SWC-3100(Simple CPE)
User Guide

SEOWON INTECH

Contents

1. A Simple CPE Overview

1.1 Product Introduction

This product receives external WiMAX signals to construct in-building infrastructure on WiMAX network and is covered by Ethernet network internally
It is also a wired and wireless internet router which allows several systems to use one internet address supplied by high-speed internet service provider.

◎ Functional Features

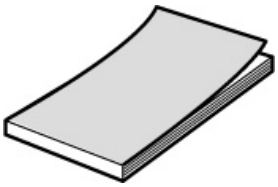
Function	Features
IEEE802.16e WiMAX Support	Wave1 = DL : 10Mbps / UL : 4Mbps Wave2 = DL : 20Mbps / UL : 6Mbps
IEEE802.3u Ethernet Support	10/100Mbps wired LAN connectable
LAN Port	1 Port 10/100Mbps Ethernet Switch built-in
Cable Auto Sense	Straight (Direct) or Cross Cable auto sensing
NAT function	Possible of max. 253 wired and connections and internet router*
Firewall function	Manages basic firewall and IP/Port/based access

1.2 Packaging Contents

<Figure: Main Unit>

<Figure: CD>

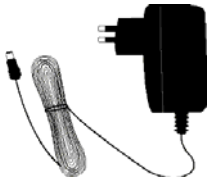
<Figure: Antenna X 2>



<Figure: Quick Guide>

<Figure: UTP Cable>

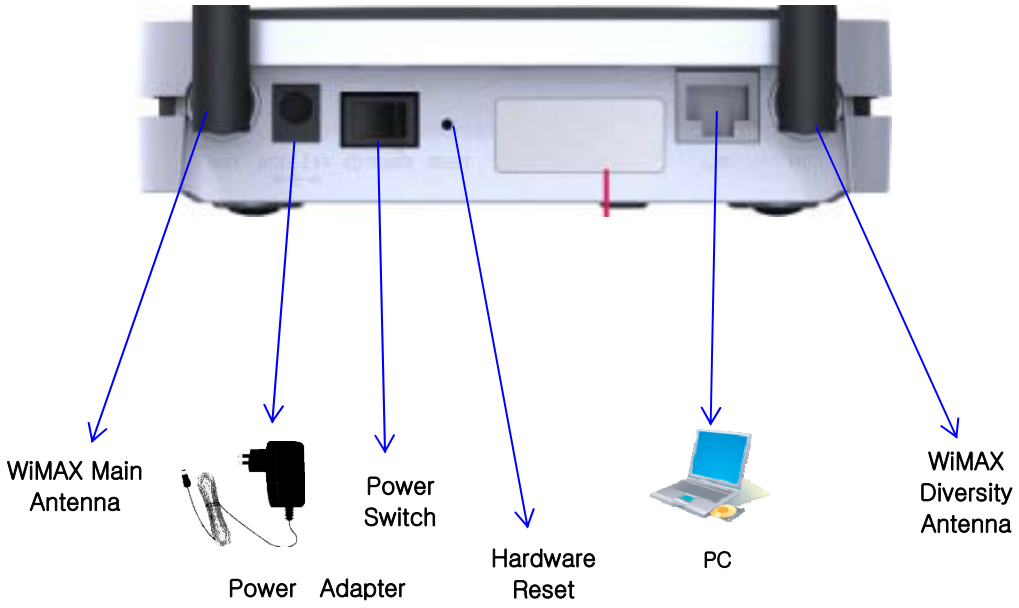
<Figure: USB Cable>



<Figure: Adapter>

1.3 Description of Product Functions(Cont')

Simple CPE Rear Side

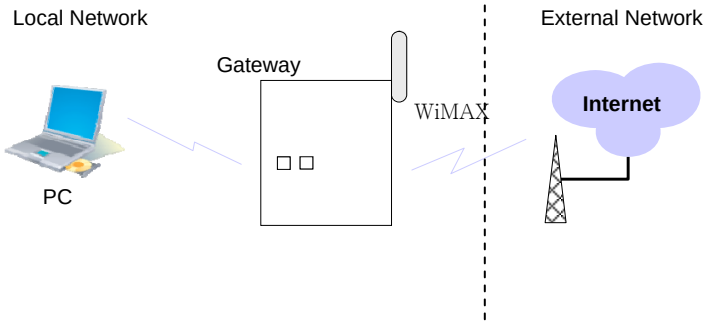


Description

Item	Details
External Antenna	ANT1: WiMAX Diversity ANT2: WiMAX Main Separable external antenna User external type antenna attachable * Antenna Classification - 3: 2.3GHz - 5: 2.5GHz - blank : 3.5GHz
Power S/W	Power On/Off Switch (On/Off by pressing right or left)
DC IN	Power Adapter connection (DC 5V)
LAN	PC or Hub connection
Factory Reset	Restore the Simple CPE Factory Default

[Note] If you lost LOGIN password for router or IP address after change, use the Reset switch to restore its original Factory Default settings.

1.4 Network Configuration



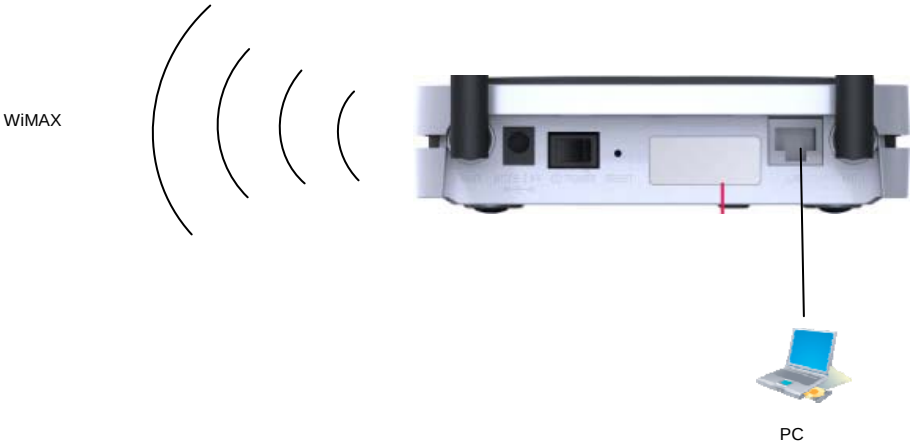
<Simple CPE Connection Example>

To Verify normal operation of router LEDs
You have to check if each LED of the router operates properly after connecting router, modem, and PC with LAN cable as follows:.

LED	Normal Operation	Actions to be taken at failure
PWR	ON when connecting adapter	Check for adapter power failure
LAN	ON when cable is connected normally	Check cable connection and PC power supply
WiMAX RSSI	Representation WiMAX received signal strength indication(RSSI), on when the mode was selected router.	Check the mode selected router

If LED light is not in “normal operation”, check if there is any failure according to actions to be taken.
Install a router after connecting to network.
„ If normal connection between router and PC is checked, you have to set up PC and router.
Router setup is to connect a router to Internet, which is suitable for the Internet line type that is connected to router. It is progressed by referring to Chapter II, depending on Internet type.

