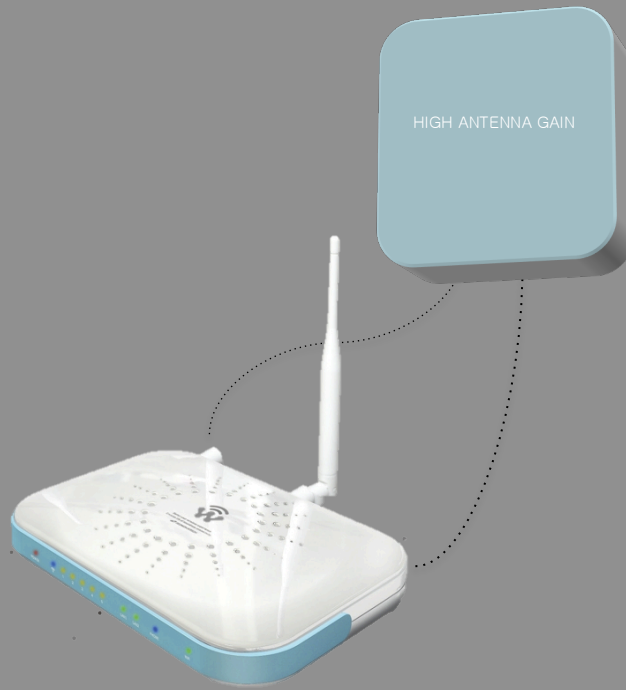


User manual

SWC-9200 VoIP CPE



Global Telecom Corp

Contents

Introduction to the Product			
1. Functional Features	04	4.8 Feature	30
2. Front side of CPE	04	4.9 Dialing	33
3. Back of CPE	05	4.10 Speed Dial	34
		4.11 FAX	35
		4.12 RTP	36
		4.13 Phone	37
		4.14 Voice	39
		4.15 Profile	41
Configuration		5. Application Setup	
1. Network Configuration	06	5.1 Firewall	42
2. Package Contents	07	5.2 DMZ & Port Forwarding	43
3. PC Configuration (Windows XP)	08	5.3 VPN pass through	45
4. How to check your IP address	09	5.4 UPnP	46
		5.5 QoS	47
		5.6 DDNS	49
		5.7 MTU	50
		5.8 NTP	51
		5.9 Remote Control	52
		6. Admin Setup	
		6.1 Version	53
		6.2 Password	53
		6.3 CPE Upgrade	54
		6.4 Reboot/Default Setting	55
		6.5 Diagnostic	56
		Troubleshooting	57
		Operating Information	60
		Safety Information	60
		Legal Information	
			61
		Warranty Information	62

Introduction to the Product

Thank you for choosing SWC-9200 , Indoor VoIP CPE. SWC-9200 allows you to share a superior data communication via an Ethernet and WiFi network. It offers easy installation, reliable network connection, advanced security & authentication features, and more.

Please read this User Manual carefully to learn about the SWC-9200. It will help you to meet your diverse communication needs, at home and at the office.

1. Functional Features

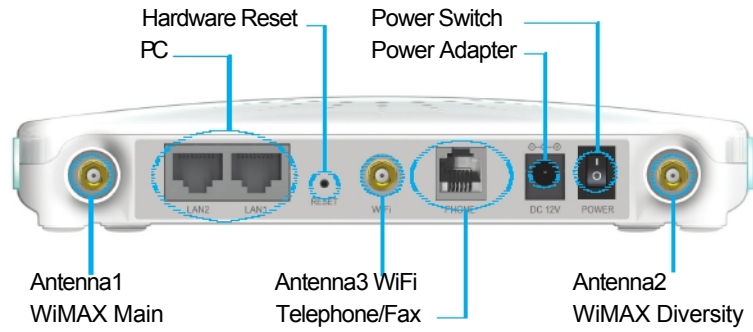
Function	Features
IEEE802.16e WiMAX Support	Wave2 = DL : 40Mbps / UL : 8Mbps 802.11b CCK MODE / 802.11n OFDM MODE
IEEE802.11 b/g/n WiFi Support	802.11g OFDM MODE
IEEE802.3u Ethernet Support	10/100Mbps wired LAN connectable
VoIP Support	1 x RJ-11 for Analog Telephone Service
LAN Port	2 x Ports 10/100Mbps Ethernet Switch built-in
NAT function	Supports up to 253 wired and wireless connections and internet routers
Firewall function	Manages basic firewall and IP/Port-based access

2. Front side of CPE



LED Indicator	Function
WiFi	802.11b/g/n
PHONE	ON when connected to Telephone
LAN1/LAN2	ON when connected to PC, Flashing during communication
WIMAX	IEEE 802.16e-2005 Wave 2
PWR	Power Supply status
RSSI	WiMAX RSSI (Received Signal Strength Indication) Status

3. Back of CPE

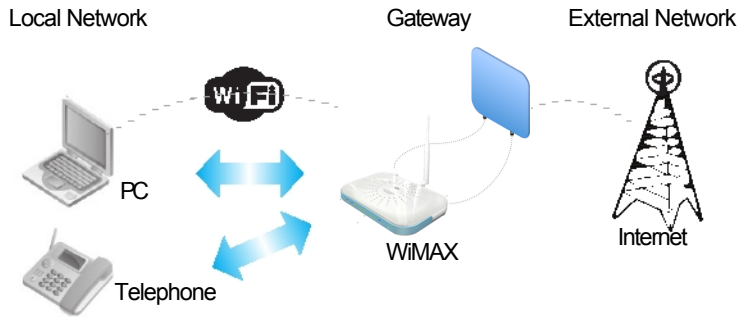


Item	Details
External Antenna	Antenna1 : WiMAX Main Antenna2 : WiMAX Diversity Antenna3 : WiFi Detachable external antenna User external antenna (attachable) * Antenna Classification - 2.3G : M23 - 2.5G : M25 - 3.5G : M35 - WiFi : WiFi
LAN1/LAN2	PC or Hub connection
PHONE	Telephone connection
DC 12V	Power Adapter connection(DC 12V ___20A)
POWER	Power On/Off Switch (Switch On/Off by pressing up or down)
RESET	Restore CPE Factory Default Settings

NOTE : If you forget the LOGIN password for the CPE or IP address after marking changes, use the Reset switch to restore the CPE to its original Factory Default settings.

Configuration

1. Network Configuration



To verify that the CPE is operating normally, check the following LEDs after connecting the CPE, modem and PC with a LAN cable, as follows:

LED	Normal Operation	Action to take if not illuminated
PWR	When power switch On	Check for adapter power failure
LAN1 / LAN2	ON when cable is connected normally	Check cable connection and PC power supply
PHONE	On when Phone cable is connected normally	Check cable connection and Telephone
WIMAX RSSI	The number of the lighting LEDs increases depending on WIMAX received signal strength(1~5)	Check WIMAX connection status

If one or more of the LED lights is not in "normal operation," refer to the actions specified in the table. If there is a normal connection between CPE and PC, you have to set up the PC and CPE.

The purpose of PC setup is to control network configuration for Windows 98, Windows 2000, Windows XP, Vista, Windows 7 or Mac OS X to use the Internet while the PC is connected to a CPE. The purpose of CPE setup is to connect the CPE to the Internet.

2. Package Contents

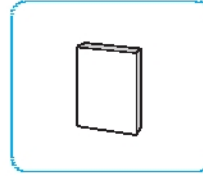
Main Unit



WIFI Antenna X 1



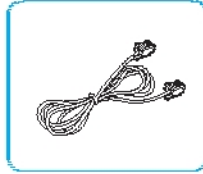
User Manual



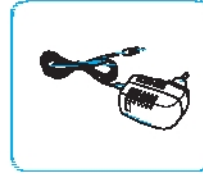
LAN Cable



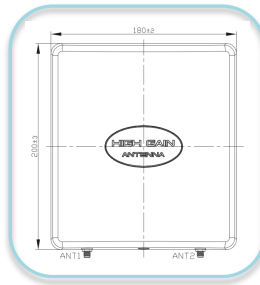
Tel. Line



Adapter



Outdoor Antenna



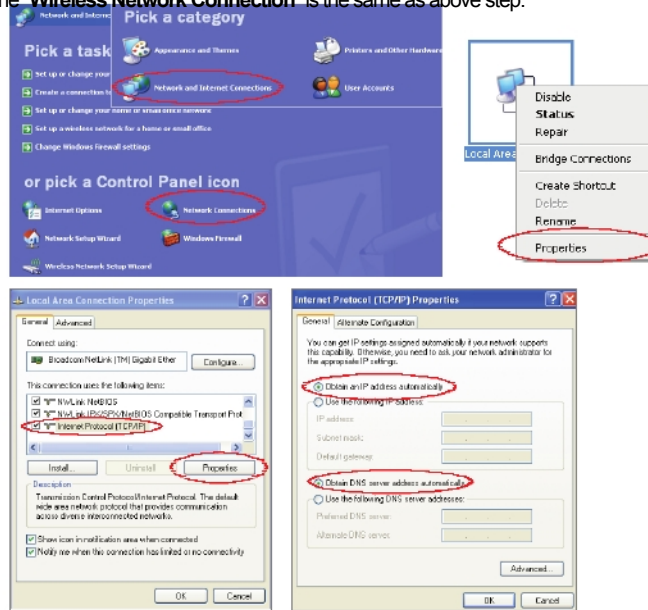
3. PC Configuration (Windows XP)

Most computers already have TCP/IP configuration enabled. For your computer to support CPE, please verify that the IP address and DNS settings are automatically generated in the Local Area connection of your Internet Protocol (TCP/IP) properties.

