User´ s Guide

SMT-CW230

JAN. 2010

FCC Compliance Information

This device complies with Part 15 of 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.

RF Radiation Exposure Statement

This equipment complies with FCC RF Radiation Exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

Warnings

This equipment has been tested and found to comply with limits for a class B digital device, pursuant to Part 15, 27 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment can generates, uses, and 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.
Of this equipment does cause unacceptable interference to radio and television reception, which can be determined by turning the equipment off and on the user is encouraged to try to correct the interference by one or more of the following measures.

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

Caution

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

Contents

1. Product Introduction

1.1 Overview

SMT-CW230, which belongs to Customer-Premises Equipment (CPE), is the combination of two devices; one is a cable modem that an existing network carrier lends and provides to users. The other is a sharing device that users formerly had to buy on their own.
Existing modems have some limitations on installation because users must relocate their cables indoors from outside. However, the SMT-CW230 uses the Wireless of the WAN that connects outside. Therefore, it can be transferred and installed easily without any space limitations.

1.2 Key Features

- Provide Internet services through the IEEE 802.16e instead of ADSL, VDSL or CABLE modems.
- Possible to connect the 802.3u 10/100Mbps wired LAN.
- Allow multiple PCs to use Internet services only with one "Internet (WAN)" IP address.
- Support the maximum 254 internal IP addresses.
- Assign floating IP addresses automatically with the DHCP server for easy management and use.
- Possible to set the firewall function to protect an internal network.
- Possible to set the DNS Relay service function.
- Possible to set the VPN Pass through function.
- Possible to set the Bridge function.
- Possible to set the Port Forwarding function.
- Possible to set the Port Triggering function.
- Provide a convenient software (firmware) upgrade function.
- Provide static & dynamic IP services.
- Support an intelligent DMZ function.

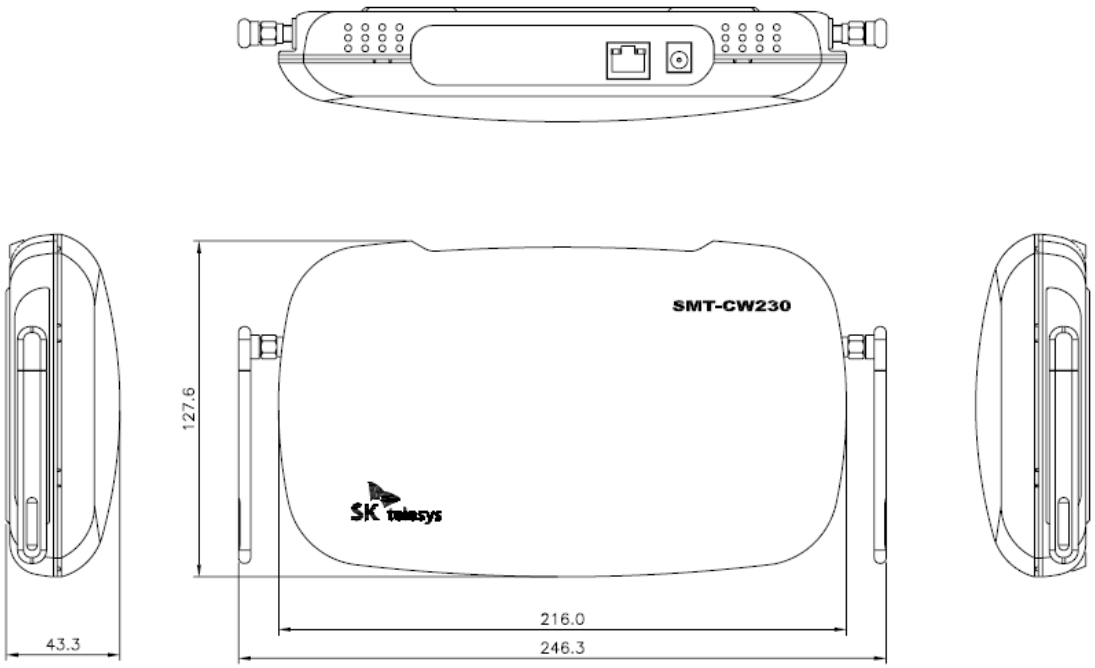
2. Product Configuration

2.1 Product Configuration

The configuration of this product is as follows. Please check the details.

No.	Item	Unit	Qty	Remarks
1	SMT-CW230 body	Set	1	
2	Antenna	Piece	2	
3	Power adapter	Piece	1	
4	LAN cable	Piece	1	
6	Quick Reference	Piece	1	

2.2 Product Appearance



[Fig. 1] SMT-CW230 Dimension

3. Product Installation & Setup

3.1 Initial Settings

The initial settings to access the SMT-CW230 configuration & setup menu are as follows.

- When you apply power to the SMT-CW230, its initial settings allow automatic access and connection to the Network.
  CM configuration: auto connection enable
- When you connect the PC with the RJ-45 terminal located at the back side of the SMT-CW230 by using the Ethernet Cable, the SMT-CW230 assigns an IP automatically by using the DHCP. The initial settings of the LAN Configuration are as follows.

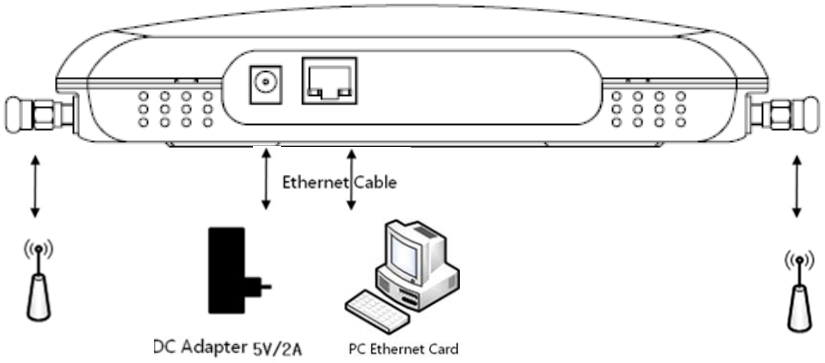
※ The network setup of the PC connected with the SMT-CW230 must be set to the DHCP enable.

SMT-CW230 IP Address: 192.168.100.254
My IP Address: between 192.168.100.100 and 109 (automatic DHCP-assigned value)
Net Mask: 255.255.255.0

3.2 Product Connection & Installation

Please try the following installation processes to use this product easily.

① Connect the antenna to the SMT-CW230. (As mentioned in Fig.)
② Connect the SMT-CW230 with the PC by using the Ethernet Cable.
※ Both Cross-cable and Direct-cable are available.
③ Connect the AC/DC Adapter to the SMT-CW230 power terminal.
④ Execute the web browser in the PC to check that the wireless Internet runs normally.



[Fig. 1] Product Installation Diagram

4. SMT-CW230 Web Setup Screen

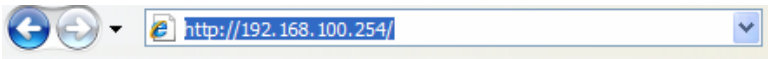
4.1 SMT-CW230 Function Configuration

You can use the following categories by accessing the SMT-CW230. They include the Network connection setup, network-related setup, firewall, security-related functions. You can also update them into a new version by using the firmware update functions on the web.

No.	Category	Sub Title	Key Functions
1	Simple Setting	System Setting	-Change a user password. -Set the time zone.
		IP Setting	Set Internet network information. (IP address, subnet mask, Start/End IP, DNS server, Default Gateway)
		Wireless Setting	Set the wireless network name (SSID) & frequency (channel).
		Security Setting	Set the security mode to be applied to wireless networks.
2	Internet Setting	LAN	Set detailed information on Internet networks. (IP address, subnet mask, Start/End IP, DNS server, Default Gateway)
		WAN	Set WiMAX connection and DHCP mode.
		LAN DHCP Info	Display the list of connected devices.
3	Wireless Setting	Wireless Setting	Set detailed information on wireless networks and the manual mode.
		Security	Set the security of selected networks.
		Station List	Display information on the WiFi devices connected to SMT-CW230.
4	Firewall	MAC/IP/Port Filter	Set the items to be filtered to enhance security.
		Port Forwarding	- Set the virtual server for port forwarding.
		DMZ	- DMZ setup screen - Open all ports to the designated internal IP address.
		Contents Filter	Block harmful sites through URL blocking.
5	System Setting	Management	-Change a user password. -Set the time zone.
		Update Firmware	- Firmware update button - Update the firmware to the newest version.
		Default Setting	- System load factory default button Restore SMT-CW230 to the default setting.
		Statistic	Display memory information and WiMAX/WiFi communication information.
		System Log	Record System Logs at real times.

4.2 Web Server Access

The SMT-CW230 enables you to change settings or check operations by accessing the web server. The web setup screen is based on the built-in web server, so you can have access to it without an Internet connection.
To access the web setup screen, you can execute the web browser and enter the numbers 192.168.100.254.



Note

Before accessing the web server of the SMT-CW230, the PC must be connected with the SMT-CW230 through a cable.
The IP of the PC must be set to auto select.

You can use the web functions by entering your ID and password into the Login Page of the SMT-CW230 and logging in. You can try login by using an initially set ID and its password admin/admin. You can also change a password by using the system setting or management page.

