User Manual

OX-250

WiMAX Outdoor CPE

Version 0.5

Nov. 8 , 2010

This Document may be subject to change, please contact with us for the latest version.

Federal Communication Commission Interference Statement

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 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.

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

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 50cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Due to the essential high output power natural of WiMAX device, use of this device with other transmitter at the same time may exceed the FCC RF exposure limit and such usage must be prohibited (unless such co-transmission has been approved by FCC in the future).

History

Revision	Date of Issue	Scope	Author
0.1	2010-10-14	First draft	IChia Lin.
0.2	2010-10-18	Add specification	IChia Lin
0.3 2010/1	0/26	Change min.30cm distance to 35cm,add install and ground guide	IChia Lin
0.4	2010/11/4	Update figure 70	IChia Lin
0.5	2010/11/8	Change min.35cm distance to 50cm	IChia Lin

Table of Contents

List of Figures

List of Tables

1. Introduction

The WiMAX Outdoor CPE Software platform comes with a Web-based Configuration Manager, which gives users the ability to manage, configure and analyze the platforms environment. The Connection Manager works with all versions of Windows after Windows 95.

The supported browser version:

- Internet Explorer 6.0 or later (Recommended)
- Netscape 7.1 and higher
- Firefox 1.0 and higher
- Mozilla 1.5 and higher

1.1. Connect

Users need to connect to the WiMAX Outdoor CPE platform. It’s assumed that the user has a fully working WiMAX Outdoor CPE platform and properly connected. From the web browser connect to the device, entering the IP address of the device; it will prompt user to enter the username and password. The default usernames and passwords are as follows.

Username/password

- Operator/operator
- guest/guest

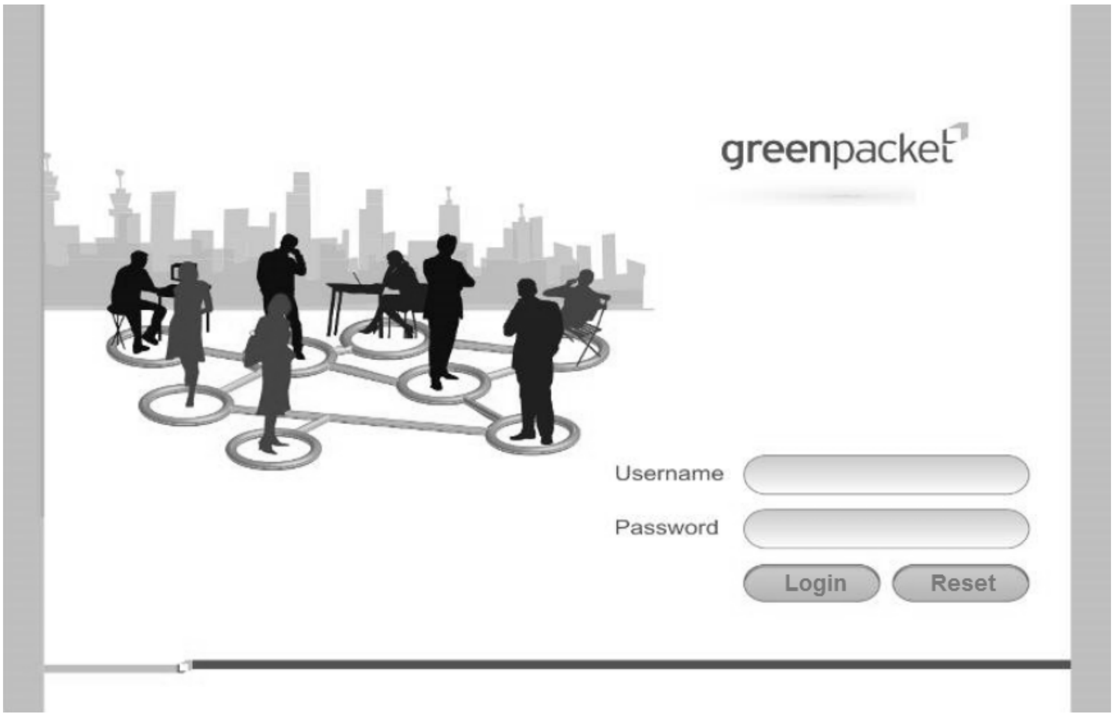
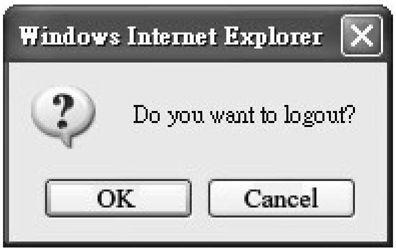
- 

Figure 1 Login page

1.2. Logout

The “Log out” window allows users to disconnect from the device and exit the Web-based Configuration Manager.

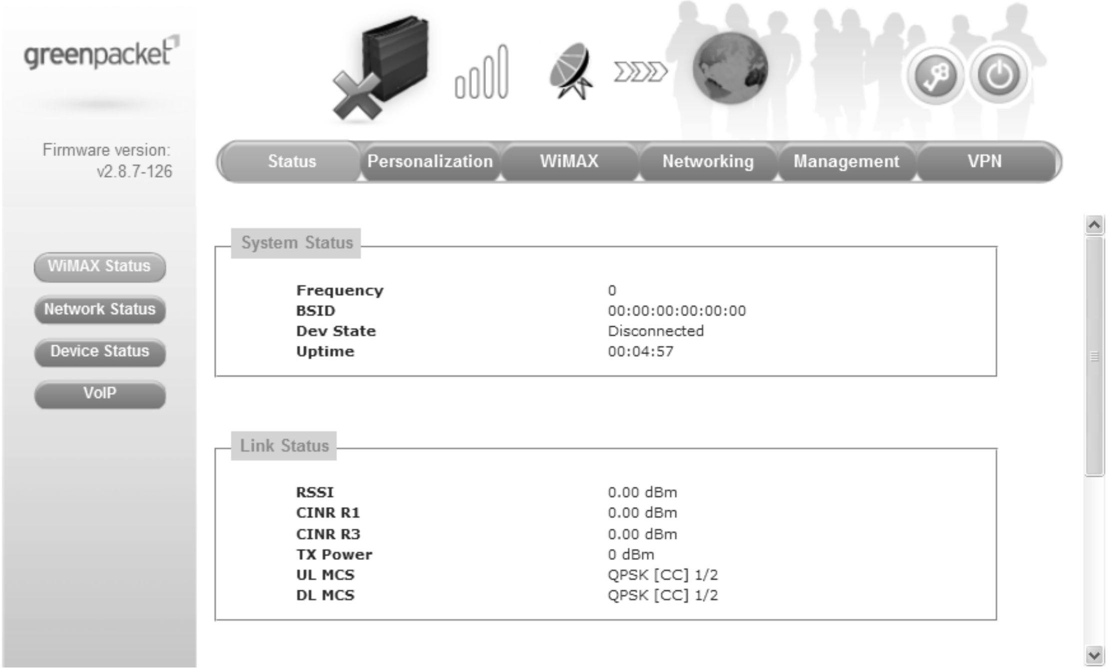


Do you want to logout?

Figure 2 Logout

1.3. Status

After user has established a connection, user will see the "Status" window. This window shows all the status and system information. It gives user an initial overview of the current st atus of the device.



Firmware version:
v2.8.7-126

System Status

Frequency	0
BSID	00:00:00:00:00:00
Dev State	Disconnected
Uptime	00:04:57

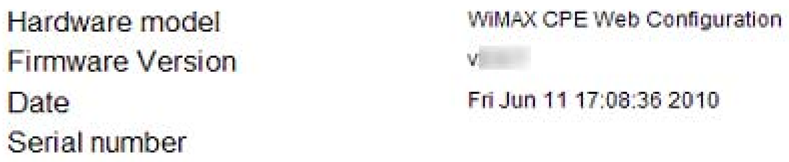
Link Status

RSSI	0.00 dBm
CINR R1	0.00 dBm
CINR R3	0.00 dBm
TX Power	0 dBm
UL MCS	QPSK [CC] 1/2
DL MCS	QPSK [CC] 1/2

Figure 3 Status window

1.4. Device Status

The "Device status" window displays firmware version information of the WiMAX Outdoor CPE.

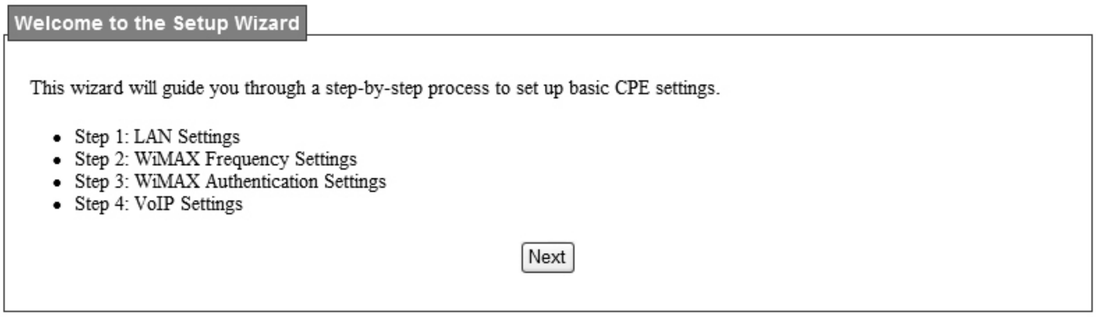


Hardware model	WiMAX CPE Web Configuration
Firmware Version	v[redacted]
Date	Fri Jun 11 17:08:36 2010
Serial number	

Figure 4 Device status

1.5. Setup Wizard

The setup wizard will allow user to quickly configure the basic networking settings on the CPE. Click the “Setup Wizard” menu item to enter the wizard. The first page will display all the steps necessary to complete the wizard settings as shown in Figure 5. Later, click the “Next” button to continue the next steps. The definition of each button shown on web page is defined in the Table 1.



Welcome to the Setup Wizard

This wizard will guide you through a step-by-step process to set up basic CPE settings.

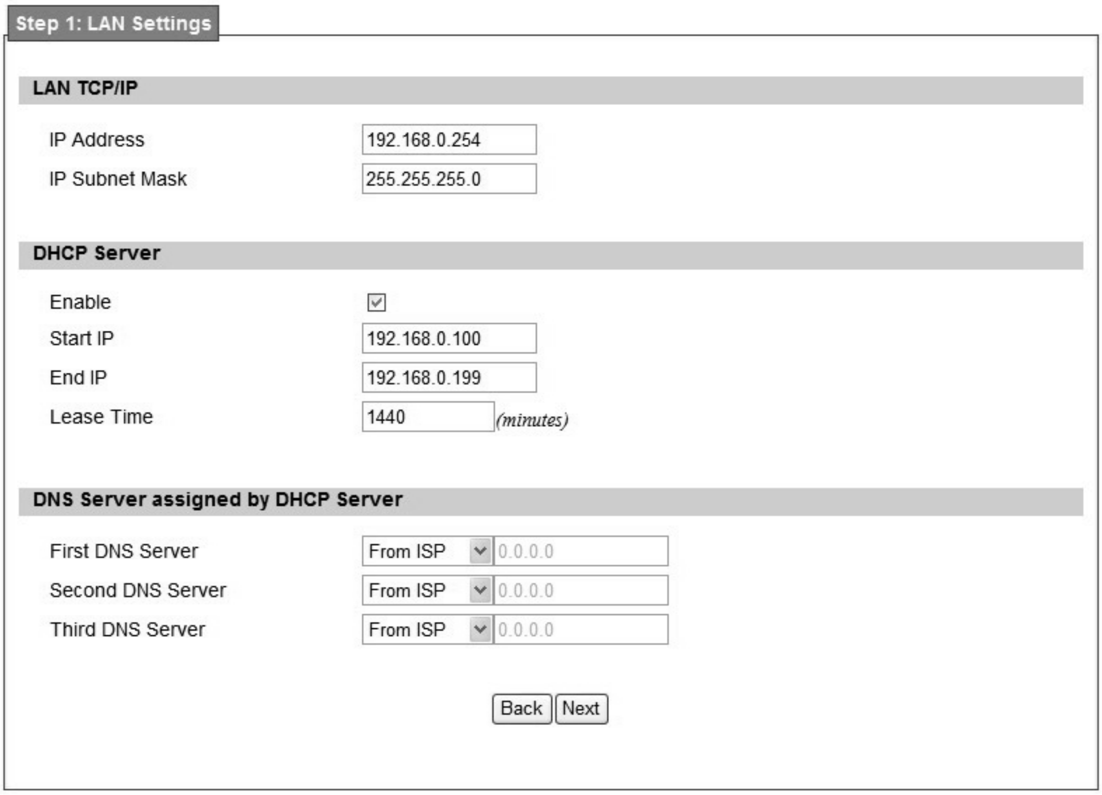
- Step 1: LAN Settings
- Step 2: WiMAX Frequency Settings
- Step 3: WiMAX Authentication Settings
- Step 4: VoIP Settings

Figure 5 Setup Wizard

Name	Description
Next	Continue to the next step
Back	Return to the previous step
Save	Commit the changes made and save to WiMAX outdoor CPE

Table 1 Button definition shown on Setup Wizard

- **Step 1:** LAN Settings. In this step user can configure both IP and DHCP configuration parameters as shown in Figure 6.



Step 1: LAN Settings

LAN TCP/IP

IP Address	192.168.0.254
IP Subnet Mask	255.255.255.0

DHCP Server

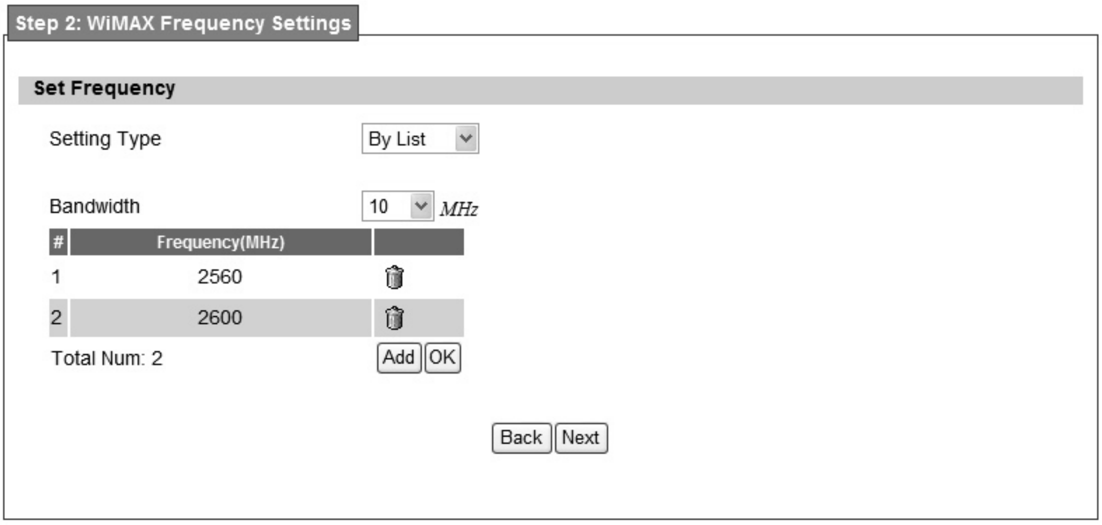
Enable	☑
Start IP	192.168.0.100
End IP	192.168.0.199
Lease Time	1440 *(minutes)*

DNS Server assigned by DHCP Server

First DNS Server	From ISP	0.0.0.0
Second DNS Server	From ISP	0.0.0.0
Third DNS Server	From ISP	0.0.0.0

Figure 6 Wizard LAN Settings in Setup Wizard

- **Step2:** WiMAX Frequency Settings. This step will quickly configure the WiMAX frequencies. There are two types of configuring the frequencies. User can configure it through simply entering a frequency in the frequency list as shown in Figure 7 or by giving a starting and ending frequency value and a step size to traverse the range as shown in Figure 8.



Step 2: WiMAX Frequency Settings

Set Frequency

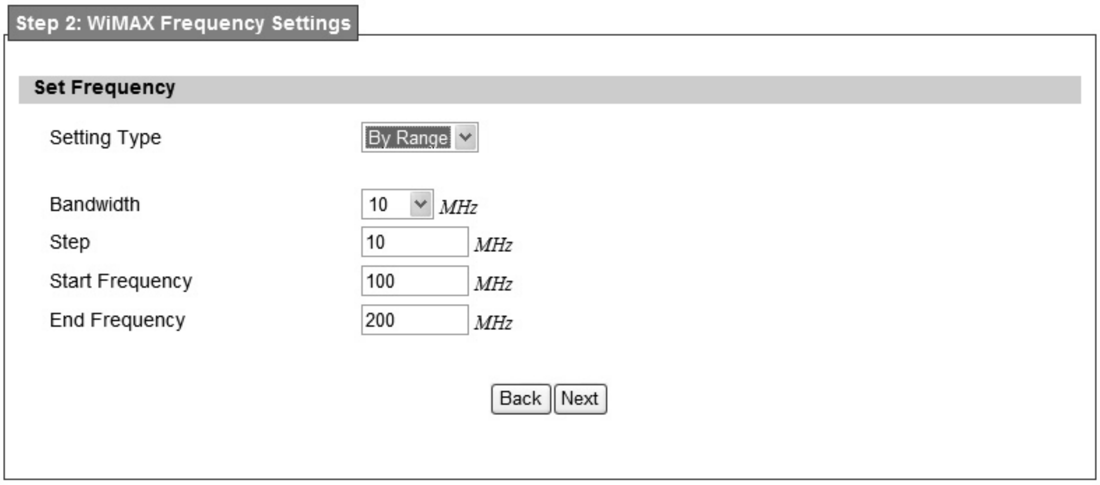
Setting Type: By List

Bandwidth: 10 MHz

#	Frequency(MHz)	
1	2560	🗑
2	2600	🗑

Total Num: 2

Figure 7 WiMAX Frequency Settings By List in Setup Wizard



Step 2: WiMAX Frequency Settings

Set Frequency

Setting Type: By Range

Bandwidth: 10 MHz

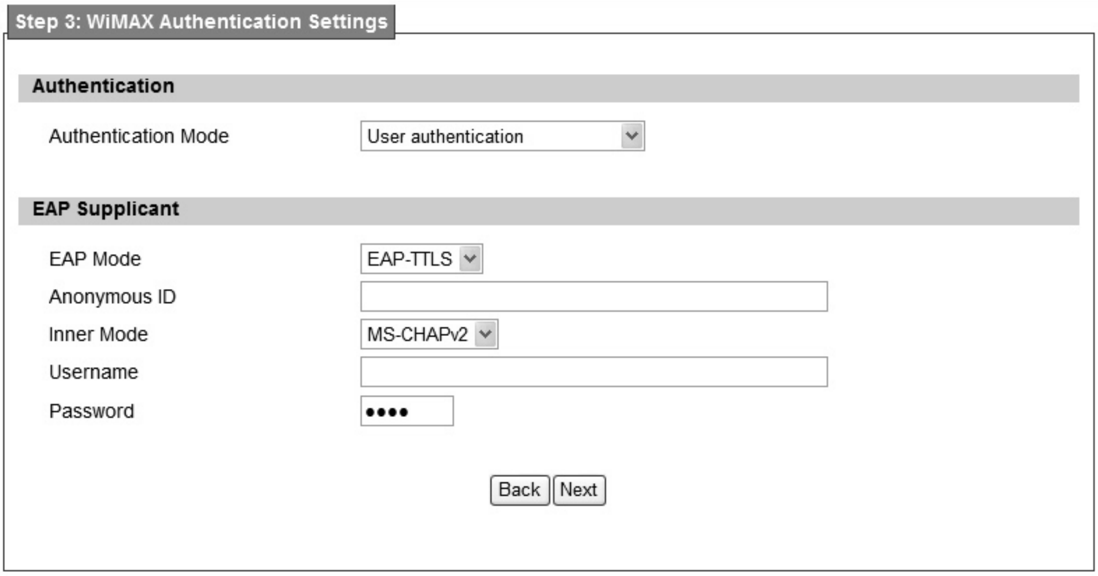
Step: 10 MHz

Start Frequency: 100 MHz

End Frequency: 200 MHz

Figure 8 WiMAX Frequency Settings By Range in Setup Wizard

- **Step 3:** WiMAX Authentication Settings. This will configure WiMAX Authentication settings. There are 4 possible options for “Authentication Mode” as No authentication, User authentication, Device authentication, and User and device authentication. Depending on which mode user selects, and it will appear different EAP settings for configuration. Except “No authentication” is selected, user needs to define the EAP supplicant as shown in Figure 9.



Authentication Mode: User authentication

EAP Mode: EAP-TTLS

Anonymous ID:

Inner Mode: MS-CHAPv2

Username:

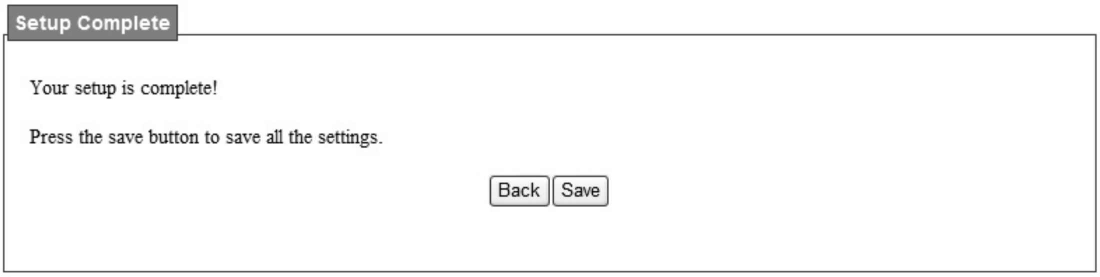
Password: ●●●●

Figure 9 WiMAX Authentication Settings in Setup Wizard

Detailed definition of each item in EAP supplicant is listed below.

- EAP Mode: WiMAX outdoor CPE supports EAP-TLS, EAP-TTLS, EAP-SIM, and EAP-AKA.
- Anonymous ID: User needs to fill the Outer ID at this field.
- Inner Mode: WiMAX outdoor CPE supports MS-CHAPv2, MS-CHAP, CHAP, MD5, and PAP.
- Username: User needs to fill username at this field.
- Password: User needs to fill password at this field.

Once the user completes all the steps, user needs to click the “Save” button to save the settings, or click “Back” button to return to previous step as shown in Figure 10. It will reload some services and return to the “Home” window after saving all settings.



Setup Complete

Your setup is complete!

Press the save button to save all the settings.

Figure 10 Wizard Save

2. Network

Refer to Figure 101, for proper network connection.