• In the Windows environment :

- Click "**Start**" >> Settings >> Select "**Control Panel**" >> Click "**Network and Internet Connection**" >> Click "**Network Connection**" >> Right-click "**Local Area Connection**" and Select "**Properties**" >> Select "**Internet Protocol (TCP/IP)**" and click "**Properties**" >> Select "**obtain an IP address automatically**" >> Click the "**OK**" button.

- The "**Wireless Network Connection**" is the same as above step.



4. How to check your IP address

- Open the Command Prompt window by clicking the "Start" button and selecting "Run".
Enter "cmd", and click the "OK" button.



- When the Command Prompt window opens, enter the "ipconfig" command to verify the IP address, Subnet mask, and Gateway, which are automatically assigned to your PC.

NOTE : All PCs connected to CPE will receive their own assigned IP address.



NOTE : If an IP address is not assigned, check the following. Then restart the PC and check whether an IP address is assigned.

- LAN cable connection between PC and CPE
- Check TCP/IP setup details

Logging in to the built-in Web Interface

The Web Interface allows you to manage the CPE and to view.

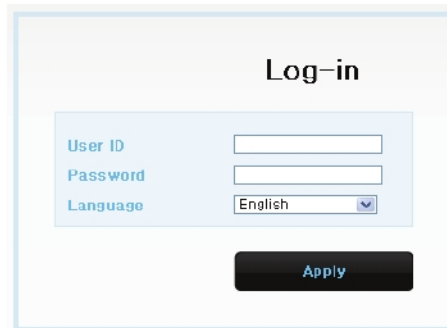
In the Address Bar :

- Type **http://192.168.1.1** and press ENTER to access the login screen.



- When the login screen appears, it prompts you for a password.
- Default user ID and password are **"admin / admin"**
- You can change the password after logging in (Passwords are case-sensitive).

ID / Password = **admin / admin**

A screenshot of a web interface titled "Log-in". It features a light blue header with the title. Below the header is a form with three input fields: "User ID", "Password", and "Language". The "Language" field is a dropdown menu currently set to "English". Below the form is a dark grey button with the text "Apply" in white.

NOTE : The Web Interface can be accessed by entering **http://192.168.1.1** in the Address Bar, regardless of the network connection status. When there is no input for 1 hour after you login to the Web Interface, you will be automatically logged out.

CPE Setup on the web page

1. WiMAX Status



- In the Top menu bar : Select "**WIMAX**" → "**Status**".
- You can view the configuration information and the current status of WiMAX.
- Please refer to the following table for detailed WiMAX Information.

WiMAX Information

MAC Address	MAC Address of WiMAX interface
WiMAX Status	Ready: WiMAX signal detected and WiMAX can be connected. OUT OF ZONE: No WiMAX signal detected
BSD	48-bit long field identifying the Base Station
CINR & RSSI Info	CINR: Carrier to Interference Ratio RSSI: Received signal strength indication
Power Control Mode	<u>Current transmitter power control mode</u>
Burst Data	WiMAX burst data information
Tx Power Info	<u>Tx power / Tx power maximum value</u>

2. LAN Setup

2.1 LAN Configuration

The screenshot shows the WIMAX LAN Configuration web interface. At the top, there is a navigation bar with icons for Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. Below this, the page title is "LAN Configuration | Status". On the left side, there is a sidebar menu with "LAN Setup" and "LAN DHCP Server Setup" options. The main content area contains a message: "Your CPE is equipped with a DHCP server that will automatically assign IP addresses to each computer on your network. The factory default settings for the DHCP server will work in any application." Below this message are two configuration sections. The first section is for IP Address and Subnet Mask, with input fields showing "192", "168", "1", "1" for IP Address and "255", "255", "255", "0" for Subnet Mask. The second section is for DHCP Server, with radio buttons for "Enable" (selected) and "Disable", a "Maximum Lease Time" field set to "1440" (min), an "IP Starting Address" field set to "192", "168", "1", "100", and a "Number of users" field set to "50". At the bottom right, there are "Save" and "Cancel" buttons.

- In the Top menu bar : Select "**LAN**" → "**LAN Configuration**"
- Configure LAN IP address :
 - Enter your LAN IP address in "**IP Address / Subnet Mask**" fields.
 - Default Values are "**192.168.1.1 / 255.255.255.0**" and only the last byte in "**Subnet Mask**" field can be modified.
- Configure LAN DHCP server :
 - Enable LAN DHCP server to lease an IP address to the computer connecting to CPE with wired LAN.
 - Enter Maximum lease time (in min), IP Starting address, Number of users.
- Click the "**Save**" button when finished.
- After "**save**", you are prompted to reboot.
- The changed configuration is applied after the CPE is rebooted.

2.2 Status

The screenshot shows the WIMAX LAN configuration status page. The top navigation bar includes icons for Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. The main content area is titled "LAN configuration : Status" and is divided into three sections: Local Network Information, DHCP Information, and DHCP Reservation.

Local Network Information

Local MAC Address	00:21:87:00:07:01
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

DHCP Information

DHCP Server	Enabled
Start IP Address	192.168.1.100
End IP Address	192.168.1.129

DHCP Reservation

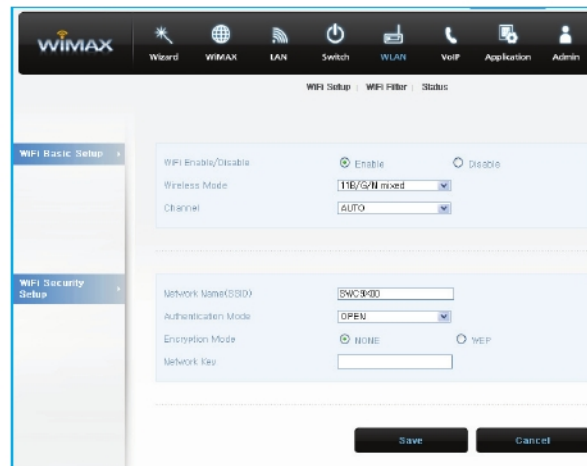
MAC Address	IP Address	Expires In
08:04:81:4E:95:C1	192.168.1.100	Expired !!
08:00:22:68:94:13:75	192.168.1.101	Expired !!

- In the Top menu bar : Select "**LAN**" → "**Status**".
- You can view the details of the LAN DHCP configuration.

3. WLAN

3.1 WiFi (Wireless LAN) Setup

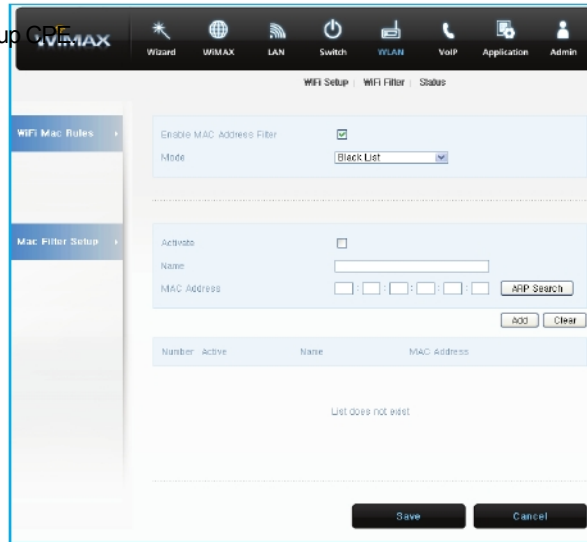
WiFi configuration can be modified when Switch mode is set to CPE (NAT) Mode.