ID	admin
Password	admin

Note) User authentication window

5. Web CM

5.1 Simple Setting

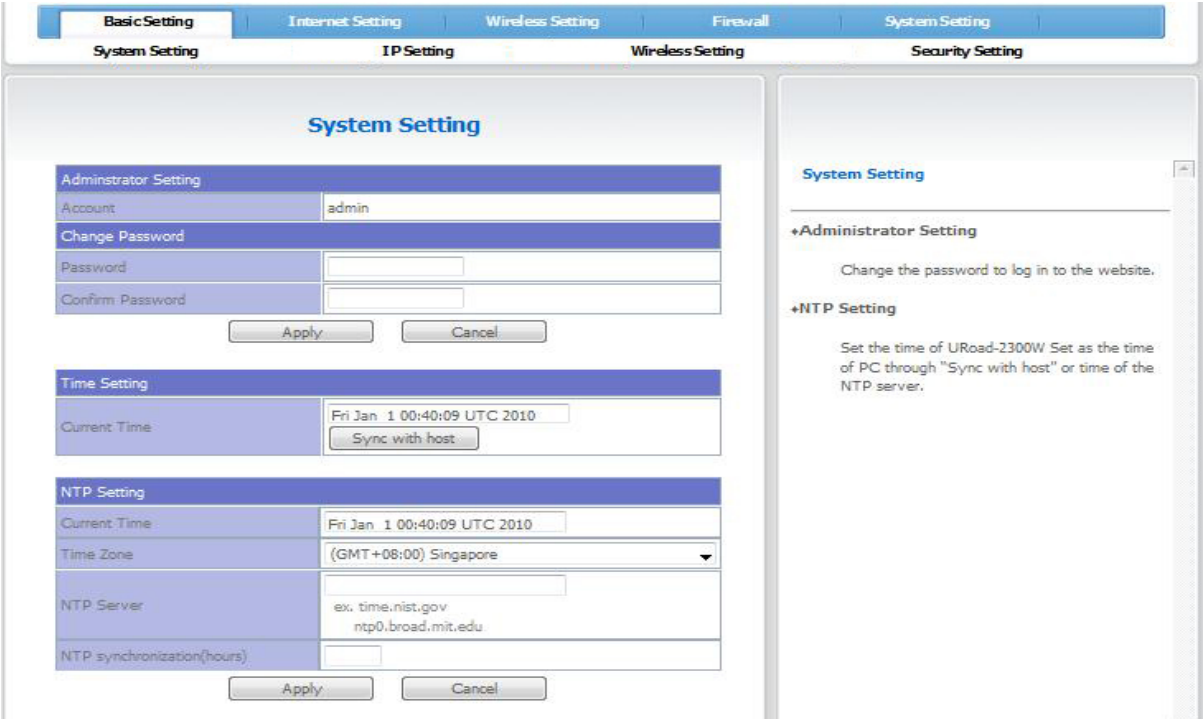
This is a menu where basic functions of all categories are gathered.

This is configured so that the settings of four sub menus such as System Setting, IP Setting, Wireless Setting and Security Setting.

5.1.1 System Setting

Simple Setting → System Setting

Set the admin password and time zone.



Change password

① Enter the new password (after changing) into the Password column.

② To check that the new Password after change has been correctly entered, enter the password into the Confirm Password window and click the 'Apply' button.

③ Then, when the user authentication window pops up, enter the changed Password to re-access the site.

Set the time zone

① Enter the NTP Server for the time zone to be applied.

② Select the time zone with the country you are in.

③ Click the 'Apply' button.

5.1.2 IP Setting

Simple Setting → IP Setting

The IP Setting indicates information on the internal network. You can set the IP address on this screen to the gateway of the internal PC

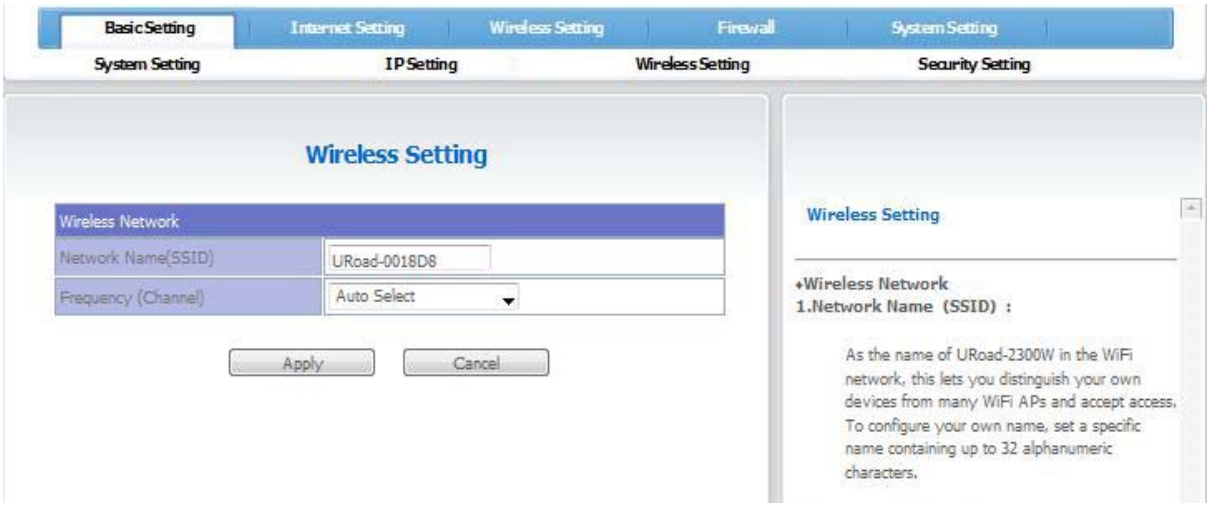
Items displayed on the setup screen of the IP Setting are as follows. After setting, save the values by clicking the Apply button.

Sub Menu	Description
IP Address	LAN IP address of the CPE, GW of the internal network. The default setting is recommended.
Subnet Mask	Set the Subnet Mask. The default setting is recommended.
Start IP Address	Set the start address of the device to be connected to SMT-CW230. Only the last three digits can be changed to values between 2~253. When setting external → internal, enter the specific IP on the Internet where security is to be set. When setting internal → external, enter the IP of the internal LAN where security is to be set.
End IP Address	Will be automatically set by the start address.
DNS Server	Set the main DNS Server. If the default setting is changed, Internet connections of several devices may be disconnected.
Secondary DNS Server	Set the secondary DNS Server.

5.1.3 Wireless Setting

Simple Setting → Wireless Setting

Set the name and frequency of the wireless network.



Items displayed on the setup screen of the Wireless Setting are as follows. After setting, you can save values by clicking the Apply button.

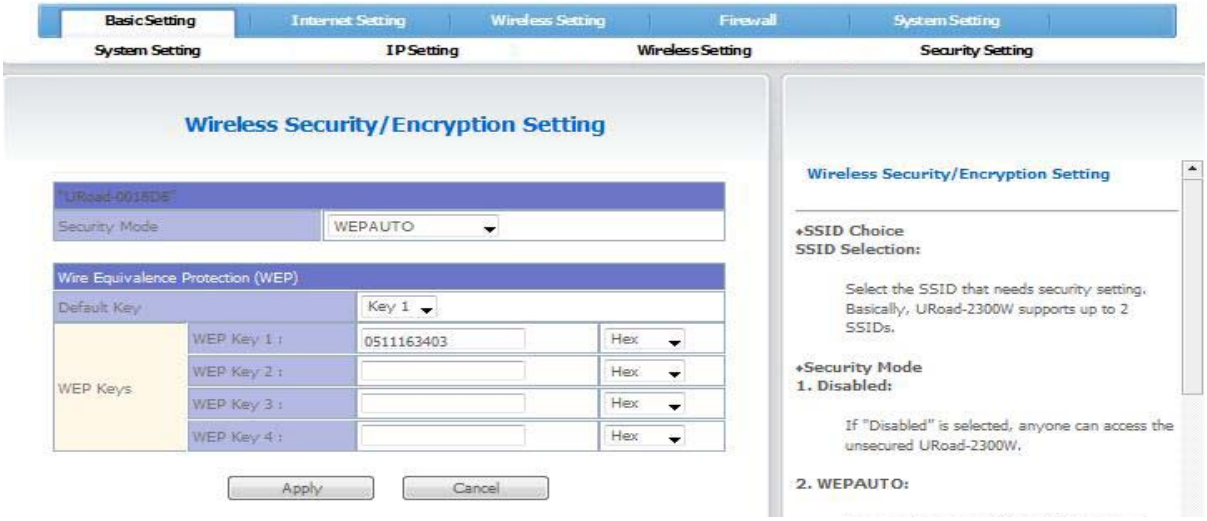
Sub Menu	Description
Network Name	Designate the name (SSID) of the wireless network of SMT-CW230. Can designate up to 32 digits with a combination of letters and numerals.
Frequency	Select the frequency (channel) band constituting the wireless network.

5.1.4 Security Setting

Simple Setting → Security Setting

This page describes how to set security for the wireless network.

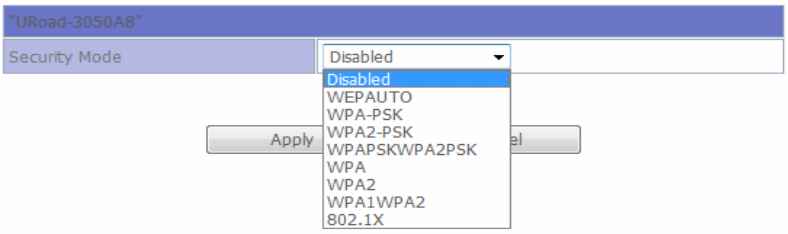
First, select the security mode to be used and then set the details based on the selected mode.



Setting a security mode

① The default setting of security modes is Disable.

② Select a desired security mode and click the 'Apply' button.