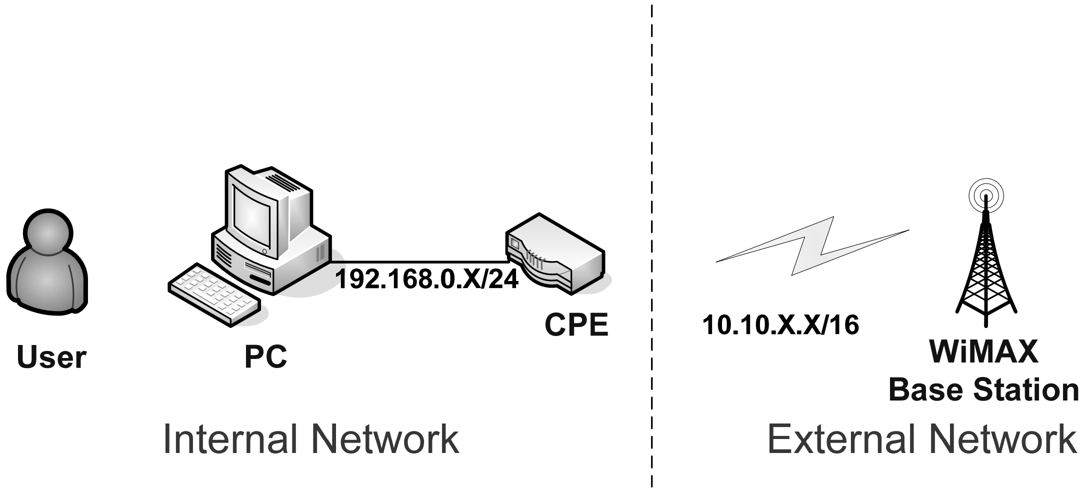
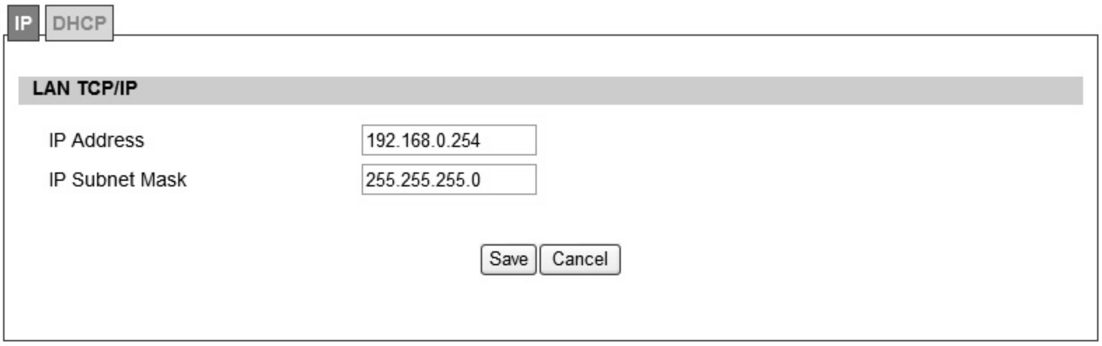


Figure 11 Network Topology

2.1. LAN

2.1.1. IP

From the “Network>LAN>IP” window, user can update the LAN information as shown in Figure 12. The definition for each field is shown on Table 2.



LAN TCP/IP

IP Address 192.168.0.254

IP Subnet Mask 255.255.255.0

Figure 12 Network>LAN>IP

Name	Description
IP Address	IP address of the WiMAX outdoor CPE
IP Subnet Mask	Subnet Mask of the WiMAX outdoor CPE
Save	Commits the changes made, and set the LAN IP information, some services will be reloaded.
Cancel	Reset the fields to the last saved values

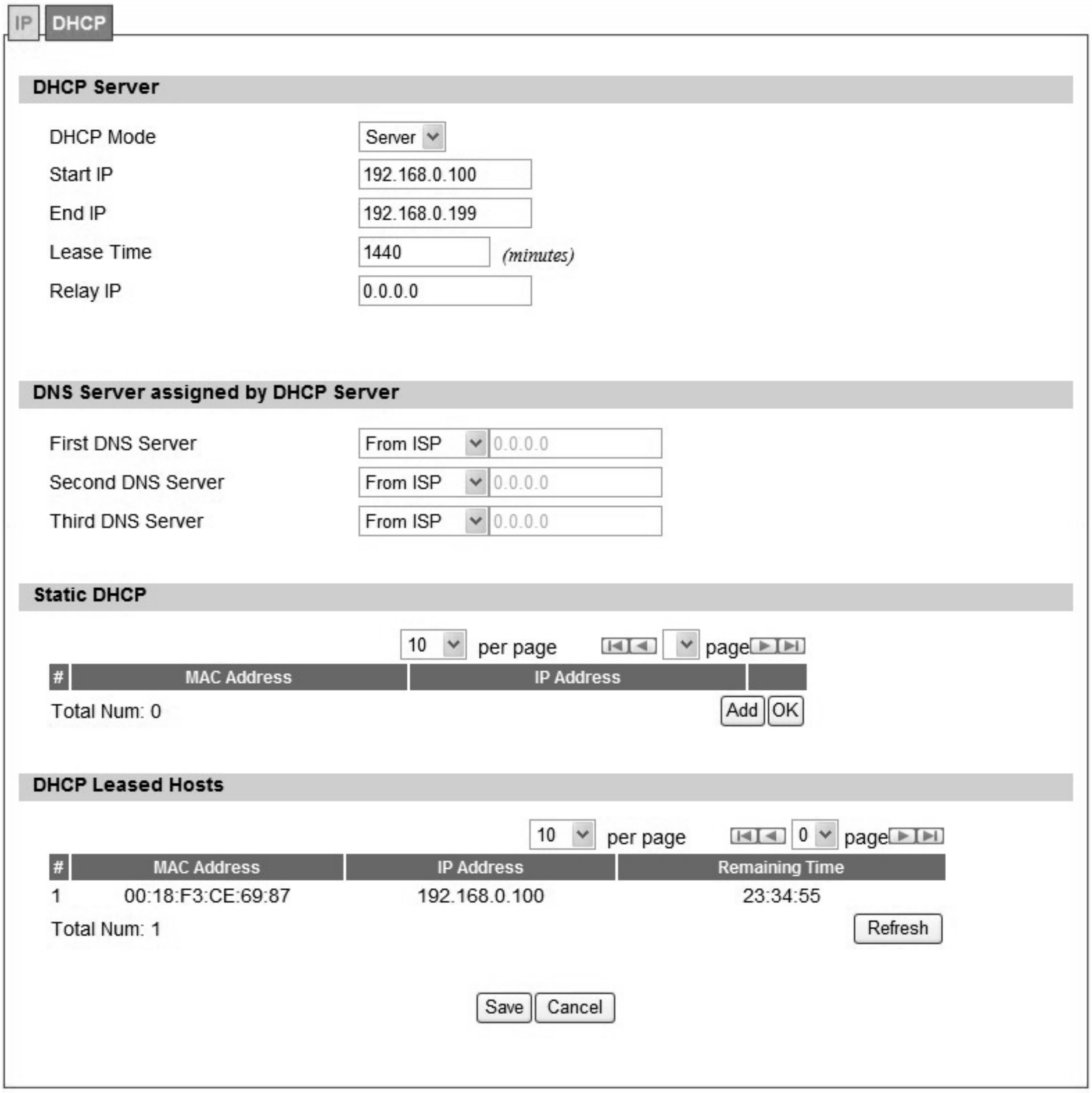
Table 2 Field definition for Network>LAN>IP

2.1.2. DHCP

Use the "Network>LAN>DHCP" tab to configure the DHCP server information. The default DHCP Server setup is enabled, and user could disable this function from setup as shown in Figure 13. When user disables the DHCP server, it requires to set a static IP address on host PC for CPE to configure. Please be noted that without the static IP address set properly on the host PC, user can not open the CPE web page for configuration.

When DHCP server is enabled, user needs to define the IP pool range for dynamically assigning the IP address. The advantage of using DHCP server is that the addresses which are no longer in use will be returned to the IP address pool so that the server can reallocate them to other machines in the network.

There are three DNS servers the user can configure to assign an IP address. Static DHCP will assign an IP address on the LAN to a specific device based on its MAC address. The definition for each field is shown on Table 3.



DHCP Server

DHCP Mode	Server
Start IP	192.168.0.100
End IP	192.168.0.199
Lease Time	1440 *(minutes)*
Relay IP	0.0.0.0

DNS Server assigned by DHCP Server

First DNS Server	From ISP	0.0.0.0
Second DNS Server	From ISP	0.0.0.0
Third DNS Server	From ISP	0.0.0.0

Static DHCP

10 per page page

#	MAC Address	IP Address	

Total Num: 0

DHCP Leased Hosts

10 per page 0 page

#	MAC Address	IP Address	Remaining Time
1	00:18:F3:CE:69:87	192.168.0.100	23:34:55

Total Num: 1

Figure 13 Network>LAN>DHCP

Name	Description
Enable	If the enable box is checked for DHCP server, the DHCP server will assign IP address to its client with the specified IP address range.
Start IP	Starting IP address range
End IP	Ending IP address range
Lease Time	The lease time is a controlled time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed (dynamic re-use of IP addresses). Lease time is measured in minutes in the Configuration Manager.
First DNS Server Second DNS Server Third DNS Server	User can specify three DNS server and select how the DNS Server is assigned. There are three options for assigning the DNS server. ● From ISP ● User Defined ● None If user selects "None", then the DHCP server will not give clients the DNS server information. If all the three DNS servers setting are set to "None", then the DHCP server will use the LAN IP address as the DNS server information for the clients. If the user chooses "User Defined" and leaves the IP address as "0.0.0.0" it will change the field to "None".
Add	Click on the "Add" button to enter a static leased IP address. Enter the MAC address of the Ethernet device and enter the IP address.
OK	Click the "OK" button to exit out of edit mode.
Save	Commit the changes made and save to WiMAX outdoor CPE, some services will be reloaded.
Cancel	Reset fields to the last saved values.

Table 3 Field definition for Network>LAN>DHCP

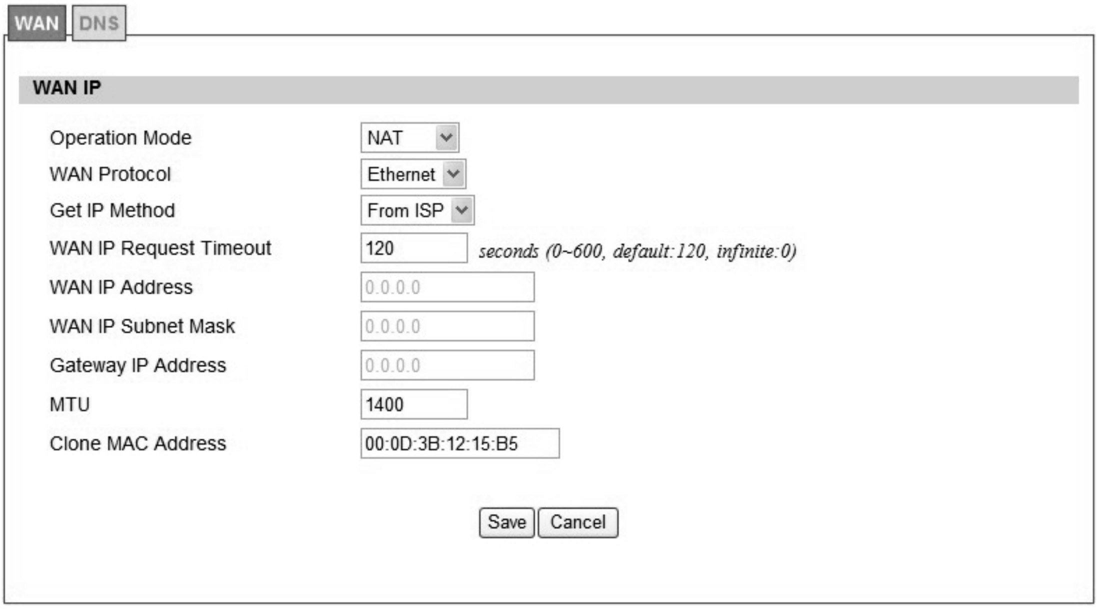
2.2. WAN

The wide area network is another network that user can connect to the internet with the

WiMAX outdoor CPE.

2.2.1. WAN

In Figure 14, it demonstrates ho w to co nfigure WAN IP on CPE web p age. The definition for each field is shown on Table 4.



WAN IP

Operation Mode	NAT
WAN Protocol	Ethernet
Get IP Method	From ISP
WAN IP Request Timeout	120 *seconds (0~600, default:120, infinite:0)*
WAN IP Address	0.0.0.0
WAN IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
MTU	1400
Clone MAC Address	00:0D:3B:12:15:B5

Figure 14 Network>WAN>WAN

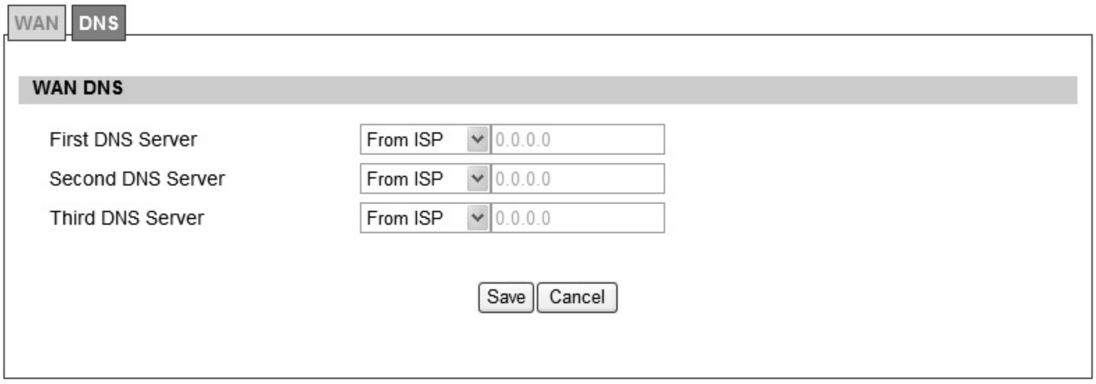
Name	Description
Operation Mode	Select the WAN operation mode ● Bridge ● Routing ● NAT
WAN Protocol	Select the WAN encapsulation protocol ● Ethernet ● PPPoE
Get IP Method	Enter the IP method ● From ISP ● User
WAN IP Request Timeout	The time the DHCP client waits to receive the IP address from the BS. If it doesn't get the IP , it will timeout and the CPE will disconnect the WiMAX connection. The default value is 120 seconds. If user enters 0, it will wait to receive the IP address infinitely until it's stopped by the user.
WAN IP Address	If user chooses "User" for IP Method, user should enter the WAN IP address
WIN IP Subnet Mask	If user chooses "User" for IP Method, user should enter the WAN IP subnet mask.
Gateway IP Address	If user chooses "User" for IP Method, user should enter IP gateway address
MTU	Enter the MTU
Clone MAC Address	Enter the clone MAC address to be used by WAN
PPPoE Setting	
User Name	The user name to connect PPPoE server via the selected Auth Protocol
Password	The password of the corresponding username
Retype Password	Type the "Password" again
Auth Protocol	The authentication protocol of the peer required. Select which Authentication protocol to use. ● PAP ● CHAP ● MSCHAPv1 ● MSCHAPv2

Encryption	Encryption Scheme No MPPE 40 bits: 40-bit encryption with MPPE MPPE 128 bits: 128-bit encryption with MPPE Auto: automatically selected
Idle Timeout	Disconnect if the link is idle for the assigned seconds
AC Name	The name of the access concentrator to connection to
Save	Commit the changes made and save to WiMAX outdoor CPE, after clicking the Save button user will get a message asking if user wants to reboot the CPE. Reboot is necessary for the device to switch to a different profile.
Cancel	Reset field to the last saved values

Table 4 Field definition for Network>WAN>WAN

2.2.2. DNS

In Figure 15, it demonstrates how to configure WAN DNS on CPE web page. The definition for each field is shown on Table 5.



First DNS Server	From ISP	0.0.0.0
Second DNS Server	From ISP	0.0.0.0
Third DNS Server	From ISP	0.0.0.0

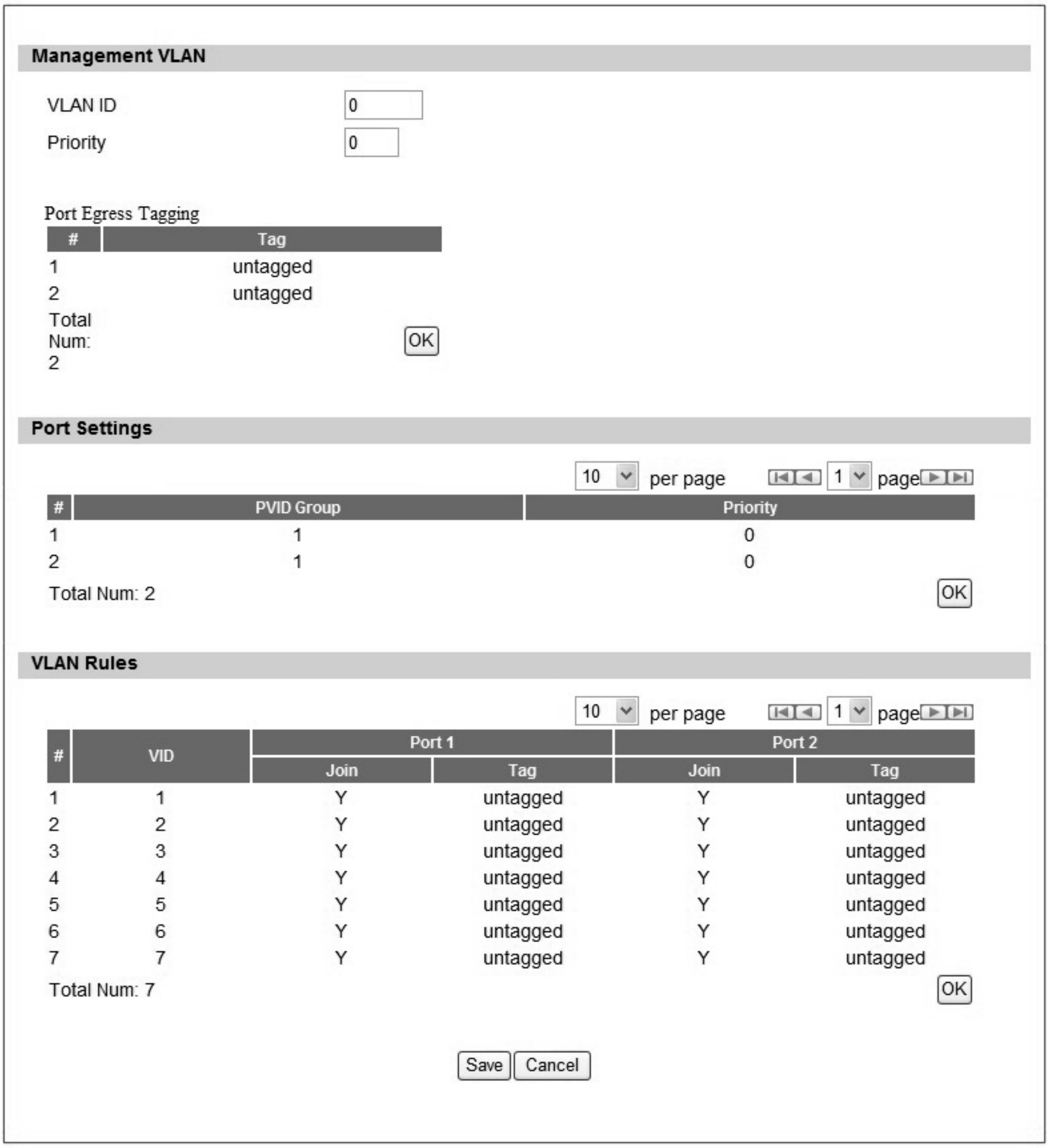
Figure 15 Network>WAN>DNS

Name	**Description**
First DNS Server	Enter the WAN DNS information. ● User Defined ● From ISP If user selects “User Define”, user needs to enter a valid IP address for the DNS server.
Second DNS Server	Same as First DNS Server
Third DNS Server	Same as First DNS Server
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 5 Field definition for Network>WAN>DNS

2.3. VLAN

In Figure 16, it demonstrates how to configure VLAN setting on CPE web page. The definition for each field is shown on Table 6.



Management VLAN

VLAN ID: 0

Priority: 0

Port Egress Tagging

#	Tag
1	untagged
2	untagged

Total Num: 2

Port Settings

#	PVID Group	Priority
1	1	0
2	1	0

Total Num: 2

VLAN Rules

#	VID	Port 1		Port 2	
		Join	Tag	Join	Tag
1	1	Y	untagged	Y	untagged
2	2	Y	untagged	Y	untagged
3	3	Y	untagged	Y	untagged
4	4	Y	untagged	Y	untagged
5	5	Y	untagged	Y	untagged
6	6	Y	untagged	Y	untagged
7	7	Y	untagged	Y	untagged

Total Num: 7

Figure 16 Network>VLAN

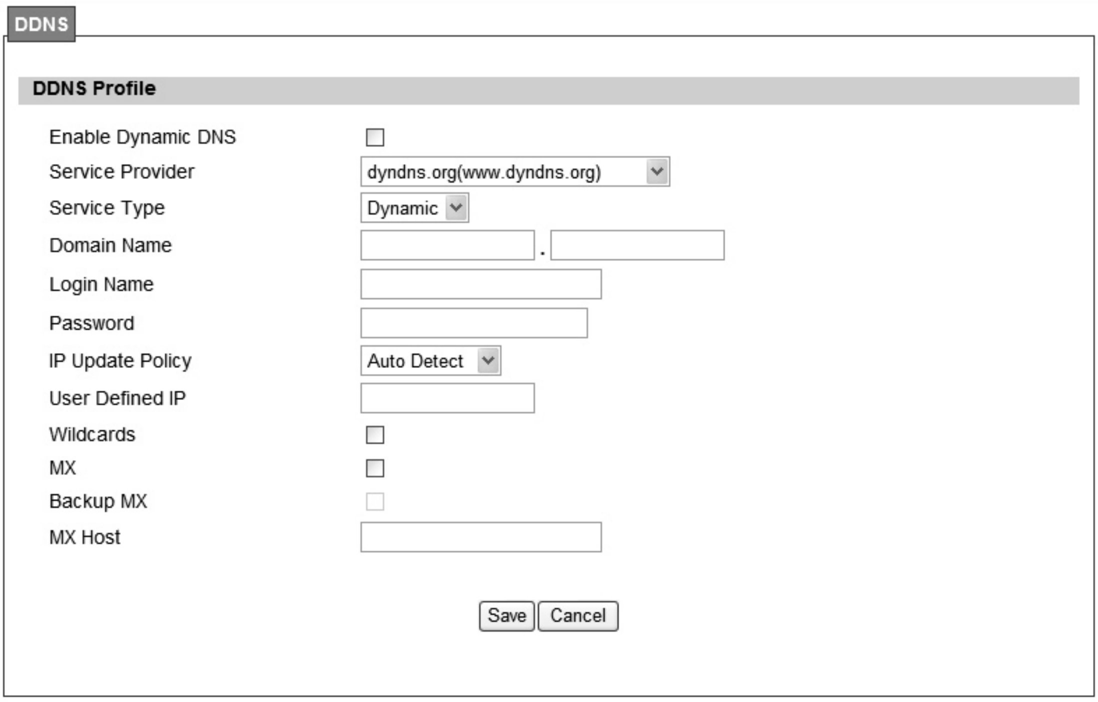
Name	**Description**
Management VLAN	
VLAN ID	Setting the management VLAN ID
Priority	Setting the management Priority
Port Settings	
PVID Group	Select the VLAN group as the PVID
Priority	Setting the port priority
VLAN Rule	
VID	Setting the VID of this group
Join	Add this port into this group
Tag	Mark the out-going packets of this port in this VLAN as tagged or untagged
Save	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values

Table 6 Field definition for Network>VLAN

2.4. DDNS

DDNS stands for Dynamic Domain Name Services. It provides a function to convert the domain name to the unique IP address. With DDNS, users is able to find and connect to CPE no matter what IP address CPE is currently using, that is, DDNS can map CP E's dynamic IP address to a static hostname. The best profit of this function allows user to access CPE from everywhere.

In Figure 17, it demonstrates how to configure DDNS on CPE web page. The definition for each field is shown on Table 7.