1.5 WiMAX Wired LAN Connection (CPE)



2. A Simple WiMAX gateway Implementation

Included in the software development package is the sample WiMAX gateway implementation. The target system has a WiMAX interface at one end and a Ethernet interface at the other end. The embedded connection manager automatically makes a connection to the WiMAX network whenever it detects one. The IP layer is configured to perform NAT so that the host in the inner (private) network can connect to internet via external WiMAX network.
The implementation also includes a simple HTTPD daemon so that some of the device configuration can be changed using the web browser from the host in the private network.

2.1. WiMAX Connection Manager

The WiMAX connection manager is responsible for the following:

- Monitor the WiMAX device state
- Initiate the connection
- EAP supplicant (in preparation, only limited support for EAP-AKA with USIM)
- Configure the WiMAX device.
- IP configuration of WiMAX device.

The developer can change various parameters that affect the behavior of WiMAX device and the connection manager. This is done by editing /etc/wcm.conf file. Controlling WiMAX connection manager by this file is explained with example cases in section 5.3.
The connection manager reads this file on startup and performs the necessary actions. In addition, one can list up the GCT WiMAX text DM commands in [DM command] section so that the connection manager executes these commands in batch mode.

2.2. Connection Manager User Interface

The WiMAX connection manager provides command line user interface, whereby the user can execute WiMAX commands on the terminal. By default, the WiMAX connection manager runs in the “monitoring mode”, where it

```
[WiBro device]
mac_address=00:0a:3b:f0:10:50 /* Sets the WiMAX device MAC address */
[WiBro connection]
/* The connection manager automatically tries to connect to the network whenever it discovers the available network */
autoconnection_enable=YES
/* If dhcp_enable is set to YES, the connection manager runs DHCP client to acquire IP configurations from the network. Otherwise, the IP informations should be statically configured */
dhcp_enable=YES
[WiBro authentication]
authentication_pkm_enable=YES
authentication_alpha_delimiter_enable=YES
#authentication_pkm_type=EAP-AKA
#authentication_pkm_type=EAP-MD5
#authentication_pkm_type=EAP-TLS
#authentication_pkm_type=EAP-TTLS-CHAP
authentication_pkm_type=EAP-TTLS-MSCHAPV2
```

```
[DM command]
d ver
wb_ru
```

keeps showing log messages from the WiMAX MAC. The user can switch it to “interactive mode” by typing in ‘q’ in the console. During interactive mode, all the MAC messages are temporarily suppressed and the connection manager shows the prompt “DM>” for the user to enter commands. The user can also switch back to “monitoring mode” by simply entering “Enter” key.

2.2.1. System Commands

2.2.1.1. param

This command shows the parameter block content.

2.2.1.2. version

This command shows the version of connection manager.

2.2.1.3. shell

This command is used to invoke a system shell (/bin/sh) inside the connection manager.

2.2.1.4. reboot

This command is used to reboot the system.

2.2.1.5. help

This command displays (not all) commands and their usage.

2.2.2. WiMAX Connection Manager Commands

2.2.2.1. wb_gs

This command is used to read the current state the device is in. The device can be in one of the following states:

- NULL: This is the initial device state when its modem and RF is turned off.
- OUT OF ZONE: The device cannot locate any available WiMAX network
- STANDBY: The device has achieved PHY and MAC synchronization and keeps listening to DCD/UDC, DL-MAP, and UL-MAP from the base station.
- NETENTRY: The device is in network entry procedure. It has the following sub-states:
- NETENTRY_RANGING: The device is in initial ranging phase.
- NETENTRY_SBC: The device is in SBC phase.
- NETENTRY_PKM: The device is in PKM phase.
- NETENTRY_REG: The device is in Registration phase.
- NETENTRY_DSX: The device is in ISF creation phase.
- ACTIVE: The device has successfully made connection to the network.

2.2.2.2. wb_ru

This command is used to turn on WiMAX modem and RF. The WiMAX device then starts scanning the WiMAX network on pre-defined channel. If the device finds available WiMAX network, the device state is changed to STANDBY; otherwise to OUT OF ZONE.

2.2.2.3. wb_rd

This command is used to turn off WiMAX modem and RF. Before doing so, it disconnect from the network if it is already connected.

2.2.2.4. wb_ne

This command is used to initiate network entry procedure when the device is in STANDBY state. This command is discarded if the device is in other states. On successful connection, the device state is changed to ACTIVE. Otherwise, it stays in STANDBY state.

2.2.2.5. wb_nd

This command is used to disconnect from the network. The device state is changed from ACTIVE to STANDBY.

2.2.2.6. wb_bs

This command is for setting the bandwidth field in parameter block. After setting the bandwidth, you should reboot. You can choose 0 for 8.75Mhz, 3 for 5Mhz, 6 for 10Mhz as an argument.

2.2.3. WiMAX Text DM Commands

GCT WiMAX MAC provides an easy way to fine-tune a numerous parameters that affect the behavior of WiMAX device.
These commands are used to control the low-level MAC behavior. For detailed information, please refer to "GCT WiMAX Text DM Reference Manual".

2.2.4. Command Batch Processing

User can list commands listed above in [DM command] section of WiMAX configuration file (/etc/wibro.conf). The WiMAX connection manager executes these commands automatically, alleviating the need to the same thing
repeatedly. For example, we have listed two commands; "d ver" is the WiMAX Text DM commands that shows the MAC-PHY version of the firmware and "wb_ru" turns on the WiMAX modem and RF.
The developers can find the MAC and PHY parameters that best fit the targeting WiMAX network by trying WiMAX Text DM commands with different parameters. Once they are found, those settings can be put into the configuration file.

2.3. Control of connection to WiMax network

2.3.1. Connection with dynamic IP allocation

WiMax connection manager automatically tries to connect to the WiMax network, if some variables defined in the configuration file for WiMax connection manger (/etc/wcm.conf) are YES, and WiMax modem and RF are turned on. As seen in the example code of /etc/wcm.conf in section 5.1, **autoconnection_enable** makes it try to connect to the network whenever it discovers the available network, **dhcp_enable** executes DHCP client to acquire IP configurations from the network service provider, and **wb_ru** in DM_command section turns on WiMax modem and RF.

Two configuration variables and one command enable the WiMax connection manager to try to connect to the WiMax network

> cat /etc/wcm.conf

…
[Wibro connection]
autoconnection_enable=YES
dhcp_enable=YES
…
[DM command]
wb_ru
…

2.3.2. Connection with static IP allocation

If some base station may not support dynamic IP address allocation, you should set your IP address manually. You can, then, turn off dhcp_enable with NO, to make WiMax connection manager not try to connect. WiMax connection manager set the IP address of WiMax device(wb0) with the value of IP variable in /etc/WM.conf, if dhcp_enable in /etc/wcm.conf is defined as NO.

> **cat /etc/WM.conf**
…
IP=192.168.2.1
NETMASK=255.255.255.0
DEFAULTGW=192.168.2.254
DNS1=192.168.20.2
DNS2=192.168.20.3
DOMAIN=gctsemi.com
…

In this example, the IP address of WiMax device will be 192.168.2.1 with 255.255.255.0 of netmask. WiMax connection manager also tries to set default gateway and name server with the predefined values in /etc/WM.conf, so you can modify the file for your own purpose. Some base stations need to know the MAC address of your mobile station before connection, and they maintain ARP list with the IP and MAC address of mobile, so your IP address should be allocated in advance by base stations or service providers.