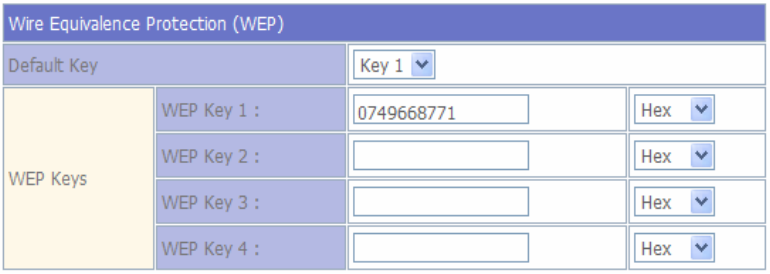


③ Set the details

[Things to be set when the WEP AUTO was selected]

Designate the password to be used when accessing the wireless network.

WEP: This is a method for users to arbitrarily set passwords to be used and the data transmitted through the wireless LAN are encoded to provide the same level of security as that of cabled networks. (defined under the IEEE802.11 standards)

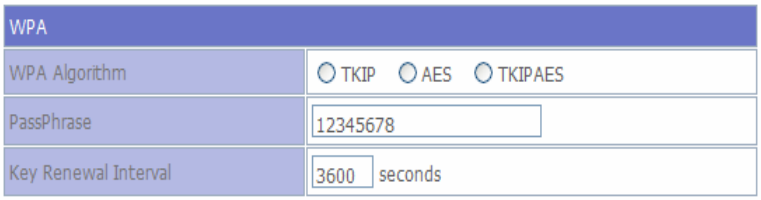


[Things to be set when WPA-PSK, WPA2-PSK, WPAPSKWPA2PSK were selected]

Select the WPA algorithm and designate a Pass Phrase.

WPA Algorithm: wireless LAN security algorithm

- TKIP : An encoding method used in WPA that changes keys for all frames.
- AES : A block password format designated as a USA standard.
- TKIPAES : A security function made by complementing the above two functions.



[Things to be set when WPA, WPA2, WPA1WPA2 were selected]

Select the WPA algorithm and set the RADIUS Server. To use this setting, an authentication server satisfying the IEEE802.1X standard is necessary.

RADIUS: The client/server protocol and software that enables you to communicate with the central server.

WPA	
WPA Algorithm	○ TKIP ○ AES ○ TKIPAES
Key Renewal Interval	3600 seconds

RADIUS Server	
IP Address	
Port	1812
Shared Secret	
Session Time-out	0
Idle Time-out	

④ Click the 'Apply' button.

If the network connection is disconnected, the security is normally applied, so, please wait for 1~2 minutes until SMT-CW230 is rebooted and then access the wireless network.

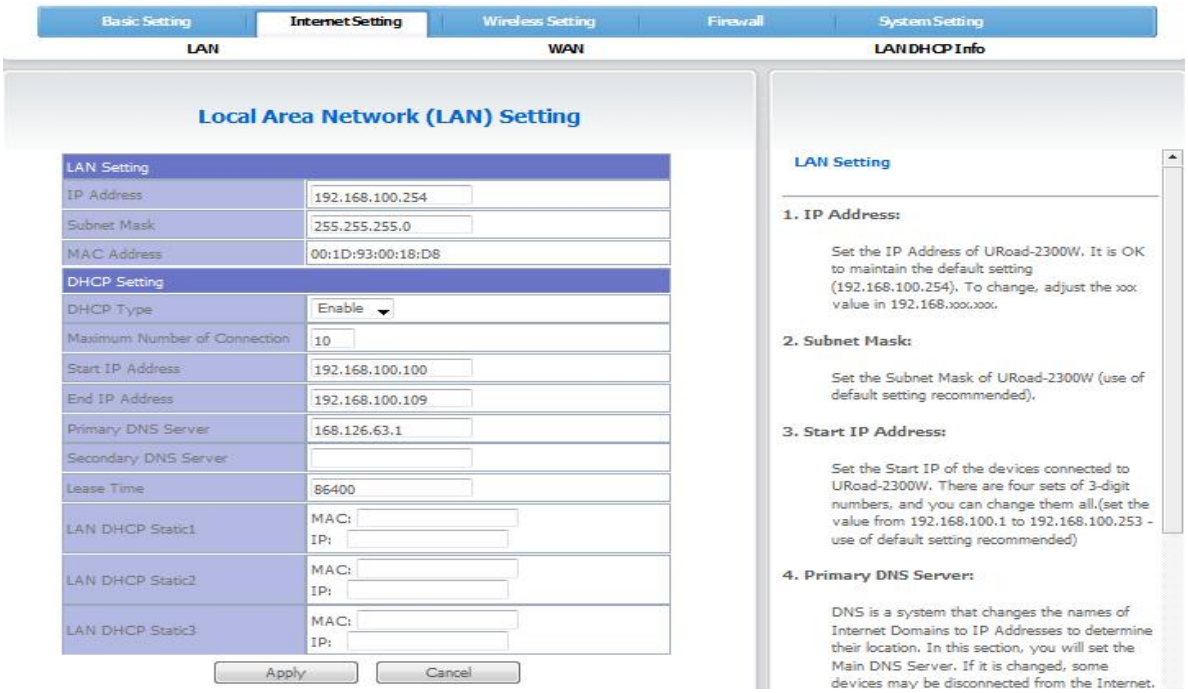
5.2 Internet Setting

There are three menus for network setting, LAN, WAN and LAN DHCP Info.

5.2.1 LAN

Internet Setting → LAN

This is a page for LAN setting. You may set IP address, subnet mask, Start IP, End IP, DNS server, Default Gateway, delay time, DHCP.



Items displayed on the setup screen of the LAN are as follows. After setting, you can save values by clicking the Apply button.

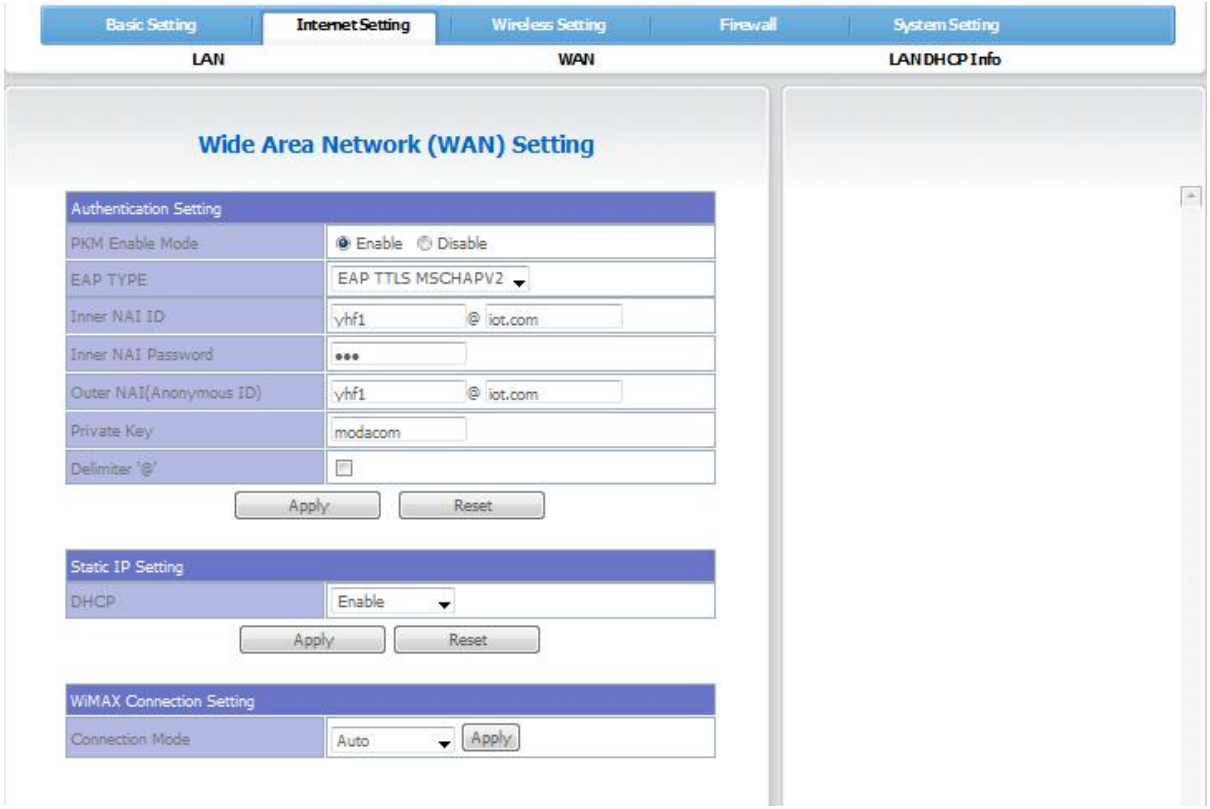
Sub Menu	Description

IP Address	Set the IP address. The default address is recommended.
Subnet Mask	Set the Subnet Mask. The default address is recommended.
Start IP	Set the start address of the device to be connected to SMT-CW230 Series. Only the numerals on the last three digits can be changed to values between 2~253. When setting external → internal, enter the specific IP on the Internet where security is to be set. When setting internal → external, enter the IP of the internal LAN where security is to be set.
DNS Server	DNS is a system that changes the names of Internet Domains to IP Addresses to determine their location. In this section, you will set the Main DNS Server. If it is changed, some devices may be disconnected from the Internet.
Lease Time	Set the re-registration time of DHCP.

5.2.2 WAN

Internet Setting → WAN

This is a Wide Area Network setting page. You may set WiMAX connection and DHCP mode.