DDNS

DDNS Profile

Enable Dynamic DNS	□
Service Provider	dyndns.org(www.dyndns.org)
Service Type	Dynamic
Domain Name	.
Login Name	
Password	
IP Update Policy	Auto Detect
User Defined IP	
Wildcards	□
MX	□
Backup MX	□
MX Host	

Figure 17 Network>DDNS

Name	Description
Enable Dynamic DNS	Click the check box to enable dynamic DNS
Service Provider	Enter the URL of the Service Provider
Service Type*	Enter the service type (DYNDNS only) ● Dynamic ● Static ● Custom
Domain Name	Enter the domain name
Login Name	Enter the username
Password	Enter the password
IP Update Policy	Select the Policy to be used ● Auto Detect ● WAN IP ● User Defined
User Defined IP	If user selects “User Defined” as the IP policy, user has to enter the IP address.
Wildcards*	Allow hostname to use wildcards such as “* ”. It will allow “*host.dyndns.org” to be aliased to the same IP address as “host.hyndns.org”
MX*	Enable mail routing
Back MX*	Enable Second mail routing
MX Host*	Host that mail will be routed to
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Note: * Supported by DYNDNS service provider.

Table 7 Field definition for Network>DDNS

3. Advanced Setting

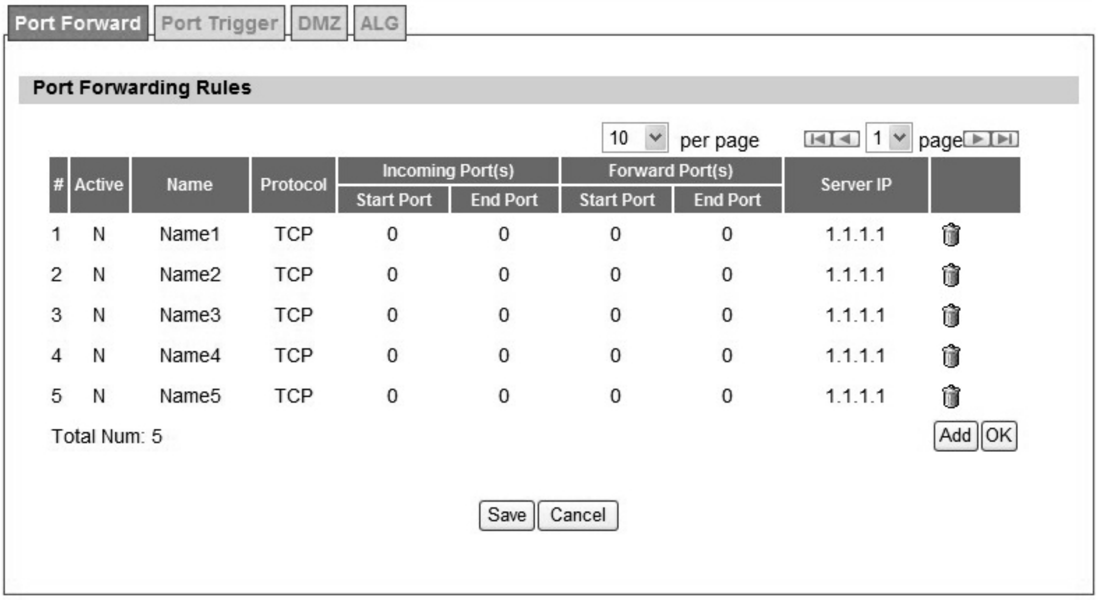
The “Advanced Settings” window will allow user to set rules for incoming and outgoing traffic.

3.1. NAT

Network Address Translation (NAT) is the process of modifying the network address information of the host in a packet while in transit, so that it can be remapped to a given address space in another network. For example, the source address of a packet in a network is changed to a different IP address known within another network.

3.1.1. Port Forward

Port forwarding, as the literal meaning, is the act of forwarding the data from WAN side to the particular port of the private IP. This function can allow remote computers to reach a port on a private IP address within a private LAN. In the following, it will introduce how to setup for Port Forward. First, user needs to click the “Add” button and then select which forward type, TCP or UDP or TCP/UDP, is preferred to trigger the special application as shown in Figure 18. User needs to assign some specific port for the WAN IP to be forwarded to the defined LAN IP and port, and then click the “Save” button to add a Port Forward rule. The definition for each field is shown on Table 8.



Port Forwarding Rules

10 per page   1 page

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP	
				Start Port	End Port	Start Port	End Port		
1	N	Name1	TCP	0	0	0	0	1.1.1.1	🗑
2	N	Name2	TCP	0	0	0	0	1.1.1.1	🗑
3	N	Name3	TCP	0	0	0	0	1.1.1.1	🗑
4	N	Name4	TCP	0	0	0	0	1.1.1.1	🗑
5	N	Name5	TCP	0	0	0	0	1.1.1.1	🗑

Total Num: 5

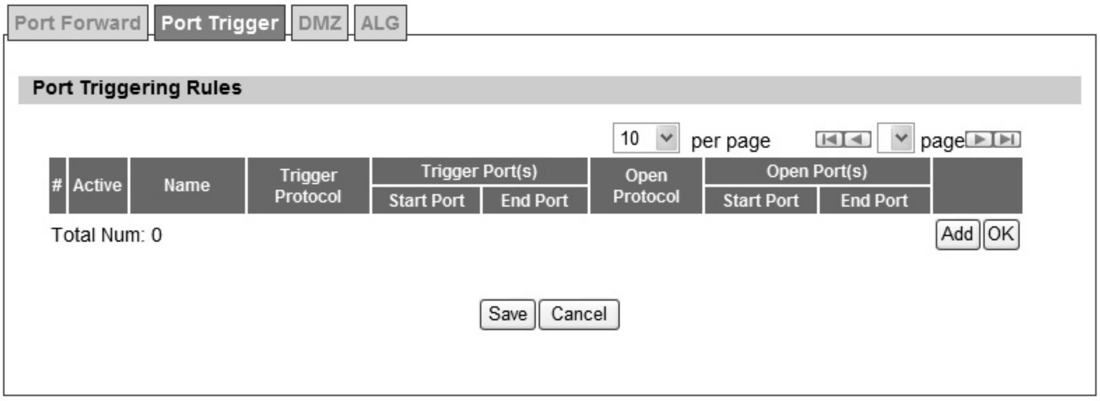
Figure 18 Advanced>NAT>Port Forward

Name	Description
Activate	Check the box to activate the “Port Forward” rule
Name	Name of the Port Forward rule
Protocol	User needs to define the desired protocol for rule. Available options are: TCP, UDP, or TCP/UDP
Incoming Port(s)	User needs to define incoming port range for Port Forwarding rule.
Forward Port(s)	User needs to define to which port range will be translated for Port Forwarding rule. The packet will be forwarded to one of these ports if it matches the rule.
Server IP	User needs to define which IP address will be translated to if it matches the Port Forwarding rule. The packet will be forwarded to this IP address if it matches the rule.
Trash	Delete the Port Forward rule
Add	Click the “Add” button to create a new Port Forward rule
OK	Click the “OK” button to exit table edit mode
Save	Commit the changes made and save to the CPE
Cancel	Reset field to the last saved values.

Table 8 Field definition for Advanced>NAT>Port Forward

3.1.2. Port Trigger

The “Advanced>NAT>Port Trigger” tab allows user to configure Port Trigger rules. Port Trigger is a way to automate port forwarding in which outbound traffic on predetermined ports (‘trigger port’) causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host, while the outbound ports are in use. This allows users behind WiMAX outdoor CPE on the LAN to provide services that would normally require the computer to have IP address on the LAN. Port triggering triggers an open incoming port (‘open port’) when a client on the local network makes an outgoing connection on a predetermined port or range of ports. The definition for each field is shown on Table 9.



Port Triggering Rules

10 per page page

#	Active	Name	Trigger Protocol	Trigger Port(s)		Open Protocol	Open Port(s)		
				Start Port	End Port		Start Port	End Port	

Total Num: 0

Figure 19 Advanced>NAT>Port Trigger

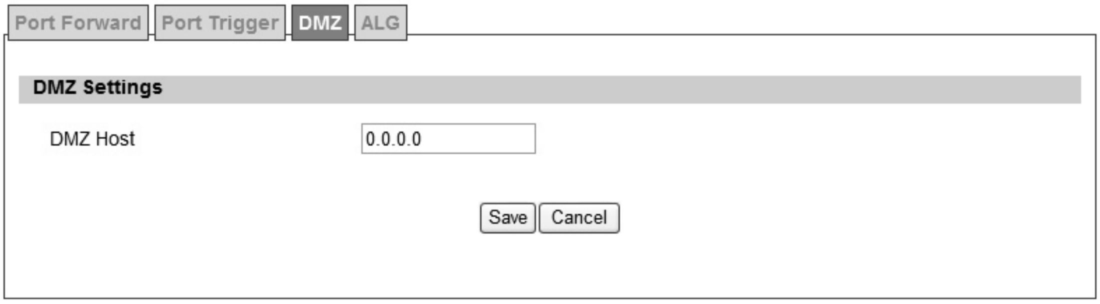
Name	Description
Activate	Check the box to activate the Port Trigger rule
Name	Name of the Port Trigger rule
Protocol	It defines which protocol the outgoing packet used will trigger the rule. Available options are TCP, UDP or TCP/UDP
Trigger Port(s)	It defines which port range the outgoing packet will trigger the rule. User needs to enter the starting and ending port range
Open Protocol	It defines which protocol will be opened if the rule had been triggered. Available options are TCP, UDP or TCP/UDP
Trash	Delete the Port Trigger rule
Add	Click the “Add” button to enter a Port Trigger rule
OK	Click the “OK” button to exit, table edit mode.
Save	Commit the changes made and save to the CPE
Cancel	Reset fields to the last saved vaules

Table 9 Field definition for Advanced>NAT>Port Trigger

3.1.3. DMZ

DMZ stands for Demilitarized Zone. It is a physical or logical sub-network that contains and exposes an organization's external services to a larger un-trusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network. The purpose of a DMZ is to add an additional layer of security to an organization's LAN; an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

The "Advanced>NAT>DMZ" tab allows user to configure a DMZ host IP address as shown in Figure 20. In DMZ Settings, user needs to enter the IP address of the DMZ host. The "Save" button will save the changes to WiMAX outdoor CPE and the "Cancel" button will reset the field to last saved value. It will disable DMZ host when entering "0.0.0.0".



DMZ Settings

DMZ Host 0.0.0.0

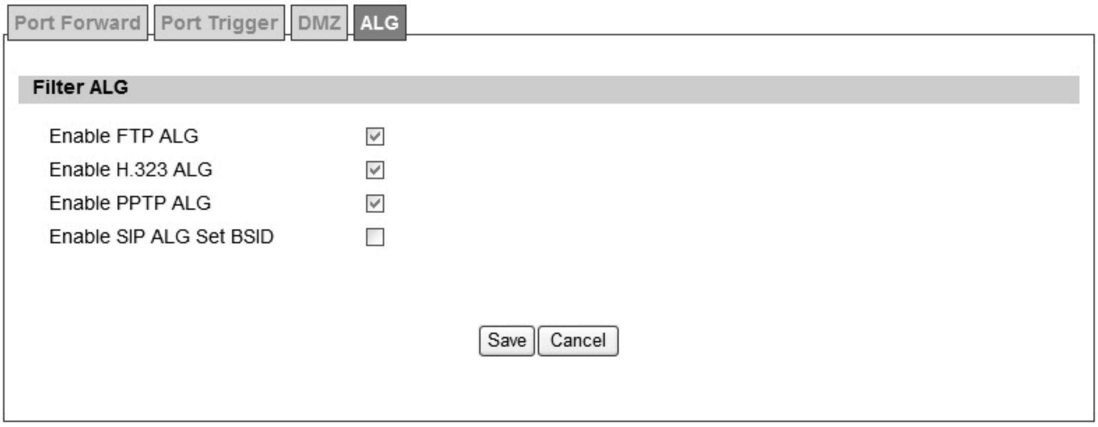
Figure 20 Advanced>NAT>DMZ

3.1.4. ALG

There are three ALGs that user can enable from “Advanced>NAT>ALG” tab. ALG allows legitimate application traffic to pass through the WiMAX outdoor CPE that would have otherwise restricted. Without ALGs, some application may not work well because of NAT/firewall settings. User could click on the check box to enable ALGs.

Note: If user is using any of these types of application protocols user needs to enable them in the ALG settings.

- FTP ALG
- H.323 ALG
- PPTP ALG
- Enable SIP ALG set BSID



Filter ALG

Enable FTP ALG ☑

Enable H.323 ALG ☑

Enable PPTP ALG ☑

Enable SIP ALG Set BSID □

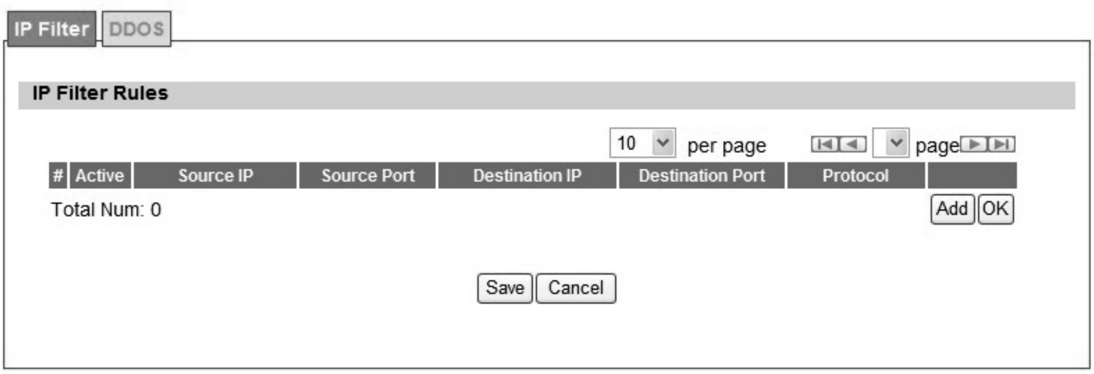
Figure 21 Advanced>NAT>ALG

3.2. Firewall

In networking, firewalls are used to block un-wanted traffic or prevent from DDOS attacks. It will prevent unauthorized devices to enter a trusted network.

3.2.1. IP Filter

The IP filter rules will drop or discard traffic that the filter criteria. User can define IP filter rules as shown in Figure 22. The definition for each field is shown on Table 10.



#	Active	Source IP	Source Port	Destination IP	Destination Port	Protocol	

Total Num: 0

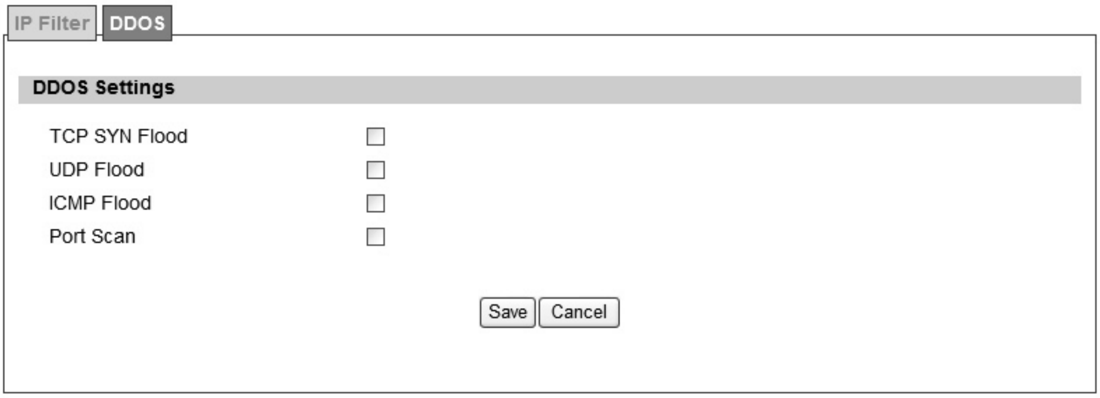
Figure 22 Advanced>Firewall>IP Filter

Name	Description
Add	Click the "Add" button to create a new IP Filter rule
OK	Click the "OK" button will exit the table edit mode
Active	Check the box to activate the IP Filter rule
Source IP	Source IP to filter on. It can be in one of the following formats: IP address (ex. 192.168.0.222) Subnet (ex. 192.168.1.0/24) IP range (ex. 192.168.0.150~192.168.0.160) 0.0.0.0/0 means any
Source Port	Source Port to filter on. It can be one of the following formats: Port number (ex. 8080) Port Range (ex. 1024~2048)
Destination IP	Destination IP to filter on. It can be in one of the following formats: IP address (ex. 192.168.0.222) Subnet (ex. 192.168.1.0/24) IP range (ex. 192.168.0.150~192.168.0.160) 0.0.0.0/0 means any
Destination Port	Destination port to filter on. It can be one of the following formats: Port number (ex. 8080) Port Range (ex. 1024~2048)
Protocol	Protocol to filter on
Trash	Delete the IP Filter rule
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 10 Field definition for Advanced> Firewall>IP Filter

3.2.2. DOS

Before taking about the DDOS service, it will introduce DDOS Attack first. DDOS attack stands for denial-of-service attack (DoS attack) or distributed denial-of-service attack. It is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the targeted machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. DDOS service here is used to prevent DDOS Attack, and it provides TCP SYN Flood, UDP Flood, ICMP Flood, and Port Scan for selection. The definition for each field is shown on Table 11.



DDOS Settings

TCP SYN Flood □
UDP Flood □
ICMP Flood □
Port Scan □

Figure 23 Advanced>Firewall>DDOS

Name	Description
TCP SYN Flood	It will prevent SYN flood from WAN or LAN
UDP Flood	It will prevent UDP flood to WiMAX outdoor CPE
ICMP Flood	It will prevent ICMP flood from WAN or LAN
Port Scan	It will prevent port scanning from WAN and issue an alarm entry in the system log.
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values.

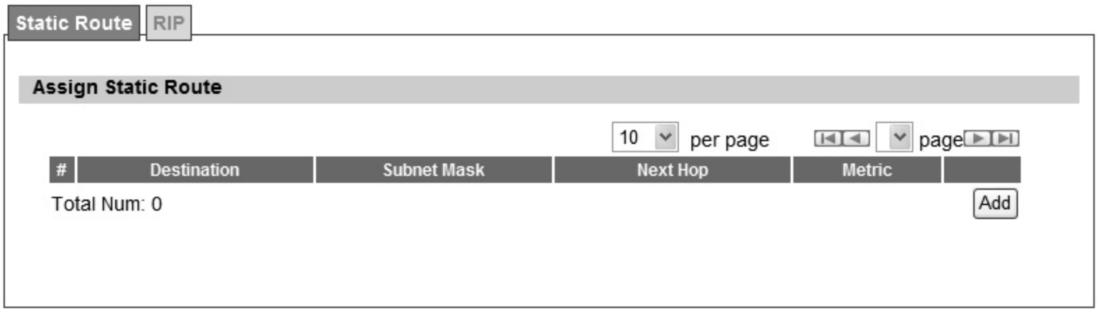
Table 11 Field definition for Advanced> Firewall>DDOS

3.3. Route

A route is a path in a network, which can direct the flow of network traffic.

3.3.1. Static Route

The static route is a hard coded path in the router that specifies how it will get to a certain subnet by using a defined path. User could manually add routes to routing table as shown in Figure 24 and Figure 25. The definition for each field is shown on Table 12.



Static Route RIP

Assign Static Route

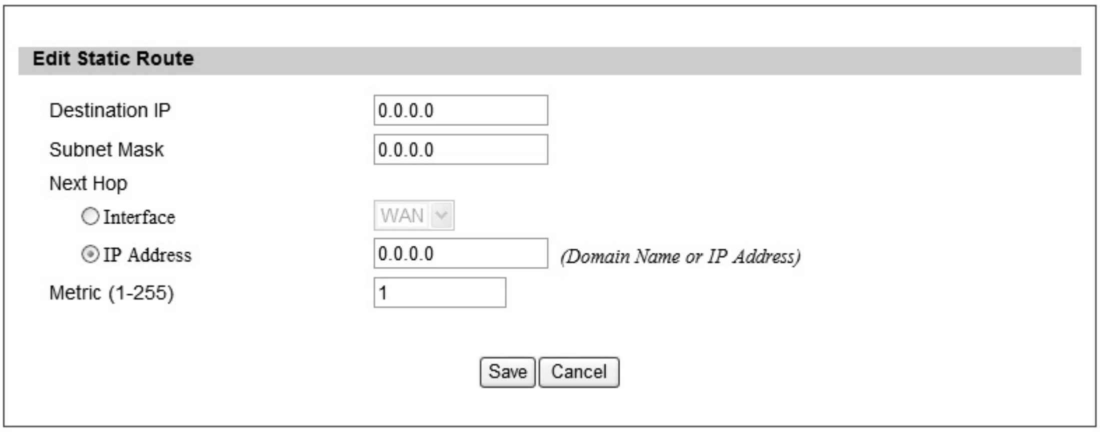
10 per page page

#	Destination	Subnet Mask	Next Hop	Metric	

Total Num: 0

Add

Figure 24 Advanced>Route>Static Route



Edit Static Route

Destination IP	0.0.0.0
Subnet Mask	0.0.0.0
Next Hop	
○ Interface	WAN
● IP Address	0.0.0.0 *(Domain Name or IP Address)*
Metric (1-255)	1

Save Cancel

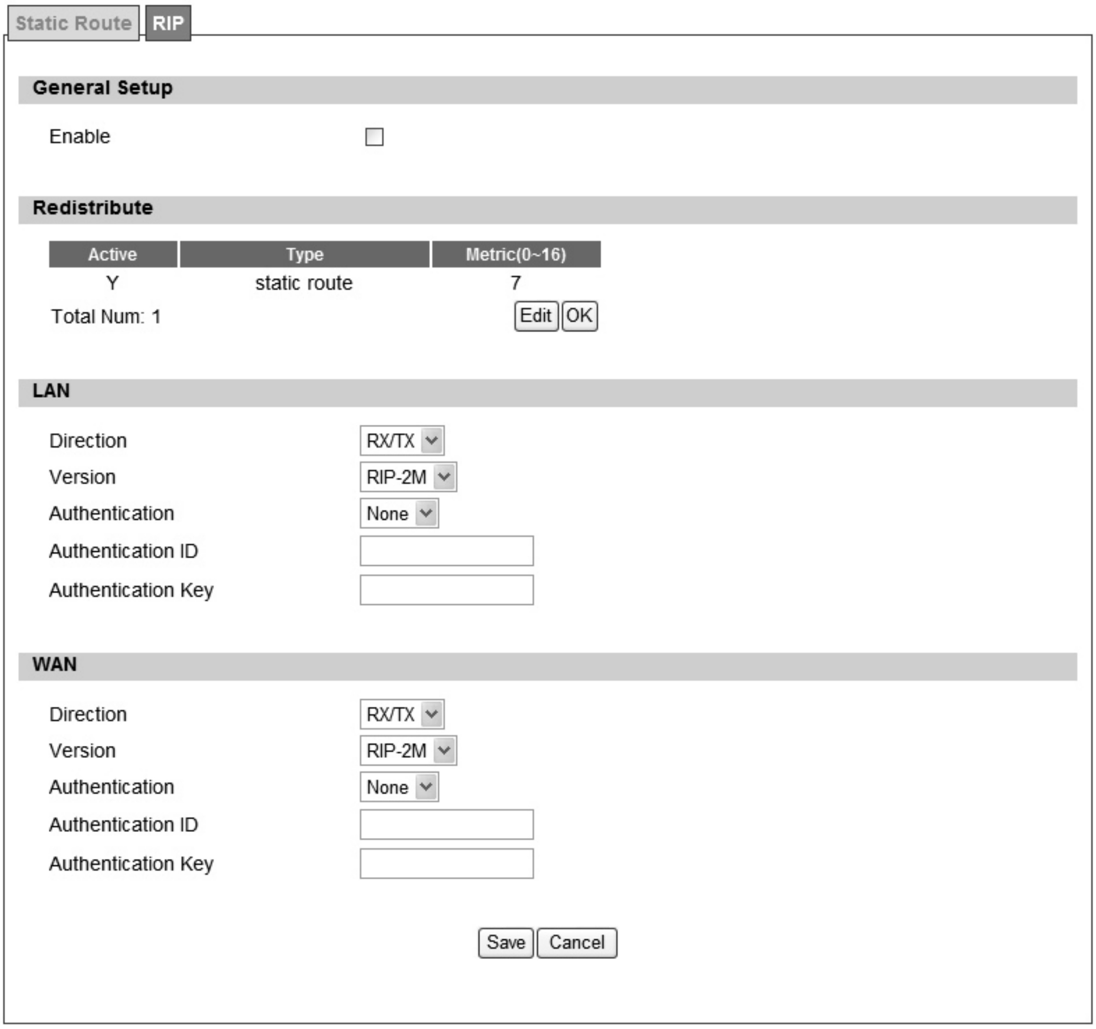
Figure 25 Advanced>Route>Static Route>Add

Name	Description
Destination IP	Enter the Destination IP address user would like to reach
Subnet Mask	Enter the subnet mask.
Next Hop	Select where the next hop will be. ● WAN or LAN interface directly ● IP Address
Metric	Enter the metric value, “cost” of transmission for routing purposes
Trash	Will remove the selected route
Add	Will enter in edit mode to add a static route
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 12 Field definition for Advanced>Route>Static Route

3.3.2. RIP

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local area networks. It allows a router to exchange routing information with other routers. User could setup the RIP routing rule as shown in Figure 26. The definition for each field is shown on Table 13.