- In the Top menu bar : Select "**WLAN**" → "**WiFi Setup**".
- Configure WiFi Basic :
 - Select whether WiFi is enabled or disabled.
 - Select the wireless mode(11B/G mixed, 11B only, 11G only, 11N only, 11B/G/N mixed)
- Configure WiFi Security :
 - Enter the new name of SSID (WiFi network name).
 - Select authentication mode(OPEN, SHARED, WPA-PSK, WPA2-PSK)
 - Set whether or not to use WEP encryption.
 - Enter the network key if using WEP encryption.
- Click the "**Save**" button when finished. Then, you will be moved to the Rebooting Screen.
- If you have finished CPE setup and want to reboot the CPE, click the "**Yes**" button to reboot the CPE.
- The changed configuration is applied after rebooting the system.

3.2 WiFi Filter

WiFi MAC address filtering allows only machines with specific MAC address access the network. You must specify which addresses are allowed when you setup



- In the Top menu bar : Select "**WLAN**" → "**WiFi Filter**".
- Configure a WiFi Filter :
 - Check the Enabled Mac Address Filter
 - Enter the Name and Mac Address
- Click the "**Save**" button when finished.

3.3 WiFi Status



- In the Top menu bar : Select "**WLAN**" → "**Status**".
- You can see various information related to the WiFi configuration.

4. VoIP

Voice over Internet Protocol(VoIP) is a method of delivery of voice communication over the internet of packet-switched network. Internet telephony refers to communications services - voices, facsimile, and / or voice-messaging applications - that are transported via the Internet, rather than the public switched telephone network(PSTN).

4.1 System

The screenshot displays the WIMAX configuration interface for VoIP. The top navigation bar includes 'Wizard', 'WIMAX', 'LAN', 'Switch', 'WLAN', 'VoIP', 'Application', and 'Admin'. The current page is 'General' under 'Account' and 'Line'. The left sidebar has expandable sections for 'SIP T1 Interval', 'Speed-UP States', 'Emergency Service', and 'Priority Numbers'. The main content area contains the following settings:

- SIP T1 Interval:** 500 (Range: 500-1000)
- Enable:** Enable Disable
- String:** [Empty field]
- Emergency Service:**
 - Emergency Enable:** Enable Disable
 - Emergency Registration:** Enable Disable
 - Emergency WIMAX Connect Timer:** 80 (Range: 1-600)
 - Emergency Number - Generic:** 112,911,119,110,120
 - Emergency Number - Police:** 112,119,911
 - Emergency Number - Medical:** 120,911
 - Emergency Number - Fire:** 119,911
- Priority Numbers:**
 - Priority - Urgent:** 1100,200,300
 - Priority - Normal:** 400,500
 - Priority - Non-Urgent:** 600,700

Buttons for 'Save' and 'Cancel' are located at the bottom right.

- In the Top menu bar : Select "VoIP" → "General" → "System".

Name	Description
SIP Timer	
SIP T1 Interval	A T1 timer defined in SIP protocol
Speed-up Dialling	
Enable	Enable speed dialing
String	The string to enter, to get to the speed dial numbers
Emergency Service	
Emergency enable	Enable emergency calls
Emergency Registration	If enabled, VoIP system will perform emergency registration before making emergency call. Else send INVITE with emergency number regardless of registration status.
EmergencyWiMAX Connect Timer	Timeout of setup emergency WiMAX connection. When CPE is not connected to WiMAX, pressed emergency number will trigger CPE to do emergency WiMAX connection. The timer is used to abort WiMAX connection and remainder call action, if connection timeout.
Emergency Number - Generic	Enter any emergency number
Emergency Number - Police	Enter any emergency police number
Emergency Number - Medical	Enter any emergency medical number
Emergency Number - Fire	Enter any emergency fire department number
Priority - Urgent	Enter any emergency fire department number
Priority Numbers	
Priority - Normal	If dialed number identical to one of setting, the INVITE will insert SIP header "Priority" with "urgent" string.
Priority - Non-urgent	If dialed number identical to one of setting, the INVITE will insert SIP header "Priority" with "normal" string.
Save	If dialed number identical to one of setting, the INVITE will insert SIP header "Priority" with "non-urgent" string.
Cancel	Commit the changes made and save to the CPE device. Reset fields to the last saved values.

4.2 Media

The screenshot displays the WIMAX configuration interface. At the top, there is a navigation bar with icons for Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. Below this, the 'General' tab is selected, and the 'Media' sub-tab is active. The interface is divided into several sections:

- System | Media | QoS | Provision**: The current sub-tab is 'Media'.
- RTCP Send Interval**: A text input field with the value '15' and a range of '1-1000'.
- Media Port Start**: A text input field with the value '8000' and a range of '4000-90000'.
- Media Port End**: A text input field with the value '9000' and a range of '4000-90000'.
- Dynamic Payload Type Setup**: A section with several rows of G.72x and ILBC codecs, each with a dropdown menu and a range:
 - G.726 18k: 96 (Range: 95-128)
 - G.726 24k: 97 (Range: 95-128)
 - G.726 30k: 98 (Range: 95-128)
 - G.726 40k: 99 (Range: 95-128)
 - ILBC: 104 (Range: 95-128)
 - Telephone-event: 101 (Range: 95-128)
- Codec Packetization Time Setup**: A section with several rows of G.711, G.723, G.726, G.729, and ILBC codecs, each with a dropdown menu and a range:
 - G.711: 30 (Range: 10-60)
 - G.723: 30 (Range: 30, 60)
 - G.726: 20 (Range: 20, 40, 60)
 - G.729: 20 (Range: 10-60)
 - ILBC: 30 (Range: 20, 40, 60 | 30, 60)
- Advanced**: A section with several options:
 - Voice Jitter Buffer Type: Dynamic (dropdown)
 - Voice Jitter Buffer Length: 120 ms (Range: 0-500ms)
 - Packet Loss Concealment: Enable Disable
 - DVC Enable: Enable Disable
 - T.38 Static Jitter Length: 210 ms (Range: 0-500ms)

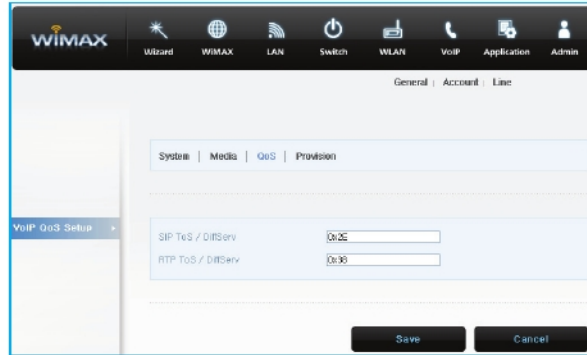
At the bottom right, there are 'Save' and 'Cancel' buttons.

- In the Top menu bar : Select "VoIP" → "General" → "Media".

Name	Description
Port Range	
Media Port Start	RTP local start port number, (start~end) defined the RTP listen port range
Media Port End	RTP local end port number
Dynamic Payload Type Setting	
G.726 16K	Default is 96
G.726 24K	Default is 97
G.726 32K	Default is 98
G.726 40K	Default is 99
ILBC	Default is 104
Telephone-event	Default is 101
Codec Packetization Time Settings	
G.711	Default is 20 ms
G.723	Default is 30 ms
G.726	Default is 20 ms
G.729	Default is 20 ms
ILBC	Default is 30 ms
Advanced	
Voice Jitter Buffer Type	Dynamic (Default) / Static / Disable
Voice Jitter Buffer Length	0-500 ms, 120 ms by default
Packet Loss Concealment	Enable by default
DVCC Enable	Enable by default
T.38 Static Jitter Length	0-500 ms, 210 ms by default
Save	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values

4.3 QoS

QoS is the differentiation between types of traffic and types of services so that the different types of service and traffic can be treated different service. This way, one type can be favored over another. In VoIP, quality simply means being able to listen and speak in a clear and continuous voice, without unwanted noise. DiffServ is a QoS protocol for managing bandwidth allocation for Internet media connections.

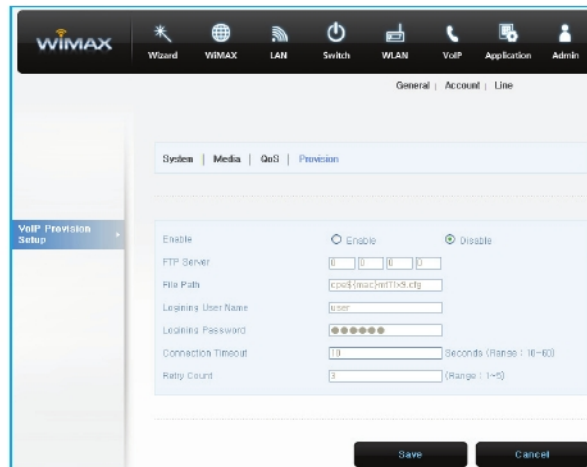


- In the Top menu bar : Select "**VoIP**" → "**General**" → "**QoS**".

