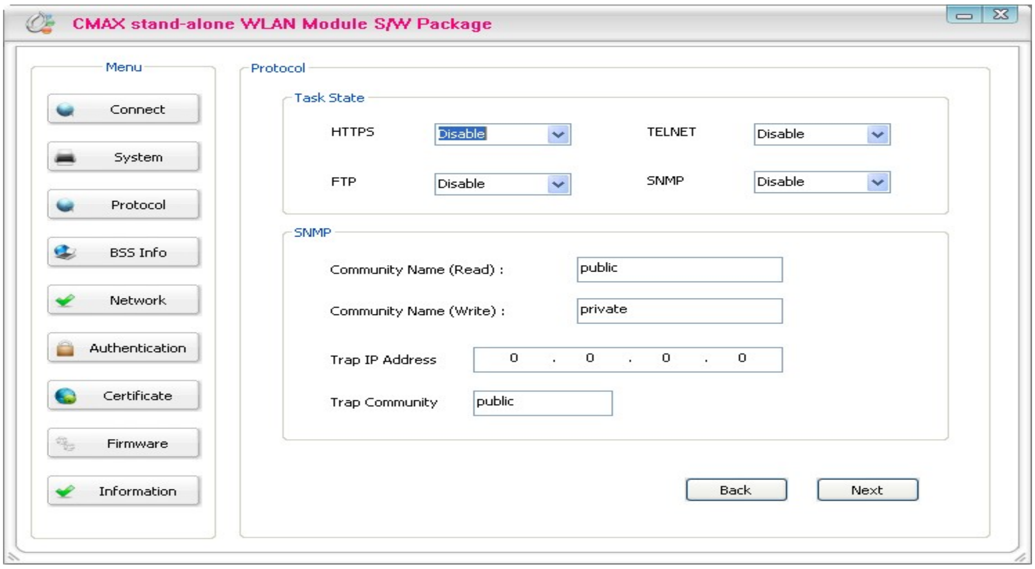
Printer Name: CMAX_WLAN_MODULE
Print Port Num: 9100
User ID: admin
User Password: ••••••••
Confirm Password: ••••••••

[Figure 3.1.4.1] System Setting

- Printer Name : Set the [Printer Name]
- Print Port Num : Set the [Print Port Num]
- User ID : Set the [User ID]
- User Password : Set the [User Password]
- Confirm Password : Set correct values of [Confirm Password]
- Next : Move to the configuration page of protocol
- Back : Move to the configuration page of connection

3.1.5 Protocol

: Select to use ftp, http and snmp that is application. For a description of each feature in the manual can be found at.



HTTPS: Disable
TELNET: Disable
FTP: Disable
SNMP: Disable

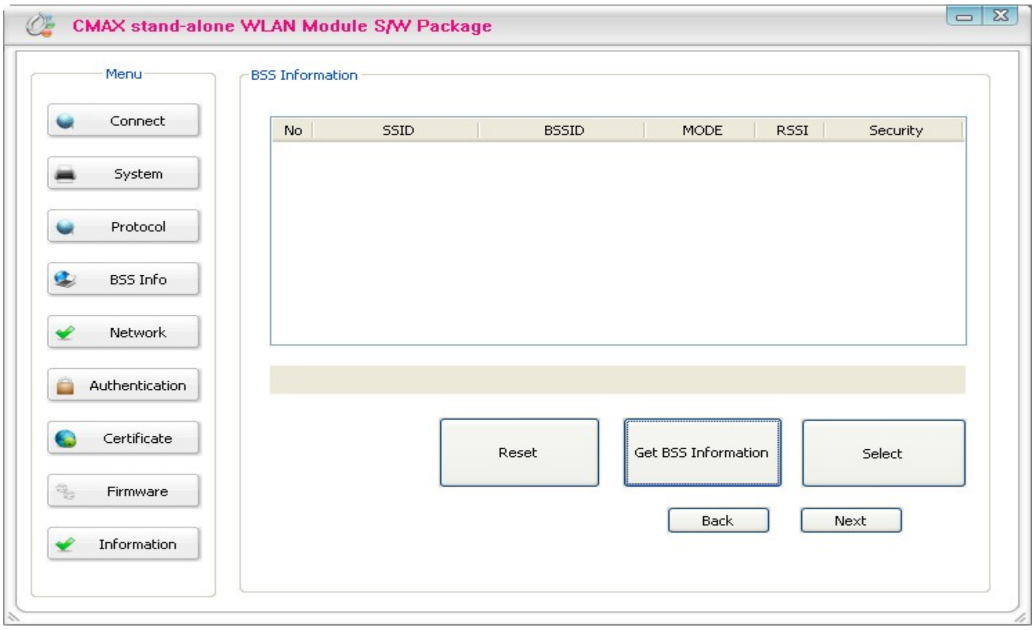
Community Name (Read) : public
Community Name (Write) : private
Trap IP Address: 0 . 0 . 0 . 0
Trap Community: public

[Figure 3.1.5.1] Protocol Setting

- Task State
  - Set the HTTPS, TELNET, FTP and SNMP that are applications if you use.
- SNMP
  - To perform SNMP sets for each item.
- Next : Move to the configuration page of BSS Information
- Back : Move to the configuration page of System

3.1.6 BSS Info

: After Searching on AP(Access Point), user can select to connect at the AP. Then, AP's SSID will be inserted automatically.



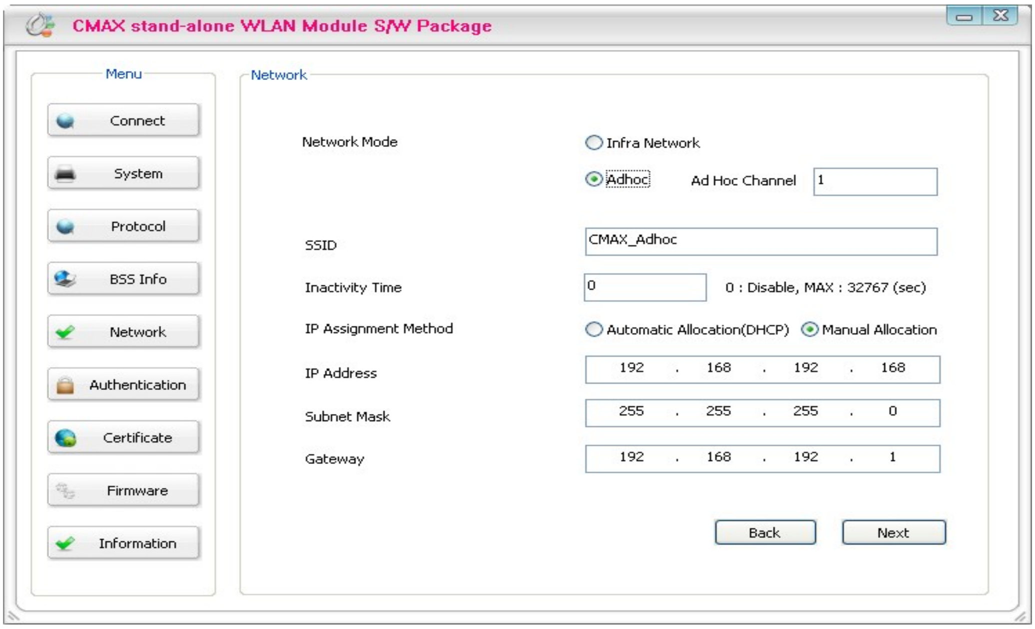
No	SSID	BSSID	MODE	RSSI	Security

[Figure 3.1.6.1] BSS Setting

- Reset : Delete current information of BSSID
- Get BSS Information : Scanning information of BSSID. If the problem of network occurs, the printers will not scan. Then, you press the [Get BSS Information] button again.
- Select : Select BSS that searched.
- Next : Move to the configuration page of Network
- Back : Move to the configuration page of Protocol

3.1.7 Network

: Set the network parameter of CMAX Module



Network

Network Mode: ○ Infra Network / ● Adhoc   Ad Hoc Channel: 1

SSID: CMAX_Adhoc

Inactivity Time: 0   0 : Disable, MAX : 32767 (sec)

IP Assignment Method: ○ Automatic Allocation(DHCP) ● Manual Allocation

IP Address: 192 . 168 . 192 . 168

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 192 . 1

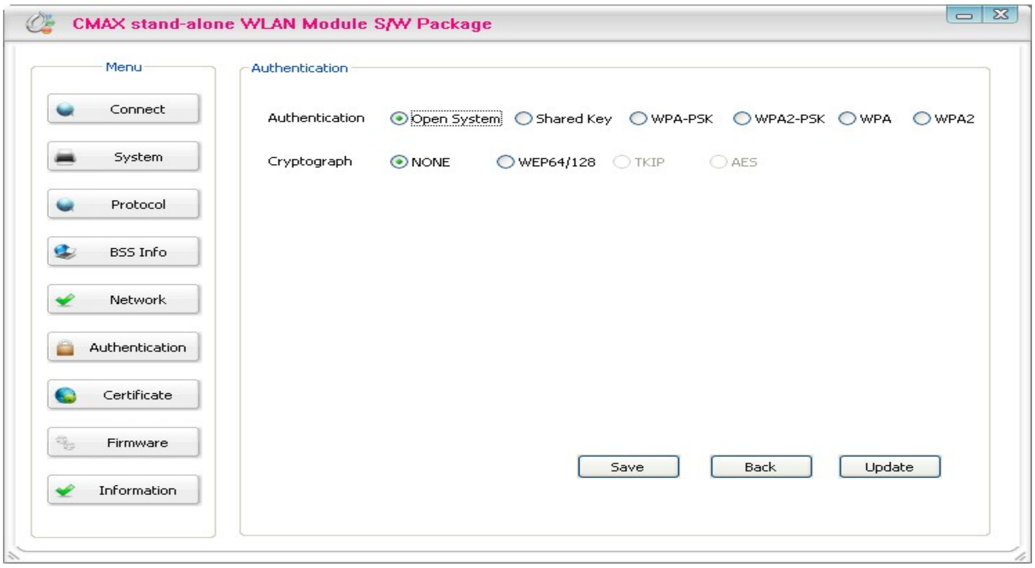
[Figure 3.1.7.1] Network Setting

- Network Mode : Select the Infra Network or Adhoc mode.
  Note : If adhoc mode user selects to connect a adhoc-channel (1~14).
- SSID : Set the SSID that user is going to connect. SSID Can set up maximum of 32 bytes.
- Inactivity Time : After connecting to the server of printer, It is time to maintain a connection with the server. Default setting : Disable, Maximun time : 32767(sec)
- IP Assignment Method : Supported Automatic Allocation(DHCP Client) or Manual Allocation. Default setting : Manual Allocation
  - Automatic Allocation(DHCP Client) : Assigns the IP Address that is assigned in the DHCP server automatically
  - Manual Allocation : Does not assign the IP address in the AP(Access Poing)'s DHCP server. User should insert the IP Address that is such as IP Address of AP.
- IP Address : Insert the [IP Address] of AP : Default IP Address : 192.168.192.168

- Subnet Mask : Insert the [Subnet Mask] of AP : Default subnet Mask : 255.255.255.0
- Gateway : Insert the [Gateway] of AP : Default Gateway : 192.168.192.1
- Next : Move to the configuration page of Authentication
- Back : Move to the configuration page of BSS Information

3.1.8 Authentication

: Set a security configuration of the CMAX Module



Authentication ● Open System ○ Shared Key ○ WPA-PSK ○ WPA2-PSK ○ WPA ○ WPA2

Cryptograph ● NONE ○ WEP64/128 ○ TKIP ○ AES

[Figure 3.1.8.1] Authentication Setting

- Authentication : It is security configuration between CMAX Module and AP(Access Point)

FIELD	DESCRIPTION	
Open System	**Cryptograph**	It should be select NONE or WEP64/128 as the setting of AP to be access
	WEP Key	You can input the max 26charater,. It Configure to WEPB64/18 if you input it like the following format. - WEP64 (5 ASCII, 10 HEX), WEP128 (13 ASCII, 26 HEX)
Shared Key	**Cryptograph**	Select a WEP64/128 same AP's configuration to be access.
	WEP Key	You can input the max 26charater,. It Configure to WEPB64/18 if you input it like the following format. - WEP64 (5 ASCII, 10 HEX), WEP128 (13 ASCII, 26 HEX)
WPA-PSK / WPA2-PSK	**Cryptograph**	You should same to configure a TKIP/AES with AP to be access.
	PSK Key	You should same to input a TKIP/AES with AP to be access.
WPA-TKIP / WPA2-AES	**Cryptograph**	You should same to configure a cryptograph with AP to be access.
	EAP	You should same to configure a EAP Mode with AP to be access.
	ID	You should Input the ID with configured certificate Server
	Password	You should Input the Password with configured certificate Server However, If EAP Configuration is a EAP-TLS, you should input the

		private_key_password that is certificate password that generated for CMAX module.

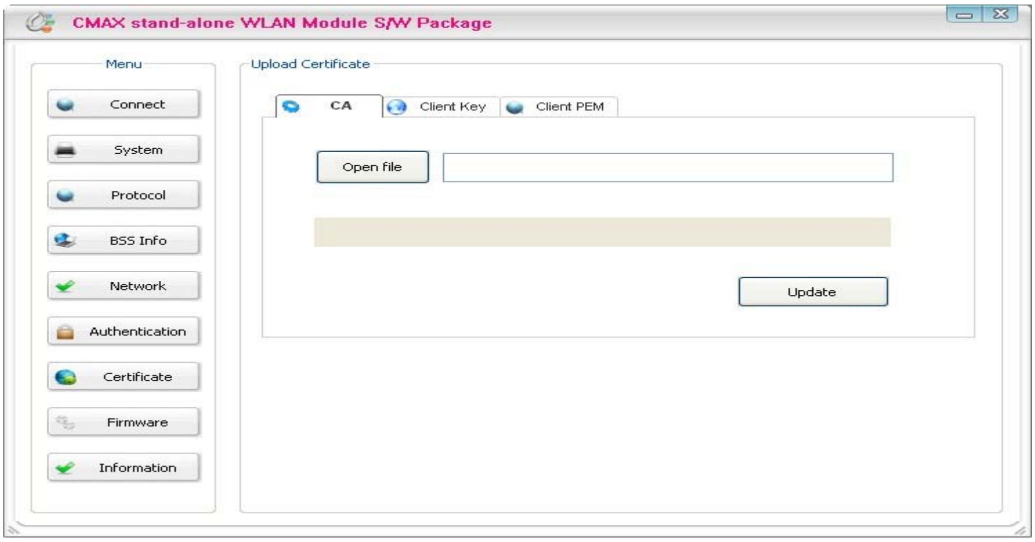
[Table 3.1.8.1] Security setting

- Save : It is function to Save the configuration information that you have set
- Saved file can set through uploading with FTP
- Update : User will save the configuration information to CMAX Module
- Back : Move to the configuration page of Network

Note : To upload a file must be named “Config” should be

3.1.9 Certification

: Can upload Certificates to CMAX Module for EAP-TLS certification

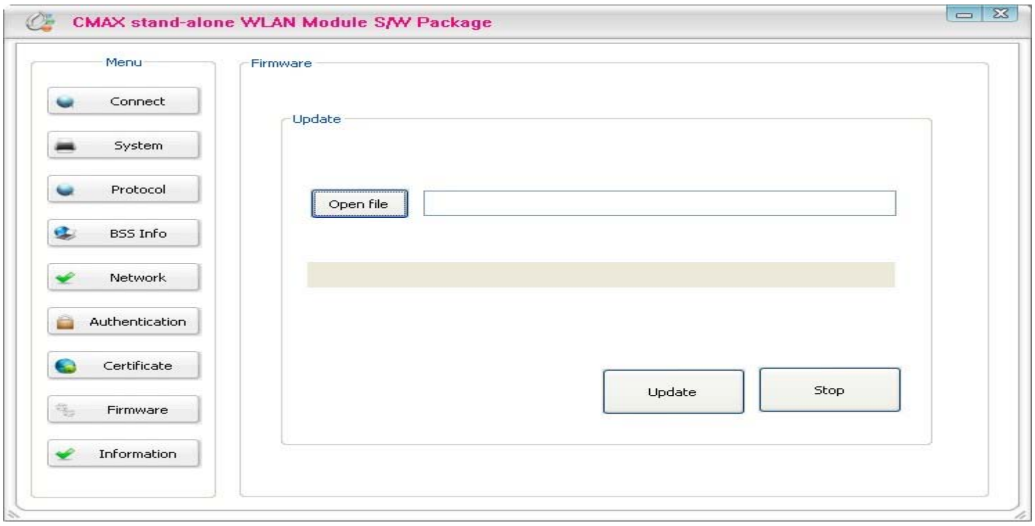


[Figure 3.1.9.1] Upload Certificate

- Upload Certification
  - Open file : Select the Certificate
  - Update : Save the Selecting a certificate to CMAX Module

3.1.10 Firmware

: It has been supporting the firmware upgrade. If It does not connect from CMAX Module, can not update the firmware. To stable firmware upgrade, we are not supported doing all of the eatures. After updating the firmware, CMAX Module must be rebooted.