2.3.3. Enabling authentication mode

To enable authentication process while in WiMAX connecting, the variable, "**Authentication_pkm_enable**", should be "YES". Then, WiMAX connection manager tries authentication processing. You can choose the kind of authentication by setting the variable, "**Authentication_pkm_type**", which can be "EAP-AKA", "EAP-TLS", "EAP-TTLS-CHAP", and "EAP-TTLS-MSCHAPV2", etc. After changing the variables, you should reboot the CPE.
While EAP-AKA type uses external USIM card which should be distributed by a wireless service provider, other authentication methods uses id/password's and certificates. Those can be set like as set-param sections in wcm.conf. You can see sections whose name is [EAPTLS setparam], [EAPTTLSCHAP setparam], and [EAPTTLSMSCHAPV2 setparam]. You should write down correct strings which you get from operators in your authentication section.
>> cat /etc/wcm.conf
…
[WiBro authentication]
authentication_pkm_enable=YES
authentication_alpha_delimiter_enable=YES
#authentication_pkm_type=EAP-AKA
#authentication_pkm_type=EAP-MD5

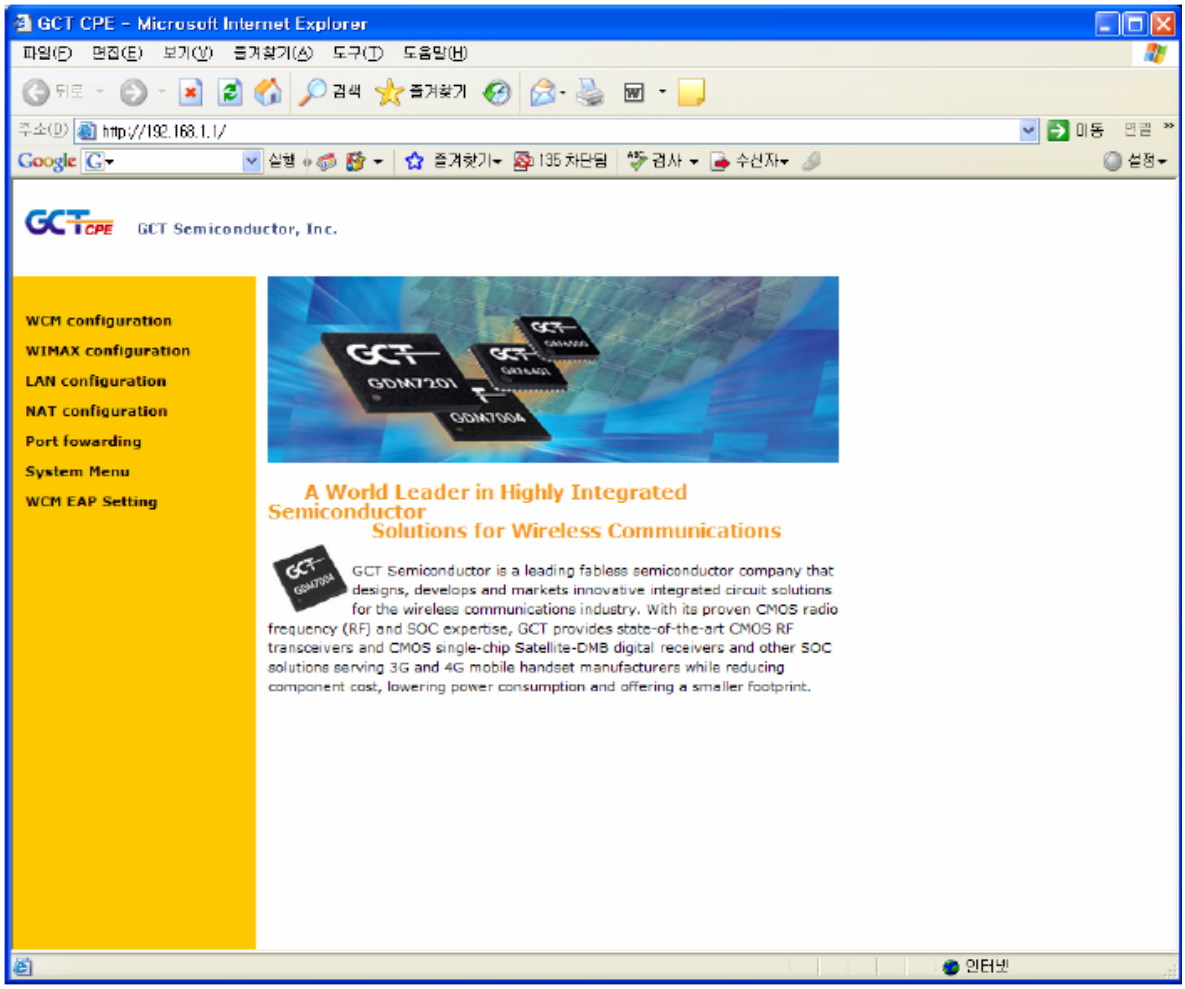
```
#authentication_pkm_type=EAP-TLS
#authentication_pkm_type=EAP-TTLS-CHAP
authentication_pkm_type=EAP-TTLS-MSCHAPV2

[EAPTLS setparam]
tls_cacert=/etc/auth/cacert.pem
tls_pricert=/etc/auth/client.pem
tls_pripasswd=whatever
tls_userid=socswtls
tls_userpasswd=whatever
[EAPTTLSCHAP setparam]
ttls-chap_cacert=/etc/auth/cacert.pem
ttls-chap_pricert=/etc/auth/client.pem
ttls-chap_pripasswd=whatever
ttls-chap_anonyid=ttls
ttls-chap_userid=socswchap
ttls-chap_passwd=whatever
[EAPTTLSMSCHAPV2 setparam]
ttls-mschapv2_cacert=/etc/auth/cacert.pem
ttls-mschapv2_pricert=/etc/auth/client.pem
ttls-mschapv2_pripasswd=whatever
ttls-mschapv2_anonyid=ttls
ttls-mschapv2_userid=socswmschap
ttls-mschapv2_passwd=whatever
…
[DM command]
wb_ru
cfg sbc param_set 0
…
```

The setparam sections have some variables, and you should fill them with the data from your service provider. **Cacert** is root certificate, and you can change file name but you should not modify the path name. **Pricert** is client client certificate with(or without) a private key. The restrictions for file and path name are same to the **cacert**. **Pripasswd** is private key. **Anonyid** is anonymous id, or outer NAI(Network Access Identifier). **Userid** is user id, or inner NAI. **Passwd** is the password for userid.
"**Authentication_alpha_delimiter_enable**" makes the character, "@", in **userid** or **anonyid** as a delimiter or as just a character. If it is YES, "@" is a delimiter, if not, "@" is a character. If your set **userid** with "aaa@bbb.ccc.com" and the variable is YES, then your **userid** is just "aaa". If it is NO, then your **userid** is "aaa@bbb.ccc.com" .
For the time being, because our EAP method support the base64 encoding, you should change the encoding format to base64 if your certificate is encoded by DER method. You can use certificate administrator's tools in MS Windows for this purpose.
You can update certificates files with FTP. That is, you change directory to /etc/auth, get CA certificate and Private certificate by binary mode FTP, and change the name of the files or change filenames in wcm.conf. Another tools for updating certificate files is web access, and it is explained in section 5.4.3.
If you want to connect to WiMAX service provider with authentication mode, then you should run a command, "cfg sbc param_set 0", after RF_UP and before NET_ENTRY. This can be done by inserting the command in "DM command" section in "wcm.conf", when booting time