Name	Description
VoIP QoS Setting	
SIP ToS/DiffServ	The SIP ToS rule will tag each SIP outgoing packet which will prioritize SIP traffic.
RTP ToS/DiffServ	The RTP ToS rule will to tag each RTP outgoing packet which will prioritize RTP traffic.
Save	Commit the changes made and save to the CPE
Cancel	device Reset fields to the last saved values

4.4 Provision

Provision is a functionality to update the configuration by the FTP protocol.



- In the Top menu bar : Select "**VoIP**" → "**General**" → "**Provision**".

Name	Description
VoIP Provision Setting	
Enable	Enable or Disable
FTP Server	FTP server address
File Path	File path and file name
Logging User Name	Login username
Logging Password	Login password
Connection Timeout	Connection timeout
Retry Count	Retry count
Save	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values

4.5 Status

Show server information, account register status and call history.

The screenshot shows the WIMAX management interface. The top navigation bar includes: Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. Below this, the breadcrumb path is General | Account | Line. The main content area is divided into four sections:

- Server Status:**

SP Register	0.0.0.0 : 8660
Proxy Server	0.0.0.0 : 8660
Outbound Server	0.0.0.0 : 8660
Register Status	Unregistered
- STUN Status:**

STUN Server	0.0.0.0 : 3478
STUN Status	Enable
- Line Status:**

Subscriber Number	1000
Account Status	Enable
Phone Status	Idle
- Call History:**

Received call	0
Missing call	0
Outgoing call	0

At the bottom of the interface, there are two buttons: **Connection** and **Disconnection**.

- In the Top menu bar : Select "VoIP" → "Account" → "Status".

4.6 Server

The screenshot displays the WIMAX configuration interface. At the top, there is a navigation bar with icons for Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. Below this, the 'General' tab is selected, and the 'Account' sub-tab is active. The 'Server' sub-tab is also selected, showing the following configuration fields:

Field	Value
Registrar Server	0.0.0.0
Port Number	5060
Separate Registrar Address	0.0.0.0
Separate Registrar Port	5060
Registrar Period Time	300 seconds (00-8535, default: 300)
Proxy Server	0.0.0.0
Port Number	5060
Outbound Server	0.0.0.0
Port Number	5060
STUN Server	0.0.0.0
Port Number	3478

At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

- In the Top menu bar : Select "**VoIP**" → "**Account**" → "**Server**".

Name	Description
Register Server	
Register Server	A SIP registrar is a server in a Session Initiation Protocol (SIP) network that accepts and processes SIP REGISTER requests. Format is "x.x.x.x".
Port Number	A registrar server port number, default is 5060.
Separate Registrar Address	Provide separate configures to send REGISTER to specific destination by Route header. If set to "0.0.0.0" register requests will send to out-bound through Route header.
Register Period Time	Register refresh time
Proxy Server	
Proxy Server	Proxy Server A SIP proxy is a server in an Session Initiation Protocol (SIP) network that route the sip message to a right place. Format is "x.x.x.x".
Port Number	A proxy server port number, default is 5060.
Outbound Server	
Outbound Server	Outbound Server The outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. Format is "x.x.x.x".
Port Number	An outbound server port number, default is 5060.
STUN Server	
STUN Server	NAT Traversal Enter the IP address of the STUN server, it will send and receive STUN requests and responses. Simple Traversal of User Datagram Protocol (STUN) through NATs is a standards-based IP protocol used as one of the methods of NAT traversal in applications of real-time voice, video, messaging, and other interactive IP communications.
Port Number	
Save	
Cancel	An STUN server port number, default is 3478.
	Commit the changes made and save to the CPE device
	Reset fields to the last saved values

4.7 User

WIMAX

Wizard WIMAX LAN Switch WLAN VoIP Application Admin

General Account Line

Status Server User Feature Dialing Speed Dial Fax RTP

SIP Account

Enable Enable Disable

SIP Local Port 5060 (default:5060)

Subscriber Number 1000

Display Name 1000

Authentication Name 1000

Password ●●●●

Codec Settings

1st Codec G.729

2nd Codec G.711_alaw

3rd Codec G.711_mu-law

4th Codec NONE

5th Codec NONE

6th Codec NONE

7th Codec NONE

8th Codec NONE

9th Codec NONE

G.723.1 Rates G.723.1

LBC Rates 30ms

Session Timer

Session Timer Enable Enable Disable

Refresh Method INVITE

Min Session Timer 90 seconds (50-65535, default:90)

Session Timer 1800 seconds (120-65535, default:1800)

Misc.

SIP User Agent Name UserAgent

Timeout for Find back 190 seconds (1-1800, default:100)

Apply Cancel

- In the Top menu bar : Select "VoIP" → "Account" → "User".

Name	Description
SIP Account	
Enable	Enable or disable the SIP account
SIP Local Port	Enter the SIP local port, default value is 5060
Subscriber Number	Enter the subscriber number for Line. The number is a unique series of digits of VoIP subscriber. It's used to interconnect with SIP server, for outgoing or incoming calls.
Display Name	The display name of the VoIP subscriber, shown when it makes outgoing calls. Maximum name size is 64 characters.
Authentication Name	A unique string of VoIP subscriber. It's used to authenticate subscriber to get authorization to perform call setup privilege.
Password	Enter the password
Codec Settings	
1st Codec	Subscriber prefers codec and it has 1st priority in codec negotiation.
2st Codec	Subscriber prefers codec and it has 2nd priority in codec negotiation.
3st Codec	Subscriber prefers codec and it has 3rd priority in codec negotiation.
4st Codec	Subscriber prefers codec and it has 4th priority in codec negotiation.
5st Codec	Subscriber prefers codec and it has 5th priority in codec negotiation.
6st Codec	Subscriber prefers codec and it has 6th priority in codec negotiation.
7st Codec	Subscriber prefers codec and it has 7th priority in codec negotiation.
8st Codec	Subscriber prefers codec and it has 8th priority in codec negotiation.
9st Codec	Subscriber prefers codec and it has 9th priority in codec negotiation.
G.723.1 Rates	Subscriber prefers codec and it has 9th priority in codec negotiation.
iLBC Rates	<ul style="list-style-type: none"> <li style="margin-right: 20px;">• 5.3kbps <li style="margin-right: 20px;">• 6.3kbps <li style="margin-right: 20px;">• 20ms • 30ms

Name	Description
Codec Settings	
Save	Commit the changes made and save to the CPE device
Cancel	Reset fields to previous settings

4.8 Feature

The screenshot displays the Wimax management interface. At the top, there is a navigation bar with icons for Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. Below this, a breadcrumb trail shows 'General' > 'Account' > 'Line'. A secondary menu bar includes 'Status', 'Server', 'User', 'Feature', 'Extns', 'Speed Dst', 'Fax', and 'RTP'. The 'Feature' section is active, showing a list of settings on the left and their configurations on the right. The settings include:

- Feature settings:** A list of features on the left, with 'Feature settings' selected.
- DTMF:** DTMF is set to 'Out-of-band/RFC 2833'. SP INFO is unchecked.
- Call Forward Settings:** All Call Forwarding (All CF) is unchecked. Unconditional CF, Busy CF, and No Answer CF are also unchecked. Their respective targets are set to '0:00'.
- Call Waiting Settings:** Call waiting is unchecked.
- Hotline Settings:** Hotline is unchecked. Hotline Target is '0:00' and Hotline Period Time is '0' seconds.

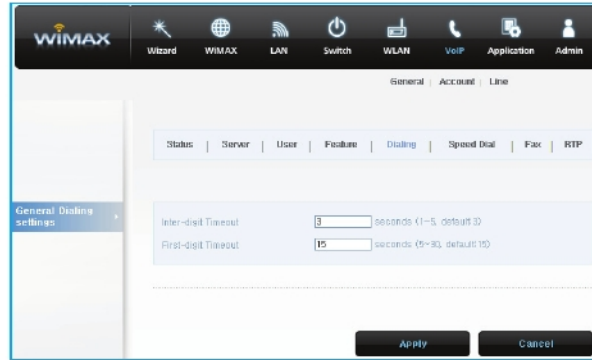
At the bottom of the interface, there are 'Apply' and 'Cancel' buttons.