[Figure 3.1.10.1] Upgrade Firmware

- Open file : Select a firmware type of [WLAN_M*.Bin]
- Update : Update a firmware to CMAX Module
- Stop : Stop the firmware upgraded

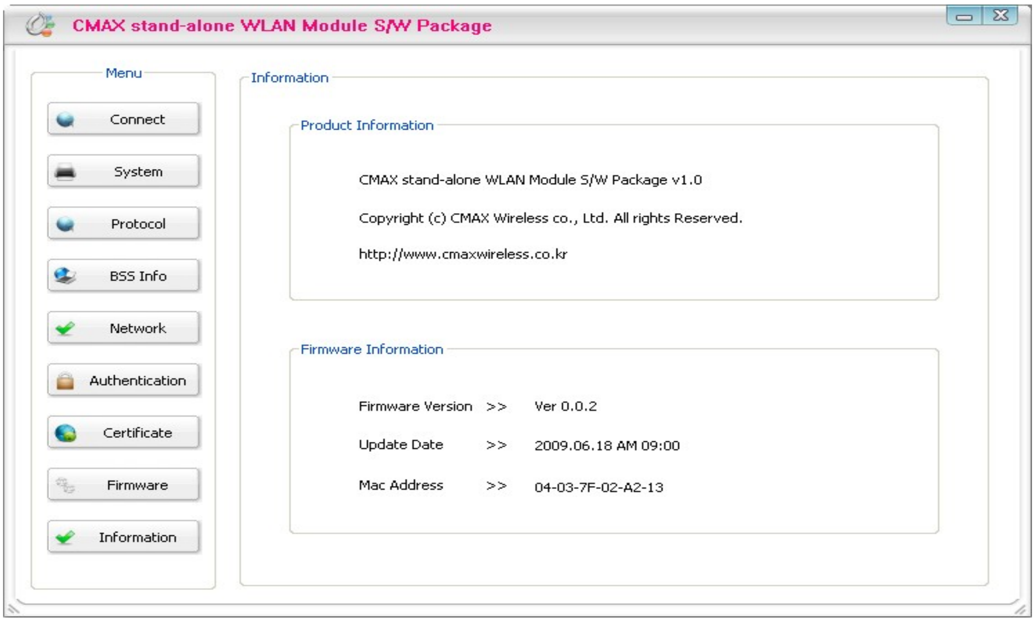
Note :

Emergency mode :

If an error occurs while firmware upgrade, CMAX module will be started to the emergency mode. Emergency mode does not support the security features. So You must update the full firmware to operate normal mode.

3.1.11 Information

: Product and firmware information is displayed



CMAX stand-alone WLAN Module S/W Package v1.0

Copyright (c) CMAX Wireless co., Ltd. All rights Reserved.

http://www.cmaxwireless.co.kr

Firmware Version >> Ver 0.0.2

Update Date >> 2009.06.18 AM 09:00

Mac Address >> 04-03-7F-02-A2-13

[Figure 3.1.11.1] Information

- Product Information : Product name
- Firmware Version : Firmware version
- Update Date : Updated date
- Mac Address : CMAX Module's Mac Address

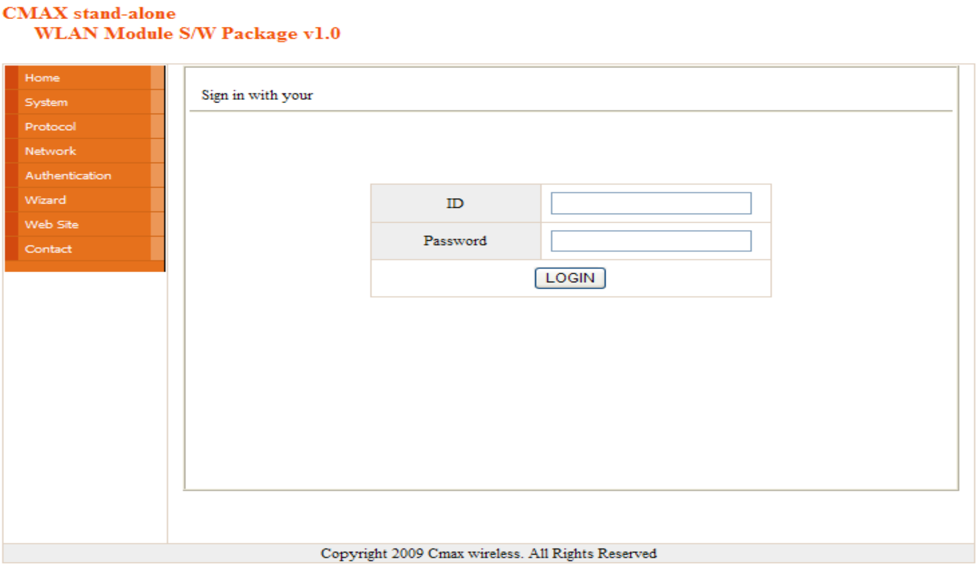
3.2 Web Configuration

Set the CMAX Modules's configuration through web connecting

3.2.1 Web Connection

: CMAX Module can Set configuration using the HTTP, HTTPS protocol. HTTP and HTTPS settings are same. Only, HTTPS secure connection is supported. Default setting is HTTP

- HTTP Connection : Start internet explorer through "http://192.168.192.168"
- Default : ID : **admin** Password : **password**
-



CMAX stand-alone
WLAN Module S/W Package v1.0

Sign in with your

ID

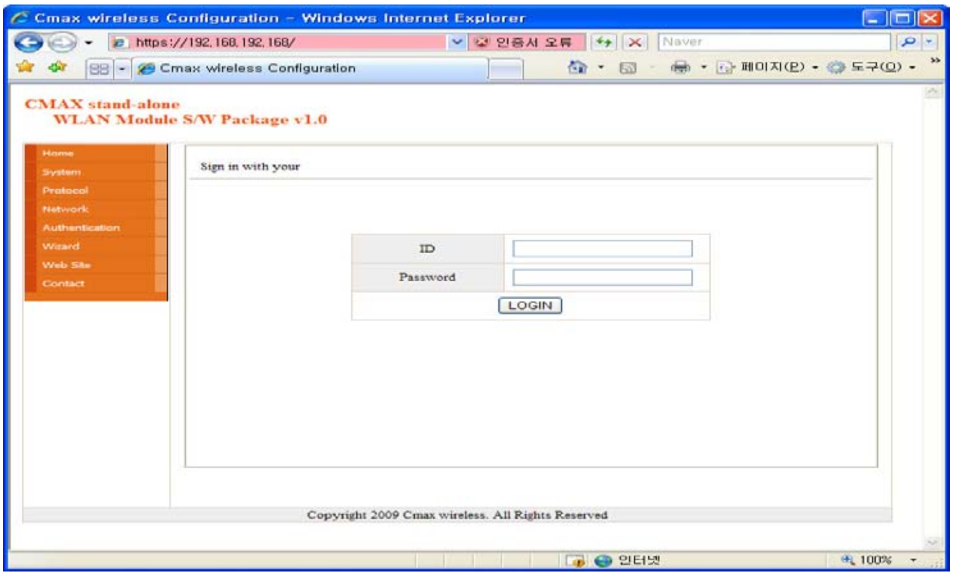
Password

Copyright 2009 Cmax wireless. All Rights Reserved

[Figure 3.2.1.1] Sign in with your

- HTTPS Connection : Start internet explorer through https://192.168.192.168
- Default : ID : **admin** Password : **password**

Note : When establishing a HTTP connection, to continue to ignore security warnings.



Cmax wireless Configuration - Windows Internet Explorer
https://192.168.192.168/
인증서 오류
Naver
Cmax wireless Configuration
페이지(P)
도구(O)
인터넷
100%

CMAX stand-alone
WLAN Module S/W Package v1.0

Sign in with your

ID

Password

Copyright 2009 Cmax wireless. All Rights Reserved

[Figure 3.2.1.2] HTTPS Sign in with your

Note :

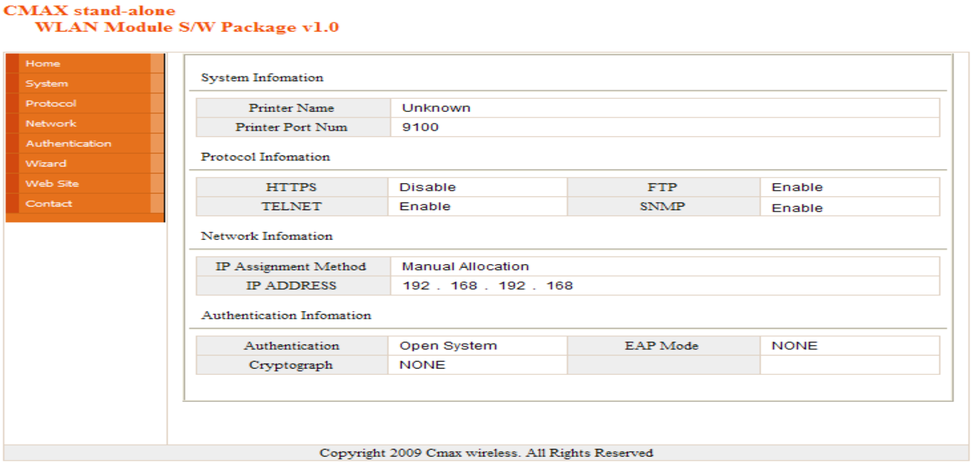
- Web Server Security feature

  - Supported the SSL 2.0, SSL 3.0 and TLS 1.0

  - For HTTPS connections, if you want to access from the computer, security protocol should be checked.

3.2.2 Home

: Display the system, protocol and network information in the CMAX Module



System Infomation

Printer Name	Unknown
Printer Port Num	9100

Protocol Infomation

HTTPS	Disable	FTP	Enable
TELNET	Enable	SNMP	Enable

Network Infomation

IP Assignment Method	Manual Allocation
IP ADDRESS	192 . 168 . 192 . 168

Authentication Infomation

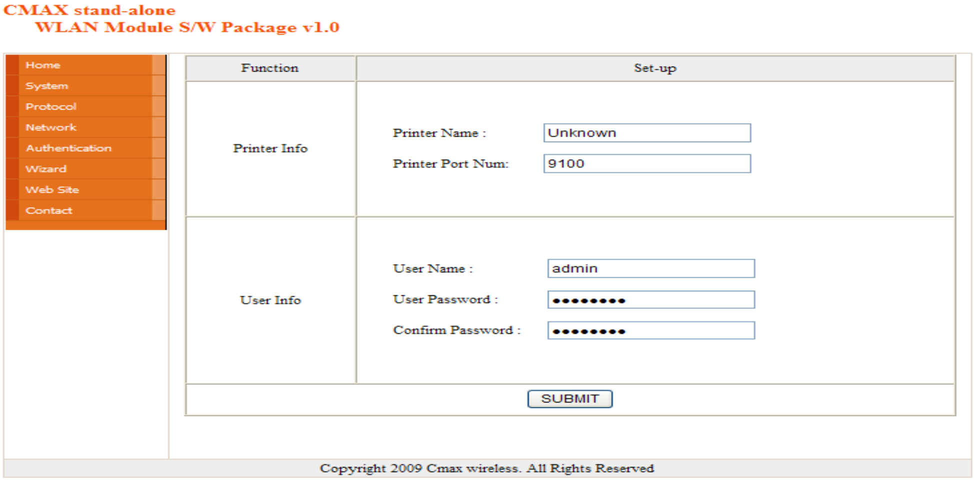
Authentication	Open System	EAP Mode	NONE
Cryptograph	NONE		

Copyright 2009 Cmax wireless. All Rights Reserved

[Figure 3.2.2.1] Home

3.2.3 System

: After inserting the [Pinter Name], [Printer Port], [User Name] and [User Password], user should press the “SUBMIT” button to set system configuration



Function	Set-up
Printer Info	Printer Name : Unknown Printer Port Num: 9100
User Info	User Name : admin User Password : •••••••• Confirm Password : ••••••••

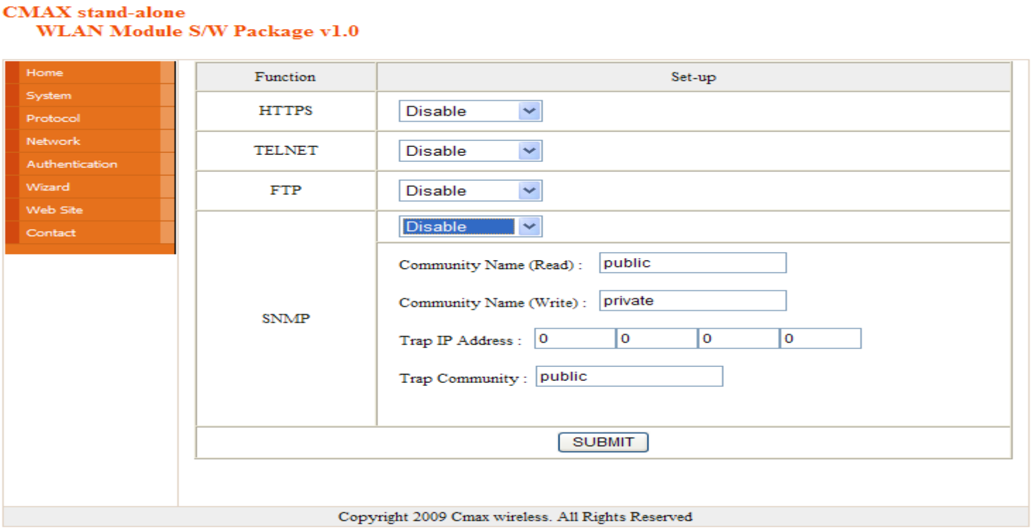
Copyright 2009 Cmax wireless. All Rights Reserved

[Figure 3.2.3.1] System Setting

- Printer Name : Set the [Printer Name]
- Print Port Num : Set the [Print Port Number]
- User ID : Set the [User ID]
- User Password : Set the [User Password]
- Confirm Password : Set correct values of [Confirm Password]
- Default : User ID : admin , User Password : password

3.2.4 Protocol

: Set the HTTPS, TELNET, FTP and SNMP that are applications if you use. Then To perform SNMP sets for each item. After inserting, user should press the “SUBMIT” button to set Protocol configuration



CMAX stand-alone
WLAN Module S/W Package v1.0

Function	Set-up
HTTPS	Disable
TELNET	Disable
FTP	Disable
SNMP	Disable Community Name (Read) : public Community Name (Write) : private Trap IP Address : 0 . 0 . 0 . 0 Trap Community : public