General Setup

Enable □

Redistribute

Active	Type	Metric(0~16)
Y	static route	7

Total Num: 1

LAN

Direction	RX/TX
Version	RIP-2M
Authentication	None
Authentication ID	
Authentication Key	

WAN

Direction	RX/TX
Version	RIP-2M
Authentication	None
Authentication ID	
Authentication Key	

Figure 26 Advanced>Route>RIP

Name	Description
General Setup | Enable	Clicking the enable check box will activate the RIP routing rule
Redistribute Edit	Click the “Edit” button to activate the static route or change the metric value. The static route refers to the static routes defined in Advanced>Route>Static Route window
Redistribute | OK	Click the “OK” button to exit edit table mode
LAN	
Direction	● None ● RX ● TX ● RX/TX
Version	If user selects “RX, TX or RX/TX” for Direction, user will get the following RIP version options available. ● RIP-1 ● RIP-2B ● RIP-2M
Authentication	If user selects RIP-2B or RIP-2M for Version, user will get the following Authentication options. ● None ● Text ● MD5
Authentication ID	If user selects “MD5” for Authentication type, user can enter the authentication ID and Key
Authentication Key	If user enters “text” for Authentication, user can enter a text authentication key. If user enters “MD5” for Authentication type, user also needs to enter an Authentication ID and Key.
WAN	
Direction	● None ● RX ● TX ● RX/TX
Version	If user selects “RX, TX or RX/TX” for Direction, user will get the following RIP version options available. ● RIP-1 ● RIP-2B ● RIP-2M

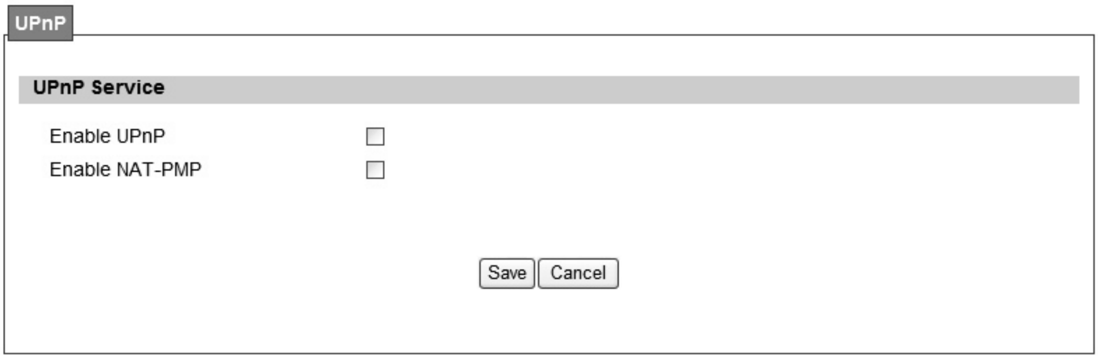
Name	Description
Authentication	If user select s RIP-2B or RIP-2M for V ersion, user will get the following Authentication options. ● Non e ● Te xt ● MD5
Authentication ID	If user sele cts “MD5” for Authentication type, user can ente r the authentication ID and Key
Authentication Key	If user enters “text” for Authentication, user ca n enter a text authentication key. If user enters “MD5” for Authenti cation type, user also needs to enter an Authentication ID and Key.
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 13 Field definition for Advanced>Route>RIP

3.4. UPnP

Two methods of simplifying the process of connecting a device to the network are available as shown in Figure 27. UPnP allows devices to connect seamlessly to networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. NAT Port Mapping Protocol (NAP-PMP) allows a computer in a privae network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact itself. The definition for each field of UPnP Setting is shown on Table 14.

3.4.1. UPnP Setting



UPnP

UPnP Service

Enable UPnP □

Enable NAT-PMP □

Figure 27 Advanced UPnP

Name	Description
Enable UPnP	Check the check box to enable UPnP
Enable NAT-PMP	Check the check box to enable NAT-PMP
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 14 Field definition for Advanced> UPnP

3.5. IGMP Proxy

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interface. The system acts as a proxy for its hosts.

3.5.1. IGMP Proxy Setting

Internet Group Management Protocol (IGMP) proxy can be used to implement multicast routing. It works by IGMP frame forwarding, and commonly is used when there is no need to use more advanced protocol, for example PIM. In WiMAX outdoor WiMAXx CPE, it provides IGMP Proxy function, and user can enable or disable this function from Web page as shown in Figure 28.

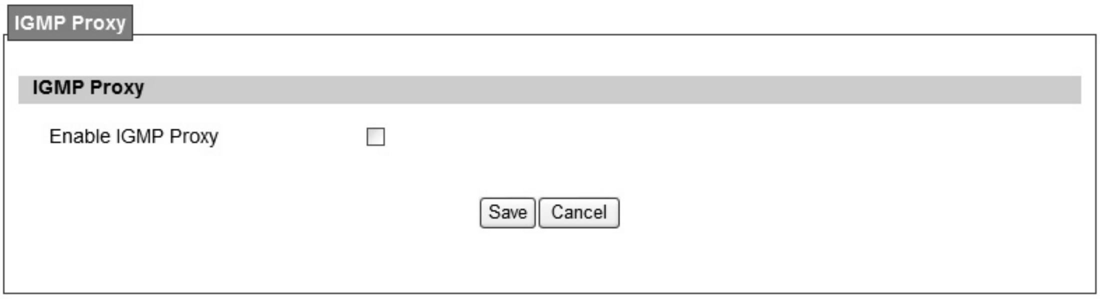


Figure 28 Advanced>IGMP Proxy

Name	Description
Enable IGMP Proxy	Check the check box to enable IGMP Proxy
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset field to the last saved values

Table 15 Field definition for Advanced>IGMP Proxy

3.5.2. VPN Setting

VPN (Virtual Private Network) is a network that is implemented in an additional software layer on top of an existing larger network for the purpose of providing a secure extension of a private network into an insecure network such as the Internet. The links between nodes of a VPN are formed over logical connections or virtual circuits between hosts of the larger network.

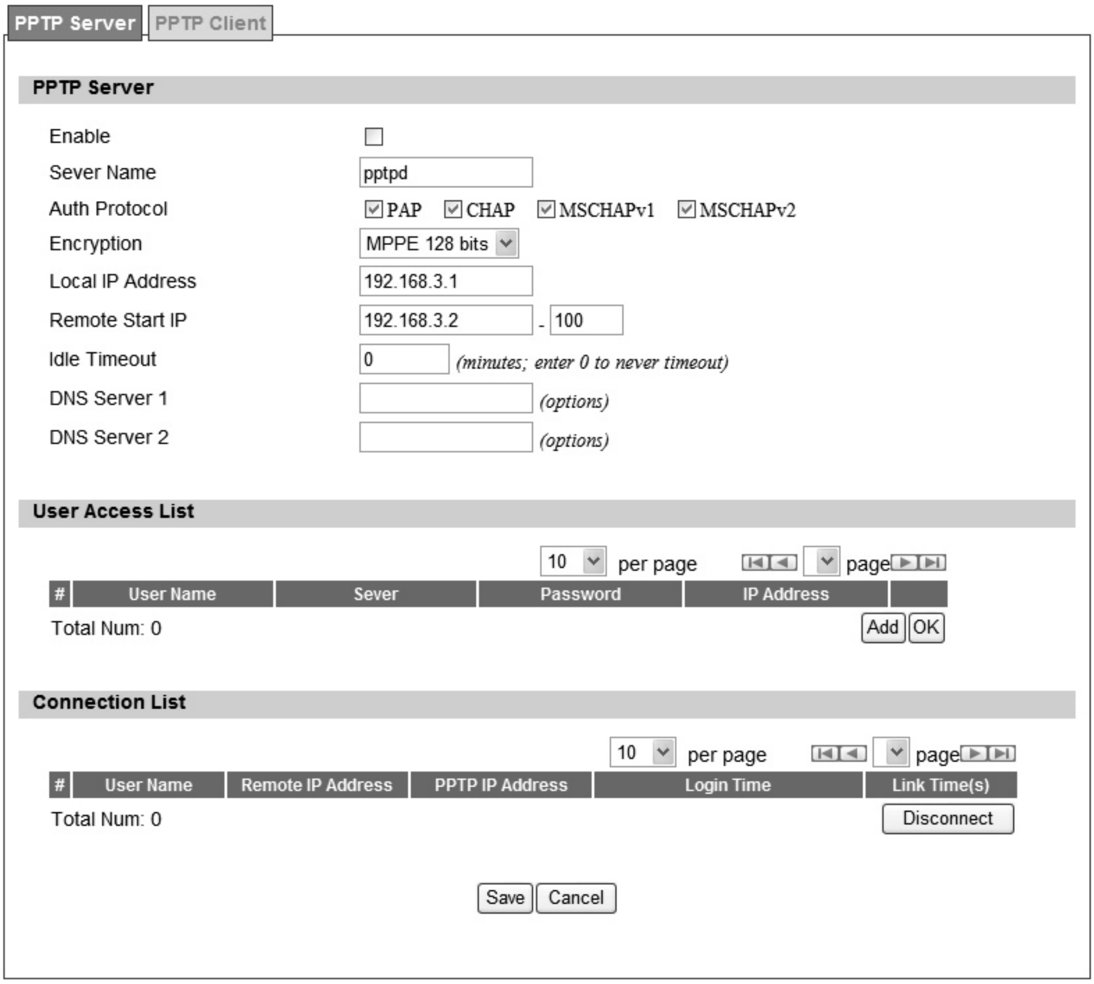
VPNs are often installed by organizations to provide remote access to a secure organizational network. Generally, a VPN has a network topology more complex than a point-to-point connection. VPNs are also used to mask the IP address of individual computers within the Internet in order, for instance, to surf the World Wide Web anonymously or to access location restricted services, such as Internet television. Here, VPN Settings allow user to set rules for VPN, and it supports PPTP, L2TP, and IPsec.

3.6. PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP does not provide confidentiality or encryption; it relies on the protocol being tunneled to provide privacy.

3.6.1. PPTP Server

A PPTP Server (Point -To-Point Tunneling Protocol) allows user to connect securely from a place (such as the house) to a LAN located in another location, such as the office. This way user can use the services provided in the office at the comfort of the house. The definition for each field of PPTP Server is shown on Table 16.



PPTP Server

Enable □

Sever Name: pptpd

Auth Protocol: ☑ PAP ☑ CHAP ☑ MSCHAPv1 ☑ MSCHAPv2

Encryption: MPPE 128 bits

Local IP Address: 192.168.3.1

Remote Start IP: 192.168.3.2 - 100

Idle Timeout: 0 *(minutes; enter 0 to never timeout)*

DNS Server 1: *(options)*

DNS Server 2: *(options)*

User Access List

10 per page page

#	User Name	Sever	Password	IP Address	

Total Num: 0

Connection List

10 per page page

#	User Name	Remote IP Address	PPTP IP Address	Login Time	Link Time(s)

Total Num: 0

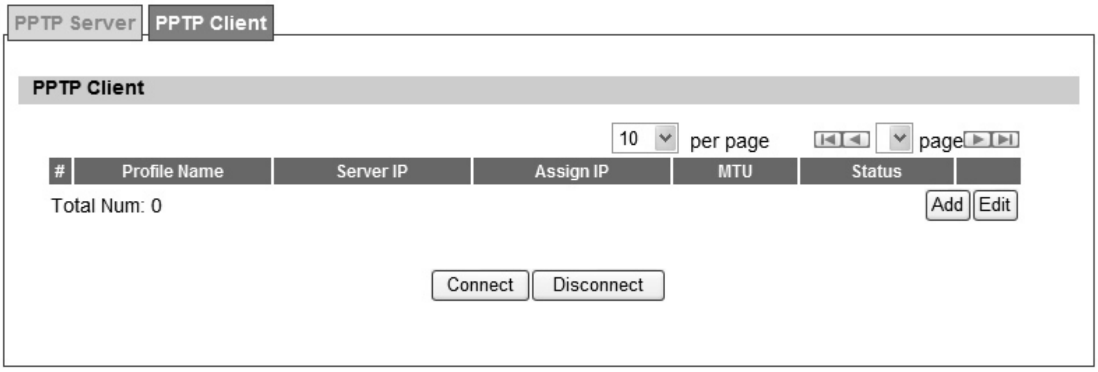
Figure 29 VPN>PPTP>Server

Name	**Description**
PPTP Server	
Enable	● Activate PPTP server.
Server Name	● Offer a service name
Auth Protocol	Require the peer to authenticate itself before allowing network packets to be sent or received. We support the following protocol: ● PAP: Password Authentication Protocol ● CHAP: Challenge Handshake Authentication Protocol ● MSCHAP: Microsoft Challenge Handshake Authentication Protocol ● MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol, Version 2
Encryption	Encryption Scheme: None MPPE 40 bits: 40-bit encryption with MPPE MPPE 128 bits: 128-bit encryption with MPPE Auto: automatically select
Local IP Address	The IP of router
Remote Start IP	As sessions are established, IP addresses are assigned starting from “Remote Start IP”
Idle Timeout	Disconnect if the link is idle for the assigned seconds
DNS Server 1	The primary DNS (Domain Name Server) addresses to clients
DNS Server 2	The secondary DNS (Domain Name Server) addresses to clients
User Access List	
User name	User ID to connect PPTP server via the selected Auth Protocol
Server	Server protocol type
Password	Password to connect PPTP server via the selected Auth Protocol
IP address	IP address of the connected client
Connection List	
User name	The user name of the connection
Remote IP address	The peer address of the connection
PPTP IP address	The assigned IP address of PPTP
Login Time	The time of the connection created
Link Time(s)	Timer from the connected time
Save	Commit the changes made and save to the CPE
Cancel	Reset fields to the last saved values

Table 16 Field definition for VPN>PPTP>Server

3.6.2. PPTP Client

User could setup PPTP Client as shown in Figure 30 and Figure 31. The definition for each field of PPTP Client is shown on Table 17.

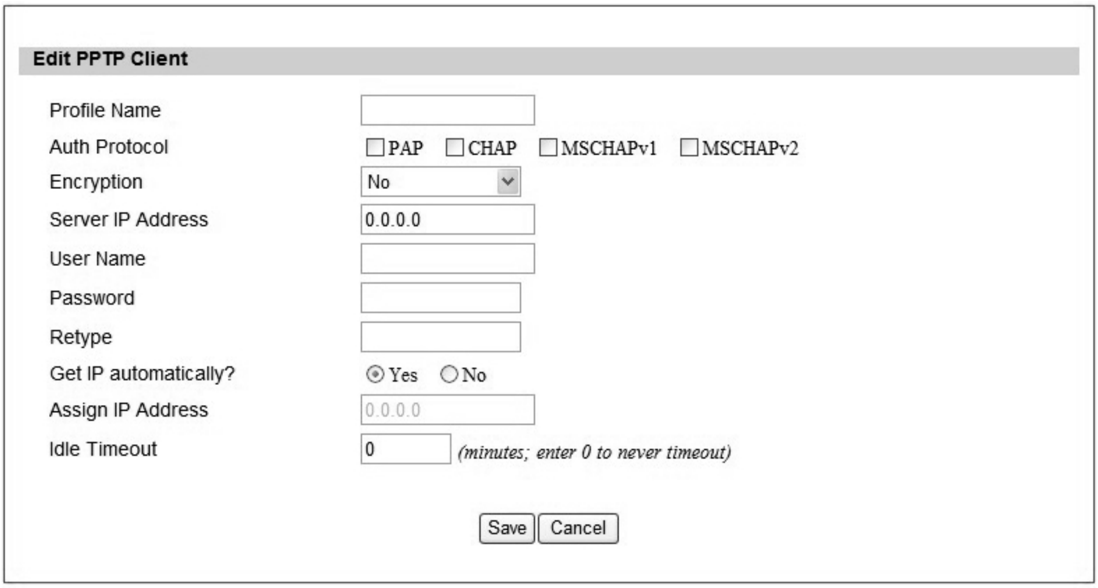


PPTP Client

#	Profile Name	Server IP	Assign IP	MTU	Status	

Total Num: 0

Figure 30 VPN>PPTP>Client



Edit PPTP Client

Profile Name	
Auth Protocol	□ PAP □ CHAP □ MSCHAPv1 □ MSCHAPv2
Encryption	No
Server IP Address	0.0.0.0
User Name	
Password	
Retype	
Get IP automatically?	● Yes ○ No
Assign IP Address	0.0.0.0
Idle Timeout	0 *(minutes; enter 0 to never timeout)*

Figure 31 VPN>PPTP>Client>Add

Name	Description
PPTP Client	
Add	Add a new connection setting
Edit	Edit the existed connection setting
Edit PPTP Client	
Profile Name	The name for this connection setting
Auth Protocol	The Authentication protocol of the peer required. Select which Authentication protocol to use. ● PAP ● CHAP ● MSCHAPv1 ● MSCHAPv2
Encryption Enc	ryption scheme
Server IP Address	The IP address of PPTP server
Username	The user ID to connect PPTP server via the selected Auth Protocol
Password	The password of the corresponding user ID
Retype	Type the “Password” again
Get IP automatically?	Obtain the dynamic IP address, assigned by the PPTP server
Assign IP Address	Assign the static IP address for this connection setting
Idle Timeout	Disconnect if the link is idle for the assigned seconds
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 17 Field definition for VPN>PPTP>Client

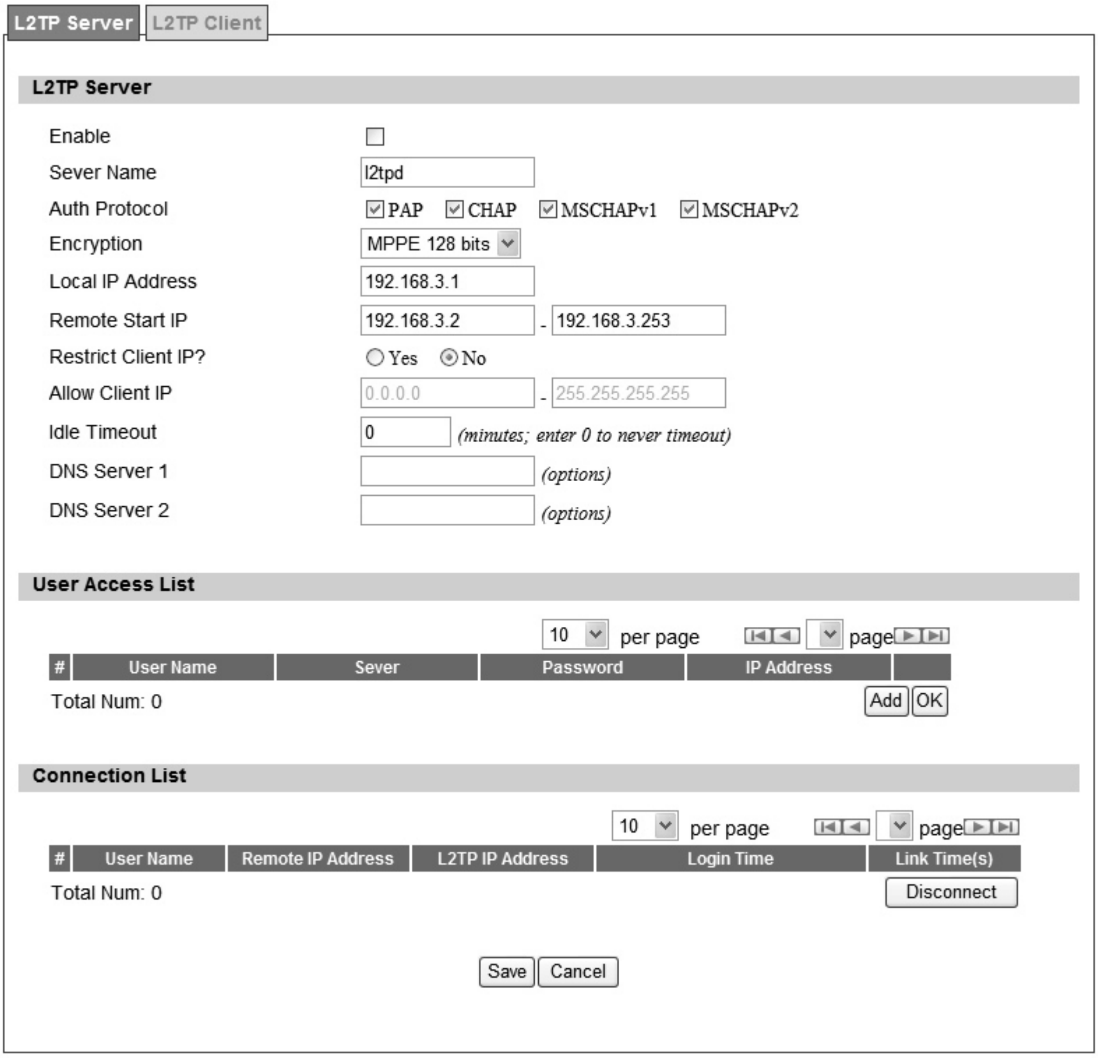
3.6.3. L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself. It relies on an encryption protocol that it passes within the tunnel to provide privacy. The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. It is common to carry Point-to-Point Protocol (PPP) session within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity.

Above is based on information from Wikipedia (http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol)

3.6.4. L2TP Server

User can setup WiMAX outdoor CPE from web page as shown in Figure 32. The definition for each field of PPTP Server is shown on Table 18.