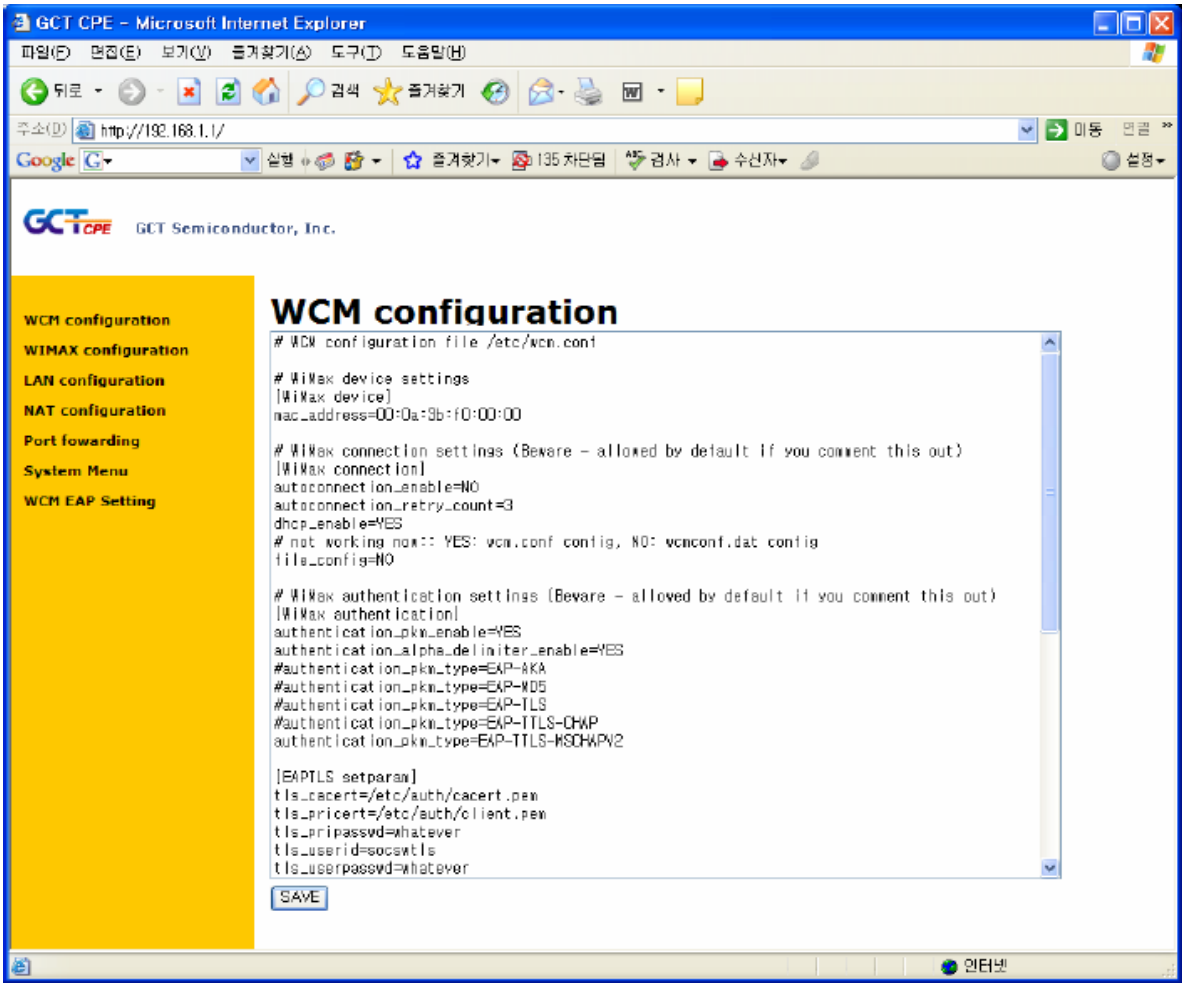
2.4. Configuring CPE with web browser

The default settings of the CPE may need change so as to meet your individual needs. You can use crossover Ethernet cable directly between PC and CPE Ethernet port. Then, you can configure the CPE with your web browser. To access CPE, enter http://192.168.1.1 in your web browser. After that, you can see a screen like this