- In the Top menu bar : Select "VoIP" → "Account" → "Feature".

Name	Description
Feature Setting	
Auto Decline Anonymous	When VoIP subscriber receives an incoming call with privacy, with display name as "anonymous". VoIP subscriber can REJECT it when the setting "Auto Decline Anonymous" is enabled. If it's not enabled it will treat it as a normal incoming call and allow the phone device to ring.
Do Not Disturb (DND)	When it is enabled, it will reject all incoming call
Hide User ID	As "Calling Line Identification Restriction (CLIR)", VoIP subscriber can enable this function to hide its identifier to others, when VoIP subscriber makes an outgoing call.
MWI	Message waiting indication. The LED on select telephones will light-up to notify the user that they have voicemail.
Hold Method	sendonly / recvoonly inactive
DTMF	
DTMF	<u>DTMF</u> RFC2833 out-of-band
SPINFO	In-band Enable / Disable the SIP INFO message while user dial
All Call Forwarding (All CF)	DTMF digits.
Call Forwarding Setting	
Unconditional CF	Enable / Disable, call forward feature
Unconditional CF Target	Enable / Disable unconditional call forward feature
Name Description Busy CF	Unconditional call forwarding target number
Busy CF Target	Enable / Disable, busy forward feature
No Answer CF	Busy forward target number
No Answer CF Target	Enable / Disable, No Answer call forward feature No answer call forward target number

Name	Description
Call Waiting Setting	
Call Waiting	Enable / Disable Call waiting feature
Hotline Setting	
Hotline	Hot line enable / disable switch
Hotline Target	Hot line target
Hotline Period Time	Hot line timeout period
Apply	Commit the changes made and save to the CPE
Cancel	device
	<u>Reset fields to the last saved values</u>

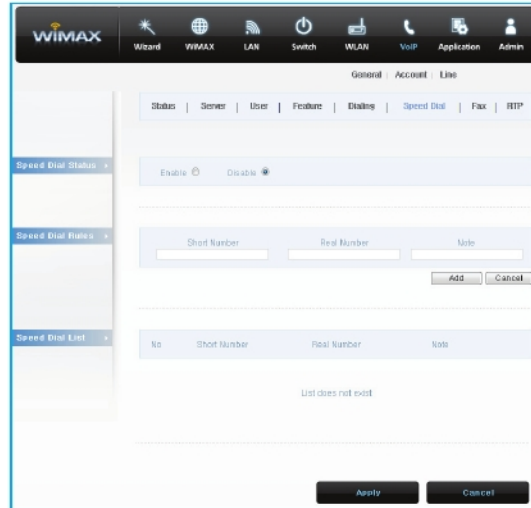
4.9 Dialing



- In the Top menu bar : Select "**VoIP**" → "**Account**"→ "**Dialing**".

<u>Name</u>	<u>Description</u>
General Dialing Setting	
Inter-digit Timeout	The time period between each digit.
First-digit Timeout	The maximum time allowed between off-hook and entering the first digit.
Apply	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values

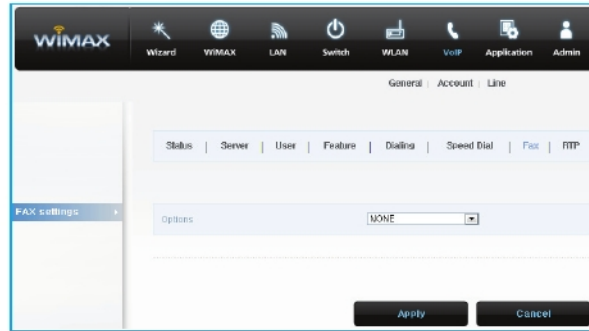
4.10 Speed Dial



- In the Top menu bar : Select "**VoIP**" → "**Account**" → "**Speed Dial**".

<u>Name</u>	<u>Description</u>
Speed Dial Status	
Active	Enable / disable rule
Speed Dial Rules	
Short Number	Predefine number of rule
Real Number	Callee's telephone number
Note	Description of rule
Add	Save current and create new entry for next rule
OK	Save current rule
Apply	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values

4.11 FAX



- In the Top menu bar : Select "**VoIP**" → "**Account**" → "**FAX**".

<u>Name</u>	<u>Description</u>
	FAX Setting
<u>Options</u>	NONE G.711A Pass Through G.711U Pass Through T.38 FAX Relay T.38 FAX Only
<u>Apply</u>	Commit the changes made and save to the CPE
<u>Cancel</u>	device <u>Reset fields to the last saved values</u>

4.12 RTP



- In the Top menu bar : Select "VoIP" → "Account" → "RTP".

Name	Description
RTP Setting	
RTP Detection Enable	Enable / disable RTP detection for RX packets
RTP Timeout	The RTP timeout is used to judge the call, is it still alive and do the right action. The range is from 10-300, 40 seconds is the default value.
RTP Packet Loss Percentage	You can specify the allowable RTP Packet Loss percentage and if it reaches the %, and do the right action.
Apply	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values

4.13 Phone

The screenshot shows the WIMAX configuration interface. At the top, there is a menu bar with icons for Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. Below the menu bar, there are tabs for General, Account, and Line. The 'Line' tab is selected, and within it, there are sub-tabs for Phone, Voice, and Profile. The 'Phone' sub-tab is active. The main configuration area is divided into two sections: 'PHONE' and 'Caller ID'. The 'PHONE' section contains the following settings: Heck Flash Detect Upper Bound (700 msec), Heck Flash Detect Lower Bound (100 seconds), Voice Tx Level (5), Voice Rx Level (5), and Ring Incedance (600mins). The 'Caller ID' section contains the following settings: Caller ID Type (PSK ETS), Voice Tx Level (After Ring), and Caller ID Power Level (0). At the bottom right, there are 'Apply' and 'Cancel' buttons.

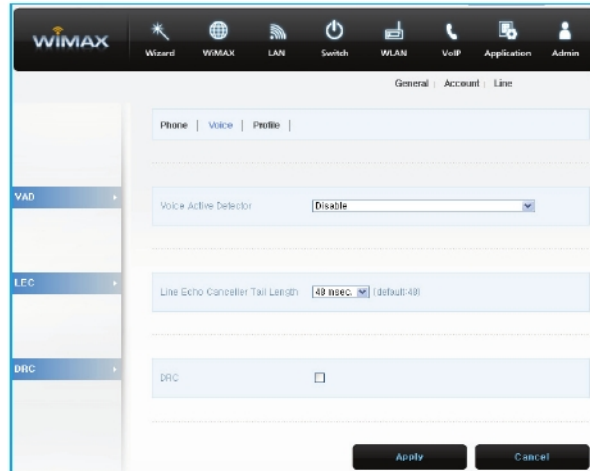
- In the Top menu bar : Select "**VoIP**" → "**Line**"→ "**Phone**".

NOTE : The following figures will apply for Line 1, Line 2, Line 3 and Line 4.

The Line and Account is one-to-one mapping, that is, the Line 1 is mapping to Account 1, Line 2 is mapping to Account 2, Line 3 is mapping to Account 3, and Line 4 is mapping to Account 4.

Name	Description
Phone	
Hook Flash Detect Upper Bound	This parameter defines the upper bound of the quick on / off-hook cycle.
Hook Flash Detect Lower Bound	This parameter defines the lower bound of the quick on / off-hook cycle.
Voice Tx Level	The voice gain level that is heard by a telephone user
Voice Rx level	The voice gain level that is received by the device
Ring Impedance	The impedance between tip and ring on the telephone line
Caller ID	
Caller ID Type	This will allow you to enable and select the Called ID type for your area. You also have the choice to disable caller ID. <ul style="list-style-type: none"> • Disable • FSK Bellcore • Japan CLIP • FSKETS!
Caller ID Display	This parameter configures when Caller ID will be displayed. <ul style="list-style-type: none"> • Before Ring • After Ring
Caller ID Power Level	The transmitting power level of caller ID to the telephone
Apply	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values

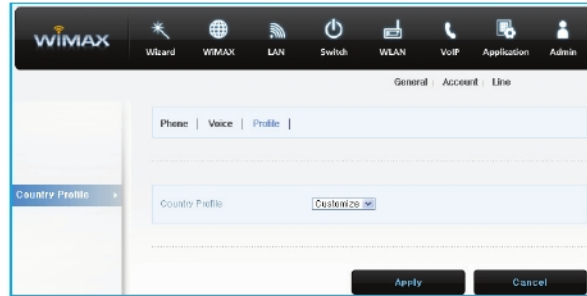
4.14 Voice



- In the Top menu bar : Select "VoIP" → "Line"→ "Voice".