L2TP Server

Enable	□
Sever Name	l2tpd
Auth Protocol	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☑ MSCHAPv2
Encryption	MPPE 128 bits
Local IP Address	192.168.3.1
Remote Start IP	192.168.3.2 - 192.168.3.253
Restrict Client IP?	○ Yes ● No
Allow Client IP	0.0.0.0 - 255.255.255.255
Idle Timeout	0 *(minutes; enter 0 to never timeout)*
DNS Server 1	*(options)*
DNS Server 2	*(options)*

User Access List

#	User Name	Sever	Password	IP Address	

Total Num: 0

Connection List

#	User Name	Remote IP Address	L2TP IP Address	Login Time	Link Time(s)

Total Num: 0

Figure 32 VPN>L2TP>Server

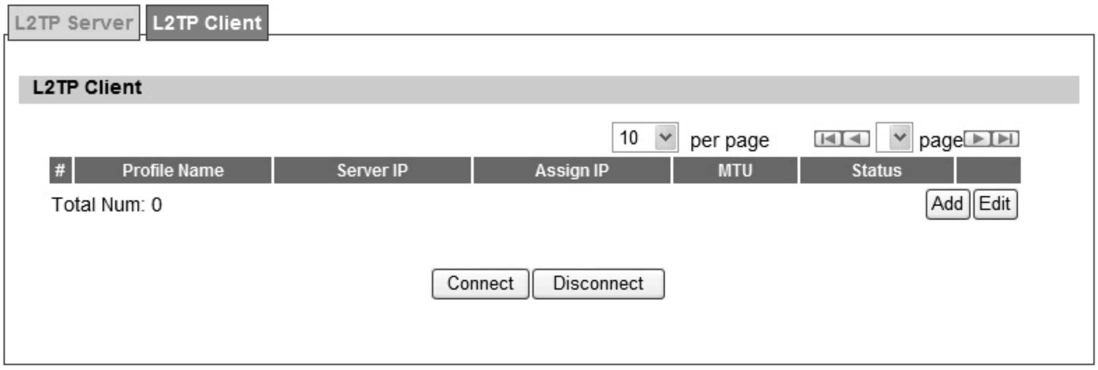
Name	**Description**
L2TP Server	
Enable	Check the check box to activate L2TP server.
Server Name	Enter a service name
Support Protocol	The supported protocol of L2TP messages
Version	● ALL: L2TPv2 and L2TPv3 ● 2: L2TPv2 only ● 3: L2TPv3 only
Auth Protocol	Require the peer to authenticate itself before allowing network packets to be sent or received. The following protocols are supported: ● PAP: Password Authentication Protocol ● CHAP: Challenge Handshake Authentication protocol ● MSCHAP: Microsoft Challenge Handshake Authentication Protocol ● MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol, Version 2
Encryption	Encryption Scheme ● None ● MPPE 40 bits: 40-bit encryption with MPPE ● MPPE 128 bits: 128-bit encryption with MPPE ● Auto: automatically select
Local IP Address	The IP of router
Remote Start IP	As sessions are established, IP addresses are assigned starting from “Remote Start IP”
Restrict Client IP?	To restrict client IP address range for the client
Allow Client IP	The IP address range for the client
Idle Timeout	Disconnect if the link is idle for the given number of seconds
DNS Server 1	The primary DNS (Domain Name Server) addresses to the clients
DNS Server 2	The secondary DNS (Domain Name Server) addresses to the clients
User Access List	
User Name	User ID to connect L2TP server via the selected Auth Protocol
Server	Server Protocol type
Password	Password to connect L2TP server via the selected Auth Protocol
IP Address	IP address of the connected client

Name	Description
Connection List	
User Name	The user name of the connection
Remote IP Address	The peer address of the connection
PPTP IP Address	The assigned IP address of L2TP
Login Time	The time of the connection created
Link Time(s)	Elapsed time connected
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 18 Field definition for VPN>L2TP>Server

3.6.5. L2TP Client

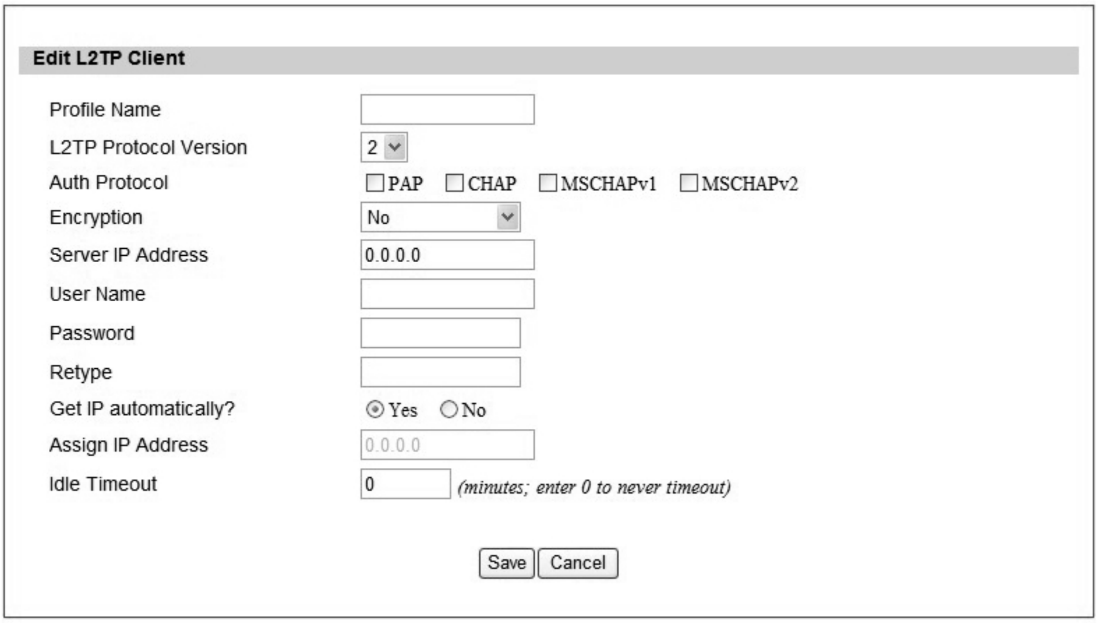
User could setup PPTP Client as sh own in Fi gure 33 and Figu re 34. The definition for each field of PPTP Client is shown on Table 19.



#	Profile Name	Server IP	Assign IP	MTU	Status	

Total Num: 0

Figure 33 VPN>L2TP>Client



Profile Name	
L2TP Protocol Version	2
Auth Protocol	□ PAP □ CHAP □ MSCHAPv1 □ MSCHAPv2
Encryption	No
Server IP Address	0.0.0.0
User Name	
Password	
Retype	
Get IP automatically?	● Yes ○ No
Assign IP Address	0.0.0.0
Idle Timeout	0 *(minutes; enter 0 to never timeout)*

Figure 34 VPN>L2TP>Client>Add

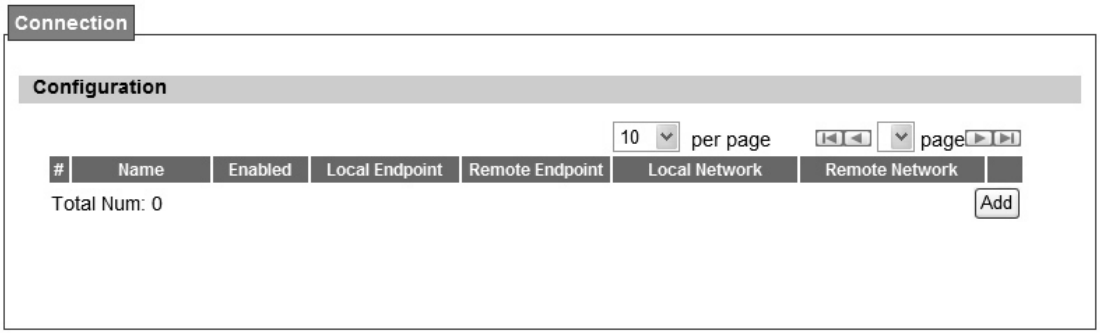
Name	Description
L2TP Client	
Add	Add a new connection setting
Edit	Edit the existed connection setting
Edit L2TP Client	
Profile Name	The name of this connection setting
L2TP Protocol Version	The message of L2TP protocol version for this connection setting ● 2 ● 3
NAT Mode	Enable or disable NAT when connected to PPTP server ● Yes: enable ● No: disable
Auth Protocol	The Authentication Protocol of the peer required. Select which Authentication protocol to use. ● PAP ● CHAP ● MSCHAPv1 ● MSCHAPv2
Encryption Enc	ryption Scheme
Server IP Address	The IP address of L2TP server
Username	The username to connect L2TP server via the selected Auth Protocol
Password	The password of the corresponding username
Retype	Type the “Password” again
Get IP Automatically?	Obtain the dynamic IP address, assigned by the L2TP server
Assign IP Address	Assign the static IP address for this connection setting
Idle Timeout	Disconnect if the link is idle for the assigned seconds
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 19 Field definition for VPN>L2TP>Client>Add

3.7. IPSec

Internet Protocol Security (IPsec) is an end-to-end security solution and operated at the IP Layer. It provides secure communication between pairs of hosts, pairs of security gateways or between security gateways and a host. It’s based on a suite of protocols for securing IP traffic by authenticating and encrypting each IP packet of the data stream.

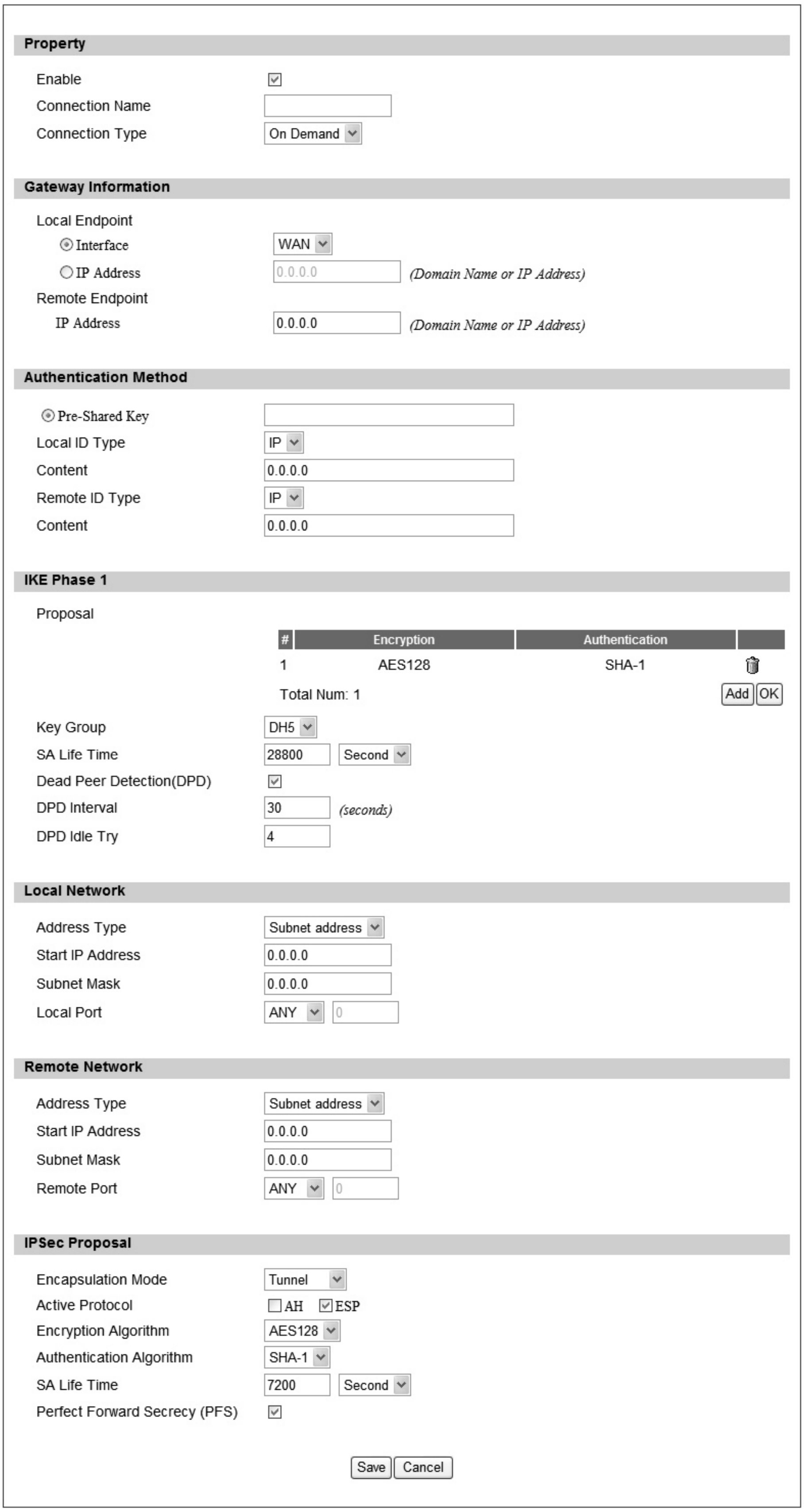
3.7.1. Connection



#	Name	Enabled	Local Endpoint	Remote Endpoint	Local Network	Remote Network	

Total Num: 0

Figure 35 VPN>IPsec Overview



Property

Enable ☑

Connection Name

Connection Type: On Demand

Gateway Information

Local Endpoint

● Interface: WAN

○ IP Address: 0.0.0.0 *(Domain Name or IP Address)*

Remote Endpoint

IP Address: 0.0.0.0 *(Domain Name or IP Address)*

Authentication Method

● Pre-Shared Key

Local ID Type: IP

Content: 0.0.0.0

Remote ID Type: IP

Content: 0.0.0.0

IKE Phase 1

Proposal

#	Encryption	Authentication	
1	AES128	SHA-1	🗑

Total Num: 1

Add OK

Key Group: DH5

SA Life Time: 28800 Second

Dead Peer Detection(DPD) ☑

DPD Interval: 30 *(seconds)*

DPD Idle Try: 4

Local Network

Address Type: Subnet address

Start IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Local Port: ANY 0

Remote Network

Address Type: Subnet address

Start IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Remote Port: ANY 0

IPSec Proposal

Encapsulation Mode: Tunnel

Active Protocol: □ AH ☑ ESP

Encryption Algorithm: AES128

Authentication Algorithm: SHA-1

SA Life Time: 7200 Second

Perfect Forward Secrecy (PFS) ☑

Save Cancel

Figure 36 VPN>IPsec>Add

Name	**Description**
Add	Click the "Add" button to add an IPsec connection rule
Property	
Enable	Enable IPsec connection.
Connection Name	The name of the connection
Connection Type	Select the connection type ● Initiator ● On Demand ● Responder
Gateway Information	
Local Endpoint Interface	The interface of the WiMAX outdoor CPE public-network interface
Local Endpoint IP Address	The IP address or Domain Name of the WiMAX outdoor CPE public-network interface
Remote Endpoint IP Address	The IP address or Domain Name of the remote peer.
Authentication Method	
Pre-Shared Key	The pre-share key that two security gateways use to authenticate
Local ID Type	States how the WiMAX outdoor CPE should be identified for authentication ● IP: The WiMAX outdoor CPE is identified by the assigned IP for authentication. The default value is 0.0.0.0.
Content	The IP address
Remote ID Type	States how the remote peer should be identified for authentication ● IP: The remote peer is identified by the assigned IP for authentication. The default value is 0.0.0.0, and this means WiMAX outdoor CPE will accept any IP.
Content	The IP address
IKE Phase 1	

Name	Description
Proposal Add	Press the Add button to enter an Encryption and Authentication algorithm Click the trash to remove the selected algorithm. Encryption Algorithm: ● DES ● 3DES ● AES128 ● AES192 ● AES256 Authentication Algorithm: ● MD5 ● SHA-1
Proposal OK	Click the OK button to exit the table edit mode
Key Group	The DH group used to negotiate the IKE/ISAKMP SA.
SA Life Time	The period that the keying channel of a connection (IKE/ISAKMP SA) should last before being renegotiated.
Dead Peer Detection (DPD)	Enable or disable the Dead Peer Detection protocol (RFC 3706)
DPD Interval	The time interval when R_U_THERE messages are sent to the peer.
DPD Idle Try	The retry counter for DPD. The timeout interval is "DPD interval" multiplied by "DPD Idle Try". After the timeout interval all connections to the peer are deleted if they are inactive.
Local Network	The private subnet behind the WiMAX outdoor CPE.
Address Type	Single Address: The private subnet consisting of one IP address. Subnet address: The private subnet consisting within the subnet IP addresses.
Start IP Address	The only IP address allowed in the subnet
Subnet Mask	The netmask of the subnet (Subnet address)
Local Port	Restrict the traffic selector to a single protocol and/or port. ● Any: No restriction ● ICMP: Restrict the traffic selector to ICMP protocol. ● TCP: Restrict the traffic selector to TCP protocol. If the port number is 0, all TCP port numbers are accepted. ● UDP: Restrict the traffic selector to UDP protocol. If the port number is 0, all UDP port numbers are accepted.
Remote Network	The private subnet behind the remote peer.
Address Type	Single Address: The private subnet consisting of one IP address. Subnet address: The private subnet consisting of subnet IP addresses.

Name	Description
Start IP Address	The only IP address allowed in the subnet
Subnet Mask	The netmask of the subnet (Subnet address)
Remote Port	Restrict the traffic selector to a single protocol and/or port. ● Any: No restriction ● ICMP: Restrict the traffic selector to ICMP protocol. ● TCP: Restrict the traffic selector to TCP protocol. If the port number is 0, all TCP port numbers are accepted. ● UDP: Re strict t he t raffic selector to UDP protoco l. If the port number is 0, all UDP port numbers are accepted.
IPSec Proposal	
Encapsulation Mode	The type of the connection: ● Tunnel: signifying a host-to-host, host-to-subnet, or subnet-to subnet tunnel. ● Transport: signifying host-to-host transport made.
Active Protocol	Whether authentication should be done as part of ESP encryption and/or separately using the AH protocol.
Encryption Algorithm	● NULL ● AES128 ● AES192 ● AES256 ● DES ● 3DES
Authentication Algorithm	● MD5 ● SHA-1
SA Life Time	The time interval a particular instance of a connection (a set of encryption/authentication key for user packets) should last, from successful negotiation to expiry.
Perfect Forward Secrecy (PFS)	Whether Perfect Forward Secrecy of keys is desired on the connection's keying channel.
Save	Commit the changes made and save to the CPE device
Cancel	Reset fields to the last saved values.

Table 20 Field definition for VPN>IPsec>Add

4. WiMAX

This technology is based on the IEEE 802.16 standard, enabling the delivery of last mile wireless broadband access.

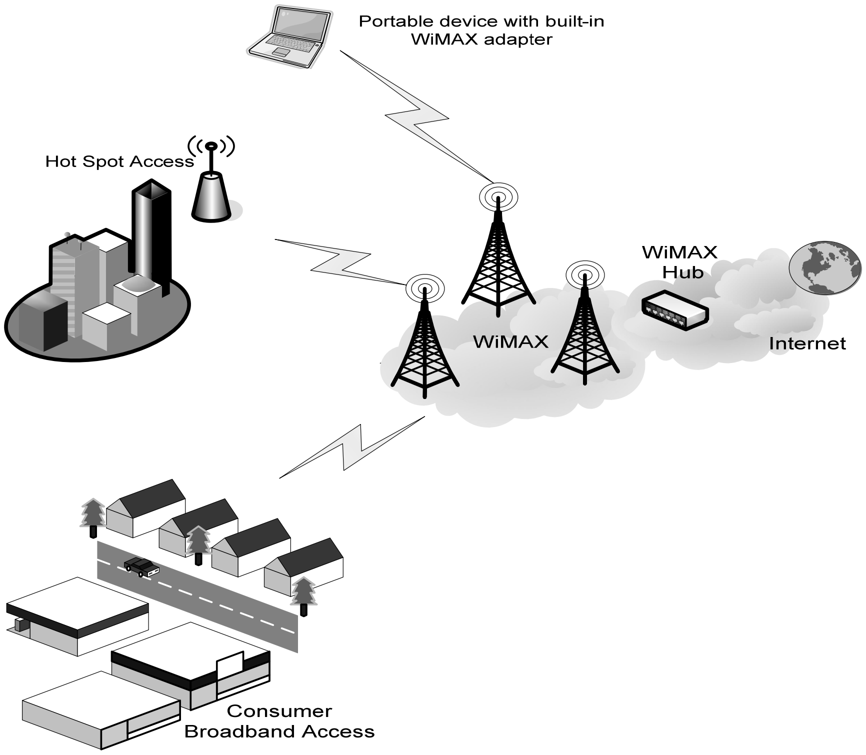
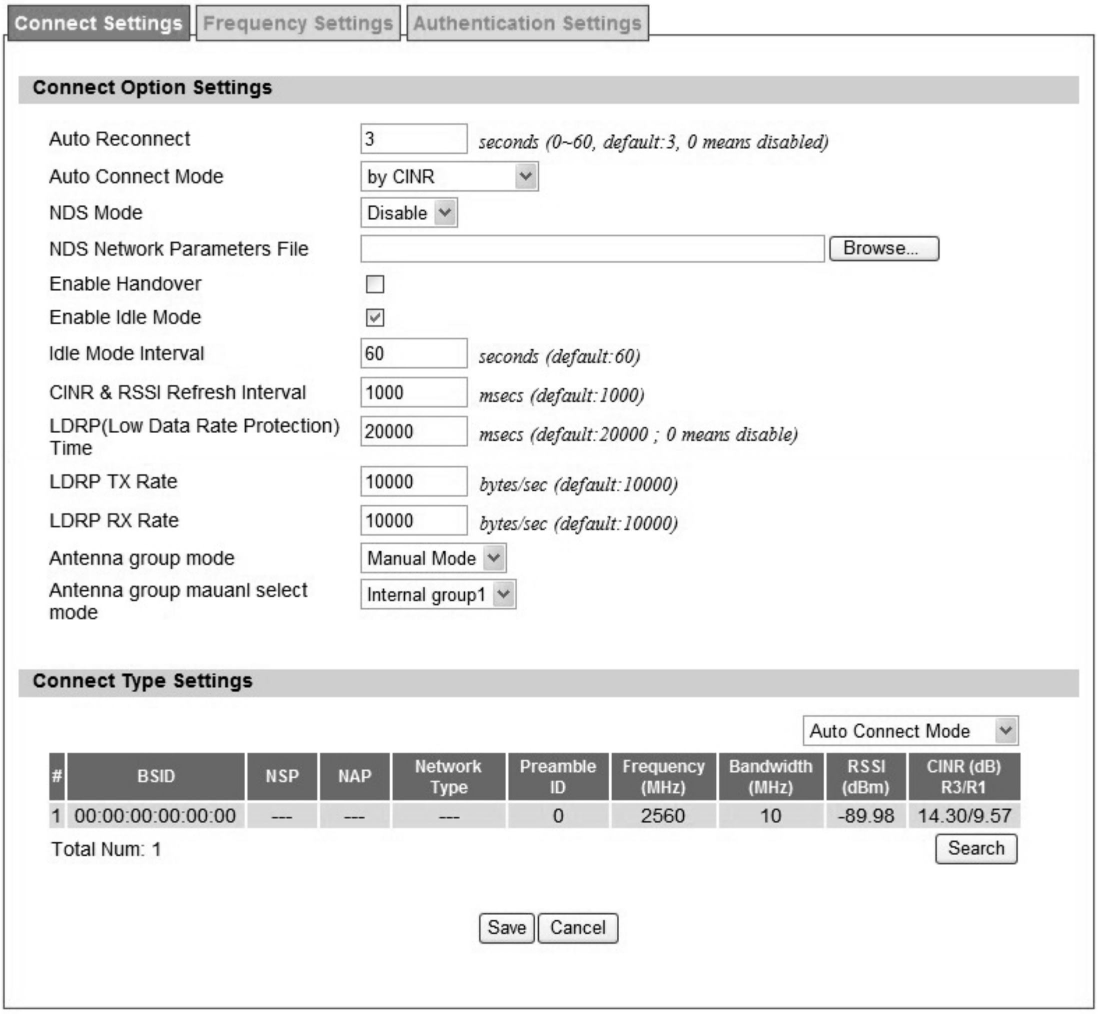


Figure 37 Wireless Broadband Access

4.1. Profile

In the profile tab, the user can set WiMAX standard settings, which include how to establish a connection, frequency information and how to authenticate.