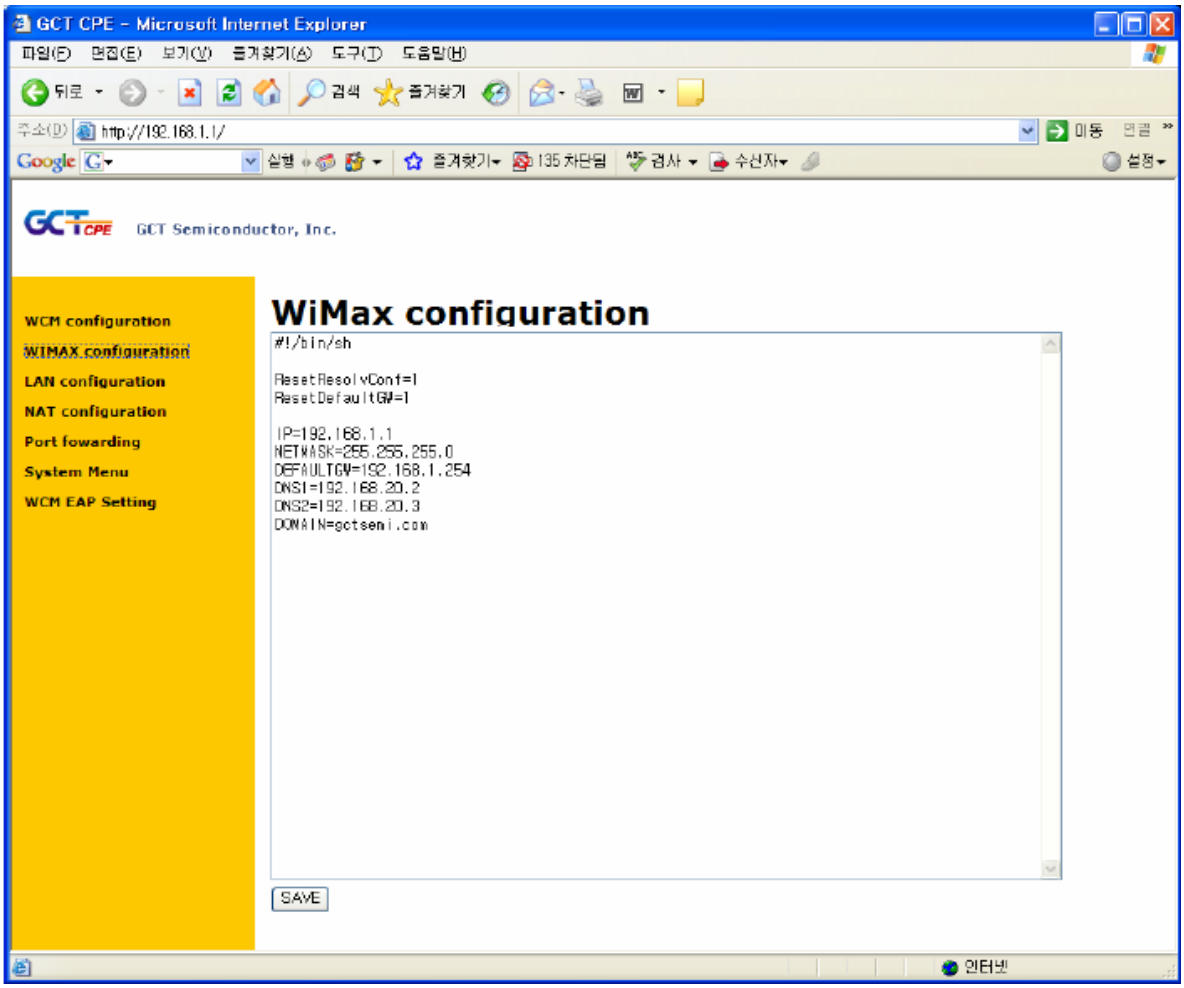


2.4.1. Network configuration

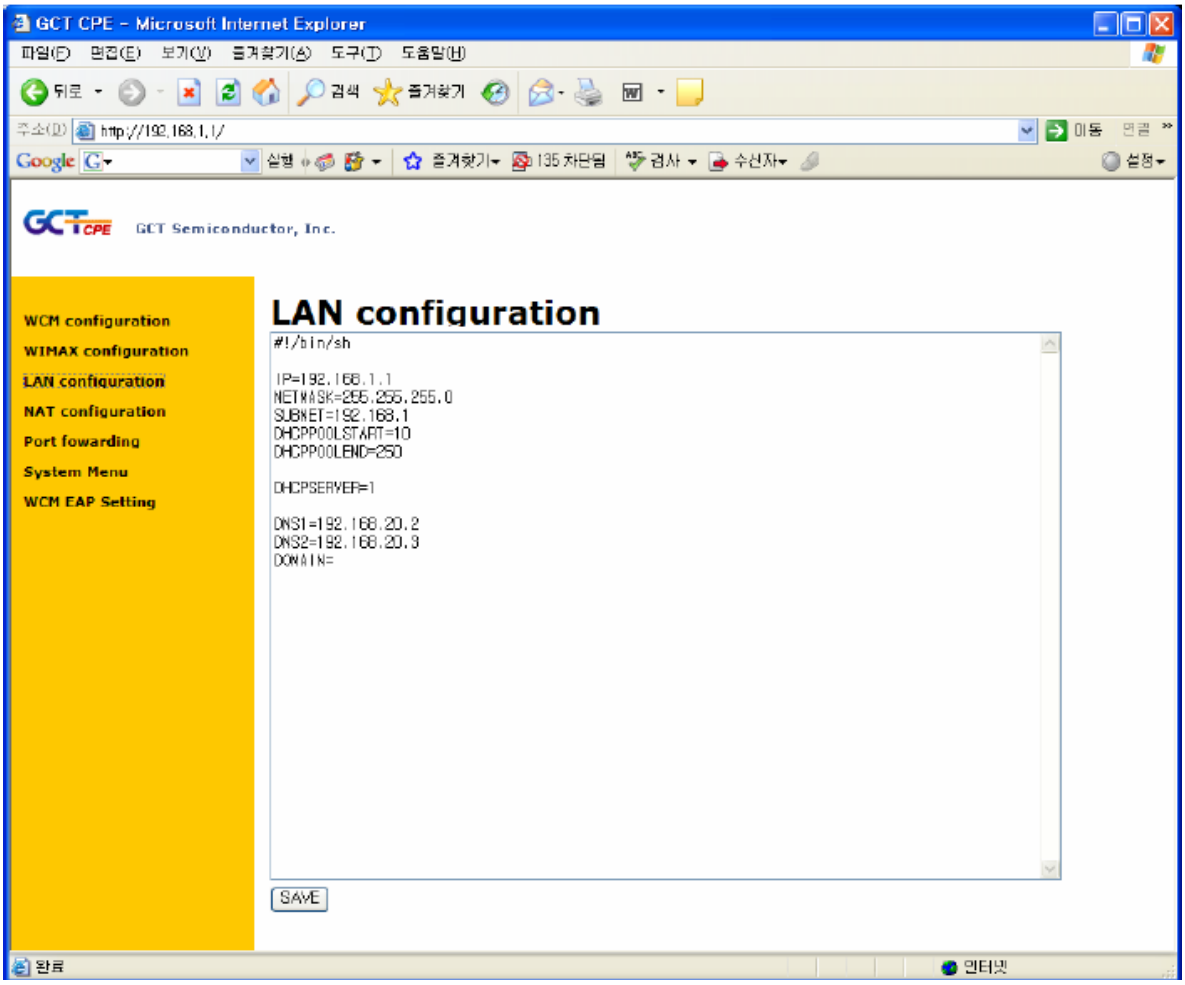
If you select “WCM configuration” in the left window, then you can change WCM configuration. The content will show up in the right window. The detailed explanation for the content is done in section 5.1 and 5.2.



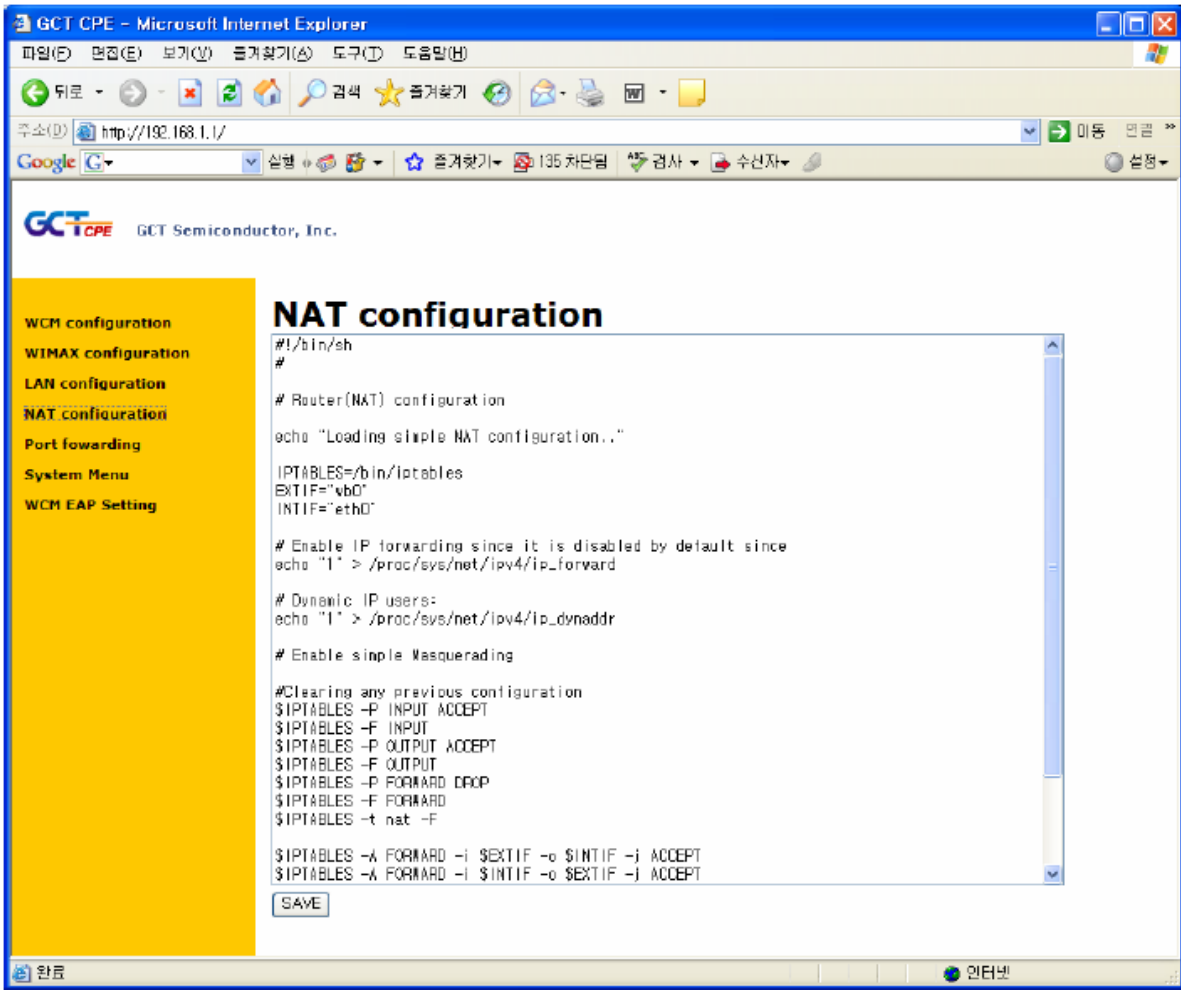
Choosing WIMAX configuration will show the following screen. This window is used for static network setup for WiMax device as shown in section 5.3.2.