Name	Description
VAD	
Voice Active Detector	<p>You can enable and select which voice activity detection to use. It can facilitate speech processing, and can also be used to deactivate some processes during non-speech segments : it can avoid unnecessary coding / transmission of silence packets in VOIP, saving on computation and on network bandwidth. There are 4 choices to select from.</p> <ul style="list-style-type: none"> • Disable • Silence Suppression - NO CNG • Silence Suppression - Only G.711 Annex II Type • Silence Suppression - Codec Specific CN (G.729 and G.723)
LEC	
Line Echo Canceller Tail Length	<p>There are processing delays in IP networks that could cause an echo. This function is used to decrease the echo effect.</p> <ul style="list-style-type: none"> • Disable • 16ms • 32ms • 48ms
DRC	
<u>Apply</u>	DRC
<u>Cancel</u>	<u>Check DRC</u>
	<u>Commit the changes made and save to the CPE device</u>
	<u>Reset fields to the last saved values</u>

4.15 Profile



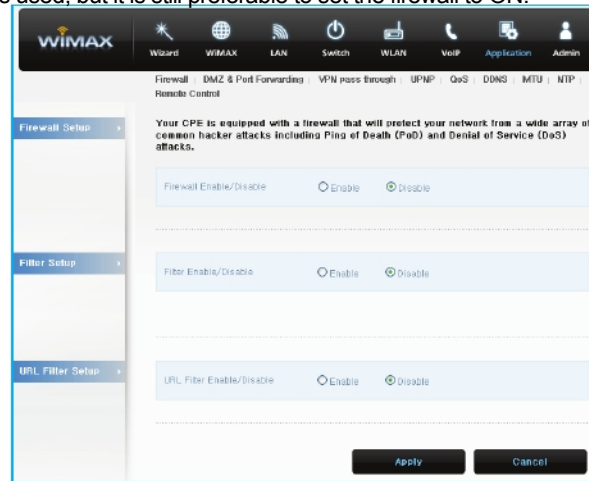
- In the Top menu bar : Select "VoIP" → "Line" → "Profile".

<u>Name</u>	<u>Description</u>
<u>Country Profile</u>	<u>Customize or USA</u>
<u>Apply</u>	<u>Commit the changes made and save to the CPE device</u>
<u>Cancel</u>	<u>Reset fields to the last saved values</u>

5. Application Setup

5.1 Firewall

Firewall enables you to set the CPE so that it is not affected by external hacking attempts, including Ping Flooding or DoS. Internal LAN PCs are usually isolated / protected from external Internet attacks even when no firewall is used, but it is still preferable to set the firewall to ON.



- In the Top menu bar : Select "**Application**" → "**Firewall**".
- If you want to use the Firewall function, Select "**Enable**".
- Click the "**Apply**" button when finished.
- The changed configuration is applied immediately.

5.2 DMZ & Port Forwarding

The DMZ feature allows you to specify one computer on your network to be placed outside of the NAT firewall. This may be necessary if the NAT feature is causing problems with certain applications, such as a game or a video conferencing application. Use this feature on a temporary basis, as the computer in the DMZ will not be protected from attacks by hackers.

The Port Forwarding function is used to forward incoming packets of specific TCP / IP ports from outside to the assigned PC. This function is useful if you have to use VoIP or P2P applications, or have to operate HTTP or FTP servers from a PC in the internal LAN.

The screenshot shows the Wimax router's configuration interface for DMZ and Port Forwarding. The top navigation bar includes Wimax, Wizard, WIMAX, LAN, Switch, WLAN, VoIP, Application, and Admin. The main menu includes Firewall, DMZ & Port Forwarding, VPN pass through, UPnP, QoS, DNS, MTU, and NAT. The sub-menu is Firewall Control.

The DMZ configuration section includes:

- DMZ Enable/Disable: Enable, Disable
- Private LAN IP: 0 0 0 0

The Port Forwarding section includes:

- Name: [Text Input]
- Protocol: BOTH (dropdown)
- Incoming Start Port: [Text Input]
- Incoming End Port: [Text Input]
- Forward Start Port: [Text Input]
- Forward End Port: [Text Input]
- Destination IP: [Text Input]
- Buttons: Add, Cancel

A table below the form shows the list of port forwarding rules:

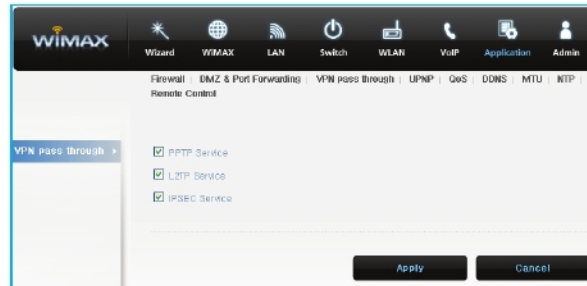
Name	Protocol	Incoming Start	Incoming End	Forward Start	Forward End	IP Address
List does not exist						

Buttons: Apply, Cancel

- In the Top menu bar : Select "**Application**" → "**DMZ & Port Forwarding**".
- Configure DMZ(Demilitarized Zone) Setup :
 - Select enable or Disable.
 - Enter "**Private LAN IP**".
 - Click the "**Save**" button when finished.
- Configure Port Forwarding Setup :
 - The port forwarding function is configurable when DMZ is disabled.
 - After entering all of the specific information to connect, click the "**Add**" button to view the added Port Forwarding information.
 - Click the "**Apply**" button.
 - To modify / delete the existing Port Forwarding, use the "**Edit**"/"**Delete**" button.
 - The changed configuration is applied immediately
- DMZ and Port Forwarding cannot be enabled at the same time.

5.3 VPN pass through

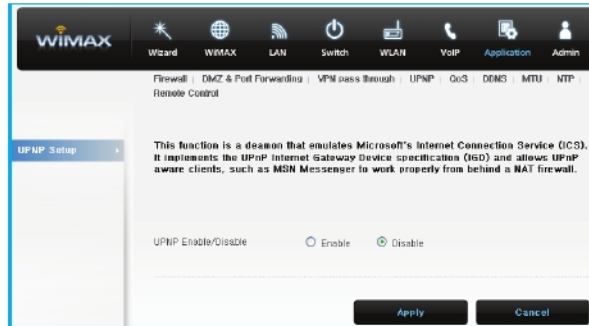
The VPN (Virtual Private Network) function is used to obtain access to a security network installed in a company or an organization via the Internet network. If there is a VPN server that you access, you can activate the security protocol supported by the appropriate VPN Server.



- In the Top menu bar : Select "**Application**" → "**VPN pass through**".
- SWC-9200 supports 3 types of service : PPTP, L2TP and IPSEC.
- Check the type(s) of VPN pass-through.
- Click the "**Apply**" button when finished. Then click the "**Apply**" button to apply the changed configuration immediately.

5.4 UPnP

UPnP (Universal Plug and Play) is the standard by which a PC, peripheral devices, intelligent home appliances, or wireless equipment can automatically detect each other by using the internet and web protocol when connected to the network. When a user can add a certain device to the network using UPnP, the device will complete its own organization, receive the TCP / IP address, and discover the HTTP-based discovery protocol to announce its existence to other devices.



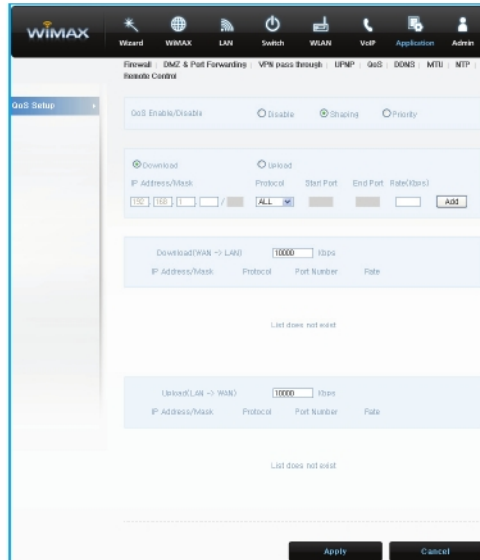
- In the Top menu bar : Select "**Application**" → "**UPnP**".
- Configure UPnP.
 - If you want to set UPnP, select "**Enable**".
 - Click the "**Apply**" button when finished. Then, you will be moved to the Rebooting Screen.

5.5 QoS

Quality of Service (QoS), in the area of computer networking, refers to the mechanisms that control resource reservation. QoS assigns different priority levels to different applications, users, or data flows. QoS also measures and improves their level of performance, such as transmission and error rate.