4.1.1. Connect Settings



Connect Option Settings

Auto Reconnect	3	*seconds (0~60, default:3, 0 means disabled)*
Auto Connect Mode	by CINR	
NDS Mode	Disable	
NDS Network Parameters File	Browse...	
Enable Handover	☐	
Enable Idle Mode	☑	
Idle Mode Interval	60	*seconds (default:60)*
CINR & RSSI Refresh Interval	1000	*msecs (default:1000)*
LDRP(Low Data Rate Protection) Time	20000	*msecs (default:20000 ; 0 means disable)*
LDRP TX Rate	10000	*bytes/sec (default:10000)*
LDRP RX Rate	10000	*bytes/sec (default:10000)*
Antenna group mode	Manual Mode	
Antenna group mauanl select mode	Internal group1	

Connect Type Settings

Auto Connect Mode

#	BSID	NSP	NAP	Network Type	Preamble ID	Frequency (MHz)	Bandwidth (MHz)	RSSI (dBm)	CINR (dB) R3/R1
1	00:00:00:00:00:00	---	---	---	0	2560	10	-89.98	14.30/9.57

Total Num: 1

Figure 38 WiMAX>Profile>Connect Settings

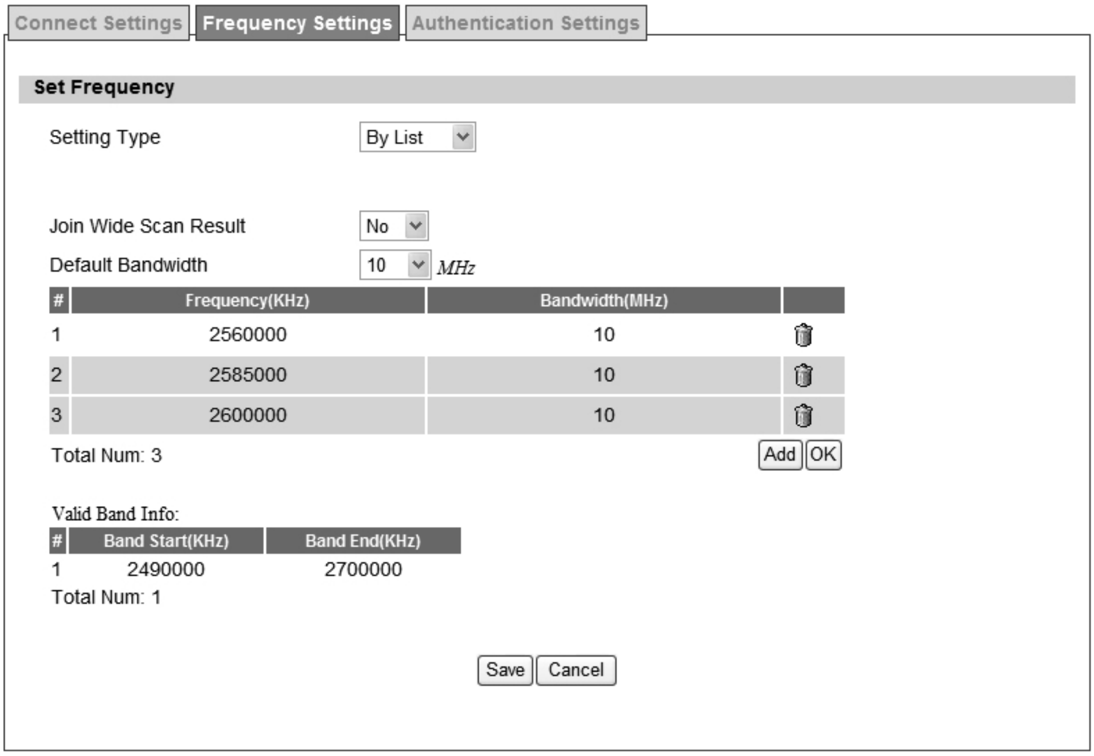
Name	**Description**
Connect Options Settings	
Auto Reconnect	Indicate th e interval in second to "a uto re connect". 0 mean s disabled.
Auto Reconnect Mode	Use CINR or RSSI as the crite rion of "Auto Connect Mode". Note that "Auto Connect Mode" refer to following "Auto Connect Mode" in "Connect Mode".
NDS Mode	Enable NDS mode or not. (NDS is still testing)
NDS parameter	Upload a file which contains NDS parameter information
Enable Handover	Enable handover or not
Enable Idle Mode	Enable Idle Mode or not
Idle Mode Interval	Only valid if previous "Enable Idle Mode" set to enable. Interval in seconds whi ch firmware will trigger Idle Mode after nit packet traffic.
CINR & RS SI Refre sh Interval	Interval in seconds to update CINR & RSSI after connected
LDRP Time	LDRP (Lo w Data Rate Protection). When it's enable, if th e uplink/downlink data rate is smaller than the LDRP time, the CPE will send disconnect command to BS.
lDRP TX/RX Rate	LDRP uplink/downlink data rate
Antenna Group Mode	Auto Mode or Manual Mode
Antenna Ma nual Sele ct Group Mode	Only valid if previous "Antenna Group Mode" set to Manual Mode. Valid options: Internal group 1 Internal group 2 External group
Connect Type Settings	
Search	Click on the search button to search for available BSID
Connect Mode	Select a connect mode Auto Connect Mode: It will connect to one of the BSID in the li st, indiscriminately. Network Search Mode: User needs to select one of the BSID from the list, it will use the BSID to co nnect to WiMAX after device i s reboot.

Search	Click on the search button to search for available BSID's
Connect Mode	Select a connect mode. ● Auto Connect Mode: It will connect to one of the BSID's in the list, indiscriminately ● Network Search Mode: User needs to select one of the BSID's from the list, it will use that BSID to connect to WiMAX after device is reboot.
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 21 Field definition for WiMAX>Profile>Connect Settings

4.1.2. Frequency Settings

The frequency list window will display all the configured frequencies and their bandwidth. To set additional frequencies, click on the “Add” button.



Set Frequency

Setting Type: By List

Join Wide Scan Result: No

Default Bandwidth: 10 MHz

#	Frequency(KHz)	Bandwidth(MHz)	
1	2560000	10	🗑
2	2585000	10	🗑
3	2600000	10	🗑

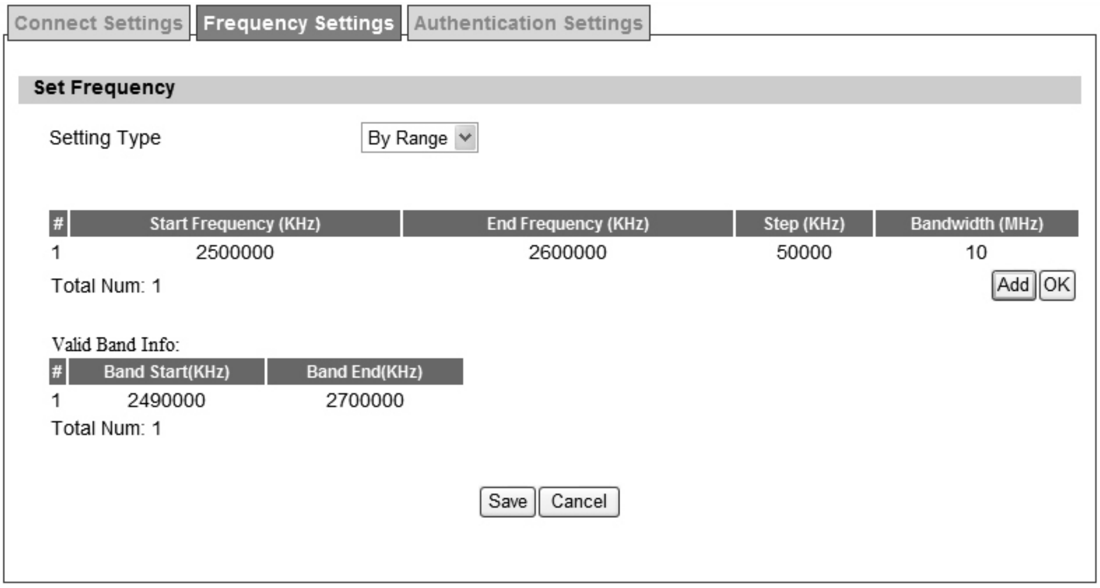
Total Num: 3

Valid Band Info:

#	Band Start(KHz)	Band End(KHz)
1	2490000	2700000

Total Num: 1

Figure 39 WiMAX>Profile>Frequency Settings>By List



Set Frequency

Setting Type: By Range

#	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)
1	2500000	2600000	50000	10

Total Num: 1

Valid Band Info:

#	Band Start(KHz)	Band End(KHz)
1	2490000	2700000

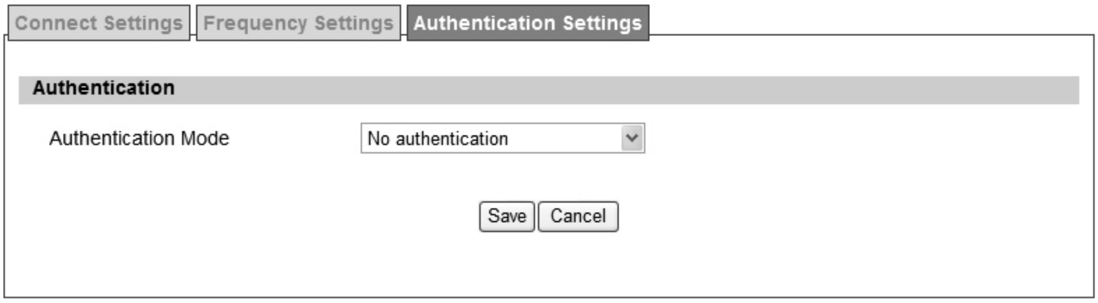
Total Num: 1

Figure 40 WiMAX>Profile>Frequency Settings>By Range

Name	Description
Setting Type	There are two display types user can select. ● User can choose to display the data by List. If user selects "By List", user also has the option to add more frequencies. ● "By Range" will display the frequency by range and the incremental value. See Figure "Frequency By Range" for more detail.
Joint Wide Scan Result	Yes means to append wide scan result to the frequency setting. Only valid when setting type is “By List”.
Default Bandwidth	Select the default bandwidth to be used in Frequency List ● 5 MHz ● 10 MHz
Valid Band Info	Valid band information. If the frequencies aren’t located using the valid band range, the frequency setting will be rejected.
Add	The "Add" button will allow user to enter more frequency lists
OK	Click the "OK" button to exit table edit mode
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

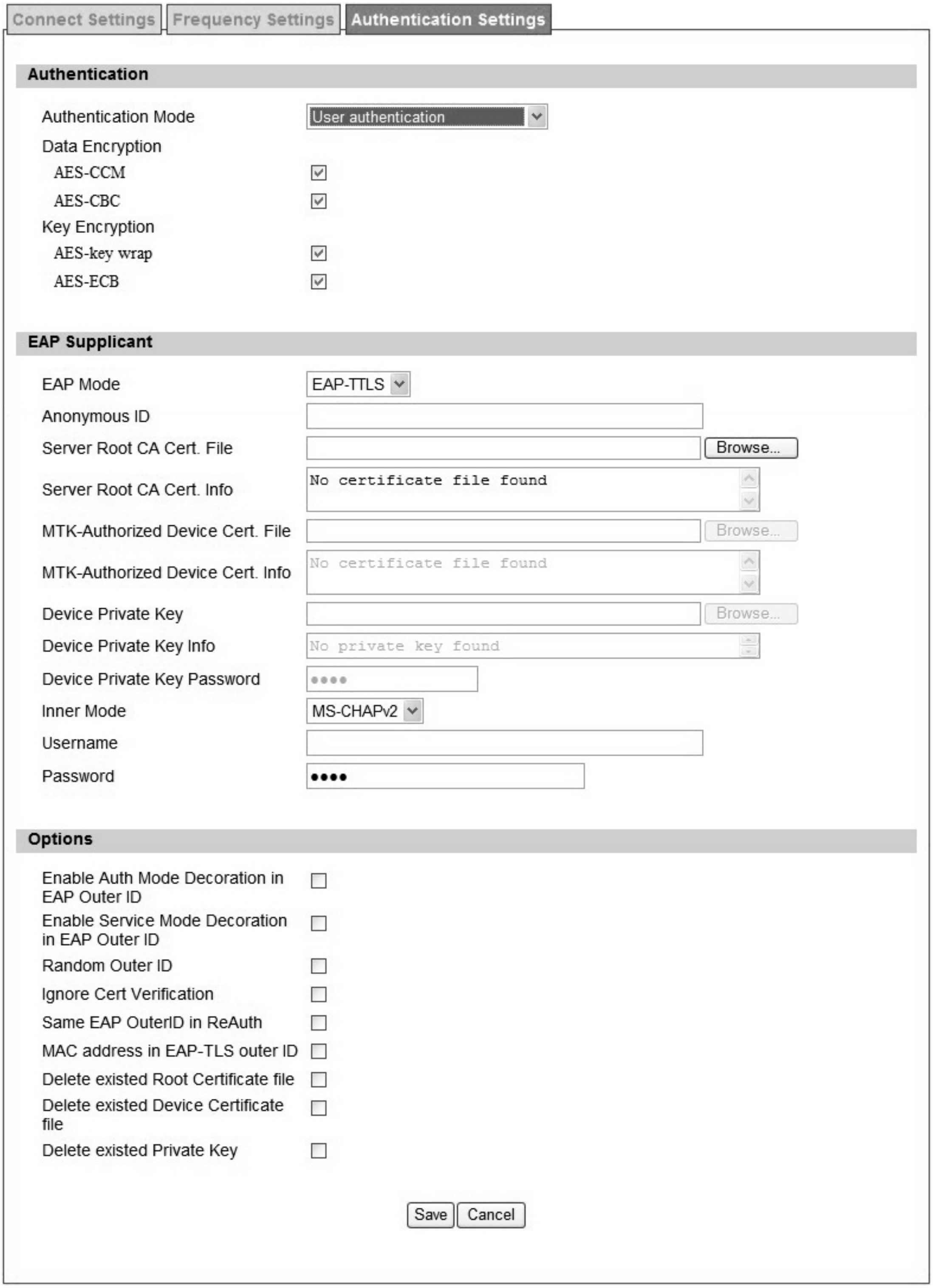
Table 22 Field definition for WiMAX>Profile>Frequency Settings>By Range

4.1.3. Authentication Settings



Authentication Mode: No authentication

Figure 41 WiMAX>Profile>Authenticaton Settings (No Authentication)



Authentication

Authentication Mode	User authentication
Data Encryption	
AES-CCM	☑
AES-CBC	☑
Key Encryption	
AES-key wrap	☑
AES-ECB	☑

EAP Supplicant

EAP Mode	EAP-TTLS
Anonymous ID	
Server Root CA Cert. File	Browse...
Server Root CA Cert. Info	No certificate file found
MTK-Authorized Device Cert. File	Browse...
MTK-Authorized Device Cert. Info	No certificate file found
Device Private Key	Browse...
Device Private Key Info	No private key found
Device Private Key Password	••••
Inner Mode	MS-CHAPv2
Username	
Password	••••

Options

Enable Auth Mode Decoration in EAP Outer ID	□
Enable Service Mode Decoration in EAP Outer ID	□
Random Outer ID	□
Ignore Cert Verification	□
Same EAP OuterID in ReAuth	□
MAC address in EAP-TLS outer ID	□
Delete existed Root Certificate file	□
Delete existed Device Certificate file	□
Delete existed Private Key	□

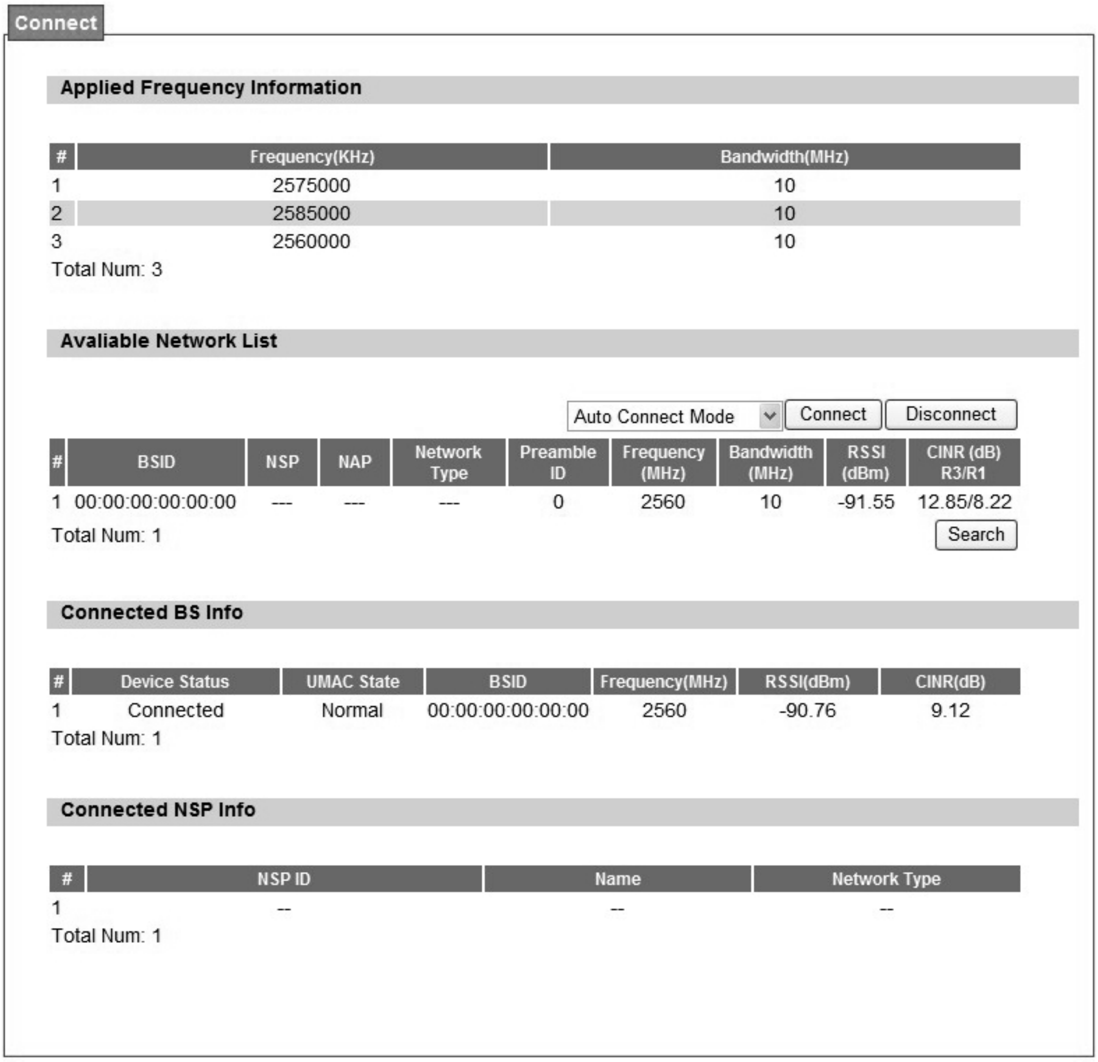
Figure 42 WiMAX>Profile>Authenticaton Settings (User Authentication)

Name	Description
Authentication	
Authentication Mode	The method used in authentication.
Data Encryption AES-CCM	Enable MS’ s cap ability of encryptin g/decrypting traf fic by AES-CCM.
Data Encryption AES-CBC	Enable MS' s ca pability of encry pting/decrypting traf fic by AES-CBC.
Key Encryption AES-key wrap	Enable MS's capability of decrypting TEK by AES-Key wrap.
Key Encryption AES-ECB	Enable MS's capability of decrypting TEK by AES-ECB.
EAP Supplicant	
EAP Mode	The EAP method used in authentication
Anonymous ID	The identity encoded in EAP Identity Response message
Root CA Certificate	The root CA's X.509 certificate.
Client CA Certificate	The MS's X.509 certificate.
Private Key	The MS' s pri vate key file corre sponding to the publ ic key enhanced in x.509 certificate
Private Key Password	The key used to decrypt the MS’s private key file
Inner Mode	The EAP-TTLS inner method
User name	The user name used in EAP-TTLS inner method
Password	The password used in EAP-TTLS inner method.
Options	
Auto Prepend Auth Mode	Enable the MS to automatically decorate “{am=i}” in the EAP Identity Resp onse me ssage Th e valu e of "i" dep ends on Authentication Mode field.
Random Outer ID	Enable MS t o gene rate 16-bytes random num ber as the user name in the EAP Identity Response message.
Ignore Cert Verification	MS ski ps t o v erify t he BS's ce rtificate receiv ed in t he EAP-TLS or EAP-TTLS procedure.
Same EAP Outer ID in ReAuth	Use the same EAP outer ID when doing re-auth
MAC address in EAP-TLS outer ID	Add MAC address in outer ID when EAP mode is EAP-TLS
Delete existed Device Certificate file	Delete device certificate file which was uploaded in the field “MTK-authorized Device Certificate”
Delete existed Private Key	Delete d evice private key which wa s uploaded in the field “Device Private Key”

Save	Commit the changes made and save to CPE
Cancel	Reset fields to the last saved values

Table 23 Field definition for WiMAX>Profile>Authentication Settings

4.2. Connect



Connect

Applied Frequency Information

#	Frequency(KHz)	Bandwidth(MHz)
1	2575000	10
2	2585000	10
3	2560000	10

Total Num: 3

Avaliable Network List

Auto Connect Mode | Connect | Disconnect

#	BSID	NSP	NAP	Network Type	Preamble ID	Frequency (MHz)	Bandwidth (MHz)	RSSI (dBm)	CINR (dB) R3/R1
1	00:00:00:00:00:00	---	---	---	0	2560	10	-91.55	12.85/8.22

Total Num: 1

Search

Connected BS Info

#	Device Status	UMAC State	BSID	Frequency(MHz)	RSSI(dBm)	CINR(dB)
1	Connected	Normal	00:00:00:00:00:00	2560	-90.76	9.12

Total Num: 1

Connected NSP Info

#	NSP ID	Name	Network Type
1	--	--	--

Total Num: 1

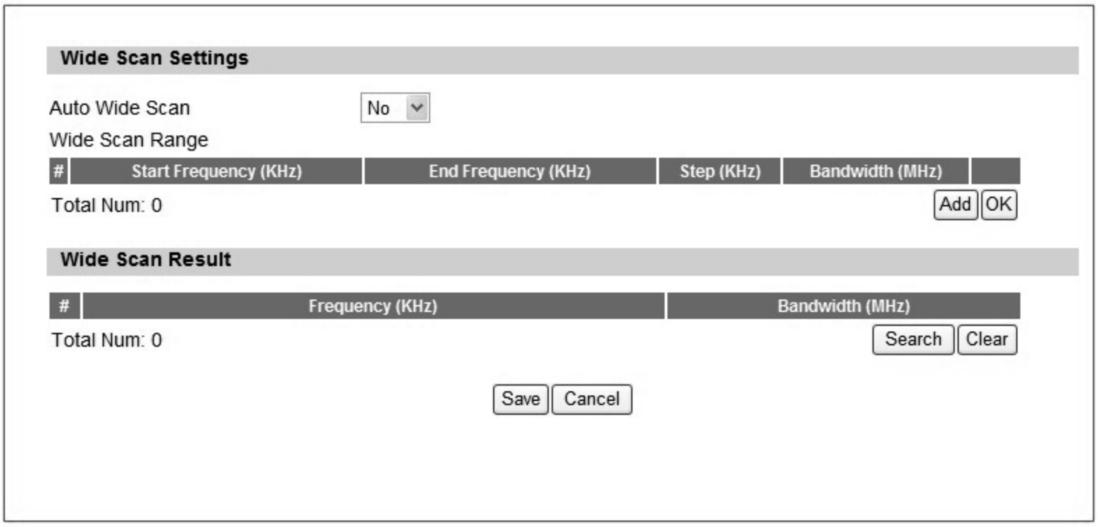
Figure 43 WiMAX>Connect>Connect

Name	Description
Disconnect	Click the disconnect button to terminate the connection
Connect	Click the connect button to connect to a BSID
Connect Mode	Select a connect mode. ● Auto Connect Mode: It will connect to one of the BSID's in the list indiscriminately ● Network Search Mode: User needs to select one of the BSID's from the list, it will use that BSID to connect to WiMAX after device is reboot.
Search	Click the search button to scan the frequency

Table 24 Field definition for WiMAX>Connect>Connect

4.3. Wide Scan

The “Wide Scan” function is used for scanning BS based on scanning rule. User can set the scan rule with defining start, stop frequency, step, and channel bandwidth, and CPE will base on this rule to scan the BS as shown in Figure 44. The definition for each field is shown on Table 25.