5.2.3 LAN DHCP Info

Internet Setting → LAN DHCP Info

This is a DHCP Client List page. It displays a list of the devices currently connected.

5.3 Wireless Setting

This menu for wireless network setting has three sub menus-- Wireless Setting, Security and Station List.

5.3.1 Wireless Setting

Wireless Setting → Wireless Setting

Set the wireless network mode, wireless network name, whether the wireless network will be used and the manual setting mode.

Items displayed on the setup screen of the Wireless Setting are as follows. After setting, you can save values by clicking the Apply button.

Sub Menu	Description
Network Mode	Select the network mode to be applied. (Refer to chapter 9. Glossary)
Network Name(SSID)	Designate the name of the wireless network of SMT-CW230 Series.
Broadcast Network Name	Select whether the SSID will be used (Disable/Enable).
WiFi MAC	Display the MAC address.
Frequency	Select the frequency (channel) band constituting the wireless network.

5.3.2 Security

Wireless Setting → Security

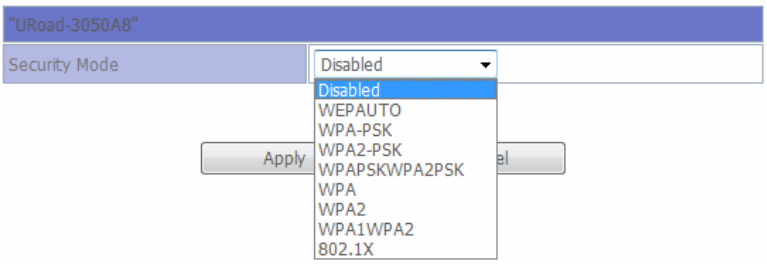
This page describes security setting. Select a security mode and set the details of the security based on the selected mode.

Security mode setting

① The default setting of security modes is Disable.

② Select a security mode.

Select a desired security mode and click the 'Apply' button.



③ Set the following details.

[Things to be set when the WEP AUTO was selected]

Designate a password to be used when accessing the wireless network.

WEP: This is a method for users to arbitrarily set passwords to be used. The data transmitted through the wireless LAN are encoded to provide the same level of security as that of cabled networks. (defined under the IEEE802.11 standards)

Wire Equivalence Protection (WEP)			
Default Key		Key 1	
WEP Keys	WEP Key 1 :	0749668771	Hex
	WEP Key 2 :		Hex
	WEP Key 3 :		Hex
	WEP Key 4 :		Hex

[Things to be set when WPA-PSK, WPA2-PSK, WPAPSKWPA2PSK were selected]

Select the WPA algorithm and designate a Pass Phrase.

WPA Algorithm: wireless LAN security algorithm

- TKIP : An encoding method used in WPA that changes keys for all frames.
- AES : A block password format designated as a USA standard.
- TKIPAES : A security function made by complementing the above two functions.

WPA	
WPA Algorithm	○ TKIP ○ AES ○ TKIPAES
PassPhrase	12345678
Key Renewal Interval	3600 seconds

[Things to be set when WPA, WPA2, WPAIWPA2 were selected]

Select the WPA algorithm and set the RADIUS Server. To use this setting, an authentication server satisfying the IEEE802.1X standard is necessary.

- RADIUS: The client/server protocol and software that enables you to communicate with the central server.

WPA	
WPA Algorithm	○ TKIP ○ AES ○ TKIPAES
Key Renewal Interval	3600 seconds

RADIUS Server	
IP Address	
Port	1812
Shared Secret	
Session Time-out	0
Idle Time-out	

⑤ Click the 'Apply' button.

If the network connection is disconnected, the security is normally applied, so, please wait for 1~2 minutes until SMT-CW230 is rebooted and then access the wireless network.

5.3.3 Station List

Wireless Setting → Station List

Display a list of the WiFi devices connected to the SMT-CW230 wireless network.

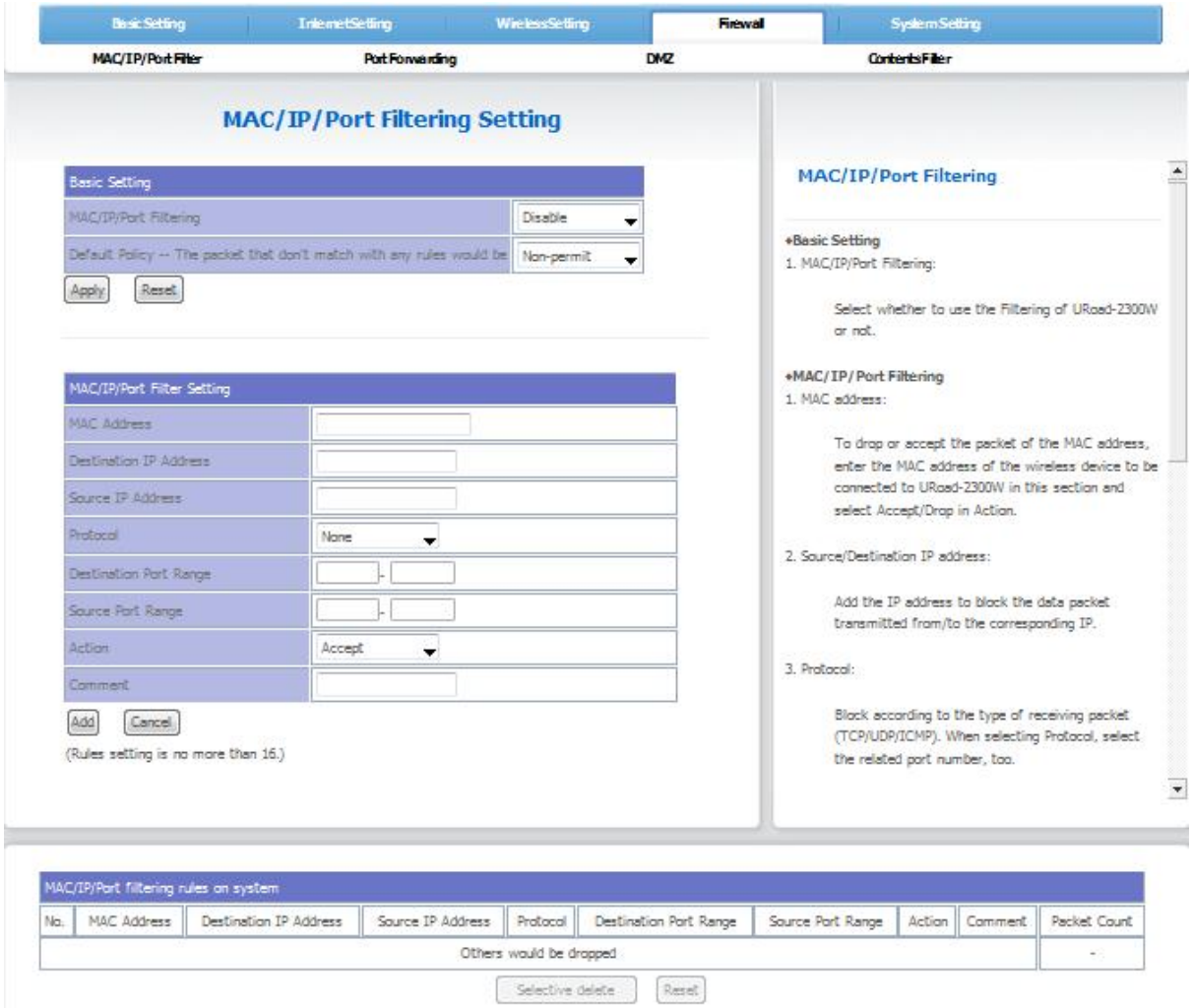
5.4 Firewall

This is a menu for firewall setting.

5.4.1 MAC/IP/Port Filter

Firewall → MAC/IP/Port Filter

This is a page for MAC/IP/Port Filter use setting.



Items displayed on the setup screen of the MAC/IP/Port Filter are as follows. After setting, you can save values by clicking the Apply button.

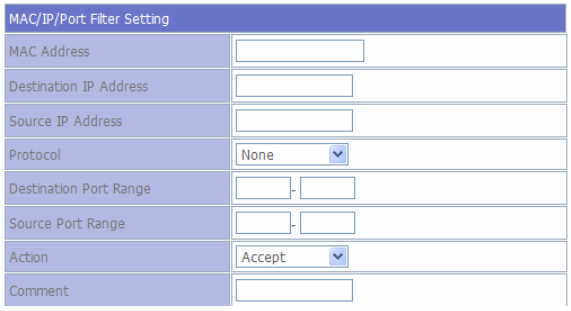
Sub Menu	Description
MAC Address	Enter the MAC address.
Destination IP Address	Set the destination address.
Source IP Address	Set the source address.
Protocol	Designate a suitable protocol among None/TCP/UDP/ICMP.
Destination Port Range	Set the destination port range.
Source Port Range	Set the source port range.
Action	Select whether to Accept/Decline the rules.
Comment	Designate rules with easily identifiable Comments to distinguish.

Firewall setting

① Set the MAC/IP/Port Filtering to Enable.

② Set MAC/IP/Port Filtering rules.

Up to 16 MAC/IP/Port Filtering rules can be registered.



③ Click the 'Apply' button.