For instance, the use of internet RSVP (Resource Reservation Protocol) allows packets passing through gateway hosts to be processed quickly according to predefined policy and reservation standards.

If a company or a user applies ATM (Asynchronous Transfer Mode), through which the service quality can be selected in advance, the QoS can monitor and improve such data flows as average delays, delay changes of a cell in the group, cell losses and transmission error rate.



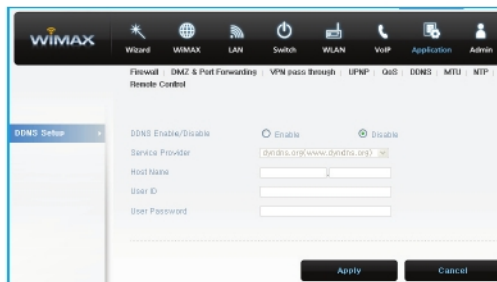
- In the Top menu bar : Select "**Application**" → "**QoS**".
- To enable QoS, select "**Shaping**" or "**priority**".
- For "**Shaping**"
 - Select "**Download**" and / or "**Upload**". Enter the required values.
 - Click the "**Add**" button when finished. Then, you can see the configured setting added below.
- For "**Priority**"
 - Enter the necessary values. Click the "**Add**" button when finished.
 - Then, you can see the configured setting added below.

5.6 DDNS

DDNS (Dynamic DNS) is a method for easily maintaining the DNS information of a PC that uses a dynamic IP address. In general, when a user accesses the internet, the internet service provider arbitrarily assigns the user one of the IP addresses that is not currently being used. This address allows the user exclusively to access the internet. Using this method, you can support many more computers with the same number of IP addresses, compared to the method in which a fixed IP address is assigned to each PC.

However, if your own domain name and IP address are registered in the DNS, each time you access the internet, a new IP address is assigned. This is very inconvenient. The DDNS service provider uses a special program run on the user's computer in order to automatically update the DNS database when a new IP address is assigned by the internet service provider.

In this way, even though the IP address corresponding to a specific domain name is frequently changed, there is no need to know the IP address that other users use to access the computer. As a result, by using the same domain name as before, you can easily access the network.



- In the Top menu bar : Select "**Application**" → "**DDNS**".
- Configure the DDNS Setup :
 - If you want to set the DDNS, Select "**Enable**".
 - Select the desired Service.
 - Enter all the necessary required for DDNS Setup.
 - Click the "**Apply**" button when finished.

5.7 MTU

The MTU (Maximum Transmission Unit) is the largest packet or frame that can be transmitted in a packet or frame-based network such as TCP / IP. In general, the unit of octets is used. TCP determines each packet size for all types of transmission. If the MTU is too large, retransmission is sometimes required when a router cannot handle the excessively large packet.

On the other hand, if the MTU is too small, the overhead size for header and transmission/receipt check tends to be large. For most computer operating systems, you should follow the recommendations of your internet service provider on whether to change the MTU setting and what value to change it to.



- In the Top menu bar : Select "**Application**" → "**MTU**".
- Configure the Interface MTU Setup :
 - Enter WIMAX MTU Size (500 ~ 1500).
 - Click the "**Apply**" button when finished.

5.8 NTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP on port 123 as its transport layer. It is designed specifically to resist the effects of variable latency by using a jitter buffer.

NTP also indicates a reference software implementation that is distributed by the NTP Public Services Project.

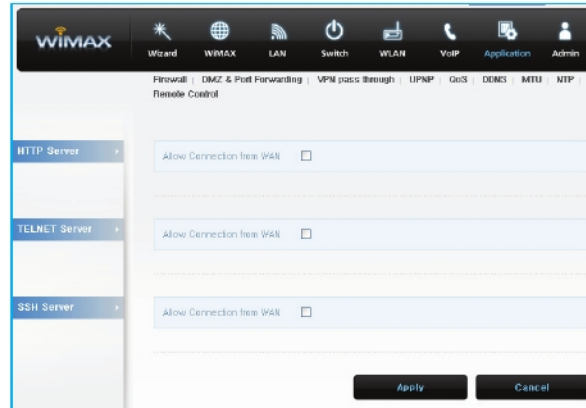
NTP is one of the oldest Internet protocols still in use (since before 1985).

NTP was originally designed by Dave Mills of the University of Delaware, who still maintains it, along with a team of volunteers. NTP is not related to the simpler DAYTIME (RFC 867) and TIME (RFC 868) protocols.



- In the Top menu bar : Select "**Application**" → "**NTP**".
- Configure Time Zone Setup :
 - If you want to set the NTP Client, select "**Enable**".
 - Enter NTP Time Server.
 - Select the desirable Time Zone.
 - Click the "**Apply**" button when finished.

5.9 Remote Control



- In the Top menu bar : Select "**Application**" → "**Remote Control**".
- Configure the HTTP Server Setup :
 - Click the Allow Connection from WAN
- Configure the TELNET Server Setup :
 - Click the Allow Connection from WAN
- Configure the SSH Server Setup :
 - Click the Allow Connection from WAN

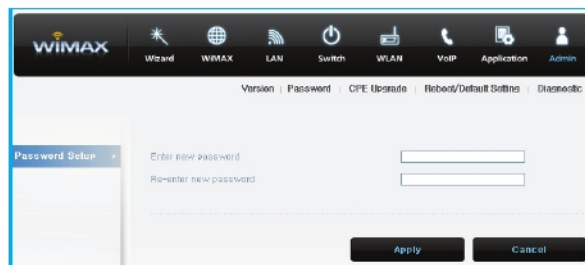
6. Admin Setup

6.1 Version



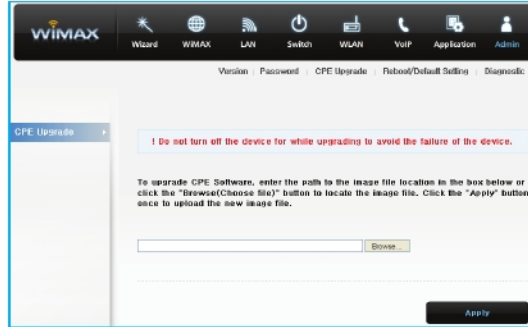
- In the Top menu bar : Select "**Admin**" → "**Version**".
- You can see the versions of the SWC-9200 firmware and the WIMAX firmware.

6.2 Password

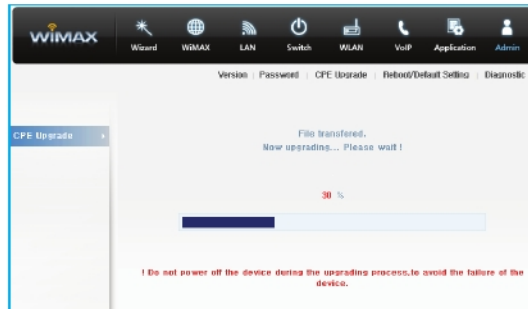


- In the Top menu bar : Select "**Admin**" → "**Password**".
- Change your password :
 - Enter a new password, and re-type it to confirm.
 - Click the "**Apply**" button when finished.
 - The changed configuration is applied immediately.


6.3 CPE Upgrade



- In the Top menu bar : Select "**Admin**" → "**CPE Upgrade**".
 - Enter the CPE firmware path. Or click the "**Browser**" button find the firmware file.
 - To start the firmware update, click the "**Apply**" button.



- This will take several minutes, and the time may vary according to the environment.
- CPE is rebooted automatically after the upgrade is complete.

 **Caution :** To avoid failure of the CPE, do not power off the CPE during the upgrade.

6.4 Reboot / Default Setting



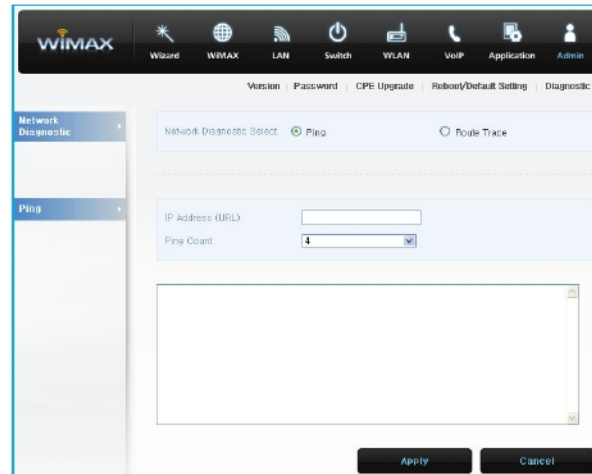
- In the Top menu bar : Select "**Admin**" → "**Reboot / Default Setting**".
 - Select "**Reboot**" to reboot CPE.
 - Select "**Reset to all default settings**" to reboot and initialize CPE to its default settings.
 - To reboot the CPE, click the "**Apply**" button.
 - CPE is rebooted automatically. Rebooting takes about 40 seconds.