Wide Scan Settings

Auto Wide Scan: No

Wide Scan Range

#	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)	

Total Num: 0

Wide Scan Result

#	Frequency (KHz)	Bandwidth (MHz)

Total Num: 0

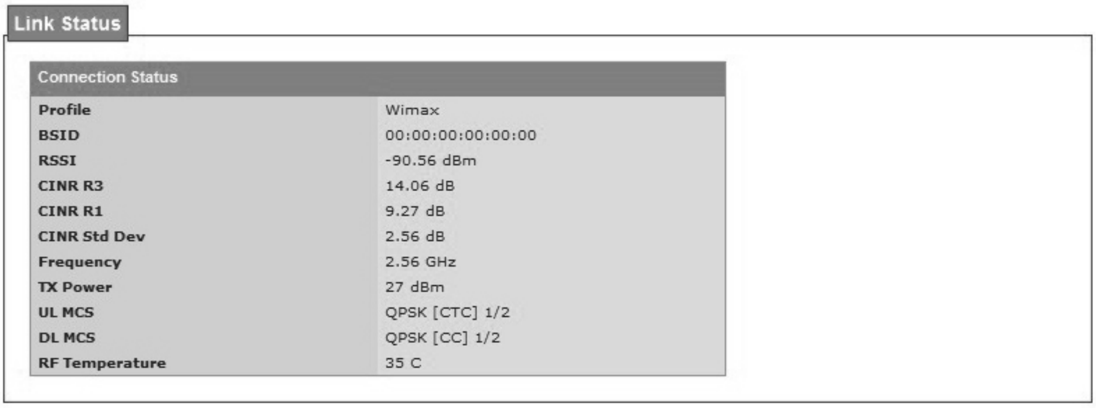
Figure 44 WiMAX>Wide Scan

Name	Description
Auto Wide Scan	Select “Yes” to do “wide scan” automatically when there are no available BS.
Wide Scan Range	
Add/Ok	User can specify the wide scan range to reduce search time
Wide Scan Result	
Search	Show the result of wide scan. Search button can trigger wide scan
Clear	Clear button clear current search result
Save/Cancel	Save/Can cel current setting

Table 25 Field definition for WiMAX>Wide Scan

4.4. Link Status

The “Link Status” menu item shows a brief profile of the current WiMAX link.



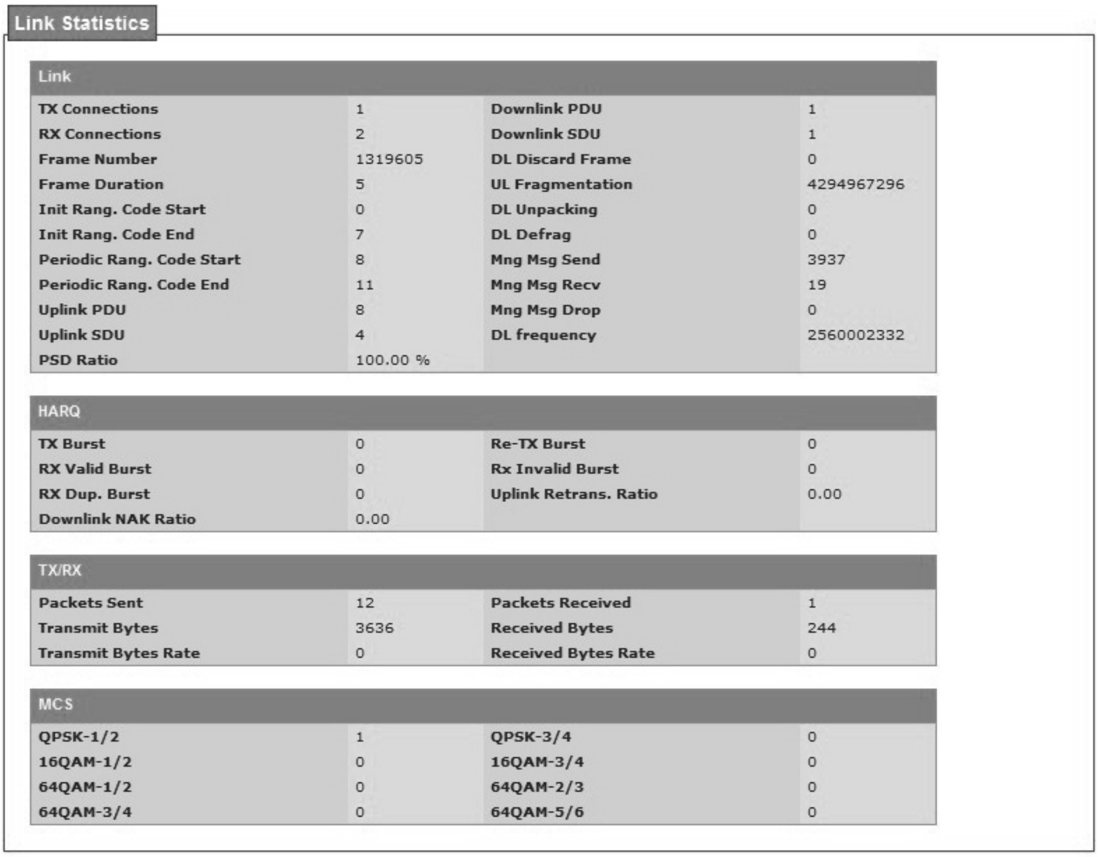
Connection Status	
Profile	Wimax
BSID	00:00:00:00:00:00
RSSI	-90.56 dBm
CINR R3	14.06 dB
CINR R1	9.27 dB
CINR Std Dev	2.56 dB
Frequency	2.56 GHz
TX Power	27 dBm
UL MCS	QPSK [CTC] 1/2
DL MCS	QPSK [CC] 1/2
RF Temperature	35 C

Figure 45 WiMAX>link Status

4.5. Link Statistics

Wimax>Link Statistics

The“Link Statistics”menu item will display statistical information in the WiMAX link.



Link Statistics

Link			
TX Connections	1	Downlink PDU	1
RX Connections	2	Downlink SDU	1
Frame Number	1319605	DL Discard Frame	0
Frame Duration	5	UL Fragmentation	4294967296
Init Rang. Code Start	0	DL Unpacking	0
Init Rang. Code End	7	DL Defrag	0
Periodic Rang. Code Start	8	Mng Msg Send	3937
Periodic Rang. Code End	11	Mng Msg Recv	19
Uplink PDU	8	Mng Msg Drop	0
Uplink SDU	4	DL frequency	2560002332
PSD Ratio	100.00 %		

HARQ			
TX Burst	0	Re-TX Burst	0
RX Valid Burst	0	Rx Invalid Burst	0
RX Dup. Burst	0	Uplink Retrans. Ratio	0.00
Downlink NAK Ratio	0.00		

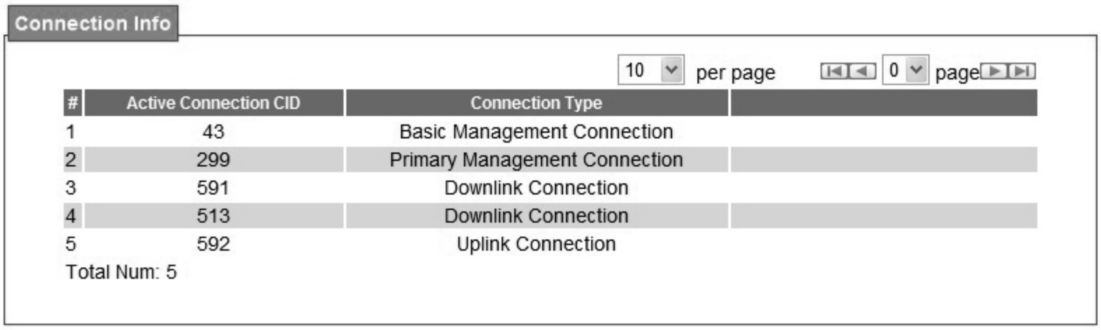
TX/RX			
Packets Sent	12	Packets Received	1
Transmit Bytes	3636	Received Bytes	244
Transmit Bytes Rate	0	Received Bytes Rate	0

MCS			
QPSK-1/2	1	QPSK-3/4	0
16QAM-1/2	0	16QAM-3/4	0
64QAM-1/2	0	64QAM-2/3	0
64QAM-3/4	0	64QAM-5/6	0

Figure 46 WiMAX Link Statistics

4.6. Connection Info

The connection info window will show the connection ID and its connection type.



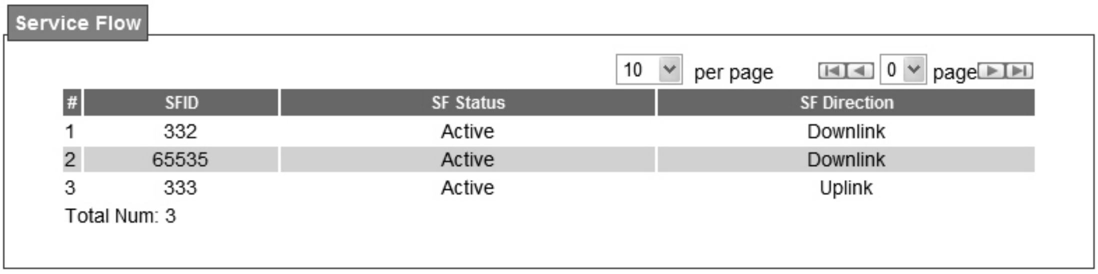
#	Active Connection CID	Connection Type	
1	43	Basic Management Connection	
2	299	Primary Management Connection	
3	591	Downlink Connection	
4	513	Downlink Connection	
5	592	Uplink Connection	

Total Num: 5

Figure 47 WiMAX Connection Info

4.7. Service Flow

The WiMAX service flow window will show the status and direction of each service flow ID.



#	SFID	SF Status	SF Direction
1	332	Active	Downlink
2	65535	Active	Downlink
3	333	Active	Uplink

Total Num: 3

Figure 48 WiMAX Service Flow

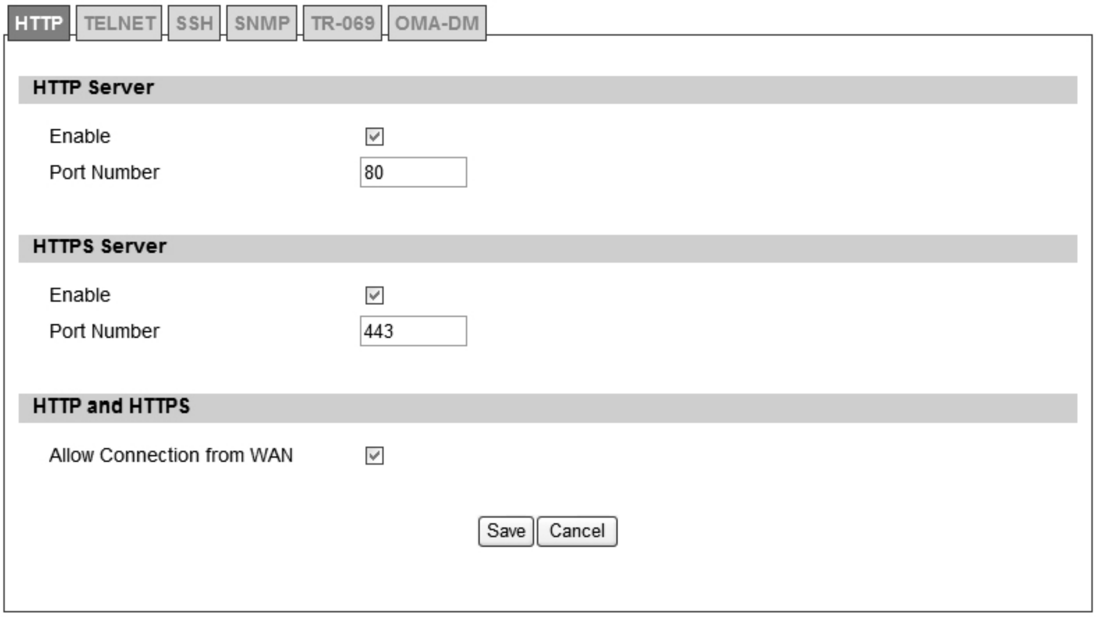
5. Administrator

5.1. Remote Control

Remote access is the ability to get access to WiMAX outdoor CPE from a remote computer or network. WiMAX outdoor CPE supports five different types of remote access protocols.

- HTTP allows user to set the port and configure both HTTP and HTTPS protocols.
- Telnet typically provides access to a command-line interface on a remote machine.
- SSH Secure Shell (SSH) is a network protocol used to allow remote connections between two devices using a secure channel. It uses public-key cryptography to authenticate the remote entity. An SSH server, by default, listens on the standard TCP port 22.
- SNMP is typically used for network management to monitor network-attached devices for conditions that warrant administrative assistance or to view and retrieve network statistical information.
- TR-069 using TR-069 the terminals can communicate with he Auto Configuration Servers (ACS) and establish the configuration automatically.

5.1.1. HTTP



HTTP Server

Enable ☑

Port Number 80

HTTPS Server

Enable ☑

Port Number 443

HTTP and HTTPS

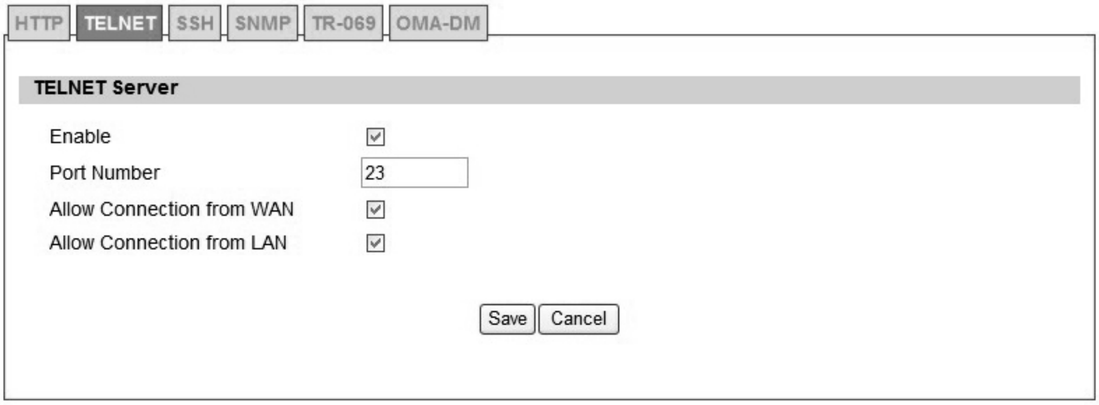
Allow Connection from WAN ☑

Figure 49 Administration>Remote Control>HTTP

Name	Description
HTTP Server	
Enable	Check the box to allow http connections.
Port Number	Enter the http port number (default is port 80)
HTTPS Server	
Enable	Check the box to allow https connections.
Port Number	Enter the https port number (default is port 443)
HTTP and HTTPS	
Allow Connection from WAN	Check the check-box to allow connections from WAN.
Save	Commit the changes made and save to WiMAX outdoor CPE.
Cancel	Reset fields to the last saved values.

Table 26 Field definition for Administration>Remote Control>HTTP

5.1.2. TELNET



TELNET Server

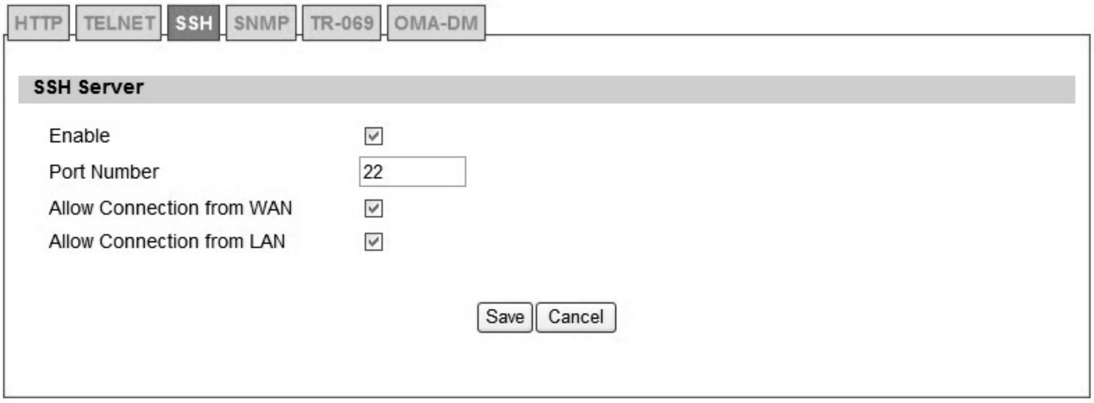
Enable	☑
Port Number	23
Allow Connection from WAN	☑
Allow Connection from LAN	☑

Figure 50 Administration>Remote Control>Telnet

Name	Description
Enable	Check the box to allow Telnet connections.
Port Number	Enter the Telent port number (default is port 23)
Allow Connection from WAN	Check the check-box to allow connections from WAN.
Save	Commit the changes ma de and save to WiMAX outdoo r CPE.
Cancel	Reset fields to the last saved values.

Table 27 Field definition for Administration>Remote Control>Telnet

5.1.3. SSH



SSH Server

Enable ☑

Port Number 22

Allow Connection from WAN ☑

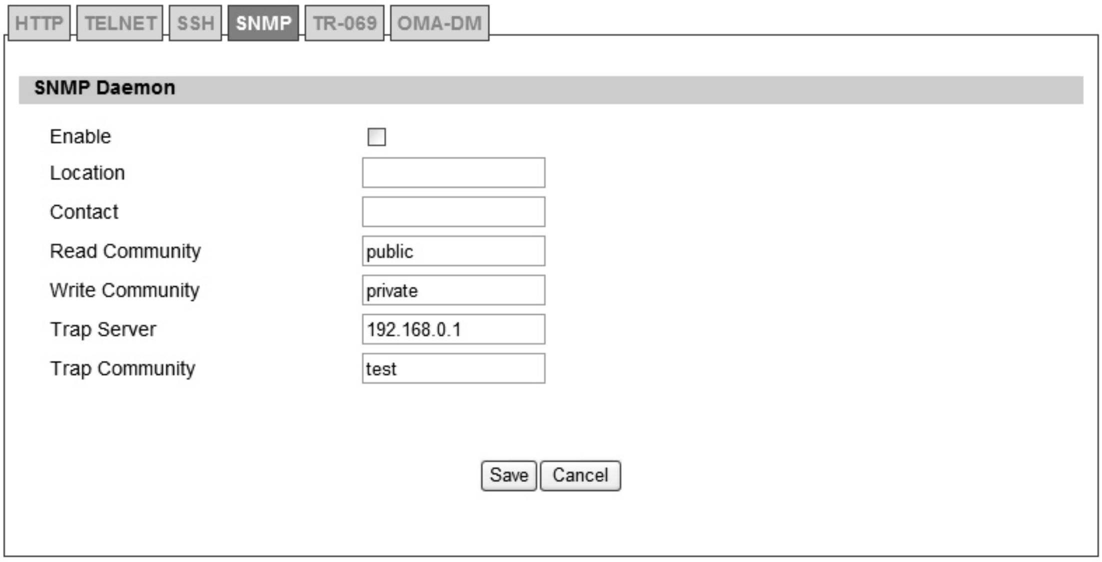
Allow Connection from LAN ☑

Figure 51 Administration>Remote Control>SSH

Name	Description
Enable	Check the box to allow SSH connections.
Port Number	Enter the SSH port (default is port 22)
Allow Connection from WAN	Check the check-box to allow connections from WAN.
Save	Commit the changes ma de and save to WiMAX outdoo r CPE.
Cancel	Reset fields to the last saved values.

Table 28 Field definition for Administration>Remote Control>SSH

5.1.4. SNMP



SNMP Daemon

Enable	□
Location	
Contact	
Read Community	public
Write Community	private
Trap Server	192.168.0.1
Trap Community	test

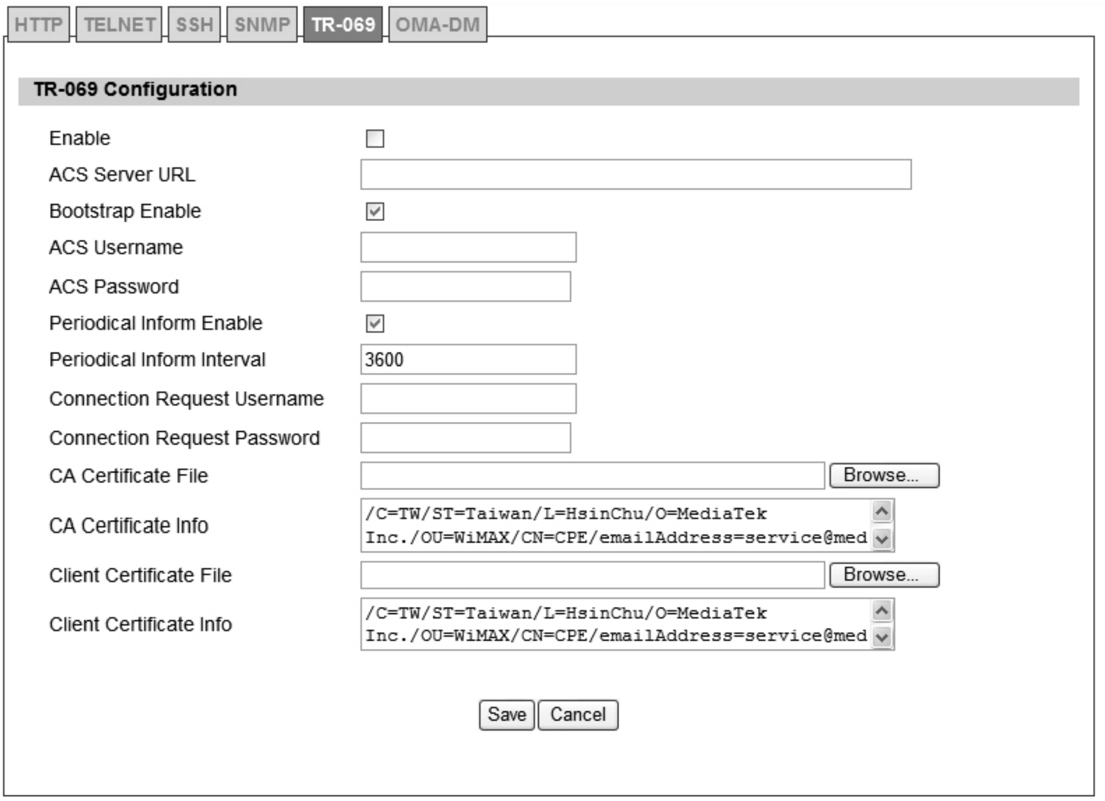
Figure 52 Administration>Remote Control>SNMP

Name	Description
Enable	Checking the enable button will allow SNMP applications to query and set some of the SNMP variables.
Location	Enter the Location SNMP string variable.
Contact	Enter the Contact SNMP string variable.
Read Community	Enter Read community string to query SNMP data.
Write Community	Enter Write community string to query SNMP variables.
Trap Server	Enter the IP Address of trap server where you want trap notifications to be sent to.
Trap community	Enter the Trap community to act as a password for sending trap notifications to the target SNMP manager.
Save	Commit the changes made and save to WiMAX outdoor CPE.
Cancel	Reset fields to the last saved values.