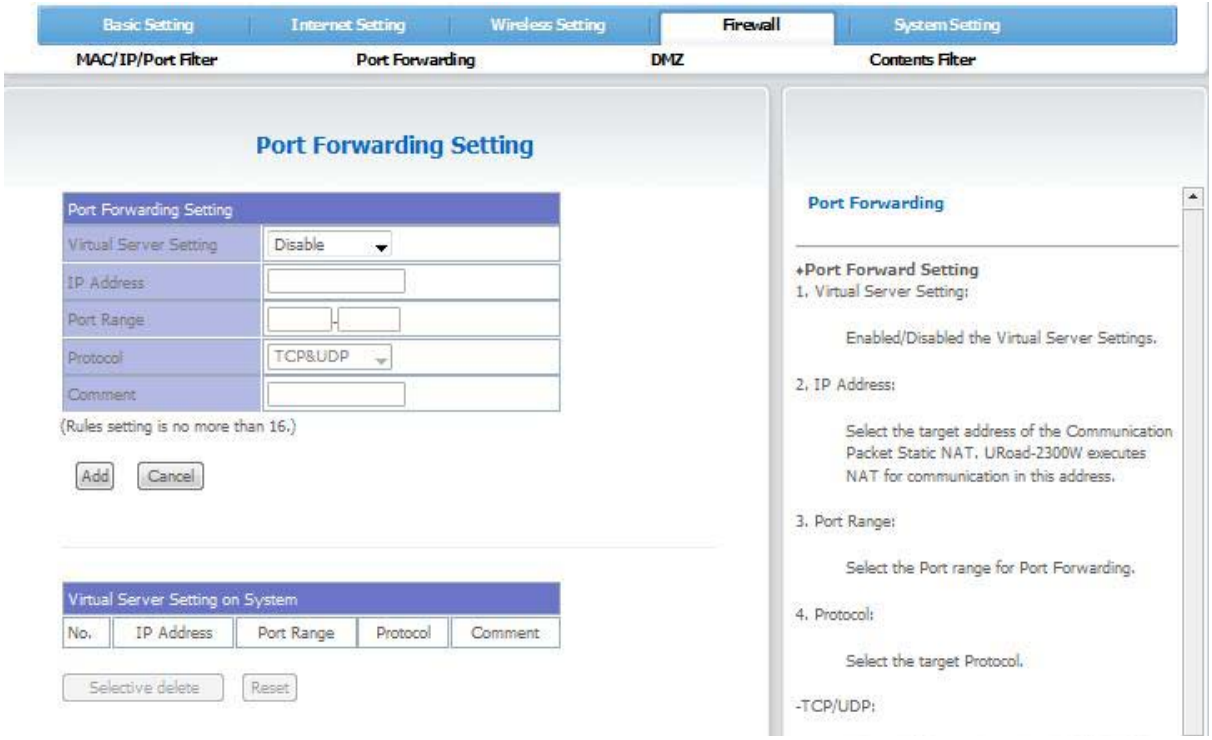
Once the application has been completed, you can identify that the rules have been registered with the MAC/IP/Port Filtering rules on the system on the bottom of the web page.

5.4.2 Port Forwarding

Firewall → Port Forwarding

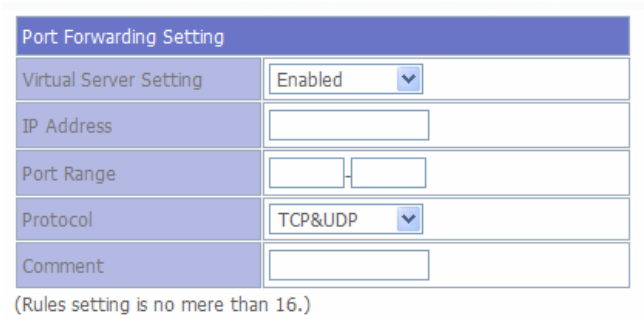
Set the Virtual Server and forward it to the desired port.

With the port forwarding setting, you can map the internal IP address and Port numbers based on external access requests.



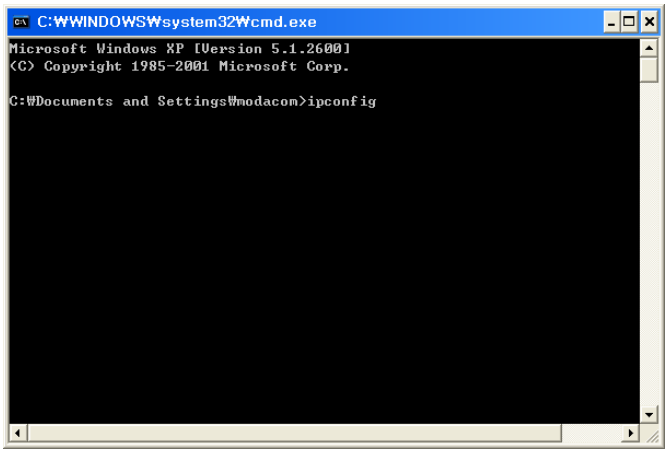
Port forwarding setting

① Click Start > execute on the window.

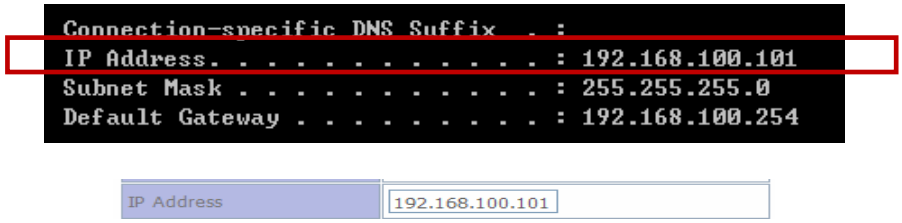


② Enter cmd into the execute window and click the 'confirm' button.

③ When the Command window pops up, enter ipconfig and press Enter.



④ Enter the address value displayed on the IP Address(XP) / IPv4(Vista) into the IP Address column.



⑤ Enter an appropriate port range based on the Server or Site to be accessed.

⑥ Select the Protocol to be used. (Refer to the Glossary (Chapter 9) for details).

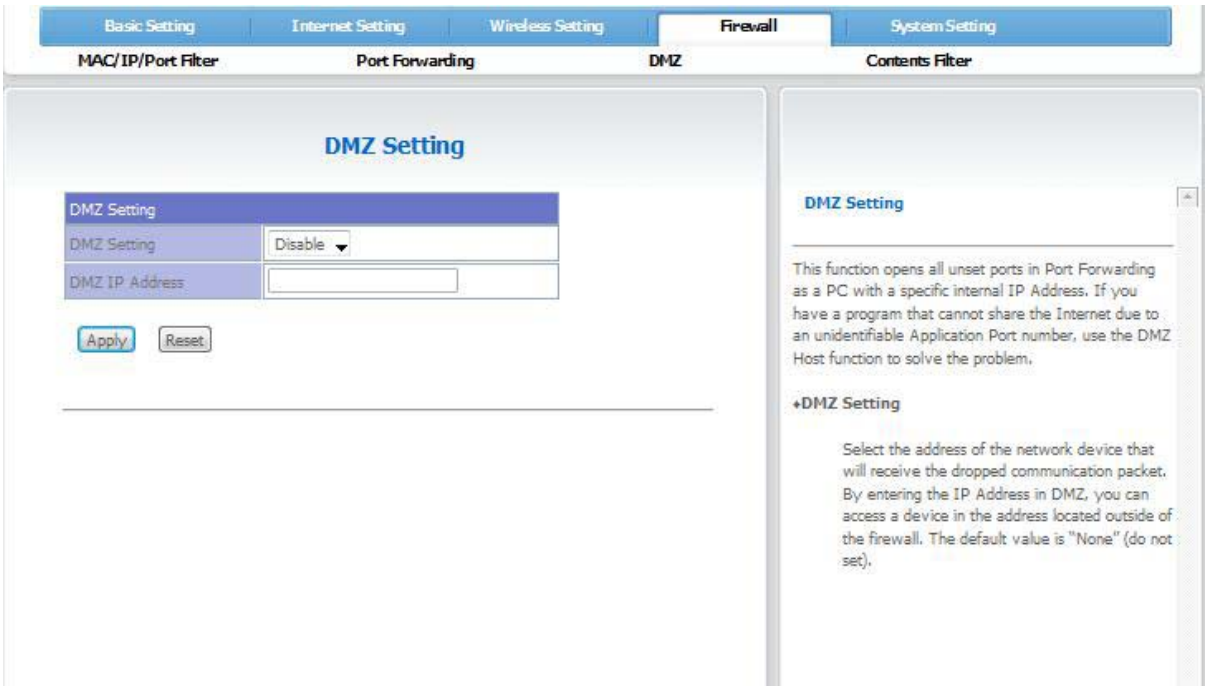
⑦ Designate the rules with easily identifiable Comments to distinguish.

⑧ Click the 'Apply' button.

5.4.3 DMZ

Firewall → DMZ

Pass all ports except for the ports set in port forwarding to the designated specific internal IP address (PC).