Copyright 2009 Cmax wireless. All Rights Reserved

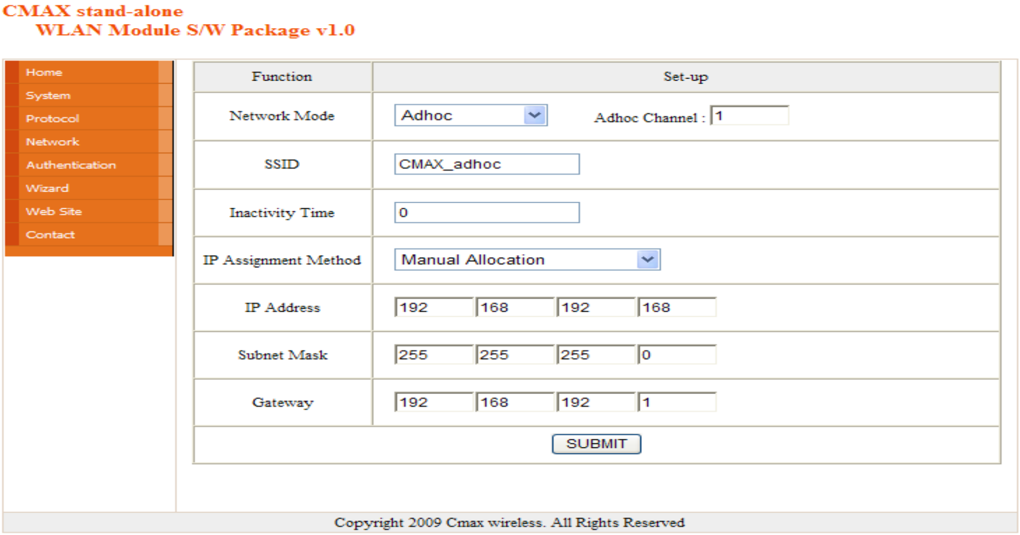
[Figure 3.2.4.1] Protocol Setting

- Setup
  - HTTPS (Default setting is HTTP)
  - TELNET (Default setting is disable)
  - FTP (Default is disable)
  - SNMP (Default is disable)

- SNMP
  - Community Name (Read) : Read Community
    - Default : Public
  - Community Name (Write) : Write Community
    - Default : Private
  - Trap IP Address : Trap IP Address.
    - Default : 0.0.0.0
  - Trap Community : Trap Community
    - Default : Public

3.2.5 Network

: After inserting the network configuration, user should press the “SUBMIT” button to set.



CMAX stand-alone
WLAN Module S/W Package v1.0

Function	Set-up
Network Mode	Adhoc, Adhoc Channel : 1
SSID	CMAX_adhoc
Inactivity Time	0
IP Assignment Method	Manual Allocation
IP Address	192 168 192 168
Subnet Mask	255 255 255 0
Gateway	192 168 192 1

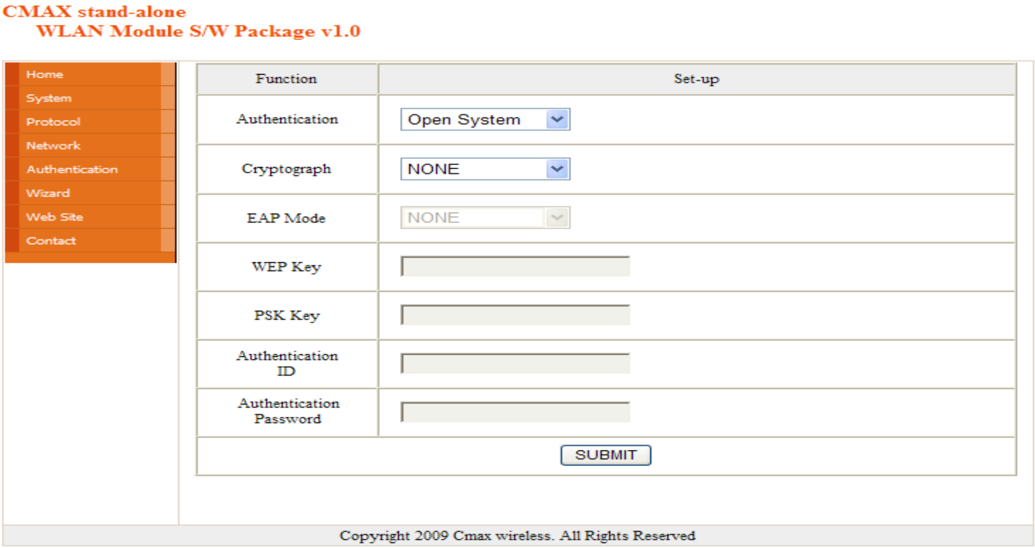
Copyright 2009 Cmax wireless. All Rights Reserved

[Figure 3.2.5.1] Network Setting

- Network Mode : Select the Infra Network or Adhoc mode.
- Note : If adhoc mode user selects to connect a adhoc-channel (1~14).
- SSID : Set the SSID that user is going to connect. SSID Can set up maximum of 32 bytes.
- Inactivity Time : After connecting to the server of printer, It is time to maintain a connection with the server. Default setting : Disable, Maximun time : 32767(sec)
- IP Assignment Method : Supported Automatic Allocation(DHCP Client) or Manual Allocation. Default setting : Manual Allocation
- Automatic Allocation(DHCP Client) : Assigns the IP Address that is assigned in the DHCP server automatically
- Manual Allocation : Does not assign the IP address in the AP(Access Poing)'s DHCP server. User should insert the IP Address that is such as IP Address of AP.
- IP Address : Insert the [IP Address] of AP : Default IP Address : 192.168.192.168
- Subnet Mask : Insert the [Subnet Mask] of AP : Default subnet Mask : 255.255.255.0
- Gateway : Insert the [Gateway] of AP : Default Gateway : 192.168.192.1

3.2.6 Authentication

: After inserting the security features, user should press the “SUBMIT” button
to apply on the system.



CMAX stand-alone
WLAN Module S/W Package v1.0

Function	Set-up
Authentication	Open System
Cryptograph	NONE
EAP Mode	NONE
WEP Key	
PSK Key	
Authentication ID	
Authentication Password	

Copyright 2009 Cmax wireless. All Rights Reserved

[Figure 3.2.6.1] Authentication Setting

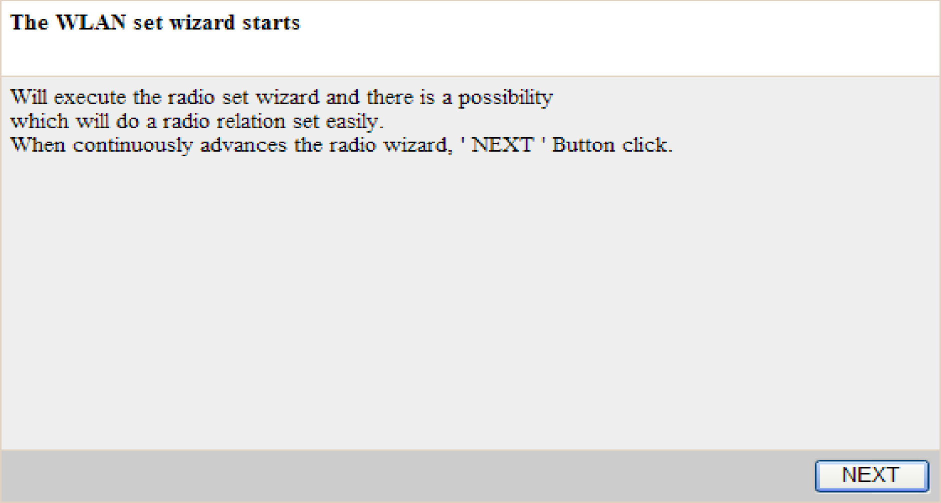
- Authentication : It is security configuration between CMAX Module and AP(Access Point)

FIELD	DESCRIPTION	
Open System	**Cryptograph**	It should be select NONE or WEP64/128 as the setting of AP to be access
	WEP Key	You can input the max 26charater,. It Configure to WEPB64/18 if you input it like the following format. - WEP64 (5 ASCII, 10 HEX), WEP128 (13 ASCII, 26 HEX)
Shared Key	**Cryptograph**	Select a WEP64/128 same AP's configuration to be access.
	WEP Key	You can input the max 26charater,. It Configure to WEPB64/18 if you input it like the following format. - WEP64 (5 ASCII, 10 HEX), WEP128 (13 ASCII, 26 HEX)
WPA-PSK / WPA2-PSK	**Cryptograph**	You should same to configure a TKIP/AES with AP to be access.
	PSK Key	You should same to input a TKIP/AES with AP to be access.
WPA-TKIP / WPA2-AES	**Cryptograph**	You should same to configure a cryptograph with AP to be access.
	EAP	You should same to configure a EAP Mode with AP to be access.
	ID	You should Input the ID with configured certificate Server
	Password	You should Input the Password with configured certificate Server However, If EAP Configuration is a EAP-TLS, you should input the private_key_password that is certificate password that generated for CMAX module.

[Table 3.2.6.1] Security setting

3.2.7 Wizard

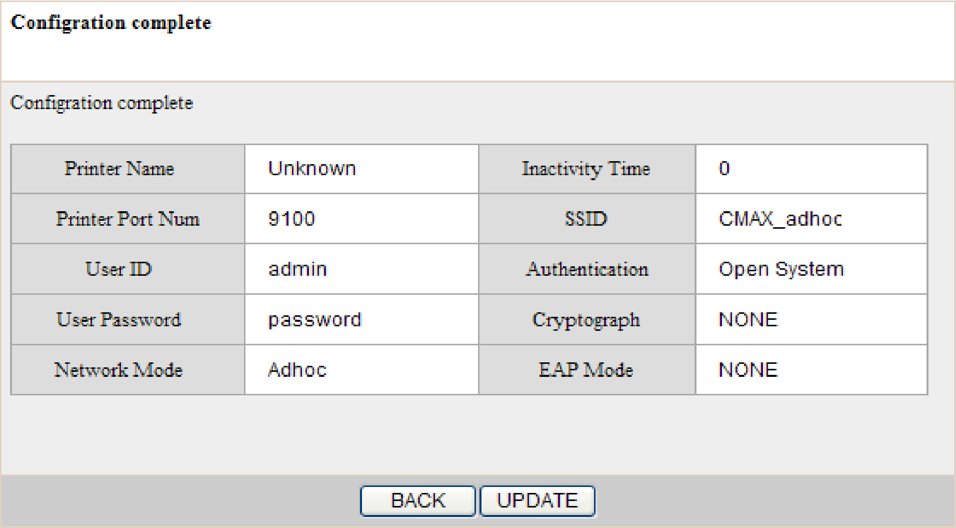
: Provides that user can easily insert the configuration of system. After inserting the configurations, user should press the "NEXT" button to apply on the system.



The WLAN set wizard starts

Will execute the radio set wizard and there is a possibility
which will do a radio relation set easily.
When continuously advances the radio wizard, ' NEXT ' Button click.

[Figure 3.2.7.1] Wizard start page



Configration complete

Configration complete

Printer Name	Unknown	Inactivity Time	0
Printer Port Num	9100	SSID	CMAX_adhoc
User ID	admin	Authentication	Open System
User Password	password	Cryptograph	NONE
Network Mode	Adhoc	EAP Mode	NONE

[Figure 3.2.7.2] Wizard result page

3.2.8 Web Site

: Move to the website of CMAX Wireless

3.2.9 Contact

: User will be connected Customer Service by the E-Mail.

3.3 TELNET

You can configure the CMAX module by TELNET

Note :

TELNET : TELNET is Text-based remote access service and based TCP/IP Protocol.

CMAX module configuration : Input the number provided on the left side of the menu and then enter the "Enter" to enter the next entry.

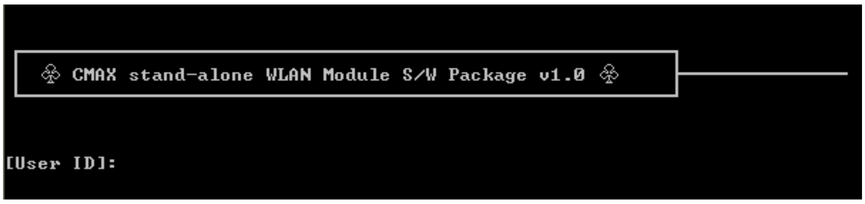
Menu move example

- Menu number : move to next menu.
- $: go to the previous menu.
- # : Go to the main menu.

3.3.1 TELNET Connection

: Connect by Telnet Client.(Microsoft Windows xp based on the description.)

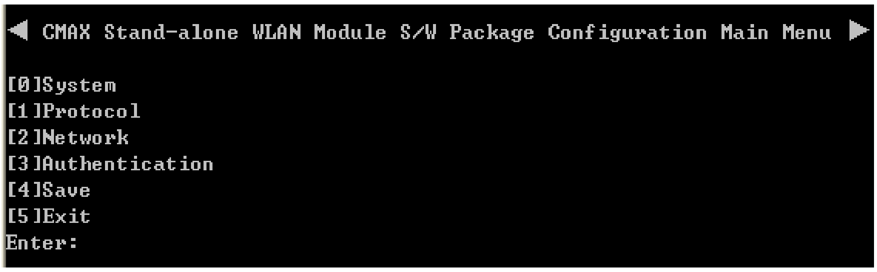
- Windows command execution.
  - Windows's Beginning – Run – input "command".
  - ■ Input "TELNET 192.168.192.168(IP Address of CMAX module)" to command windows.
    Default : IP Address : 192.168.192.168



```
♧ CMAX stand-alone WLAN Module S/W Package v1.0 ♧

[User ID]:
```

[Figure 3.3.1.1] TELNET Configuration Server Connection Screen

  - Input "User ID, User Password" and then enter the "Enter"
  - ■ Default : User ID : admin   User Password : password



```
◀ CMAX Stand-alone WLAN Module S/W Package Configuration Main Menu ▶

[0]System
[1]Protocol
[2]Network
[3]Authentication
[4]Save
[5]Exit
Enter:
```

[Figure 3.3.1.2] TELNET Configuration major menu

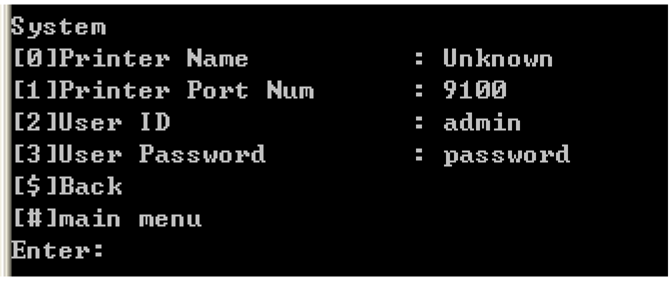
- [1] System: Configure System information.
- [2] Protocol: You can select to Enable(1) or disable(0) the application of the activities.
- And configure SNMP access information. (Default setting HTTP)
- [2] Protocol: You can select to Enable(1) or disable(0) the application of the activities. And configure SNMP access information. (Default setting HTTP)
- Network: Configure Network parameter of CMAX module.

- Authentication: Configure security parameter of CMAX module.
- Save: You can store the configuration information that input so far to the CMAX module
- Exit : Terminate TELNET connection.

3.3.2 System

: You can configure Printer Name, Print Port Number, ID and User Password. User ID and User Password is applied to all application of CMAX module.