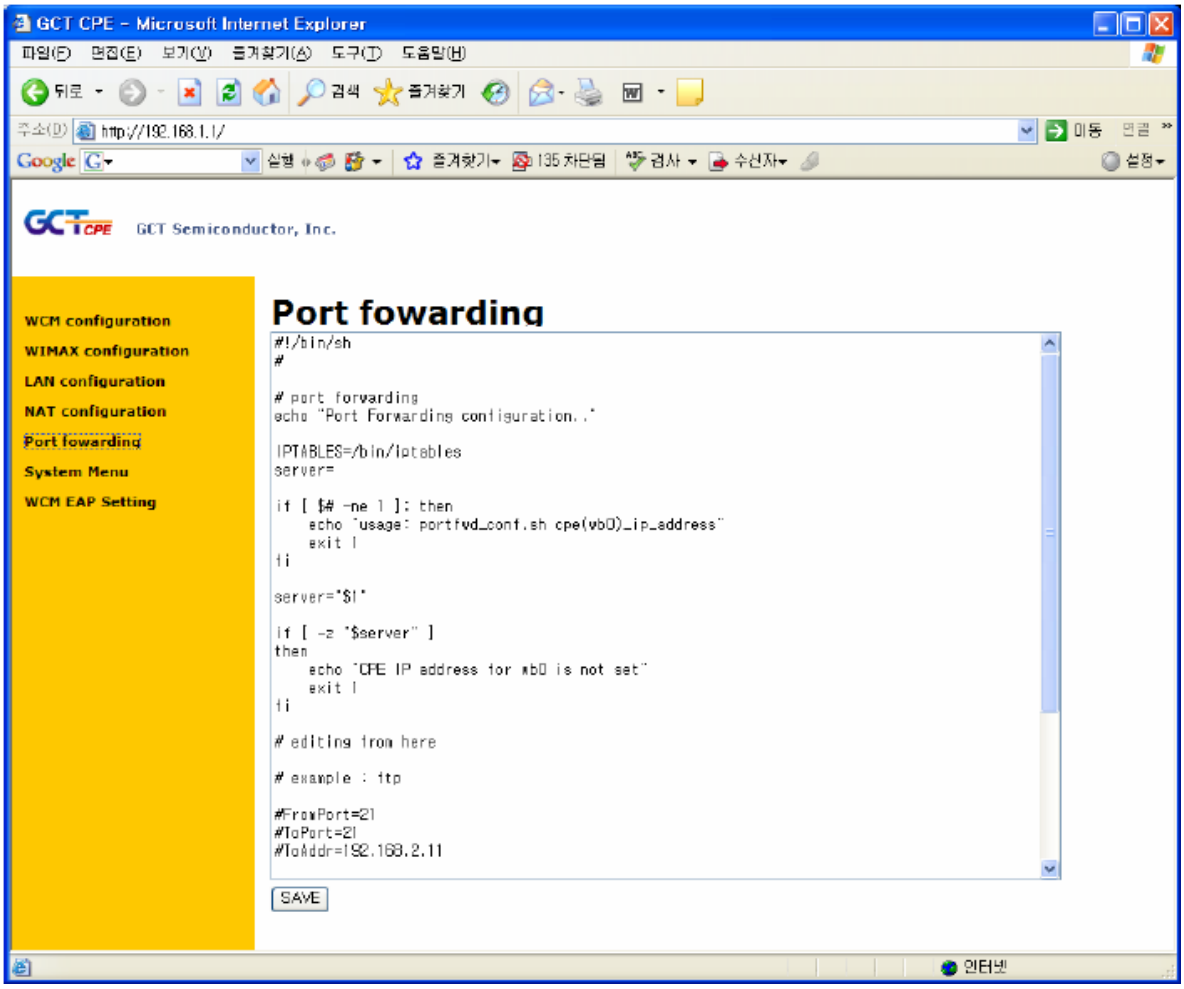
For local area network in CPE, Ethernet dev, “eth0”, should be set like the following window. In this example, IP address of eth0 is 192.168.1.1 and its netmask is 255.255.255.0. IP address pool for DHCP server on eth0, “dhcpd”, starts with 10, ends to 250, and its subnet is 192.168.1. The variable, “DHCPSERVER” will control whether DHCP server will run or not.



NAT configuration in uClinux system can be changed by this window, but no change in this window is recommended.