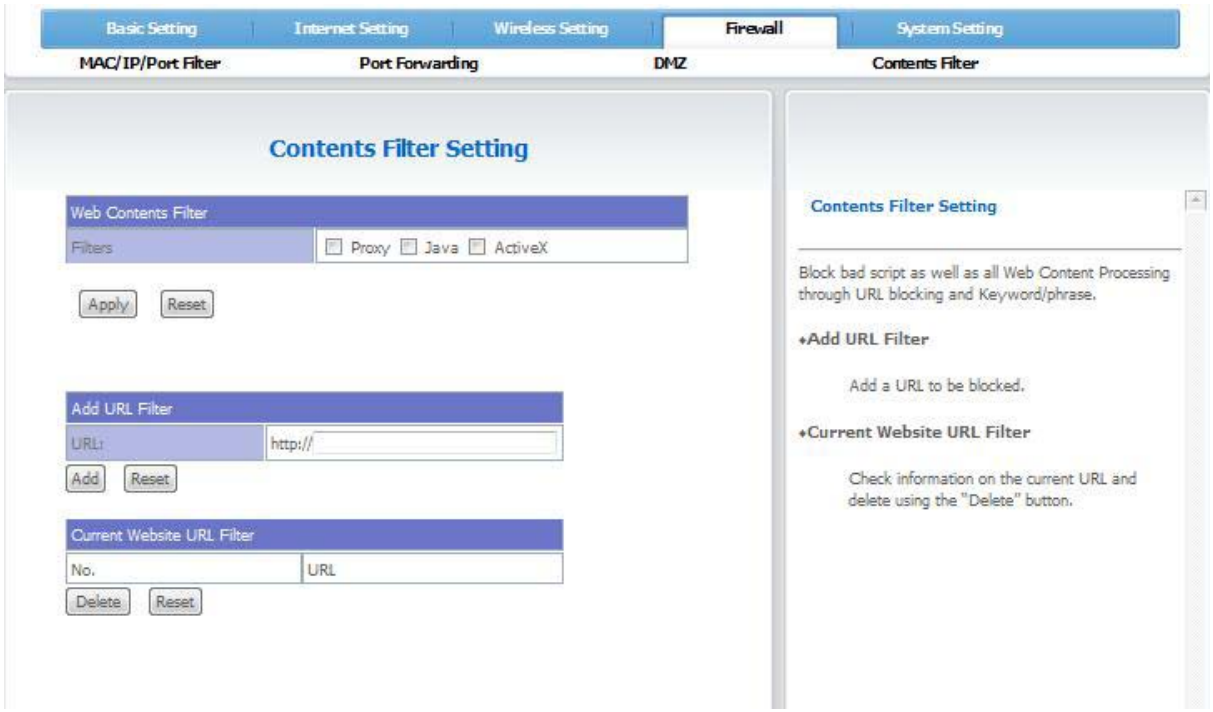
DMZ setting

① Set the DMZ Setting to Enable.
② Click Start>Execute and enter cmd.
③ Enter ipconfig into the Command window.
④ Enter the address value displayed on the IP Address (XP) / IPv4(Vista) into the DMZ IP Address column.
⑤ Click the 'Apply' button.

5.4.4 Contents Filter

Firewall → Contents Filter

Provides a filter setting that can prevent access to harmful Contents.
Prevents access to Web Contents and URLs arbitrarily designated by users.



Items displayed on the setup screen of the Contents Filter are as follows. After setting, you can save values by clicking the Apply button.

Sub Menu	Description
Web Contents Filter	Prevent accesses of applications implemented by Proxy / JAVA / ActiveX.
Add URL Filter	Set the URLs to be blocked. Ex. When www.SMT.com has been set, even if www.SMT.com has been entered into the address window of Internet Explorer, no access will be made to the relevant site.
Current URL Filter	Display a list of blocked URLs.

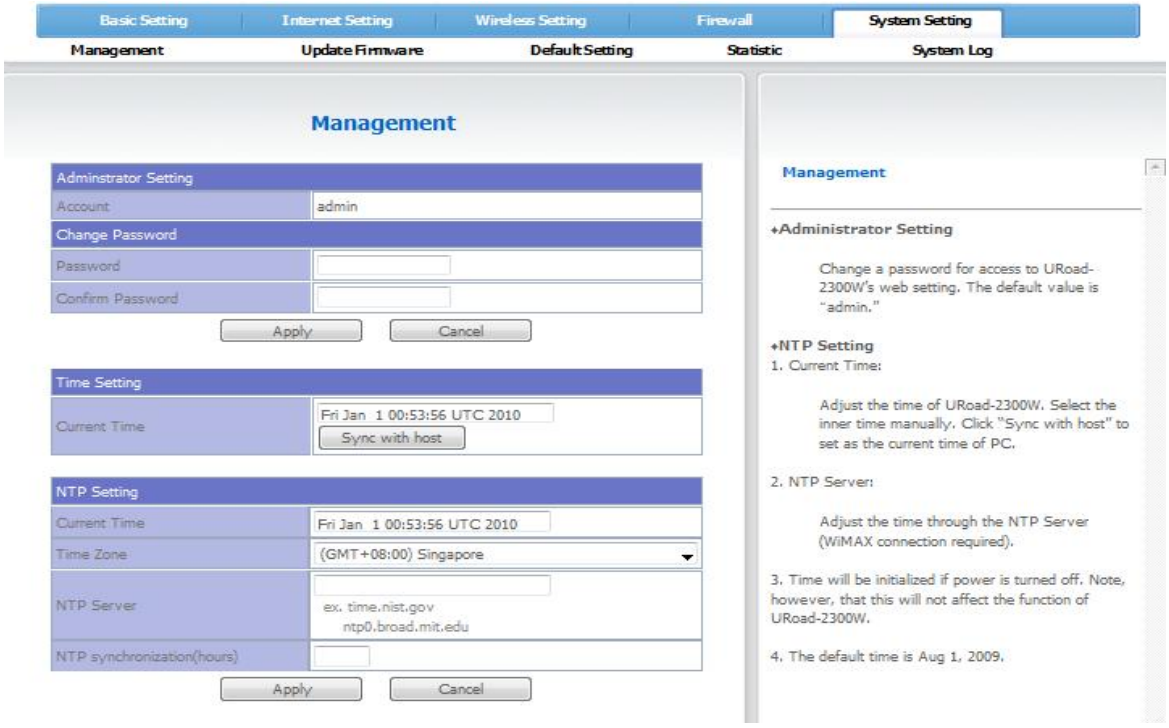
5.5 System Setting

Provide a system setting function consisting of five sub menus such as Management, Update Firmware, Default Setting, Statistic and System Log.

5.5.1 Management

System Setting → Management

Set a password and a standard time zone. (The same function as the System Setting of the Simple Setting)



Password changing

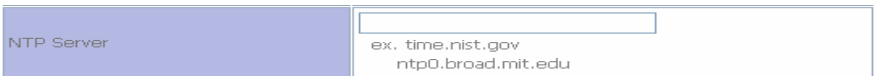
① Enter the new password after change into the Password column.

② To check if the new Password after change has been correctly entered, enter the password into the Confirm Password window and click the 'Apply' button.

③ Then, when the user authentication window pops up, enter the changed Password to re-access the site.

Changing the standard time zone

① Enter the NTP Server for the time zone to be applied.



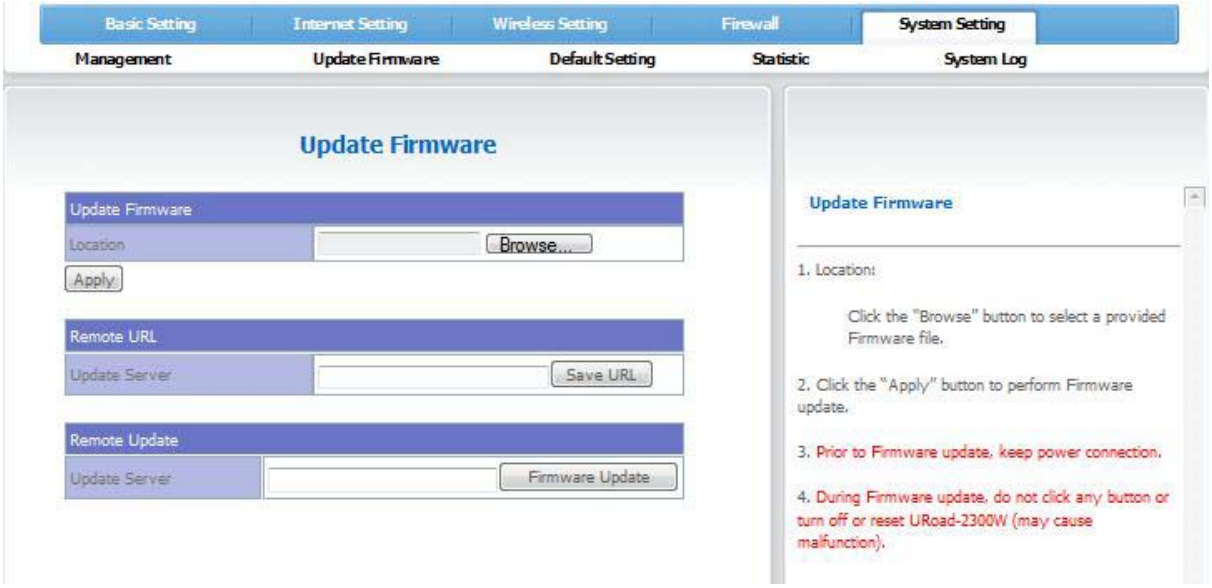
② Select the Time Zone with the country you are in.

③ Click the 'Apply' button.

5.5.2 Update Firmware

System Setting → Update Firmware

Update the Firmware to the newest version.



Firmware Updating

① Download the file of the newest Version to the computer.

② Click 'Browse' .

③ Select the downloaded file on the file selection window and press the 'Open' button.

④ Click the 'Apply' button.

⑤ The update will begin. It will take approximately three minutes and once the Update has been completed, the SMT-CW230 will be rebooted.