- Select “[1]System” to “configuration main menu”.



```
System
[0]Printer Name            : Unknown
[1]Printer Port Num        : 9100
[2]User ID                 : admin
[3]User Password           : password
[$]Back
[#]main menu
Enter:
```

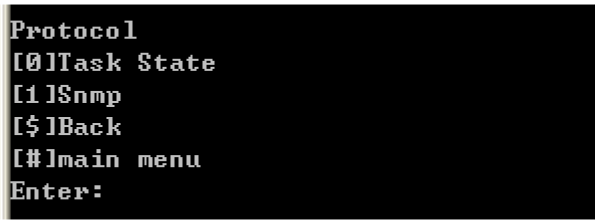
[Figure 3.3.2.1] TELNET System information menu

- [0] System Name : Configure CMAX Module name
- [1] TCP Server Port Num: Configure TCP Server port number.
- [2] User ID: Configure user ID.
- [3] User Password : Configure user password.
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.

3.3.3 Protocol

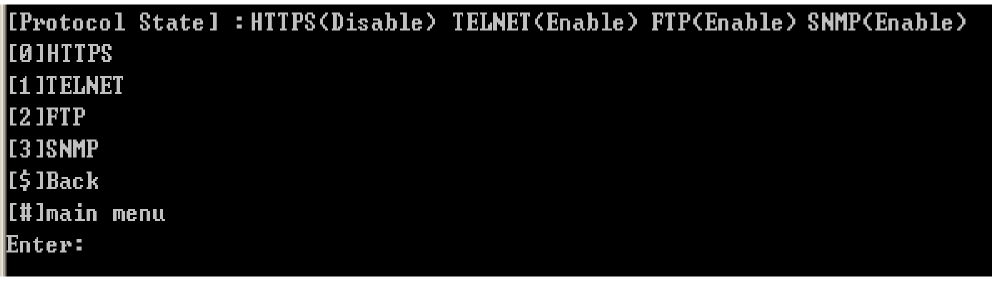
: You can select to enable or disable the application(HTTP, HTTPS, TELNET, FTP, SNMP) of the use and configure SNMP Parameter(Community, Trap IP Address, Trap Community).

- Select [2]Protocol to “Configuration main menu.”



```
Protocol
[0]Task State
[1]Snmp
[$]Back
[#]main menu
Enter:
```

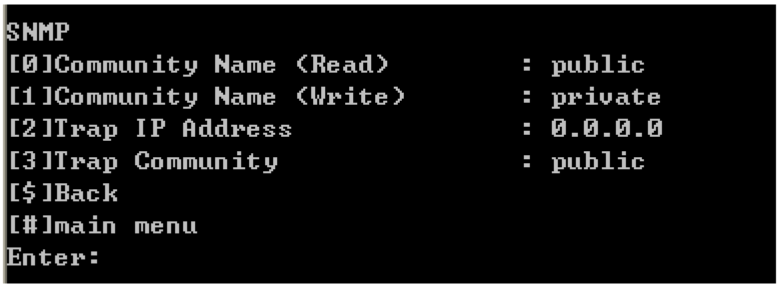
[Figure 3.3.3.1] TELNET Protocol menu



```
[Protocol State] :HTTPS(Disable) TELNET(Enable) FTP(Enable) SNMP(Enable)
[0]HTTPS
[1]TELNET
[2]FTP
[3]SNMP
[$]Back
[#]main menu
Enter:
```

[Figure 3.3.3.2] TELNET Task State Protocol menu

- Select "[0]Task State" to "Protocol menu."
  - [0] HTTPS : Configure to Enable(1) or Disable(0) to HTTPS. (default HTTP)
  - [1] TELNET : Configure to Enable(1)/Disable(0) to TELNET.
  - [2] FTP : Configure to Enable(1)/Disable(0) to FTP
  - [3] SNMP : Configure to Enable(1)/Disable(0) to SNMP.



```
SNMP
[0]Community Name (Read)         : public
[1]Community Name (Write)        : private
[2]Trap IP Address               : 0.0.0.0
[3]Trap Community                : public
[$]Back
[#]main menu
Enter:
```

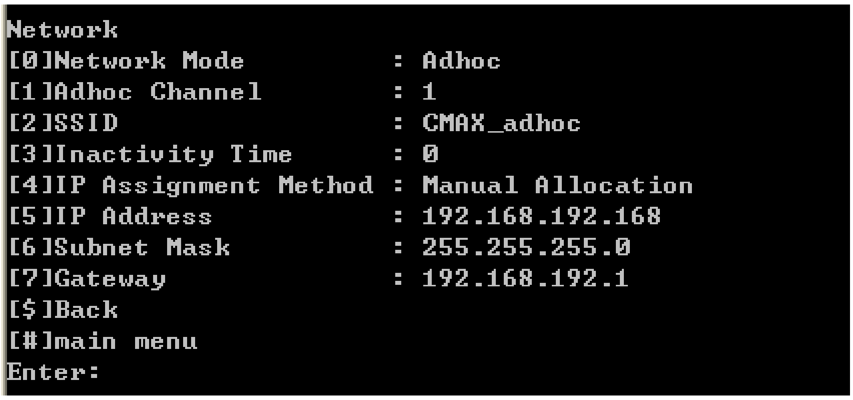
[Figure 3.3.3.3] TELNET SNMP Connection Information menu

- Select "[1] SNMP" to Protocol menu.
  - [0] Community Name (Read) :If SNMP is Enable(1) state, you can configure to accessed community of read mode..
  - [1] Community Name (Write) : If SNMP is Enable(1) state, you can configure to accessed community of write mode.
  - [2] Trap IP Address : If SNMP is Enable(1) state, you can configure to IP Address that received Trap message.
  - [3] Trap Community : If SNMP is Enable(1) state, you can configure to Trap community.
  - [$] Back: Go to the previous menu.
  - [#] Main Menu : Go to the main menu.

3.3.4 Network

: Configure Network parameter of CMAX module.

- Select "[3] Neteork" to Configuration main menu.



```
Network
[0]Network Mode           : Adhoc
[1]Adhoc Channel          : 1
[2]SSID                   : CMAX_adhoc
[3]Inactivity Time        : 0
[4]IP Assignment Method : Manual Allocation
[5]IP Address             : 192.168.192.168
[6]Subnet Mask            : 255.255.255.0
[7]Gateway                : 192.168.192.1
[$]Back
[#]main menu
Enter:
```

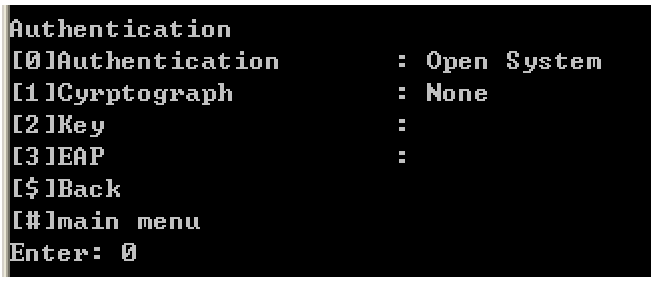
[Figure 3.3.4.1] TELNET Network menu

- [0] Network Mode : Select a network mode(Infra Network(0) / Adhoc(1)).
- [1] Adhoc Channel : Configure Adhoc Channel(1~14) to Connection.
- [2] SSID : It should be configured the SSID same as AP's SSID to be access.
- [3] Inactivity Time : It means a time limit keeping connection that without data communication between client and server.
- [4] IP Assignment Method : Select IP Assignment megthod(DHCP(0)/Manual Alloccation(1)).
- [5] IP Address : If you selected Manual Alloccation(1), configure IP Address.
- [6] Subnet Mask : If you selected Manual Alloccation(1), configure Subnet Mask.
- [7] Gateway : If you selected Manual Alloccation(1), configure Gateway.
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.

3.3.5 Authentication

: Configure CMAX Module Security. It should be configured the Security same as AP's Security to be access.

- Select "[4]Authentication" to "configuration main menu".

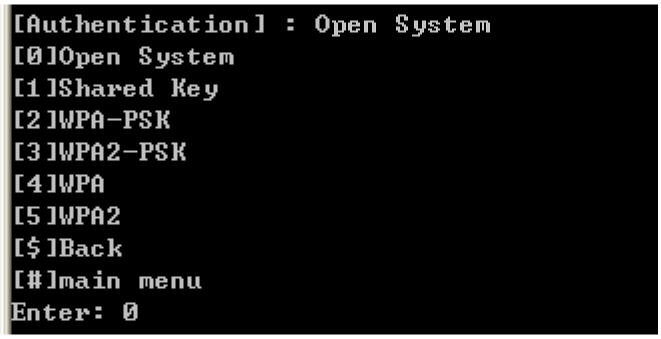


```
Authentication
[0]Authentication         : Open System
[1]Cyrptograph            : None
[2]Key                    :
[3]EAP                    :
[$]Back
[#]main menu
Enter: 0
```

[Figure 3.3.5.1] TELNET Security main menu

- [0] Authentication : You configure a security method.. Reference [Table 3.3.5.1]
- [1] Cyrptograph : Configure an encryption method according to security methods.
- [2] Key : Configure a key of WEP or PSK.
- [3] EAP : Configure an EAP Mode according to WPA/WPA2

- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.



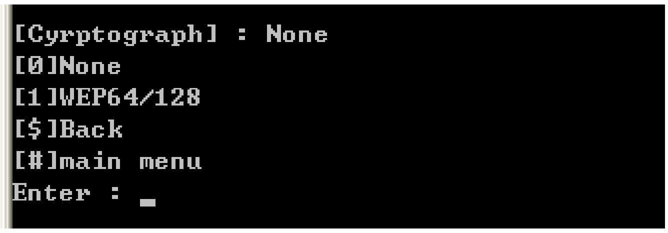
```
[Authentication] : Open System
[0]Open System
[1]Shared Key
[2]WPA-PSK
[3]WPA2-PSK
[4]WPA
[5]WPA2
[$]Back
[#]main menu
Enter: 0
```

[Figure 3.3.5.2] TELNET Open System Security main menu

- [0~5] Authentication : Configure a Security Mode. Reference [Table 3.3.5.1]
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.
- "Authentication" is a function that CMAX module does authenticate to AP through to wireless

FIELD	DESCRIPTION	
Open System	Cryptograph	It should be select NONE or WEP64/128 as the setting of AP to be access
	WEP Key	You can input the max 26charater,. It Configure to WEPB64/18 if you input it like the following format. - WEP64 (5 ASCII, 10 HEX), WEP128 (13 ASCII, 26 HEX)
Shared Key	Cryptograph	Select a WEP64/128 same AP's configuration to be access.
	WEP Key	You can input the max 26charater,. It Configure to WEPB64/18 if you input it like the following format. - WEP64 (5 ASCII, 10 HEX), WEP128 (13 ASCII, 26 HEX)
WPA-PSK / WPA2-PSK	Cryptograph	You should same to configure a TKIP/AES with AP to be access.
	PSK Key	You should same to input a TKIP/AES with AP to be access.
WPA-TKIP / WPA2-AES	Cryptograph	You should same to configure a cryptograph with AP to be access.
	EAP	You should same to configure a EAP Mode with AP to be access.
	ID	You should Input the ID with configured certificate Server
	Password	You should Input the Password with configured certificate Server However, If EAP Configuration is a EAP-TLS, you should input the private_key_password that is certificate password that generated for CMAX module.

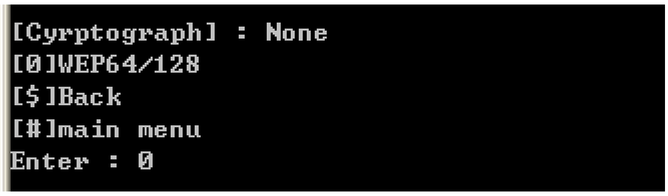
[Table 3.3.5.1] Security setting



```
[Cyrptograph] : None
[0]None
[1]WEP64/128
[$]Back
[#]main menu
Enter : _
```

[Figure 3.3.5.3] TELNET Open System Cryptograph menu

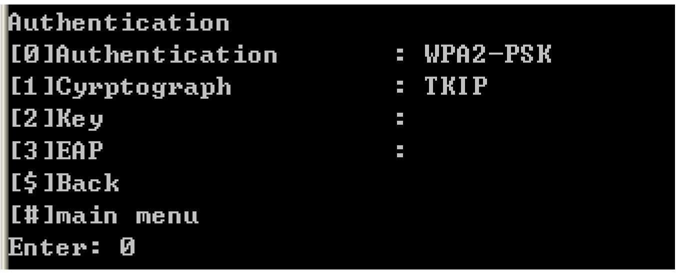
- [0] Open System : You should select 'NONE[0]' or 'WEP64/128[1]'
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.



```
[Cyrptograph] : None
[0]WEP64/128
[$]Back
[#]main menu
Enter : 0
```

[Figure 3.3.5.4] TELNET Shared Key Cryptograph menu

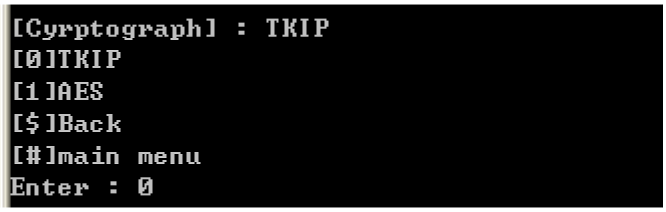
- [1] Shared Key : You should select 'WEP64' or 'WEP128'
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.



```
Authentication
[0]Authentication        : WPA2-PSK
[1]Cyrptograph           : TKIP
[2]Key                   :
[3]EAP                   :
[$]Back
[#]main menu
Enter: 0
```

[Figure 3.3.5.5]TELNET WPA-PSK/WPA2-PSK a detailed menu.

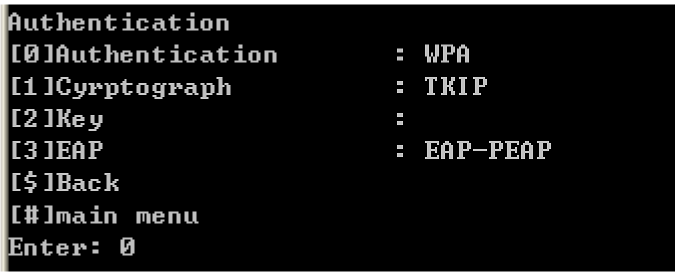
- [0] Authentication : you should configure a authentication mode.
  Reference [Table 3.3.5.1]
- [1] Cyrptograph : You should configure a Cryptograph mode according to authentication mode
- [2] Key : You should a WEP key of PSK Key.
- [3] EAP : You should configure a EAP Mode according to WAP/WAP2
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.



```
[Cyrptograph] : TKIP
[0]TKIP
[1]AES
[$]Back
[#]main menu
Enter : 0
```

[Figure 3.3.5.6] TELNET WPA-PSK/WPA2-PSK Cryptograph menu

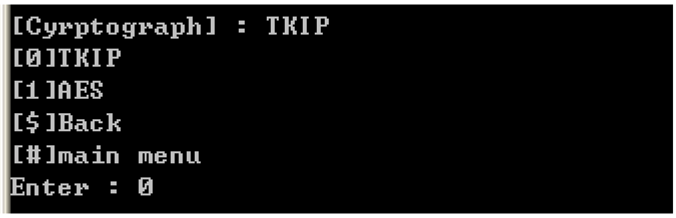
- [2] WPA-PSK : You should select a ‘TKIP[0]’ or ‘AES[1]’
- [3] WPA2-PSK : You should select a ‘TKIP[0]’ or ‘AES[1]’
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.



```
Authentication
[0]Authentication        : WPA
[1]Cyrptograph           : TKIP
[2]Key                   :
[3]EAP                   : EAP-PEAP
[$]Back
[#]main menu
Enter: 0
```

[Figure 3.3.5.7]TELNET WPA/WPA2 a detailed menu.