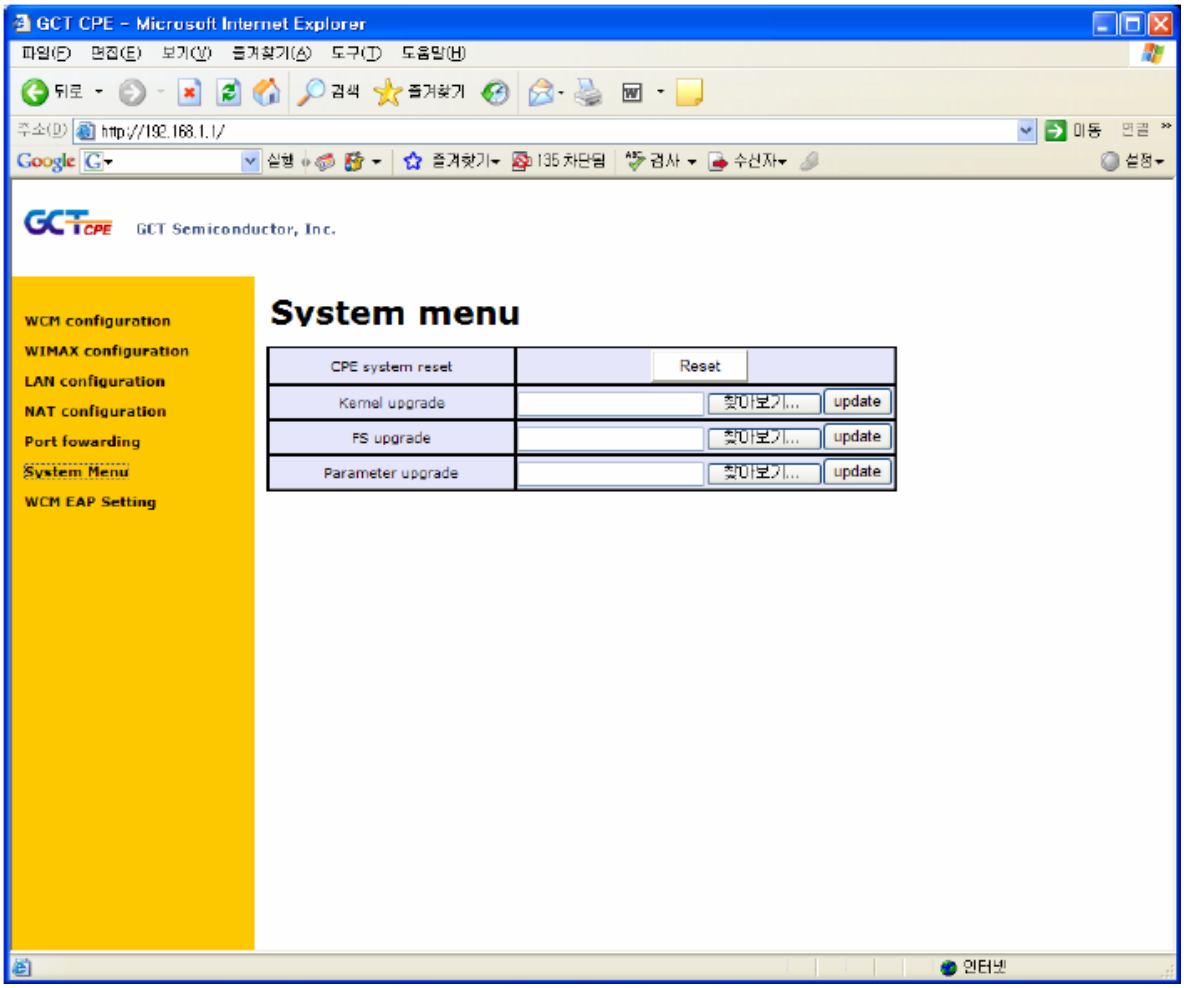


Some users want to set up a server in local area network of CPE, that is, enabling outer world to connect the internal server, for this purpose they should set up port-forwarding method in uClinux. In this example, user can open some port with “iptables” command.


GCT CPE - Microsoft Internet Explorer
http://192.168.1.1/
GCT Semiconductor, Inc.
WCM configuration
WIMAX configuration
LAN configuration
NAT configuration
Port fowarding
System Menu
WCM EAP Setting
Port fowarding
#!/bin/sh
#
port forwarding
echo "Port Forwarding configuration.."
IPTABLES=/bin/iptables
server=
if [$# -ne 1]; then
echo "usage: portfwd_conf.sh cpe(vb0)_ip_address"
exit 1
fi
server="$1"
if [-z "$server"]
then
echo "CPE IP address for vb0 is not set"
exit 1
fi
editing from here
example : ftp
#FromPort=21
#ToPort=21
#ToAddr=192.168.2.11
SAVE
인터넷

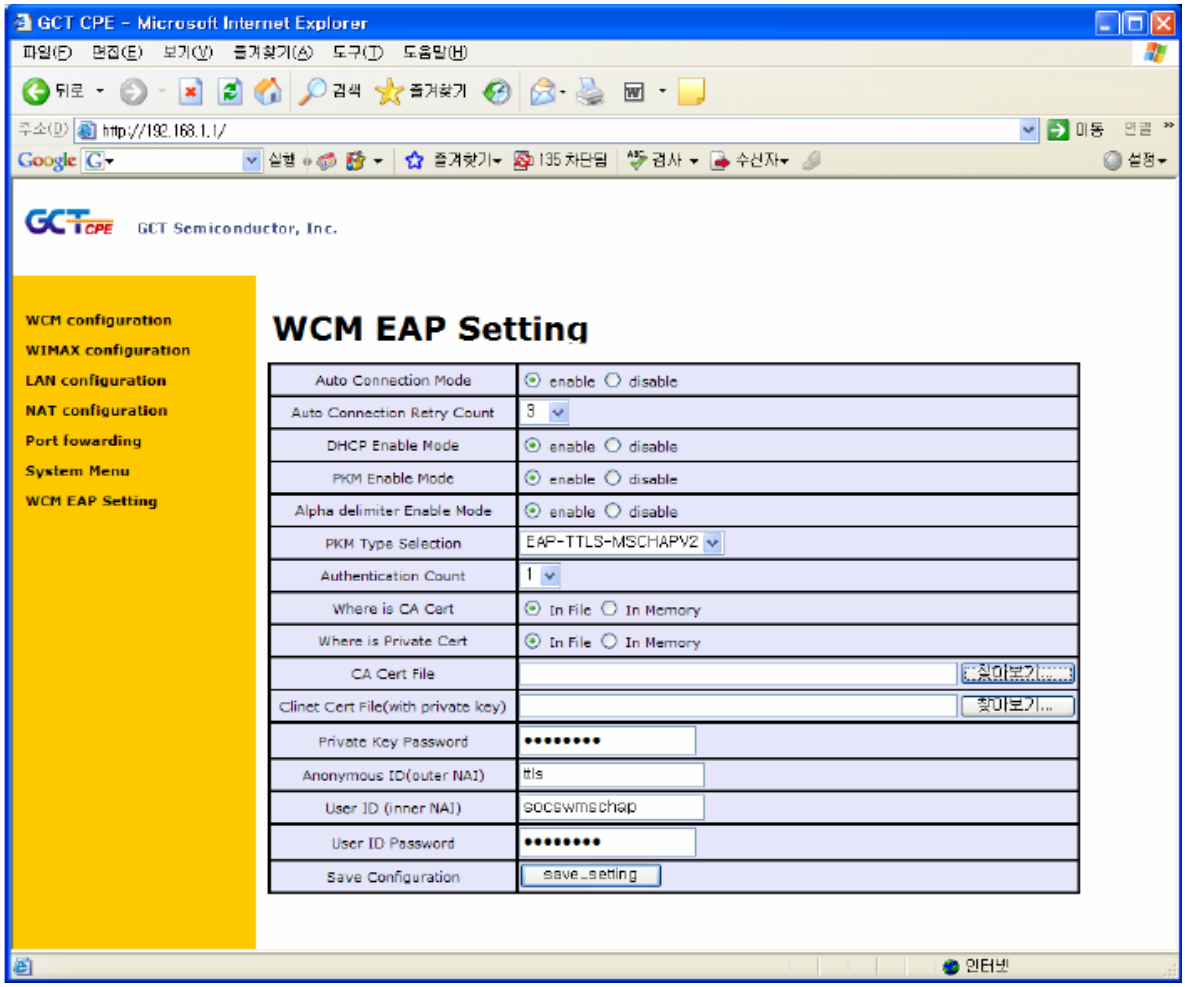
2.4.2. Firmware upgrade

You can update the kernel image, file system image, and parameter block image with the web browser. This also can be updated in RedBoot mode, but it cannot be used in commercial product. So, “System Menu” in left window help you to update the images.
At first, you should find a image to update with “Browse…” or “찾아보기…” button, then, you can upload the image to the CPE, and write it to flash file system with “update” button. This step could be repeated until three images are uploaded and programmed to flash system. After that, you can press “Reset” button to reboot the CPE.