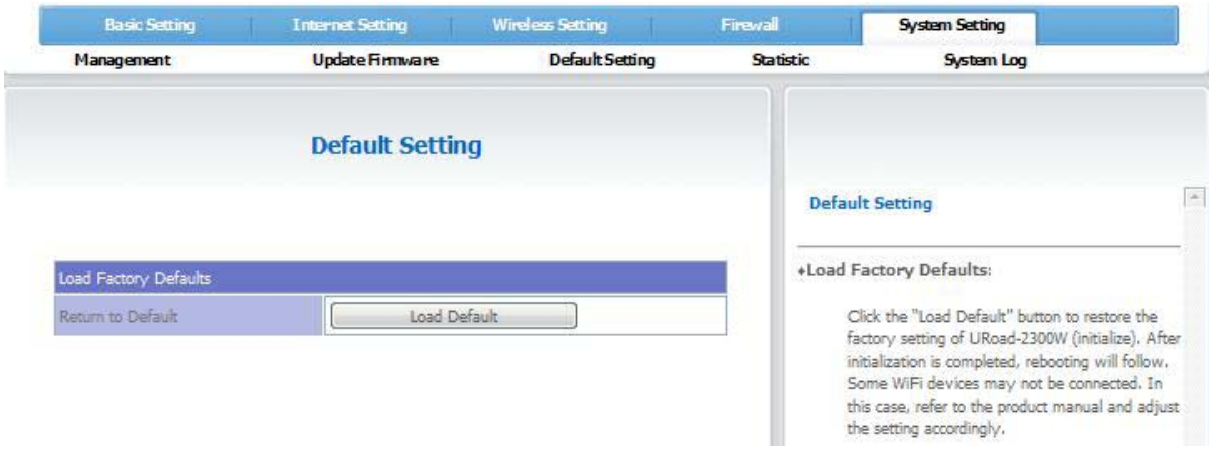
⚠ Caution!	During an update, do not move to another menu on the site, disconnect the network connection or turn off the power. (Such actions may cause a breakdown.) The system may be damaged if the firmware is uploaded with any other file than the firmware file.

5.5.3 Default Setting

System Setting → Default Setting

Provide a function to restore all settings of SMT-CW230 to the default setting.

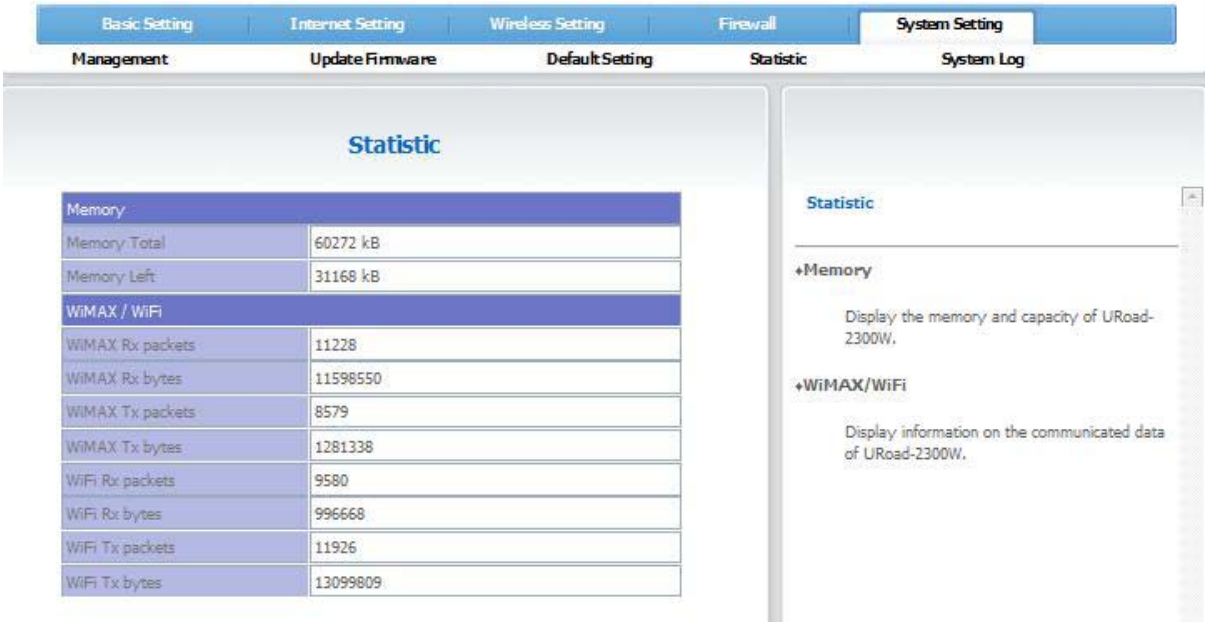
Click Load Default, then the wireless network connection will be disconnected and SMT-CW230 will be rebooted.



5.5.4 Statistic

System Setting → Statistic

Display the information on the memory of SMT-CW230 and detailed information on WiMAX / WiFi.



Items displayed on the setup screen of the Statistic are as follows. After setting, you can save values by clicking the Apply button.

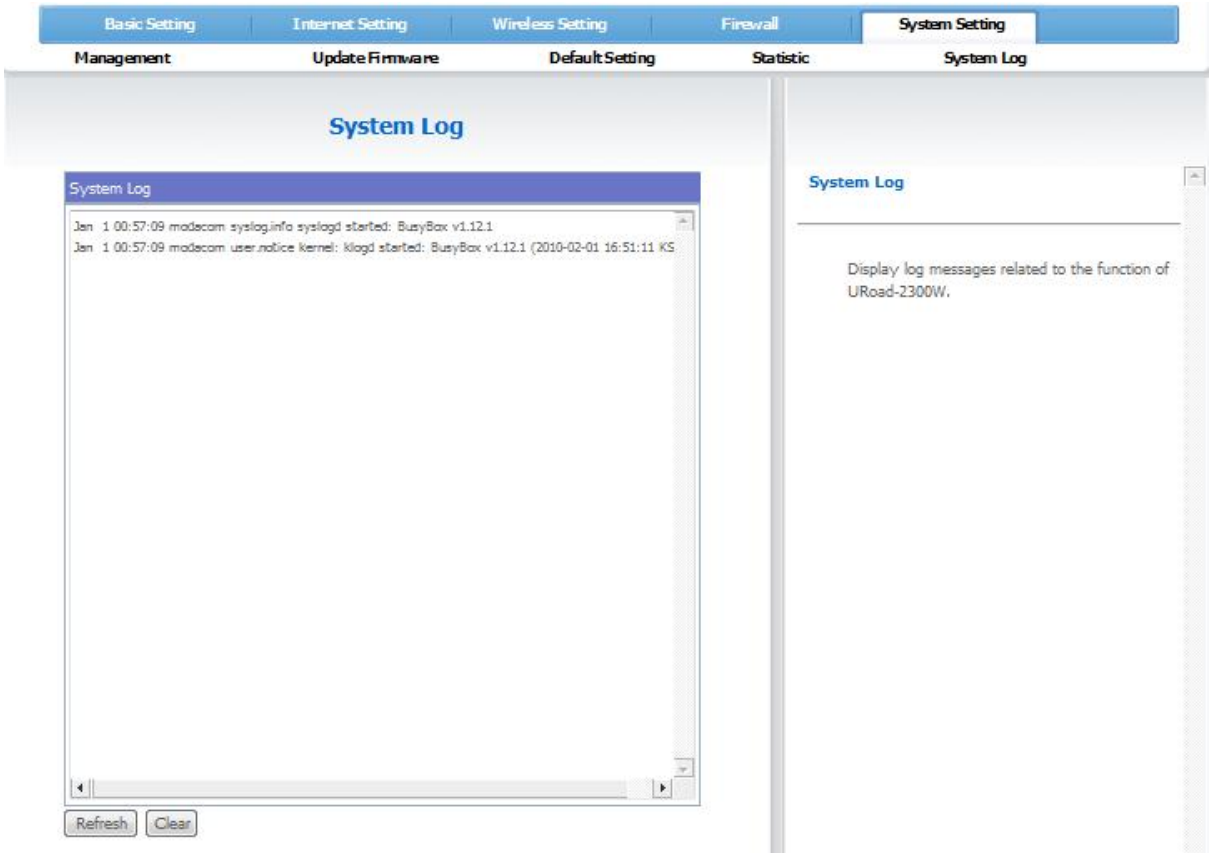
Sub Menu	Description
Memory	Display the total memory of SMT-CW230 and the available memory.
WiMAX / WiFi	Display the information on the Data communication of WiMAX / WiFi.

5.5.5 System Log

System Setting → System Log

Record System Logs in real time.

By using the System Log function, you can identify the content of SMT-CW230 operation in real time.



6. Troubleshooting

6.1. Checkpoints for Internet Disconnection

① Check the power connection of the SMT-CW230.
- Check the connection of the power adapter.

② Check the IP address of the PC.
- Execute the [Start → Program → Sub Program] → [Command Prompt] and check an IP address with the 'ipconfig /all' command.

③ When an IP address is not normal, try setup as follows.
- Execute the [Start → Control Panel → Network & Internet Connection], double-click the [Local Area Connection], click the [Property].
- Click the registry information of the [Internet Protocol (TCP/IP)] out of components.
- Click the [Use the following IP address] and enter the following.

```
IP address ; 192.168.100.101
Subnet mask : 255.255.255.0
Default gateway : 192.168.100.254
```

- Click the [Use the following DNS server address] and enter the following.

```
Basic setup DNS server : 168.126.63.1
Sub DNS server : 168.126.63.2
```

- Click the [Confirm] button of the [Local Area Connection Properties] window.

④ Execute the [Start] -> [Program] ->[Sub Program] ->[Command Prompt] and try the Ping test as follows.
- Execute the [ping 192.168.100.254] command.
- The message of the [Reply from 192.168.100.254: byte=32 time=1ms TTL=64] must appear.
- When the Ping test does not run normally, please contact the customer support center.