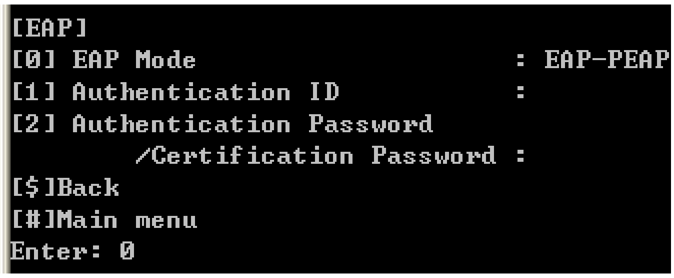
- [0] Authentication : You should configure a authentication method.
  Reference [Table 3.3.5.1]
- [1] Cyrptograph : Configure an encryption method according to security methods.
- [2] Key : Configure a key of WEP or PSK.
- [3] EAP : Configure an EAP Mode according to WPA/WPA2
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.



```
[Cyrptograph] : TKIP
[0]TKIP
[1]AES
[$]Back
[#]main menu
Enter : 0
```

[Figure 3.3.5.8]TELNET WPA/WPA2 Cryptograph menu

- Cryptograph : It should be configured a cryptograph method with ‘TKIP[0]’ or ‘AES[1]’
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.



```
[EAP]
[0] EAP Mode                    : EAP-PEAP
[1] Authentication ID           :
[2] Authentication Password
        /Certification Password :
[$]Back
[#]Main menu
Enter: 0
```

[Figure 3.3.5.9] TELNET EAP Configuration Menu.

- [0] EAP Mode: It should be selected same as AP's EAP mode
- [1] EAP ID/PASSWORD: it should be configured same as AP's EAP ID and password.
- [$] Back: Go to the previous menu.
- [#] Main Menu : Go to the main menu.

3.3.6 Save

: To save a changed configuration information on CMAX module, select the '[5]Save' in the configuration main menu.

3.3.7 Exit

: To terminate a TELNET connection, select the '[6] Exit' in the configuration main menu.

3.4 FTP

It is function to Upload or Download 'Config file' for CMAX module configuration by FTP. If you modify the 'Config file' and upload that, it will be changed CMAX module setup.

Note :

FTP : File Transfer Protocol (FTP) is a standard network protocol used to exchange and manipulate files over a TCP/IP-based network(between server and client).

Supported FTP command

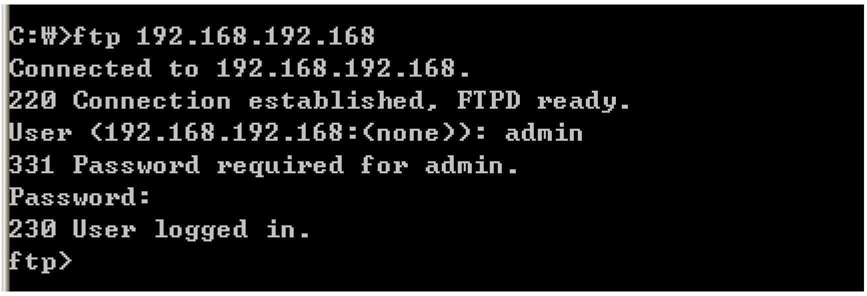
- ls : List contents of remote directory
- Get: : Receive config file
- Put : Send config file

CAUTION : To Upload a file, don't use file-extension and use "config" to filename.

3.4.1 FTP Connection

: It should be executed to Microsoft Windows xp Command line.

- Execute Windows command
  - Microsoft Windows xp's beginning – run – input 'command'
  - It should be input command 'FTP 192.168.192.168 (CMAX module's IP Address)'
    - Default : IP Address : 192.168.192.168



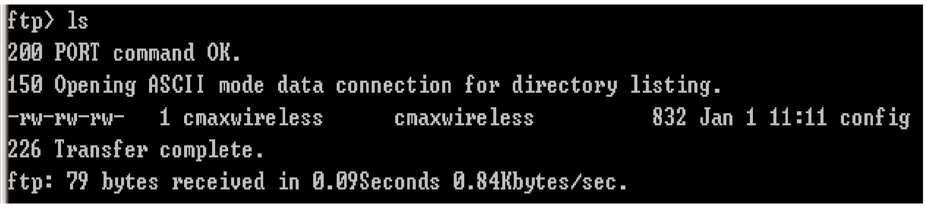
```
C:₩>ftp 192.168.192.168
Connected to 192.168.192.168.
220 Connection established, FTPD ready.
User (192.168.192.168:(none)): admin
331 Password required for admin.
Password:
230 User logged in.
ftp>
```

[Figure 3.4.1.1] FTP Connection Screen

- User ID, User Password 를 입력 후 "Enter"를 칩니다.
- It should be input User ID and User password.
    - ■ Default : User ID : admin   User Password : password

3.4.2 Config File list view

: It should be confirmed a file as you input 'ls'.

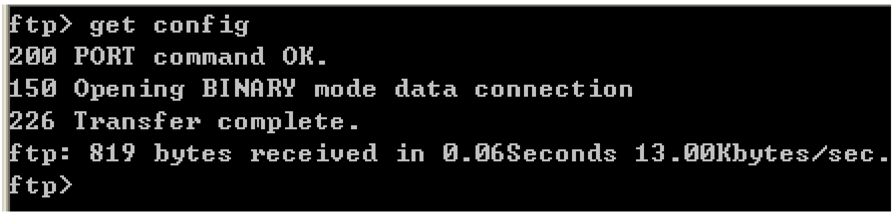


```
ftp> ls
200 PORT command OK.
150 Opening ASCII mode data connection for directory listing.
-rw-rw-rw-   1 cmaxwireless      cmaxwireless         832 Jan 1 11:11 config
226 Transfer complete.
ftp: 79 bytes received in 0.09Seconds 0.84Kbytes/sec.
```

[Figure 3.4.2.1] FTP 'ls' command executed screen

3.4.3 Config File download

:It should be downloaded a file as you input 'get config'.

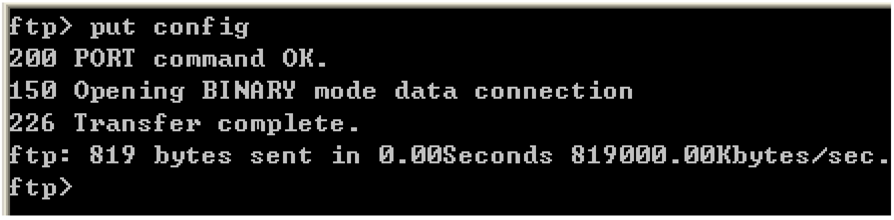


```
ftp> get config
200 PORT command OK.
150 Opening BINARY mode data connection
226 Transfer complete.
ftp: 819 bytes received in 0.06Seconds 13.00Kbytes/sec.
ftp>
```

[Figure 3.4.3.1] FTP 'get config' command screen

3.4.4 Config File Upload

: It should be uploaded a file as you input 'put config'. you must use file name as 'config'.



```
ftp> put config
200 PORT command OK.
150 Opening BINARY mode data connection
226 Transfer complete.
ftp: 819 bytes sent in 0.00Seconds 819000.00Kbytes/sec.
ftp>
```

[Figure 3.4.4.1] FTP 'put config' command screen

3.4.5 Config File Specification

: Table 3.4.5.1 is downloaded file's content from CMAX module by 'get config' command. To change a configuration value, input without blank in 'bracket'([ ]).

```
** Caution!!!
** Do not change the order or contents of the menu.
** Only need to change the settings, please.

[1] System
        1. Printer Name: [unknown]
        2. Printer Port Num: [9100]
        3. User ID: [admin]
        4. User Password: [password]

[2] Protocol
        1. Task State
                1) HTTPS: [0]
                2) TELNET: [0]
                3) FTP: [0]
                4) SNMP: [0]
        2. SNMP
                1) Community Name (Read): [public]
                2) Community Name (Write): [private]
                3) Trap IP Address: [0.0.0.0]
                4) Trap Community: [public]

[3] Network
        1. Network Mode
                1) Infra Network(0) / Adhoc(1): [1]
                2) Adhoc Channel: [1]
        2. SSID:   [CMAX_adhoc]
        3. Inactivity Time: [0]
        4. IP Assignment Method: [1]
        5. IP Address: [192.168.192.168]
        6. SubnetMask: [255.255.255.0]
        7. Gateway: [192.168.192.1]

[4] Authentication
        1. Authentication: [0]
        2. Cryptograph: [0]
        3. EAP Mode: [0]
        4. WEP Key: []
        5. PSK Key: []
        6. Authentification ID: []
        7. Authentification Password: []
```

[Table 3.4.5.1] FTP 'config' file's content

- Describes in detail how the file should be configure.

[1] System: Configure the system information.

1. Printer Name: Configure the system name.
2. Printer Port Num: Configure the TCP server port.
3. User ID: Configure the user ID.
4. User Password: Configure the user password.

[2] Protocol: Configure the Application (HTTPS, TELNET, FTP, SNMP) as Enable(1) or Disable(0). And configure the SNMP connect information.

1. Task State
   1) HTTPS: Configure the HTTPS as Enable(1) or Disable(0).(default configuration is HTTP)
   2) TELNET: Configure the TELNET as Enable(1) as Disable(0).
   3) FTP: Configure the FTP as Enable(1) as Disable(0).
   4) SNMP: Configure the SNMP as Enable(1) or Disable(0).
2. SNMP
   1) Community Name (Read): Configure the Read mode community..
   2) Community Name (Write): Configure the Write mode community.
   3) Trap IP Address: If SNMP's state is Enable(1), Configure the IP address for Trap message received.
   4) Trap Community: If SNMP's state is Enable(1), Configure the Trap community.

[3] Network: Configure the CMAX module's Network parameter.

1. Network Mode
   1) Infra network(0) / Adhoc(1) : Select a network mode to connect
   2) Adhoc Channel: If you selected Adhoc, you select channel(1~11) .

2. SSID: CMAX_adhoc: It should be input SSID as the setting of AP to be access
3. Inactivity Time: It should be configured a time limit keeping connection that without data communication between client and server.
4. IP Assignment Method: Select DHCP(0) or Manual Alloccation(1)
5. IP Address: If you selected Manual Alloccation(1), you configure a IP Address.
6. SubnetMask: If you selected Manual Alloccation(1), you configure a Subnet Mask.
7. Gateway: If you selected Manual Alloccation(1), you configure a Gateway.

[4] Authentication: It should be configured the Security same as AP's Security to be access.

1. Authentication: Open System(0), Shared Key(1), WPA-PSK(2), WPA-PSK2(3), WPA(4), WPA2(5)
2. Cryptograph: NONE(0), WEP64/128(1), TKIP(2), AES(3)
3. EAP Mode: EAP-PEAP(0), EAP-TTLS(1), EAP-TLS(2), EAP-LEAP(3)
4. WEP Key: It should be configure the WEB key same as AP's WEP key.
5. PSK Key: It should be configure the PSK key same as AP's PSK key.

6. Authentication ID: It should be configure the Authentication ID same as AP's Authentication ID.

7. Authentication Password: It should be configured the Authentication password same as AP's Authentication password to be access.

3.5 SNMP

It is managed a network information through SNMP (supported SNMPv1).

Note :

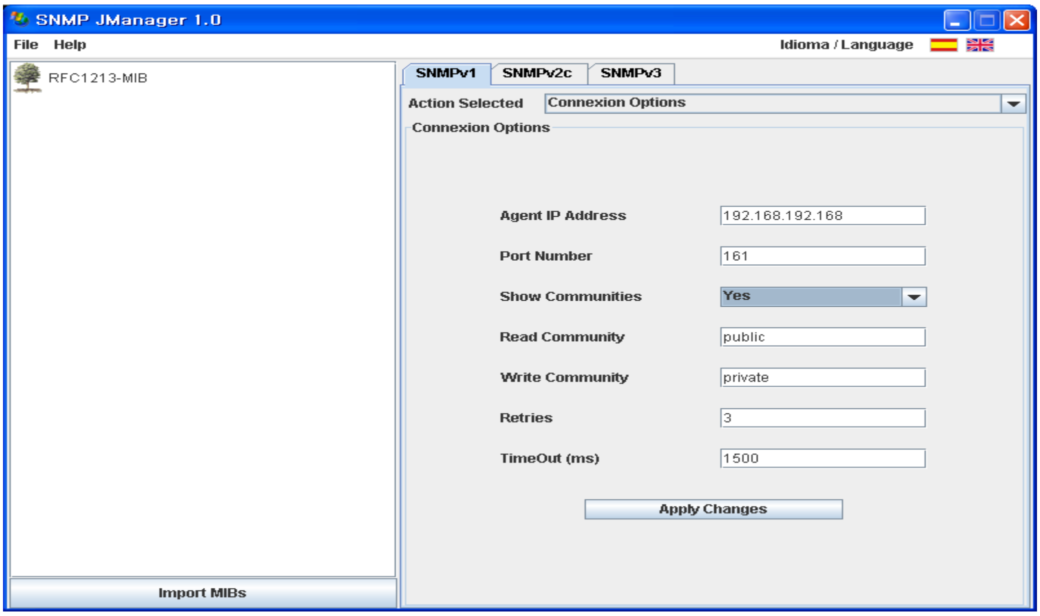
SNMP stands for 'Simple Network Management Protocol' and it is used for network management.

SNMP is only a protocol to transfer messages so it need the Application program to get Network management information using SNMP. SNMP has SNMP manager and agent, as in common network application is composed server and client model. SNMP agent is a part of SNMP module and it is installed in managed system to collect the network or system information. SNMP manager is also part of the SNMP module and it request the network information to SNMP agent.

3.5.1 SNMP Connection

: It should be connect a SNMP Agent through SNMP Manager. It is introduced a SNMP operation at this manual as used SNMP-JManger-v1.0.

- SNMP-JManager-v1.0 running
  - Input the address(192.168.192.168 , CMAX module's IP Address) to 'Agent IP Address'.
    - ■ Default : IP Address : 192.168.192.168
  - Input the Read Community, Write Community and then click "Apply Changes" button.
    - ■ Default : Read Community : public Write Community : private



Action Selected: Connexion Options

Connexion Options

Agent IP Address: 192.168.192.168

Port Number: 161

Show Communities: Yes

Read Community: public

Write Community: private

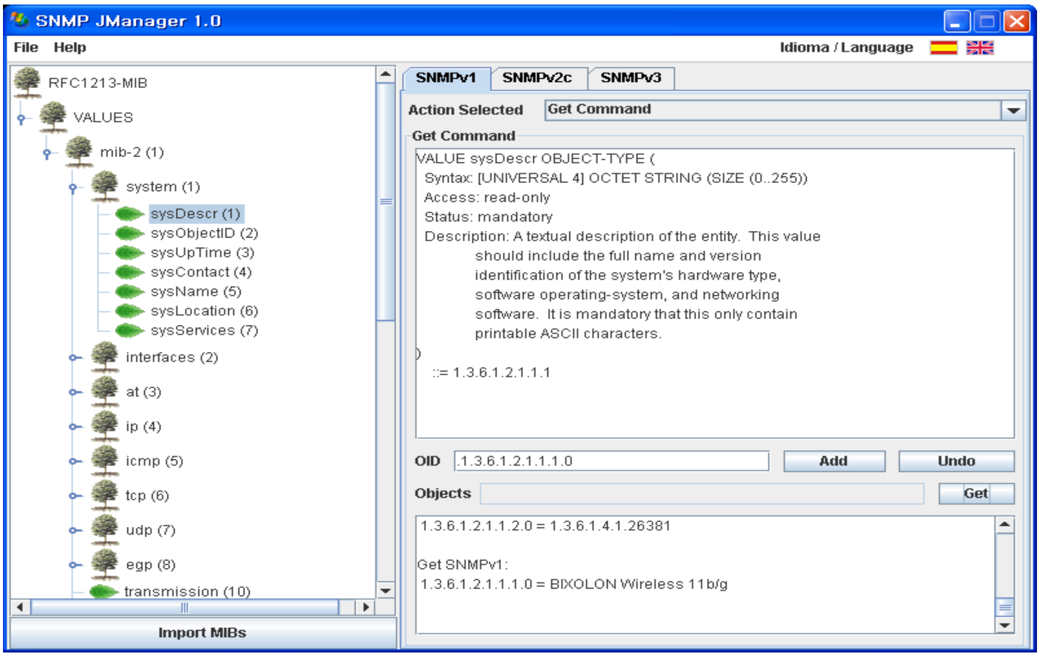
Retries: 3

TimeOut (ms): 1500

[Figure 3.5.1.1] SNMP Connection configuration screen

3.5.2 SNMP Manager operation test: it is description of basic SNMP operation.

- If you selected terminal node to ‘Get Tree’, get this value(client note value).