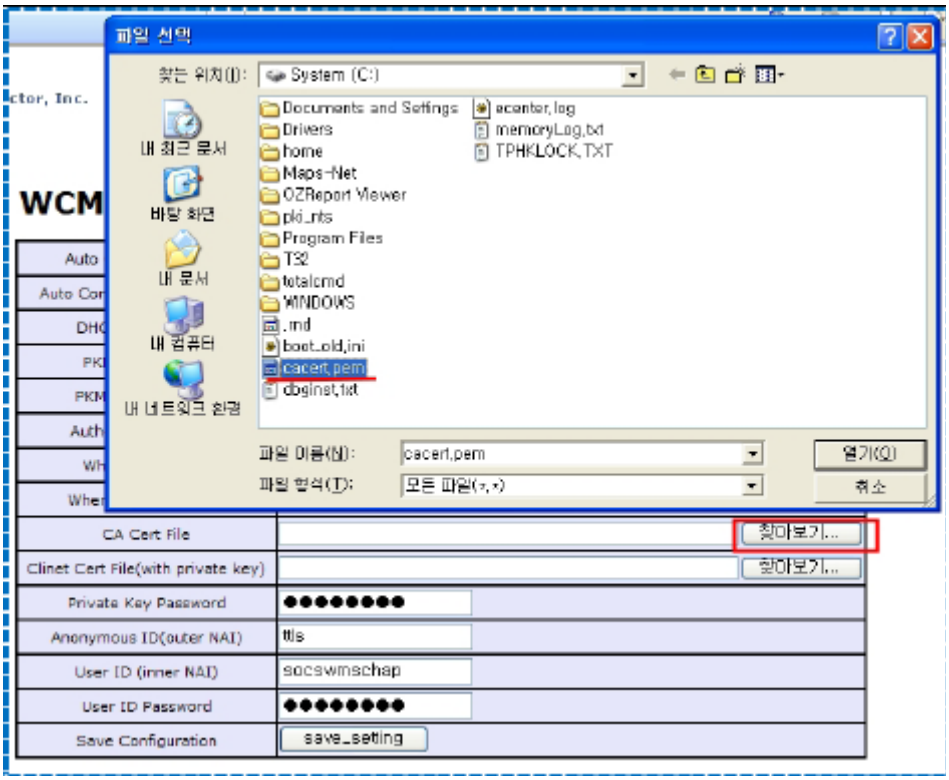


2.4.3. EAP configuration

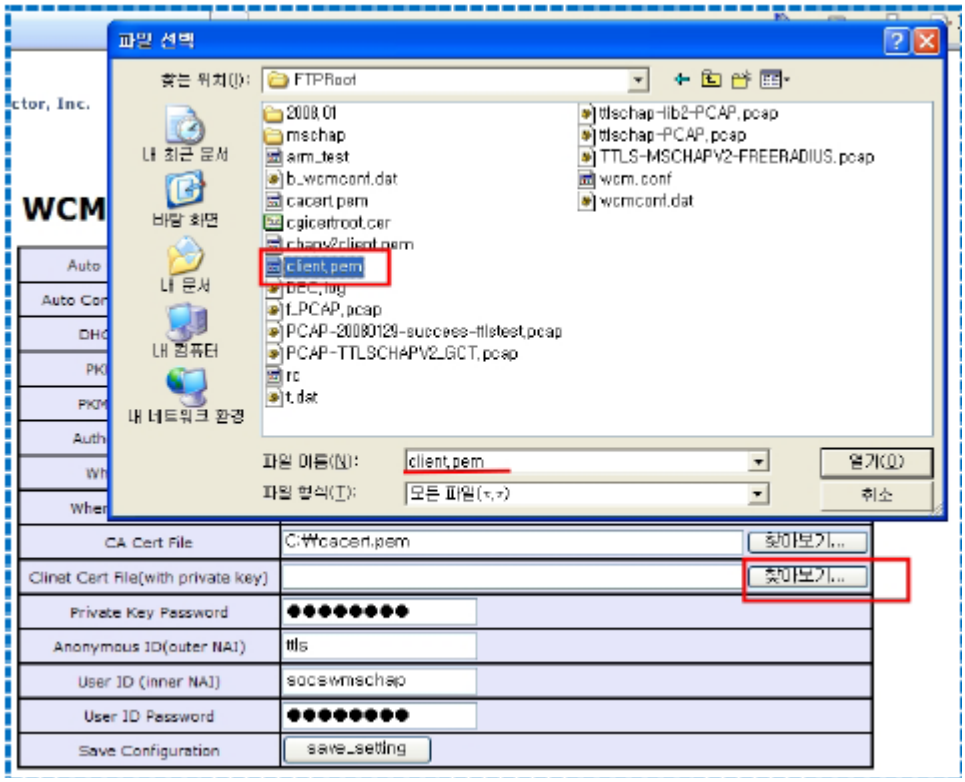
You can update certificate files with web access, so you click the button, “ WCM EAP Setting”, then, you can see the following



With this menu, you can update the certificate files. If you click “Browse…” or “찾아보기…” button in “CA Cert File” field, then you can see the following popup menu. You should choose an appropriate CA certificate files which the service provider gives to you.



In “Client Cert File(with private key) “field, the operation is same as in “CA Cert File” field.



Then, you can see the following screen, and you can save the certificate files by clicking “save_setting” button.

Other fields in the “WCM EAP Setting” menu are not effective with distributed WCM(WiMAX Connection Manager”. If you are also provided with WCM source code, you should turn on the code, “#define WCM_CONF_ENV_FROM_BINARY” in “config.h”, and recompile the source codes of WCM. Then, your executable, “wcm”, does not use /etc/wcm.conf, but uses /etc/wcmconf.dat. Therefore, all fields in “WCM EAP Setting” menu should be written with correct values as in /etc/wcm.conf., and each field has same meaning as in /etc/wcm.conf.

Regulatory Notices

Caution: The **WiMAX device** has been tested for compliance with FCC RF exposure limits. The **WiMAX device** should not be used with external antennas that are not approved for use with this device. Use of this device in any other configuration may exceed the FCC RF exposure compliance limits.

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.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. There is no guarantee that interference will not occur in a particular installation

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Caution: Any changes or modifications not expressly approved by Sprint could void the user’s authority to use the equipment.