⑤ Try login to the web setup screen of the SMT-CW230, and check the Internet connection of the sharer setup screen.

⑥ Turn off the SMT-CW230 power and try connection again.

⑦ When connection fails despite trying all the setups above, please contact our customer support center.

6.2. Checkpoints for web disconnection of the SMT-CW230

① Check the IP address of the PC.
- Execute the [Start → Program → Sub Program] → [Command Prompt] and check an IP address with the 'ipconfig /all' command.

② When an IP address is not 192.168.100.xxx but global IP
- Execute the [Start → Control Panel → Network & Internet Connection], double-click the [Local Area Connection], click the [Property].
- Click the registry information of the [Internet Protocol (TCP/IP)] out of components.
- Click the [Use the following IP address] and enter the following.

IP address ; 192.168.100.101
Subnet mask : 255.255.255.0
Default gateway : 192.168.100.254

➢ Click the [Use the following DNS server address] and enter the following.

Basic setup DNS server : 168.126.63.1
Sub DNS server : 168.126.63.2

➢ Click the [Confirm] button of the [Local Area Connection Properties].

③ Try to login to the web setup screen of the SMT-CW230, and check the Internet connection of the sharer setup screen.

➢ When the Bridge mode out of the SMT-CW230 functions is set to enable, you should set it to disable.

④ If still unsuccessful despite system initialization, please contact our customer support center.

7. Product Specifications

7.1. Hardware Specifications

Specification			Remark
Class	Item		
WiMAX RF	Standard	IEEE802.16e	Support WiMAX Forum Wave2 Profile
	Frequency Range	2.3GHz	
	Channel Bandwidth	5/10 MHz	
	Access/Duplex	OFDMA/TDD	
	RF Paths	2 x RX, 1 x TX	
	Modulation (UL)	QPSK, 16 QAM	
	Demodulation (DL)	QPSK, 16 QAM, 64 QAM	
	Rx. Sensitivity	QPSK 1/2, 512Kbps	-95dBm
	Maximum Tx Power	15dBm	@ Antenna Port
	Antenna	Main / Diversity (External tilt Antenna)	Peak 5.9dBi
		Antenna Connection	Standard SMA
	Max. Throughput	DL : 30Mbps	
		UL : 6Mbps	
	QoS	Scheduling	UGS,BE,nrtPS,rtPS,ertPS
		Data Delivery	UGS,BE,NRT-VR,RT-VR,ERT-VR
WiFi RF	Standard	IEEE802.11b/g(Draft2.0)	
	Frequency	2.412~2.462Ghz	
	Channels	1~11	1~11 : North America
	Channel Bandwidth	802.11b/g : 20MHz	
	RF Paths	1 x RX, 1 x TX	
	Modulation	802.11b/DSSS 802.11g/OFDM	64QAM, 16QAM, QPSK, BPSK 64QAM, 16QAM, QPSK, BPSK CCK, DQPSK, DBPSK
	Rx.Sensitivity	802.11b :11Mbps at -88dBm 802.11g :54Mbps at -73dBm	
	Maximum Tx Power	802.11b ; 12dBm 802.11g ; 9Bm	@ Antenna Port
	Antenna	Internal Dipole Antenna	Peak -2.7dBi
		Antenna Connection	U.FL-R-SMT
	Data Rate	11g: 54Mbps	54/48/36/24/18/12/9/6
		11b: 11Mbps	

	Security	11b: 11/5.5/2/1 Mbps	11/5.5/2/1
		WEP (64/128K), WAP, WAP2	
		MAC filtering	
	Authentication Network	EAP-MD5	
		EAP-TLS, EAP-TTLS	
		MAC Authentication	
		IEEE 802.11g bridge	
		IEEE 802.11b bridge -DHCP Server -Relay/Client, SNTP	
Baseband	Chipset	RT3052	
	Memory	NORFLASH	128Mbit
		SDRAM	512Mbit
	Power Supply	External Adapter	5V/2A (SMPS)
		Power Consumption	3.5W< @15dBm Tx power / QPSK1/2
Environment	Temperature	Storage	-30~+80℃
		Operating	-20~+50℃
	Humidity	Non-condensing	10~90%

7.2. Software Specifications

7.2.1. General Network SW Specifications

Specifications			Comments
Class.	Item	Detailed Items	Remarks
WiMAX Network	EAP Supplicant	EAP-TLS	X.509 Certificate
		EAP-TTLS-CHAP	X.509 Certificate
		EAP-TTLS-MSCHAPV2	X.509 Certificate
	Security/Encryption	PKMv2 privacy with AES-CCM	
Networking	Protocols	TCP/UDP over IPv4	
	Bridge	802.1D transparent bridge	Optional
	Network	NAT(NAPT)	
		Port Forwarding	
		Port Triggering	
	Firewall	IP filtering	
		DMZ control	
		URL filtering	
		Domain blocking	IP based filtering
	Security	DoS attack protection	

		Stateful packet inspection	
	DHCP	DHCP server	Private network (LAN)
		DHCP client	WAN
	DNS	DNS Relay / cache	
	Pass through	PPPoE / PPTP / L2TP	
	NTP	SNTP Client	
Manage-ment	Web-based device configuration	WiMAX Network configuration	
		Local Network configuration	
		Firmware Update	
	Local/Remote device management	Serial interface	
		TR.069	Optional
		Telnet Server	Optional

7.2.2. WLAN SW Specifications

Specifications			Comments
Class.	Item	Detailed Items	Remarks
WiFi Config	WiFi Mode	11b/g	
	Basic Config	SSID	Up to 7
		Frequency Control	
		Operation Mode	Mixed Mode/Green Field
		Bandwidth	20
		Guard Interval	Long/Auto
		Beacon Control	
		Threshold Control	Fragment/RTS
		Tx Power Control	Percentage
		MCS	
	Security	Security Mode	Enable/Disable
		WPS/WPS-2	

8. Product Warranty & Customer Support

Product Warranty

Thank you for buying our product.

The warranty period for this product is counted from the day of your purchase. Therefore, make sure that you have your date of purchase written down to receive further services.

- **Product Name:** SMT-CW230
- **Product Warranty Guide**
  - ① The free A/S warranty period shall be one year from its purchase date.
  - ② Its compensations for repair, exchange and refund shall comply with all consumer damage compensation regulations.
  - ③ If there is neither warranty card nor related contents, its warranty shall follow the Consumer Protection Laws.
- **Warranty Contents**
  - ① We guarantee that this product has passed a stringent quality control inspection.
  - ② We provide free service for any failure that occurs under normal use during the warranty period.
  - ③ However, charged services shall be applied to the following cases even within the warranty period.
    - ◆ Failure and damage resulting from careless handling
    - ◆ Failure resulting from customer' s attempted repair or remodeling
    - ◆ Failure resulting from natural disasters
    - ◆ Possessing neither product warranty nor related contents
  - ④ We provide charged services for failures that occur after the warranty period.

9. Terminology

- **DHCP** (Dynamic Host Configuration Protocol)

  Dynamic Host Configuration Protocol automates network-parameter assignment to network devices from one or more fault-tolerant DHCP servers. Even in small networks, DHCP is useful because it makes adding new machines to the network easier. When a DHCP-configured client (a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the DNS servers, other servers such as time servers, and so forth. On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting, and must be completed before the client can initiate IP-based communication with other hosts.

- **DNS Server**

  The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

- **Gateway**

  In a communications network, a network node equipped for interfacing with another network that uses different protocols.

  A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.

- **IP Address**

  An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. An IP address serves two principal functions in networking: host identification and location addressing. The role of the IP address has also been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

- **LAN: Local Area Network**

  A local area network (LAN) is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school or an airport. The defining characteristics of LANs, in contrast to wide-area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

- **Wireless LAN**

  Wireless Local Area Networks (WLANs) provide a Local Area Network (LAN) using radio instead of wires over a small area such as a home, office, or school. Most wireless LANs are based on the IEEE 802.11 standards. Wi-Fi: Wi-Fi is increasingly used as a synonym for 802.11 WLANs, although it is technically a certification of interoperability between 802.11 devices.

  Fixed Wireless Data: This implements point-to-point links between computers or networks at two locations, often using dedicated microwave or laser beams over line-of-sight paths. It is often used in cities to connect networks in two or more buildings without physically wiring the buildings together

- **NTP Server**

  The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

- **Protocol**

  Protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.

  TCP : The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original

components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as TCP/IP. Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer.

UDP: one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

- SSID (Service Set Identifier)

Service set identifier, or SSID, is a name that identifies a particular 802.11 wireless LAN. A client device receives broadcast messages from all access points within range advertising their SSIDs. The client device can then either manually or automatically, based on the configuration, select the network with which to associate. The SSID can be up to 32 characters long. As the SSID displays to users, it normally consists of human-readable ASCII characters.

- Subnet mask

A subnetwork, or subnet, is a logically visible, distinctly addressed part of a single Internet Protocol network.[1] The process of subnetting is the division of a computer network into groups of computers that have a common, designated IP address routing prefix.

Subnetting breaks a network into smaller realms that may use existing address space more efficiently, and, when physically separated, may prevent excessive rates of Ethernet packet collision in a larger network. The subnets may be arranged logically in a hierarchical architecture, partitioning the organization's network address space (see also Autonomous System) into a tree-like routing structure.

- WPA Algorithm: 3 WLAN algorithm

TKIP : Temporal Key Integrity Protocol

TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement of legacy hardware. This was necessary because the breaking of WEP had left WiFi networks without viable link-layer security, and a solution was required for already deployed hardware.

AES : Advanced Encryption Standard

Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael.

TKIPAES : complementary measures of TKIP and AES