Action Selected: Get Command

Get Command

```
VALUE sysDescr OBJECT-TYPE (
  Syntax: [UNIVERSAL 4] OCTET STRING (SIZE (0..255))
  Access: read-only
  Status: mandatory
  Description: A textual description of the entity.  This value
          should include the full name and version
          identification of the system's hardware type,
          software operating-system, and networking
          software.  It is mandatory that this only contain
          printable ASCII characters.
)
   ::= 1.3.6.1.2.1.1.1
```

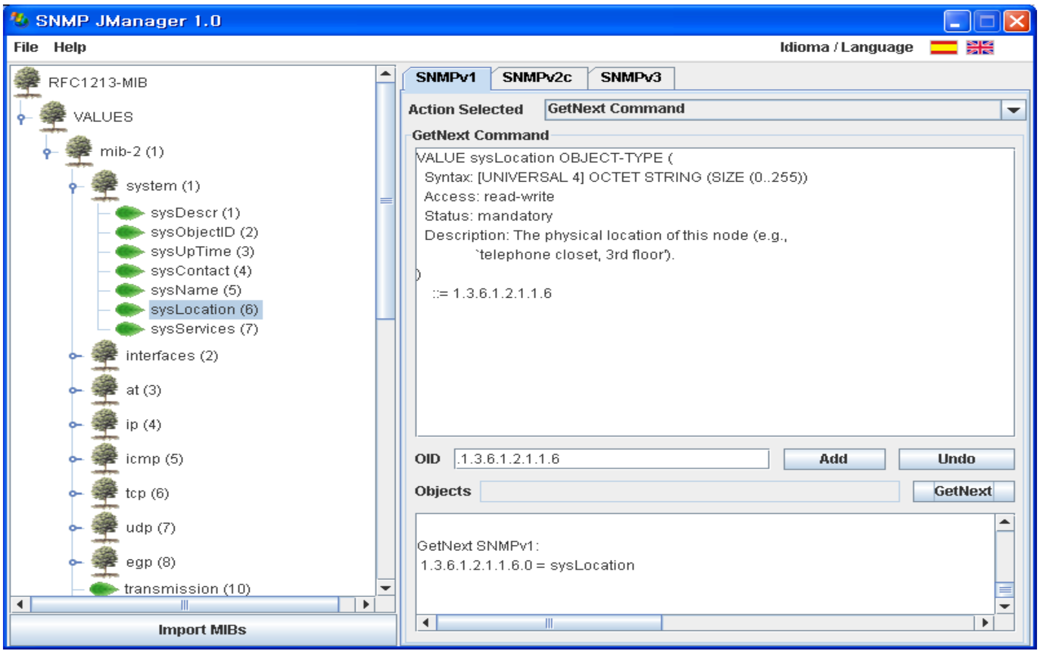
OID: .1.3.6.1.2.1.1.1.0

Objects:

```
1.3.6.1.2.1.1.2.0 = 1.3.6.1.4.1.26381

Get SNMPv1:
1.3.6.1.2.1.1.1.0 = BIXOLON Wireless 11b/g
```

[Figure 3.5.2.1] SNMP ‘get’ message operation screen

- Get Next : You can bring the value at trees as selected a terminal node.



Action Selected: GetNext Command

GetNext Command

```
VALUE sysLocation OBJECT-TYPE (
  Syntax: [UNIVERSAL 4] OCTET STRING (SIZE (0..255))
  Access: read-write
  Status: mandatory
  Description: The physical location of this node (e.g.,
          `telephone closet, 3rd floor').
)
  ::= 1.3.6.1.2.1.1.6
```

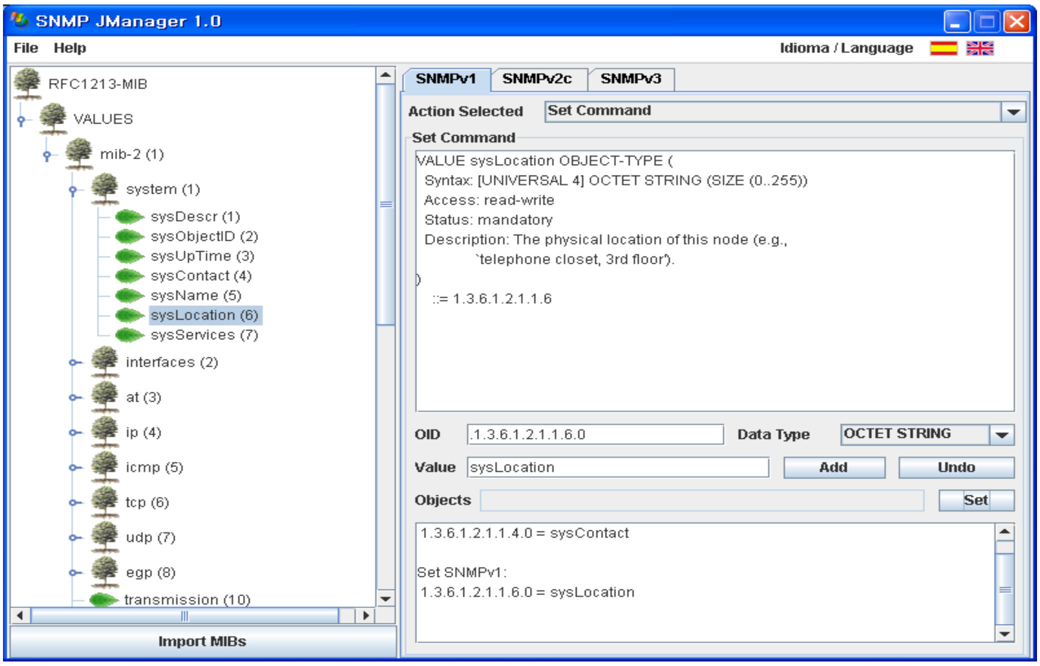
OID: 1.3.6.1.2.1.1.6

Objects:

```
GetNext SNMPv1:
1.3.6.1.2.1.1.6.0 = sysLocation
```

[Figure 3.5.2.2] SNMP ‘getnext’ message opration screen

- You can configure the terminal node value to ‘set tree’. (You can set only the contents had set on "Write")



Action Selected: Set Command

Set Command

```
VALUE sysLocation OBJECT-TYPE (
  Syntax: [UNIVERSAL 4] OCTET STRING (SIZE (0..255))
  Access: read-write
  Status: mandatory
  Description: The physical location of this node (e.g.,
          `telephone closet, 3rd floor').
)
  ::= 1.3.6.1.2.1.1.6
```

OID: 1.3.6.1.2.1.1.6.0 Data Type: OCTET STRING

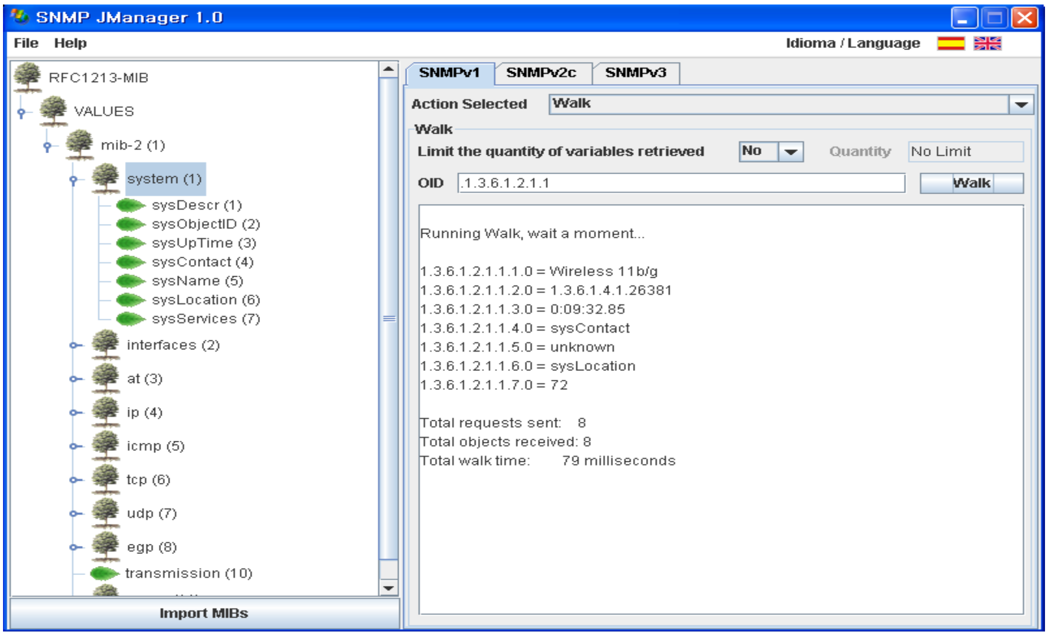
Value: sysLocation

Objects:

```
1.3.6.1.2.1.1.4.0 = sysContact

Set SNMPv1:
1.3.6.1.2.1.1.6.0 = sysLocation
```

[Figure 3.5.2.3] SNMP ‘set’ message operation screen

■ Walk: It can get the all item that terminal node of tree or terminal node of node.



Action Selected: Walk

Walk

Limit the quantity of variables retrieved: No — Quantity: No Limit

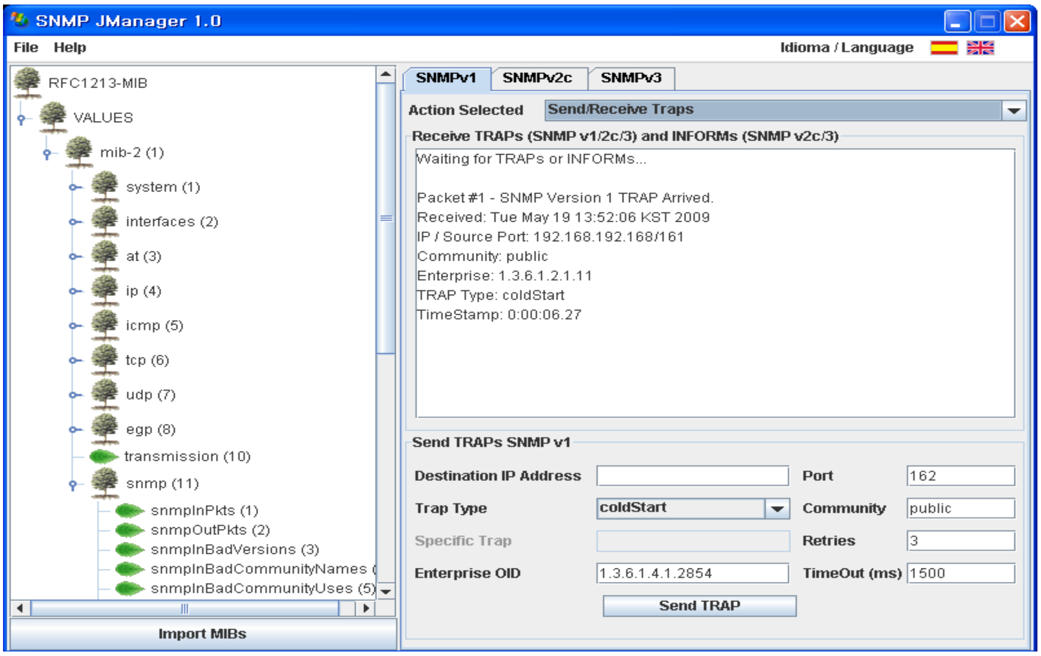
OID: .1.3.6.1.2.1.1

```
Running Walk, wait a moment...

1.3.6.1.2.1.1.1.0 = Wireless 11b/g
1.3.6.1.2.1.1.2.0 = 1.3.6.1.4.1.26381
1.3.6.1.2.1.1.3.0 = 0:09:32.85
1.3.6.1.2.1.1.4.0 = sysContact
1.3.6.1.2.1.1.5.0 = unknown
1.3.6.1.2.1.1.6.0 = sysLocation
1.3.6.1.2.1.1.7.0 = 72

Total requests sent:   8
Total objects received: 8
Total walk time:       79 milliseconds
```

[Figure 3.5.2.4] SNMP 'walk' message operation screen

■ Traps: If a specific event occurs, relevant(in the event) message is transmitted to trap address.

- ColdStart: when a terminal rebooting works, coldstart message is transmitted to trap address.



Action Selected: Send/Receive Traps

Receive TRAPs (SNMP v1/2c/3) and INFORMs (SNMP v2c/3)

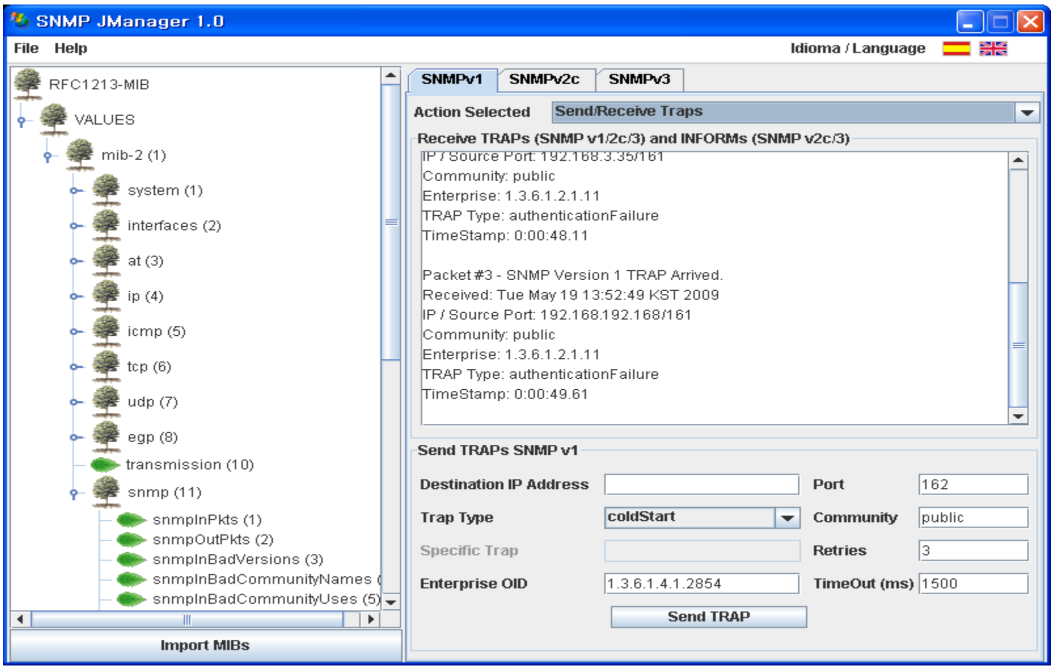
```
Waiting for TRAPs or INFORMs...

Packet #1 - SNMP Version 1 TRAP Arrived.
Received: Tue May 19 13:52:06 KST 2009
IP / Source Port: 192.168.192.168/161
Community: public
Enterprise: 1.3.6.1.2.1.11
TRAP Type: coldStart
TimeStamp: 0:00:06.27
```

Send TRAPs SNMP v1

Destination IP Address		Port	162
Trap Type	coldStart	Community	public
Specific Trap		Retries	3
Enterprise OID	1.3.6.1.4.1.2854	TimeOut (ms)	1500

[Figure 3.5.2.5] SNMP coldStart message received screen

- AuthenticationFailure: If 'Read', 'Write' Community is not correct, AuthenticationFailure message is transmitted to trap address.