6.5 Diagnostic

Diagnostic are used in diagnosis and troubleshooting the network problems.

Ping test : Helps in discovering the status of a network device, that is whether the device is alive or not.

Trace route : Records the route followed in the network between the sender's computer and a specific destination computer.



- In the Top menu bar : Select "**Admin**" → "**Diagnostic**".
- Configure the Network Diagnostic Setup.
 - If you want to set Network Diagnostic, Select "**Ping**".
 - Enter IP Address (URL).
 - Select the desirable Ping Count.
 - Click the "**Apply**" button when finished.

Troubleshooting

Refer to the following if you are having trouble connecting to the Internet

- 1 Check the LED status of CPE.
 - Check if the POWER LED is illuminated.
 - Check if the LEDs of WiMAX are illuminated.
 - For LAN port, check if the lamp of the port connected to the PC is illuminated.

- 2 Check the IP address of your PC.
 - In Windows 98/ME
 - Click [Start] >> [Run] and enter the [winipcfg] command to open the [IP Address] window, then check the [IP Address].
 - In Windows 2000/XP
 - Run [Command Prompt] and enter the [ipconfig] command to check the [IP address].

- 3 If IP Address is not normal - Set the IP Address of the PC manually.
 - In Windows 98/ME
 - Execute [Run >> Control Panel >> Network], and then click Properties of [TCP/IP] for LAN card.
 - Ⓜ Check [Use the assigned IP address], enter [192.168.1.100] for [IP Address] and [255.255.255.0] for [Subnet Mask].
 - Select [Gateway] and enter [192.168.1.1] for [New Gateway], and then click [Add].
 - Select [DNS Configuration], check [Use DNS], enter any name for [Host], enter [DNS Server Address to search], and click [Add].
 - Click [OK], click [OK] again in the [Network Properties] window, and then click [OK] in the [Change System Setup] window to reboot the PC

 - In Windows 2000
 - Select [Start -> Control Panel -> Network and Dial-UP Connections], double-click [Local Area Connection], and click [Properties].
 - Click Properties of [Internet Protocol (TCP/IP)] among Components.
 - Click [Use the following IP address].
 - Enter [192.168.1.100] for [IP Address], [255.255.255.0] for [Subnet Mask], and [192.168.1.1] for [Default Gateway].
 - Click [Use the following DNS Server Address].
 - For [Basic Setup DNS Server], enter the communication company server of each country.
 - Click [OK]. Click [OK] again in the [Local Area Connection Properties] window.

In Windows XP

- Select [Start -> Control Panel -> Network and Internet Connection], double-click [Local Area Connection], and click [Properties].
Click Properties of [Internet Protocol (TCP/IP)] among Components.
- Click [Use the following IP address].
- Enter [192.168.1.100] for [IP Address], [255.255.255.0] for [Subnet Mask], and [192.168.1.1] for [Default Gateway].
- Click [Use the following DNS Server Address].
- For [Basic Setup DNS Server], enter the communication company server of each country.
- Click [OK]. Click [OK] again in the [Local Area Connection Properties] window.

In Windows Vista

- Select [Start -> Control Panel -> Network and Internet -> Network and Sharing Center -> Manage network connections] double-click [Local Area Connection], and click [Properties].
Click Properties of [Internet Protocol Version 4(TCP/IPv4)] among Components.
- Click [Use the following IP address].
- Enter [192.168.1.100] for [IP Address], [255.255.255.0] for [Subnet Mask], and [192.168.1.1] for [Default Gateway].
- Click [Use the following DNS Server Address].
- For [Preferred DNS Server], enter the communication company server of each country.
- Click [OK]. Click [OK] again in the [Local Area Connection Properties] window.

In Windows 7

- Select [Start -> Control Panel -> Network and Internet -> Network and Sharing Center -> Change adapter settings], double-click [Local Area Connection], and click [Properties].
Click the Properties of [Internet Protocol Version 4 (TCP/IPv4)] among Components.
- Click [Use the following IP address].
- Enter [192.168.1.100] for [IP Address], [255.255.255.0] for [Subnet Mask], and [192.168.1.1] for [Default Gateway].
- Click [Use the following DNS Server Address].
- For [Preferred DNS Server], enter the communication company server of each country.
- Click [OK]. Click [OK] again in the [Local Area Connection Properties] window.

In MAC OS X

- From the "Apple" menu, select "System Preferences."
- Click on the [Network] icon in the [Internet & Wireless] category.
- Click on the [Ethernet] option in the left-hand side of the Network setting window.
- Select the [Manually] option from the [Configure] drop-down menu.
- Enter [192.168.1.100] for [IP Address], [255.255.255.0] for [Subnet Mask], and [192.168.1.1] for [Router].
- For [DNS Server], enter the communication company server of each country.
- Click [Apply].

4 Run [MS-DOS] or [Command Prompt] and then perform a PING Test with [192.168.1.1].

A message [Reply from 192.168.1.1: bytes=32 time=1ms TTL=64] should appear when running [ping 192.168.1.1] command. If the result of the Ping test does not arrive properly, please contact the Customer Support Center.

Operating Information

Temperature Range and power rating for the SWC-9200

- Operating temperature for the units is 0°C ~ 40°C

Power rating AC for the SWC-9200

- 100-240V ~ 50/60Hz 0.6A Max
- **Antenna Installation SWC-9200**
- Out door antenna must be installed by a professional for optimum performance and fixed operations



Safety Information

Caution

Minor injury or product damage can occur the following directions are violated.

- Do not put any object on the product.
- Avoid heating devices.
- Do not disassemble, repair or redesign the product.
- Be careful not to allow any foreign matter inside the product.
- Do not leave the Product in a location where it is exposed to severe static electricity, as this can cause the product to malfunction.
- Do not put any metallic object (coin, hair pin) or flammable object inside the product, or drop the product.

Legal Information

EU Regulatory Conformance

Hereby, SEOWON INTECH Co., Ltd. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

For the declaration of conformity, visit the Web site

<http://www.seowonintech.co.kr/en/customer/regulatory.asp>



Reduction of Hazardous Substances

This device is compliant with the EU Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) Regulation (Regulation No 1907/2006/EC of the European Parliament and of the Council) and the EU Restriction of Hazardous Substances (RoHS) Directive (Directive 2002/95/EC of the European Parliament and of the Council).

WEEE Notice

The disposal of this device is subject to the Waste from Electrical and Electronic Equipment (WEEE) Directive of the European Union. The Directive aims to promote environmentally-friendly handling of WEEE by ecological disposal or reuse/refurbishment of the collected WEEE.



This symbol on the device signifies that the device must not be discarded with normal household garbage. You are obliged to hand over this device to a certified collection point at the end of its life.

Separating WEEE from other waste helps minimize any of their hazardous effects on environment and human beings. For more information, please contact a municipal office or the retail stores where you purchased this device.

FCC Compliance Statement

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.

Caution: Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.



FCC ID : S3KSWC9200

Note: 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.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

RF exposure statements :

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Warranty Information

This product is the result of high quality craftsmanship based on strict quality control procedures.

- In the event of Product failure or malfunction during normal usage, your product will be repaired free of charge within the Limited Warranty period.
- The Consumer shall bear any labor or parts charges not covered by this Limited Warranty.
- When requesting repair under the warranty, you must provide the proof of purchase and the warranty.
- Keep the warranty in a safe location, as it will not be reissued.

Purchase date		
Quality warranty period	1(one) year	
Seller		
Telephone number		
Consumer	Name	
	Address	
	Telephone number	
	E-mail	

The Consumer shall have no coverage or benefits under this Limited Warranty if the Product has been:

- Subjected to inappropriate use, improper storage, nauthorized repair, unauthorized modifi cations, neglect abuse, inadequate installation, misuse, damage in shipping, etc.
- Damaged by fire, flooding, windstorm, lighting, earthquake, theft, blown fuse, internet viruses, worms, Trojan Horses, etc.
- Treated with its Product Serial # removed or defaced.



GLOBAL TELECOM CORP, INC

5000 BIRCH STREET
SUITE 3000
NEWPORT BEACH, CA 92660
TEL 1-818-665-2068
FAX 1-9249-204-3943
E-MAIL info@aimws.com
www.aimws.com