Action Selected: Send/Receive Traps

Receive TRAPs (SNMP v1/2c/3) and INFORMs (SNMP v2c/3)

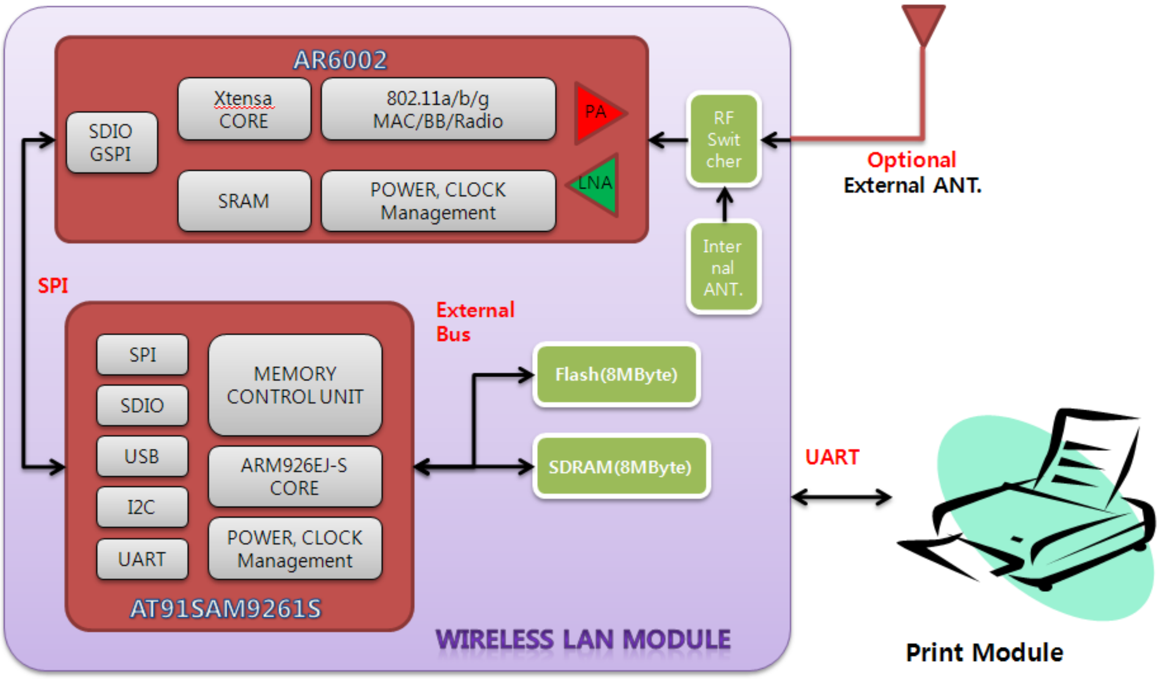
```
IP / Source Port: 192.168.3.35/161
Community: public
Enterprise: 1.3.6.1.2.1.11
TRAP Type: authenticationFailure
TimeStamp: 0:00:48.11

Packet #3 - SNMP Version 1 TRAP Arrived.
Received: Tue May 19 13:52:49 KST 2009
IP / Source Port: 192.168.192.168/161
Community: public
Enterprise: 1.3.6.1.2.1.11
TRAP Type: authenticationFailure
TimeStamp: 0:00:49.61
```

Send TRAPs SNMP v1

Destination IP Address		Port	162
Trap Type	coldStart	Community	public
Specific Trap		Retries	3
Enterprise OID	1.3.6.1.4.1.2854	TimeOut (ms)	1500

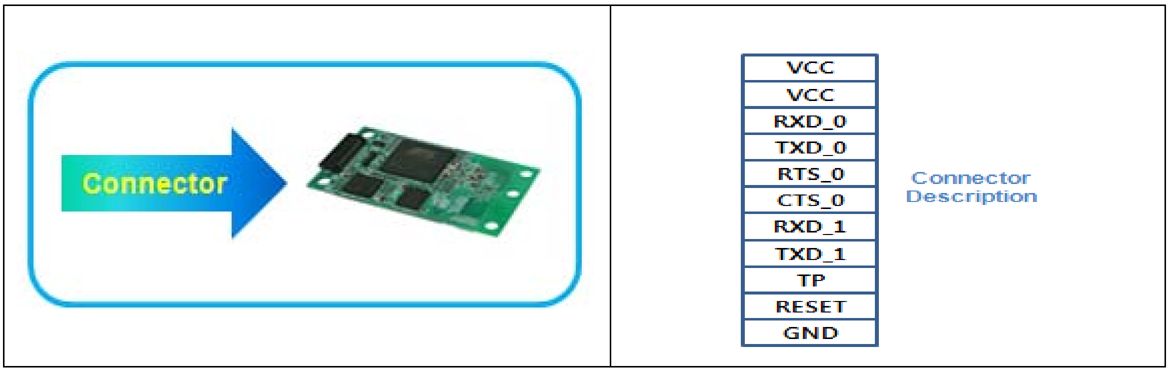
[Figure 3.5.2.6] SNMP AuthenticationFailure message received screen

4. Hardware Block Diagram



[Figure 4.1] Hardware Block Diagram

4.1 Hardware Pin Array



NUM	NAME	IN/OUT	DESCRIPTION
1	VCC		3.3V Power
2	VCC		3.3V Power
3	RXD_0	I	UART RXD
4	TXD_0	O	UART TXD
5	RTS_0	O	UART RTS
6	CTS_0	I	UART CTS
7	RXD_1	I	Debug UART RXD
8	TXD_1	O	Debug UART TXD
9	TP		TEST POINT
10	WLAN_RESET	I	Active Low
11	GND		GROUND
12	GND		GROUND

5. Demo and Test

This chapter explains several examples that it can be used for functional testing of CMAX module. Test environment is as follows.

5.1 Test environment

5.1.1 Hardware

- RS232 serial port with a PC
- CMAX module & CMAX test board
- PC's COM port and CMAX for the module's serial port to connect the serial cable is required.

5.1.2 Software

- Configuration Tool of CMAX module
- Hyper Terminal(or other Terminal program)

5.2 Start Test

5.2.1 STEP1.

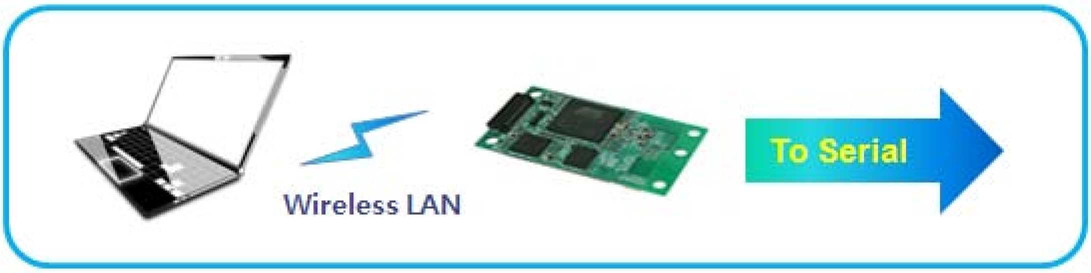
- It should be connect to CMAX Test board and PC's Serial port.
- It should be turn on the CMAX test board.
- It should be connected the PC to CMAX module through serial interface.
- It should be run a Terminal program of PC by connected Serial(ex, HyperTerminal)

5.2.2 STEP2. (Wireless Configuration to between CMAX module and PC).

- It should be connected the PC to CMAX module through wireless LAN.
- It should be configured the PC's Network to next value. IP(192.168.192.XXX), subnet(255.255.255.0), gateway(192.168.192.1)
- It should be confirmed wireless connection of CMAX module and PC by Ping response.

5.2.3 STEP3. (Data Transfer)

- It should be run a Terminal program of PC by connected WLAN(ex, HyperTerminal)
- It should be input a charater to HyperTerminal.
- It should be confirmed a Receive Data on serial Terminal.



[Figure 5.2.3.1] Wireless LAN to Serial

6. Configuration Tool Command List

It should be explained the command for CMAX module and PC through Serial interface and WLAN.

6.1 Configuration Tool Protocol

6.1.1 Serial Operation Specification

OPERATION		SPECIFICATION
1	Configuration Data Get	Baud Rate : 115200 Hardware Handshaking : CTS/RTS
2	Configuration Data Set	Baud Rate : 115200 Hardware Handshaking : CTS/RTS

3	Firmware Upload	Baud Rate : 115200 Hardware Handshaking : CTS/RTS
4	Certificate Upload	Baud Rate : 115200 Hardware Handshaking : CTS/RTS
5	BSS Info Request	Baud Rate : 115200 Hardware Handshaking : CTS/RTS
6	BSS Info Response	Baud Rate : 115200 Hardware Handshaking : CTS/RTS

[Table 6.1.1.1] Serial Operation Specification

6.1.2 WLAN Operation Protocol & Port

OPERATION		PROTOCOL & PORT
1	Configuration Data Get	TCP , 3318
2	Configuration Data Set	TCP , 3318
3	Firmware Upload	TCP , 3318
4	Certificate Upload	TCP , 3318
5	BSS Info Request	TCP , 3318
6	BSS Info Response	TCP , 3318
7	Printer Search Request	UDP , 3337
8	Printer Search Response	UDP , 9000

[Table 6.1.2.1] WLAN Operation Protocol & Port

6.2 Serial & WLAN Command

6.2.1 Serial Operation

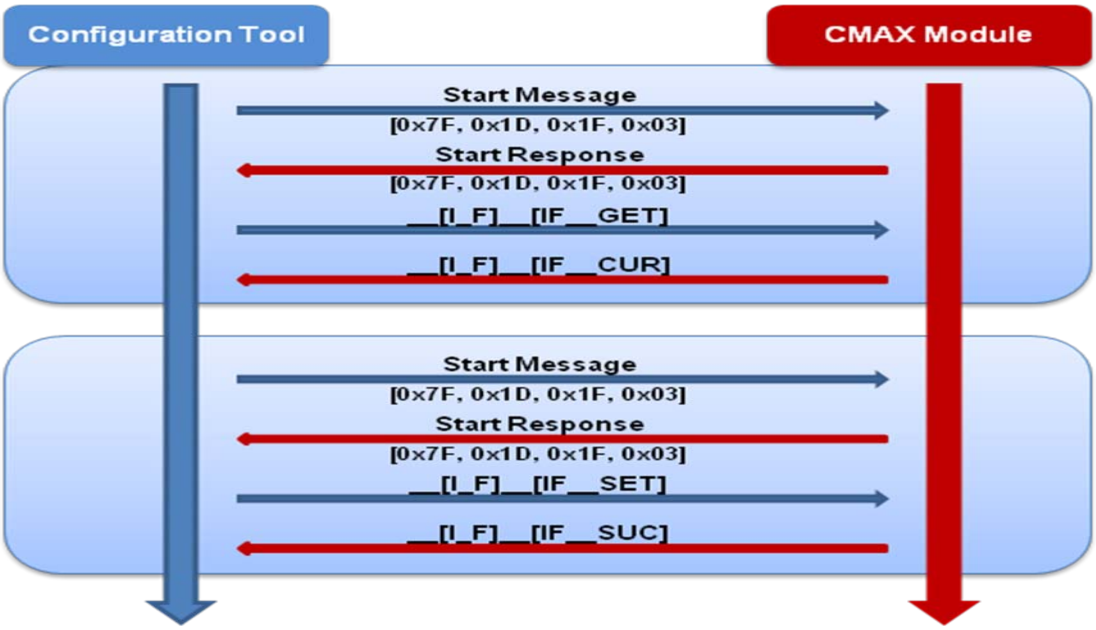
- Serial mode Configuration Tool work should need 'Start Message' before sending real command.
- Serial mode Configuration Tool command should change all 'byte' to ASCII code. And next transmit.

  - Ex : Command Frame
  - If it changes hexadecimal code to '__[I_F]__[IF__GET]'. It is '0x5F, 0x5F, 0x49, 0x49, 0x5F, 0x46, 0x47, 0x5F, 0x5F, 0x5B, 0x49, 0x46, 0x5F, 0x5F, 0x5D, 0x45, 0x54, 0x47'.
  - It should be transmitted ASCII value that the above hexadecimal value changed
  - '0x5F' is separated ASCII '5'(==0x35) and ASCII'F'(==0x46). and then WLAN module send them by serial interface.

ASCII	_	[	I	F	]	G	E	T
HEX	0x5F	0x5B	0x49	0x46	0x47	0x5D	0x45	0x54

[Table 6.2.1.1] Serial Command ASCII, HEX

- Serial Command Sequence



[Figure 6.2.1.1] Serial Command Sequence

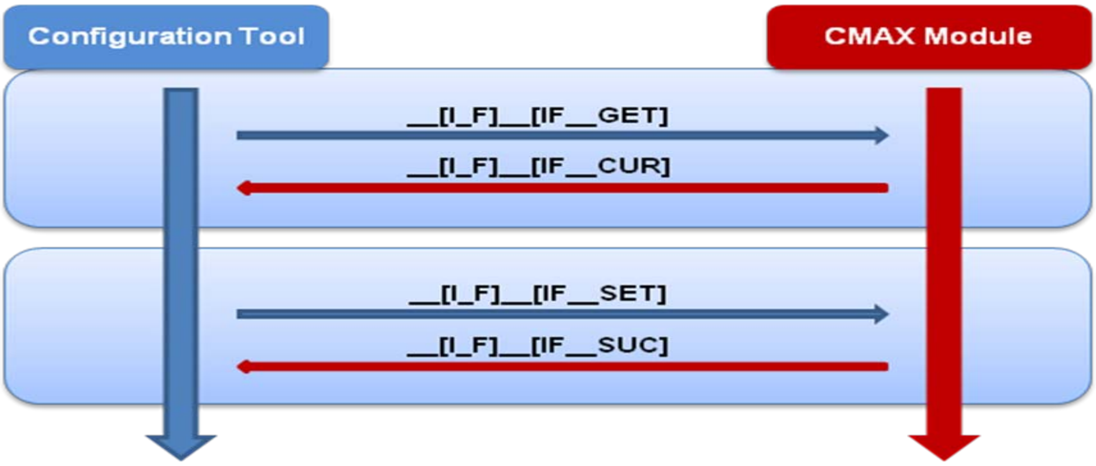
- Serial Start Message Format

SERIAL START MESSAGE	VALUE	DIRECTION	COMMENT
Configuration Start Message	[0x7f, 0x1D, 0x1F, 0x03]	Host → Device	
Configuration Start Response	[0x7f]	Device → Host	
Firmware Update Start Message	[0x80, 0x1D, 0x1F, 0x03]	Host → Device	
Firmware Update Start Response	['S', 'T', 'R', 'T']	Device → Host	
CA_CER Update Start Message	[0x81, 0x1D, 0x1F, 0x03]	Host → Device	
CA_CER Update Start Response	['S', 'T', 'R', 'T']	Device → Host	
CL_KEY Update Start Message	[0x82, 0x1D, 0x1F, 0x03]	Host → Device	
CL_KEY Update Start Response	['S', 'T', 'R', 'T']	Device → Host	
CL_PEM Update Start Message	[0x83, 0x1D, 0x1F, 0x03]	Host → Device	
CL_PEM Update Start Response	['S', 'T', 'R', 'T']	Device → Host	
RSSI Request Message	[0x85, 0x1D, 0x1F, 0x03]	Device → Mobile Printer	
RSSI response Message	[0x1D, 0x49, 0x02] + RSSI[2Byte]	Mobile Printer → Device	RSSI value is a negative number
ETC	- if end of data is '0x03', 'Printer Server' send bypass at serial port(no data operation). - if 'printer socket''s state is 'close', received data is dumped.		

[Table 6.2.1.2] Serial Start Message Format

6.2.2 Wireless LAN Operation

- Wireless LAN Command Sequence



[Figure 6.2.2.1] Wireless LAN Command Sequence

6.2.3 Serial & Wireless LAN Command Format

- Request Frame Format

DESCRIPTOR	STX (COMMAND CODE)	PARAMETER	ETX
Length(bytes)	18	Variable	2

[Table 6.2.3.1] Request Frame Format (Serial & WLAN)

- Response Frame Format

DESCRIPTOR	STX (COMMAND CODE)	PARAMETER	ETX
Length(bytes)	18	Variable	2

[Table 6.2.3.2] Response Frame Format (Serial & WLAN)

- ETX Frame Format

SETTING	FORMAT
ETX	ETXETX = 0x030x03

[Table 6.2.3.3] ETX Frame Format (Serial & WLAN)

- STX (Command Code) Frame Format

FUNCTION	OPERATION	MESSAGE VALUE	SIZE	COMMENT
PRINTER SEARCH	WLAN MODE ONLY			
	Search Request (Host→Device)	Search Request CMD("__[I_F]__[PRT_REG]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	Search Response (Device→Host)	Search Response CMD("__[I_F]__[PRT_RSP]")	unsigned char[18]	
		PrinterType	unsigned char[32]	Maximum

		SystemName	unsigned char[32]	MessageSize : 9KByte below Device information(Printer Type to Printer Port) is able to added repeatedly (MAX Device : 100)
		SystemVersion	unsigned char[9]	
		IP Address	unsigned char[4]	
		MAC Address	unsigned char[6]	
		Printer Port	unsgined char[2]	
		Check sum	unsigned char[2]	
	Message FAIL (Host↔Device)	FAIL CMD("__[I_F]__[___FAIL]")	unsigned char[18]	Fail response
		Check sum	unsigned char[2]	
GET CONFIGURATION	SERIAL & WLAN			
	Connect Request (Host→Device)	System Request CMD("__[I_F]__[SYS_REQ]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	Connect Request (Device→Host)	Search Request CMD("__[I_F]__[SYS_RSP]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	Configuration Get Value (Host→Device)	Configuration Get Value CMD("__[I_F]__[IF__GET]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	Configuration Current Value (Device→Host)	Configuration Current Value CMD("__[I_F]__[IF__CUR]")	unsigned char[18]	
		SystemName	unsigned char[32]	
		Region	unsigned char	Region information(RF)
		NetworkMode	unsigned char	Infra/Adhoc
		IpConfigMode	unsigned char	Static/DHCP
		IP Address	unsigned char[4]	
		SubNetMask	unsigned char[4]	
		Gateway	unsigned char[4]	
		SSID	unsigned char[32]	
		AUTH Mode	unsigned char	Open, Shared, WPA1PSK, WPA2PSK, WPA1EAP, WPA2EAP
		Crypto Mode	unsigned char	WEP64/128, TKIP, AES
		WEP Key_0	unsigned char[26]	It use one only.
		WEP Key_1	unsigned char[26]	
		WEP Key_2	unsigned char[26]	
		WEP Key_3	unsigned char[26]	
		PSK Key	unsigned char[64]	
		Adhoc channel	unsigned char	

		EAP Mode	unsigned char	TLS, TTLS, PEAP, LEAP
		EAP ID	unsigned char[32]	
		EAP PASSWORD	unsigned char[32]	
		USER NAME	unsigned char[32]	System ID
		USER PASSWORD	unsigned char[32]	System Password
		PRINTER Port	unsigned char[2]	
		Dummy	unsigned char	Channel Search
		SysContact	unsigned char[64]	
		SysLocation	unsigned char[64]	
		ipDefaultTTL	unsigned char	
		Dummy	unsigned char	powersave
		isWebSSL	unsigned char	
		isTelnet	unsigned char	
		isFTP	unsigned char	
		isSNMP	unsigned char	
		isSNMPTrap	unsigned char	
		SNMPSetCommunity	unsigned char[16]	
		SNMPGetCommunity	unsigned char[16]	
		SNMPTrapCommunity	unsigned char[16]	
		TrapIP	unsigned char[4]	
		IncativityTime	unsigned char[2]	
		Check sum	unsigned char[2]	
	Message FAIL (Host↔Device)	FAIL CMD("__[I_F]__[___FAIL]")	unsigned char[18]	Fail response
		Check sum	unsigned char[2]	
SET CONFIGURATION	SERIAL & WLAN			
	Connect Request (Host→Device)	System Request CMD("__[I_F]__[SYS_REQ]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	Connect Request (Device→Host)	Search Request CMD("__[I_F]__[SYS_RSP]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	Configuration Set Value (Host→Device)	Configuration Set Value CMD("__[I_F]__[IF__SET]")	unsigned char[18]	
		SystemName	unsigned char[32]	
		Region	unsigned char	Region information(RF)
		NetworkMode	unsigned char	Infra/Adhoc
		IpConfigMode	unsigned char	Static/DHCP
		IP Address	unsigned char[4]	
		SubNetMask	unsigned char[4]	
		Gateway	unsigned char[4]	
		SSID	unsigned char[32]	

		AUTH Mode	unsigned char	Open, Shared, WPA1PSK, WPA2PSK, WPA1EAP, WPA2EAP
		Crypto Mode	unsigned char	WEP64/128, TKIP, AES
		WEP Key_0	unsigned char[26]	It use one only.
		WEP Key_1	unsigned char[26]	
		WEP Key_2	unsigned char[26]	
		WEP Key_3	unsigned char[26]	
		PSK Key	unsigned char[64]	
		Adhocchannel	unsigned char	
		EAP Mode	unsigned char	TLS, TTLS, PEAP, LEAP
		EAP ID	unsigned char[32]	
		EAP PASSWORD	unsigned char[32]	
		USER NAME	unsigned char[32]	System ID
		USER PASSWORD	unsigned char[32]	System Password
		PRINTER Port	unsigned char[2]	
		Dummy	unsigned char	Channel Search
		SysContact	unsigned char[64]	
		SysLocation	unsigned char[64]	
		ipDefaultTTL	unsigned char	
		Dummy	unsigned char	powersave
		isWebSSL	unsigned char	
		isTelnet	unsigned char	
		isFTP	unsigned char	
		isSNMP	unsigned char	
		isSNMPTrap	unsigned char	
		SNMPSetCommunity	unsigned char[16]	
		SNMPGetCommunity	unsigned char[16]	
		SNMPTrapCommunity	unsigned char[16]	
		TrapIP	unsigned char[4]	
		IncativityTime	unsigned char[2]	
		Check sum	unsigned char[2]	
	Message SUCCESS (Device→Host)	SUCCESS CMD("__[I_F]__[IF__SUC]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	Message FAIL (Host↔Device)	FAIL CMD("__[I_F]__[___FAIL]")	unsigned char[18]	Fail response
		Check sum	unsigned char[2]	
BSS INFORMATION	SERIAL & WLAN			
	BSS Information Request	BSS Info Request CMD("__[I_F]__[BSS_REQ]")	unsigned char[18]	

	(Host→Device)	Check sum	unsigned char[2]	
	BSS Information Response (Device→Host)	BSS Info Response CMD("__[I_F]__[BSS_RSP]")	unsigned char[18]	
		SSID Type	unsigned char	Maximum MessageSize : 5KByteb below(WLAN) 10Kbyte below(Serial) AP information('SSID' to 'Security') is able to added repeatedly (MAX Device : 100)
		SSID Length	unsigned char	
		SSID Value	Valiable (MAX 32)	
		BSSID Type	unsigned char	
		BSSID length	unsigned char	
		BSSID Value	unsigned char[6]	
		NetworkMode	unsigned char	
		RSSI	unsigned char[2]	
		Security	unsigned char	WEP64 0, WEP128 1, WPA1 2, WPA2 3
		Check sum	unsigned char[2]	
	Message FAIL (Host↔Device)	FAIL CMD("__[I_F]__[__FAIL]")	unsigned char[18]	Fail response
		Check sum	unsigned char[2]	
FIRMWARE UPLOAD	SERIAL & WLAN			
	FW Data Message (Host→Device)	FW Data CMD("__[I_F]__[FW_DATA]")	unsigned char[18]	
		FW Data Length	unsigned char[8]	
		FW Data	valiable	MAX Size : 20Kbyte(WLAN), 15Kbyte(Serial)
		Check sum	unsigned char[2]	
	Message SUCCESS (Device→Host)	SUCCESS CMD("__[I_F]__[IF__SUC]")	unsigned char[18]	Receive Success response
		Check sum	unsigned char[2]	
	FW END Message (Host→Device)	FW END CMD("__[I_F]__[FW__END]")	unsigned char[18]	End of Firmware transmit
		Check sum	unsigned char[2]	
	Message SUCCESS (Device→Host)	SUCCESS CMD("__[I_F]__[IF__SUC]")	unsigned char[18]	Success response
		Check sum	unsigned char[2]	
	Message FAIL (Host↔Device)	FAIL CMD("__[I_F]__[__FAIL]")	unsigned char[18]	Fail response
		Check sum	unsigned char[2]	
	FW CANCEL Request (Host→Device)	FW CRC ERROR("__[I_F]__[FW_XREQ]")	unsigned char[18]	
		Check sum	unsigned char[2]	

	FW CANCEL Response (Device→Host)	FW CRC ERROR("__[I_F]__[FW_XRSP]")	unsigned char[18]	
		Check sum	unsigned char[2]	
	FW CRC ERR Message (Host↔Device)	FW CRC ERROR("__[I_F]__[CRC_ERR]")	unsigned char[18]	Verify does ‘FW Data’ after Flash write one.
		Check sum	unsigned char[2]	
CERTIFICATE (CA, CLIENT KEY, CLIENT PEM, FAST PAC) UPLOAD	SERIAL MODE ONLY			
	Certificate Data Message (Host→Device)	Certificate Data CMD("__[I_F]__[FW_CERT]")	unsigned char[18]	In serial Mode ‘Certificate Data Message’ is performed only by using the ‘Certificate Upload’. (Certificate is classified by using the ’ Serial Start command) Max Size : 500byte
		Certificate Size	unsgiend char[8]	
		Cerifiacate Data	valiable	
		Check sum	unsigned char[2]	
	Certificate Data End Message (Device→Host)	Certificate Data END CMD("__[I_F]__[CERTEND]")	unsigned char[18]	
		Certificate Size	unsgiend char[8]	
		Cerifiacate Data	valiable	Max Size : 500byte
		Check sum	unsigned char[2]	
	Message SUCCESS (Device→Host)	SUCCESS CMD("__[I_F]__[IF__SUC]")	unsigned char[18]	Success response
		Check sum	unsigned char[2]	
CA UPLOAD	WLAN MODE ONLY			
	CA Data Message (Host→Device)	CA Data CMD("__[I_F]__[CA_CERT]")	unsigned char[18]	
		CA Data Size	unsgiend char[8]	
		CA Data	valiable	Max Size : 500byte
		Check sum	unsigned char[2]	
	Certificate Data End Message (Device→Host)	Certificate Data END CMD("__[I_F]__[CERTEND]")	unsigned char[18]	
		Certificate Size	unsgiend char[8]	
		Cerifiacate Data	valiable	Max Size : 500byte
		Check sum	unsigned char[2]	
	Message SUCCESS (Device→Host)	SUCCESS CMD("__[I_F]__[IF__SUC]")	unsigned char[18]	Success reseponse
		Check sum	unsigned char[2]	
CLIENT KEY UPLOAD	WLAN MODE ONLY			
	Client Key Data Message (Host→Device)	Client Key Data CMD("__[I_F]__[CK_CERT]")	unsigned char[18]	
		Client Key Data Size	unsgiend char[8]	

		Client Key Data Data	valiable	Max Size : 500byte
		Check sum	unsigned char[2]	
	Certificate Data End Message (Device→Host)	Certificate Data END CMD("__[I_F]__[CERTEND]")	unsigned char[18]	
		Certificate Size	unsgiend char[8]	
		Cerifiacate Data	valiable	Max Size : 500byte
		Check sum	unsigned char[2]	
	Message SUCCESS (Device→Host)	SUCCESS CMD("__[I_F]__[IF__SUC]")	unsigned char[18]	Success response
		Check sum	unsigned char[2]	
CLIENT PEM UPLOAD	WLAN MODE ONLY			
	Client PEM Data Message (Host→Device)	Client PEM Data CMD("__[I_F]__[CP_CERT]")	unsigned char[18]	
		Client PEM Data Size	unsgiend char[8]	
		Client PEM Data Data	valiable	Max Size : 500byte
		Check sum	unsigned char[2]	
	Certificate Data End Message (Device→Host)	Certificate Data END CMD("__[I_F]__[CERTEND]")	unsigned char[18]	
		Certificate Size	unsgiend char[8]	
		Cerifiacate Data	valiable	Max Size : 500byte
		Check sum	unsigned char[2]	
	Message SUCCESS (Device→Host)	SUCCESS CMD("__[I_F]__[IF__SUC]")	unsigned char[18]	Success response
		Check sum	unsigned char[2]	

[Table 6.2.3.4] STX Command Frame Format (Serial & WLAN)

7. Technical Support, Warranty, and Precaution

7.1 Technical Support

If you have any question regarding operation of the product, visit the message board on CMAX Wireless's web site or send us an email at the following address:

- □E-mail: support@cmaxwireless.com
- □For more information, visit our website at http://www.cmaxwireless.co.kr

7.2 Warranty

7.2.1 Refund

Upon the customer's request to refund the product within two weeks after purchase, CMAX Wireless will refund the product.

7.2.2 Free Repair Services

For product failures occurring within one year after purchase, CMAX Wireless provides free repair services or exchange the product. However, if the product failure is due to user's fault, repair service fees will be charged or the product will be replaced at user's expense.

7.2.3 Charged Repair Services

For product failures occurring after the warranty period (one year) or resulting from user's fault, repair service fees will be charged and the product will be replaced at user's expense.

7.3 Precaution

- CMAX Wireless is not responsible for product failures occurring due to user's alternation of the product.

- Specifications of the product are subject to change without prior notice for performance improvement.

- CMAX Wireless does not guarantee successful operation of the product if the product was used under conditions deviating from the product specifications.

- Reverse engineering of firmware and applications provided by CMAX Wireless is prohibited.

- Use of firmware and applications provided by CMAX Wireless for purposes other than those for which they were designed is prohibited.

- Do not use the product in an extremely cold or hot place or in a place where vibration is severe.

- Do not use the product in an environment in which humidity is high or a lot of oil exists.

- Do not use the product where there is caustic or combustible gas.

- CMAX Wireless does not guarantee normal operation of the product under the conditions a lot of noise exists.

- Do not use the product for a purpose that requires exceptional quality and reliability relating to user's injuries or accidents - aerospace, aviation, health care, nuclear power, transportation, and safety purposes.

- CMAX Wireless is not responsible for any accident or damage occurring while using the product.

7.4 USA-Federal Communications Commission (FCC)

- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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. If not installed and used in accordance with the instructions, it 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 tuning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the distance between the equipment and the receiver.
  - Connect the equipment to outlet on a circuit different from that to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help.

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

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

7.4.1 Labeling

FCC ID: YC9CWE-100SA

The proposed with FCC ID label format is to be placed on the module. If FCC ID is not visible when the module is installed into the system, "Contains FCC ID: YC9CWE-100SA" shall be placed on the outside of final host system.

Caution: Exposure to Radio Frequency Radiation.

To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

COPYRIGHT NOTICE

For more information, visit our website at http://www.cmaxwireless.co.kr