Table 29 Field definition for Administration>Remote Control>SNMP

5.1.5. TR-069

Using TR-069 the terminals can communicate with the Auto Configuration Servers (ACS) and establish the configuration automatically. It's the current standard for activation of terminals in the DSL broadband market.



TR-069 Configuration

Enable	□
ACS Server URL	
Bootstrap Enable	☑
ACS Username	
ACS Password	
Periodical Inform Enable	☑
Periodical Inform Interval	3600
Connection Request Username	
Connection Request Password	
CA Certificate File	
CA Certificate Info	/C=TW/ST=Taiwan/L=HsinChu/O=MediaTek Inc./OU=WiMAX/CN=CPE/emailAddress=service@med
Client Certificate File	
Client Certificate Info	/C=TW/ST=Taiwan/L=HsinChu/O=MediaTek Inc./OU=WiMAX/CN=CPE/emailAddress=service@med

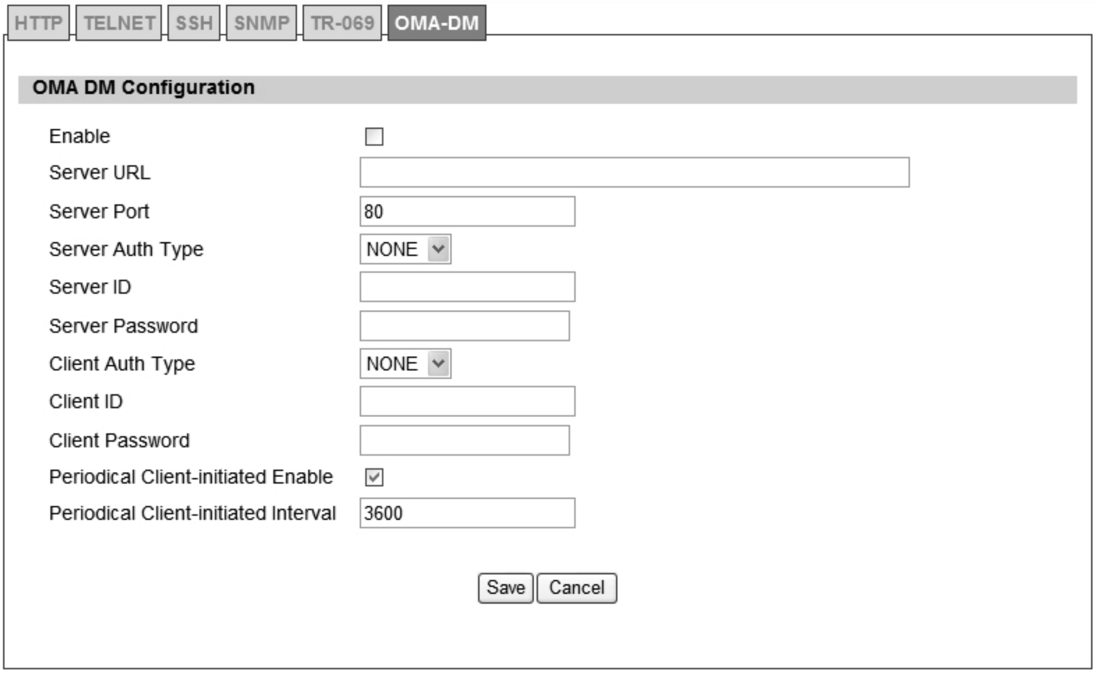
Figure 53 Administration>Remote Control>TR-069

Name	**Description**
Enable	To enable or disable the TR-069 activity on the WiMAX outdoor CPE.
ACS Server URL	The ACS URL for the WiMAX outdoor CPE to connect to.
ACS Username	The username for the WiMAX outdoor CPE when connected to ACS.
ACS Password	The password for the WiMAX outdoor CPE when connected to ACS.
Periodical Inform Enable	To enable or disable the periodical inform to ACS for the WiMAX outdoor CPE.
Periodical Inform Interval	The interval between two periodical inform.
Connection Request Username	Enter the username for the ACS to perform connection request to WiMAX outdoor CPE.
Connection Request Password	Enter the password for the ACS to perform connection request to WiMAX outdoor CPE.
CA Certificate File	The CA certificate file is used to identify the certificate of ACS when D-230 communicated ACS with HTTPS URL.
CA Certificate Info	Displays the subject field of the CA Certificate.
CLIENT Certificate File	The CLIENT certificate file is used when WiMAX outdoor CPE communicates with HTTPS URL.
CLIENT Certificate Info	Displays the subject field of the CLIENT Certificate.
Save	Commit the changes made and save to WiMAX outdoor CPE.
Cancel	Reset fields to the last saved values.

Table 30 Field definition for Administration>Remote Control>TR-069

5.1.6. OMA-DM

Using OMA DM the terminals can communicate with the OMA DM Server and establish the configuration automatically. It's the current standard for activation of terminals in OMA (Open Mobile Alliance).



OMA DM Configuration

Enable	□
Server URL	
Server Port	80
Server Auth Type	NONE
Server ID	
Server Password	
Client Auth Type	NONE
Client ID	
Client Password	
Periodical Client-initiated Enable	☑
Periodical Client-initiated Interval	3600

Figure 54 Administration>Remote Control>OMA-DM

Name	Description
Enable	To enable or disable the OMA-DM activity of the WiMAX outdoor CPE.
Server URL	The DM Server URL for the WiMAX outdoor CPE to connect to.
Server Port	The DM Server Port for the WiMAX outdoor CPE to connect to.
Server Auth Type	The DM Server authentication type.
Server ID	The Server ID for the WiMAX outdoor CPE when connected to DM Server.
Server Password	The Server password for the WiMAX outdoor CPE when connected to DM Server.
Client Auth Type	The DM Client authentication type.
Client ID	The Client ID for the WiMAX outdoor CPE when connected to DM Server.
Client Password	The Client password for the WiMAX outdoor CPE when connected to DM Server.
Periodical Client-initiated Enable	To enable or disable the periodical client-initiated session to DM server for the WiMAX outdoor CPE.
Periodical Client-initiated Interval	The interval between two periodical client-initiated session.
Save	Commit the changes made and save to WiMAX outdoor CPE.
Cancel	Reset fields to the last saved values.

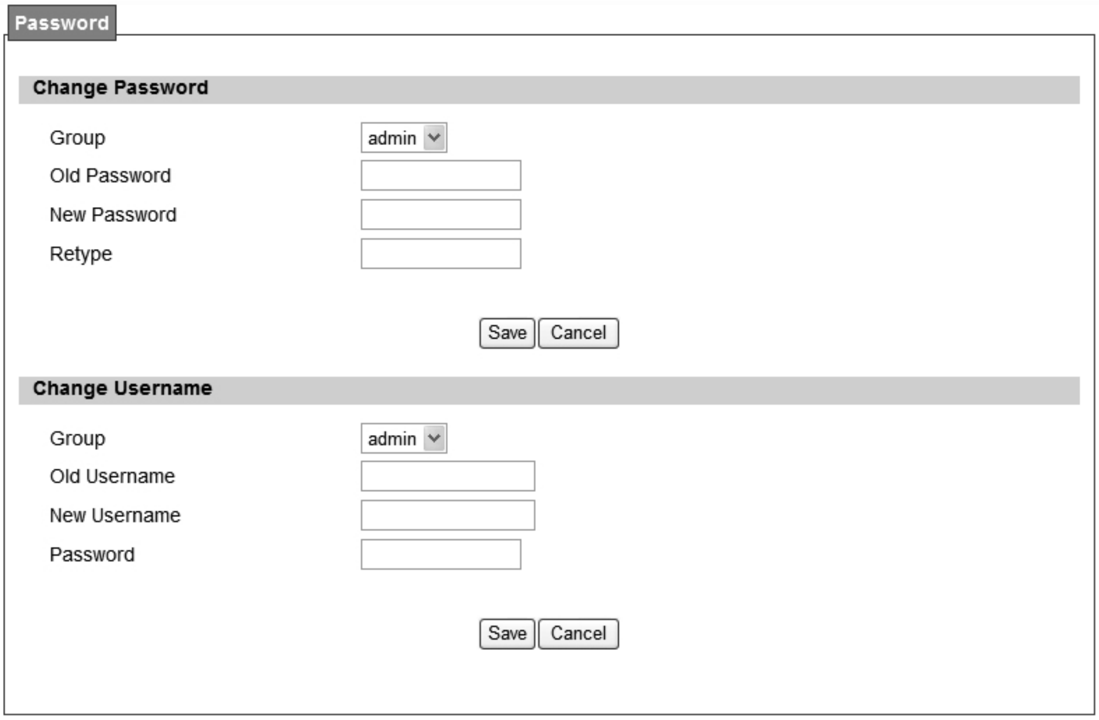
Table 31 Field definition for Administration>Remote Control>OMA-DM

5.2. Password

Note: The default usernames and passwords admin/admin and guest/guest.

The user with administrative privileges (belonging to the “admin” group) has access to all the features in the software. A user with “guest” privileges (belonging to the “guest” group)only has a subset of the features available to them.

Note: There can only be one username in each of the groups (one to one relationship).



Password

Change Password

Group: admin
Old Password
New Password
Retype

Change Username

Group: admin
Old Username
New Username
Password

Figure 55 Administrator>Password

Name	Description
Change Password	
Group	Select which group the user belongs to that you would like to change the password for. ● admin, if the user is part of the admin group, they have full access to tall the features. ● guest, if the user is part of the guest group, they have limited access to the features.
Old Password	Enter the old password.
New Password	Enter the new password.
Retype	Retype the new password.
Save	Commit the changes made and save to WiMAX outdoor CPE, it will only commit the change made to the password.
Cancel	Reset fields to the last saved values.
Change Username	
Group	Select which group the user belongs to that you would like to change the username for. ● admin, if the user is part of the admin group, they have full access to tall the features. ● guest, if the user is part of the guest group, they have limited access to the features.
Old Username	Enter the username you want to change.
New Username	Enter the new username.
Password	Enter the original password, the password will not change. If you enter an incorrect or different password the change will not be committed
Save	Commit the changes made and save to WiMAX outdoor CPE, it will only commit the change made to the username.
Cancel	Reset fields to the last saved values.

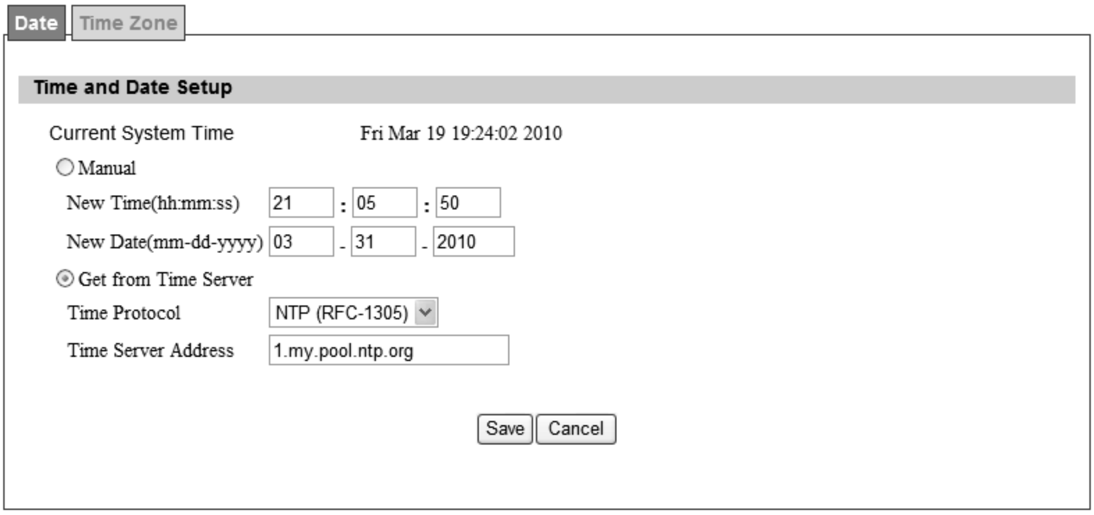
Table 32 Field definition for Administrator>Password

6. System

6.1. Date and Time

User can configure the date and time on the device. The user can manually configure the system time, or choose to get the date and time from a time server. The “Save” button will commit the configuration, and the “Cancel” button will clear the fields. The “Time Zone” tab will allow you to set the time zone and set the starting and finish time for daylight saving period. User can also enable or disable “Daylight Savings Time”.

NOTE: If user doesn’t configure the time on the WiMAX outdoor CPE it will use the default system starting time. The default system starting time is set to 1970/1/1 00:00:00



Time and Date Setup

Current System Time Fri Mar 19 19:24:02 2010

○ Manual

New Time(hh:mm:ss) 21 : 05 : 50

New Date(mm-dd-yyyy) 03 - 31 - 2010

● Get from Time Server

Time Protocol NTP (RFC-1305)

Time Server Address 1.my.pool.ntp.org

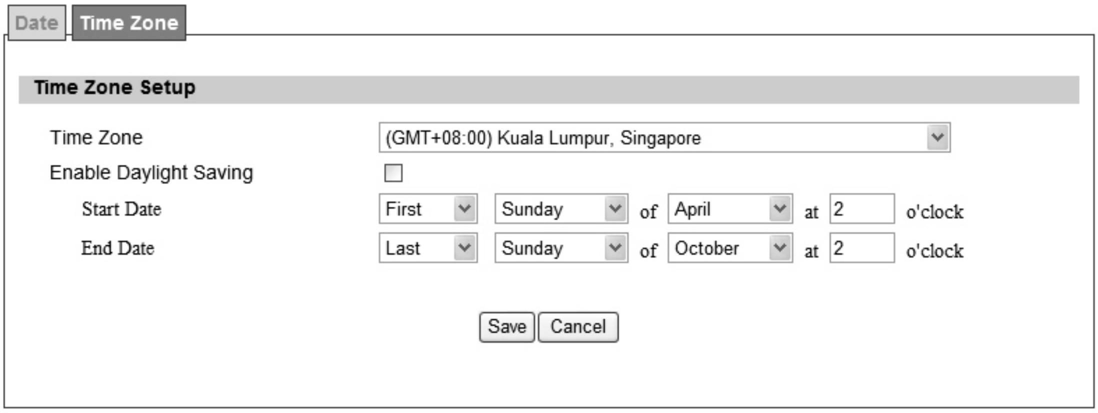
Figure 56 System>Date/Time>Date

6.1.1. Date

Name	Description
Manual	If user selects the Manual option, then use need to enter the time and date manually.
New Time	New time manually entered
New Date	New date manually entered
Get From Time Server	If user select s this option it will get th e local time from a time server automatically.
Time Protocol	Select the Time protocol
Time Server Address	Enter the address of the time server.
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 33 Field definition for Administrator>Password

6.1.2. Time Zone



Time Zone Setup

Time Zone (GMT+08:00) Kuala Lumpur, Singapore

Enable Daylight Saving □

Start Date First Sunday of April at 2 o'clock

End Date Last Sunday of October at 2 o'clock

Figure 57 System>Date/Time>Time Zone

Name	Description
Time Zone	Enter the time zone of for the location
Enable Daylight Savings	If user wants to enable Daylight Savings Time, user needs to check the box.
Start Date	Enter the beginning date for Daylight Savings time
End Date	Enter the end date for Daylight Savings time.
Save	Commit the changes made and save to WiMAX outdoor CPE
Cancel	Reset fields to the last saved values

Table 34 Field definition for System>Date/Time>Time Zone

6.2. Upgrade Firmware

The “Upgrade” window allows user to upgrade the firmware on your device. Users can choose to upgrade the firmware by entering the file path or entering the URL of the upgrade file.

Note: After pressing the “Upgrade” button. It will automatically reboot the WiMAX outdoor CPE and upgrade the firmware with the specified file. User will be prompted to login to the WiMAX outdoor CPE after the upgrade is complete.

6.2.1. Upgrade File

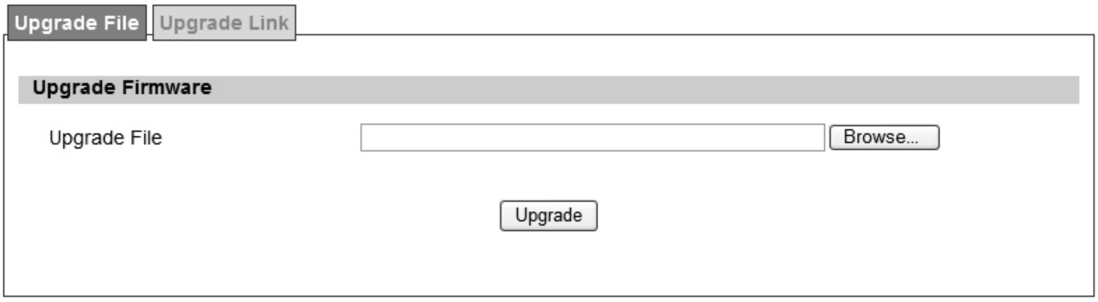


Figure 58 System>Upgrade Firmware>Upgrade File

Name	Description
Browse	Enter the full path of the file you want to upgrade. The "browse" button will help user to find the file on the server.
Upgrade	It will start upgrading the file
Status	The status bar will display which segment it's processing and what percentage of the upgrade has been completed.

Table 35 Field definition for System>Upgrade Firmware>Upgrade File

6.2.2. Upgrade Link

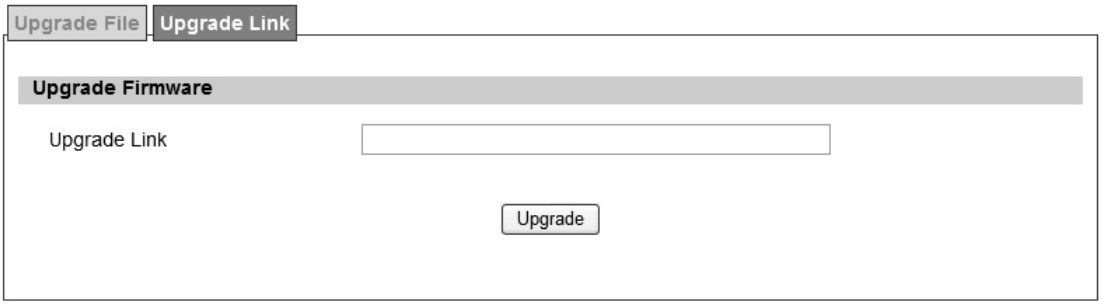


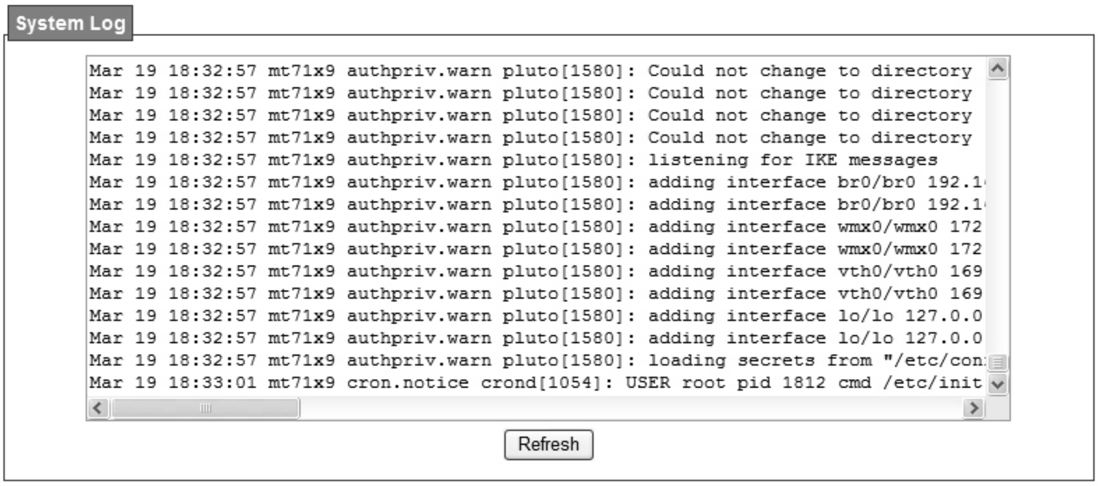
Figure 59 System>Upgrade Firmware>Upgrade Link

Name	Description
Upgrade Link	Enter the complete URL path of the file that user wants to upgrade
Upgrade	It will start upgrading the file
Status	The status window will display which segment it's processing and what percentage of the upgrade has been completed.

Table 36 Field definition for System>Upgrade Firmware>Upgrade Link

6.3. Log

The “System>Log” will display system log output. The “Refresh” button will clear the log window and display the most current system log information.



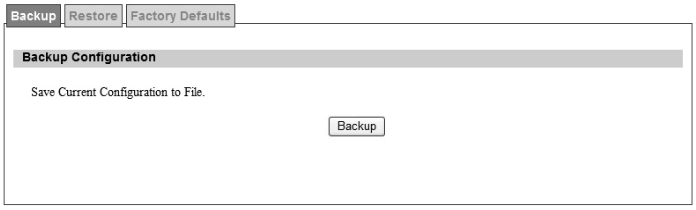
```
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: Could not change to directory
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: Could not change to directory
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: Could not change to directory
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: Could not change to directory
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: listening for IKE messages
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface br0/br0 192.1
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface br0/br0 192.1
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface wmx0/wmx0 172
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface wmx0/wmx0 172
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface vth0/vth0 169
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface vth0/vth0 169
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface lo/lo 127.0.0
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: adding interface lo/lo 127.0.0
Mar 19 18:32:57 mt71x9 authpriv.warn pluto[1580]: loading secrets from "/etc/con
Mar 19 18:33:01 mt71x9 cron.notice crond[1054]: USER root pid 1812 cmd /etc/init
```

Figure 60 System Log

6.4. Backup/Restore

The Backup/Restore tab will allow user to save and restore the configuration on the WiMAX outdoor CPE . User can also reset the WiMAX outdoor CPE to factory defaults from the “Factory Defaults” tab.

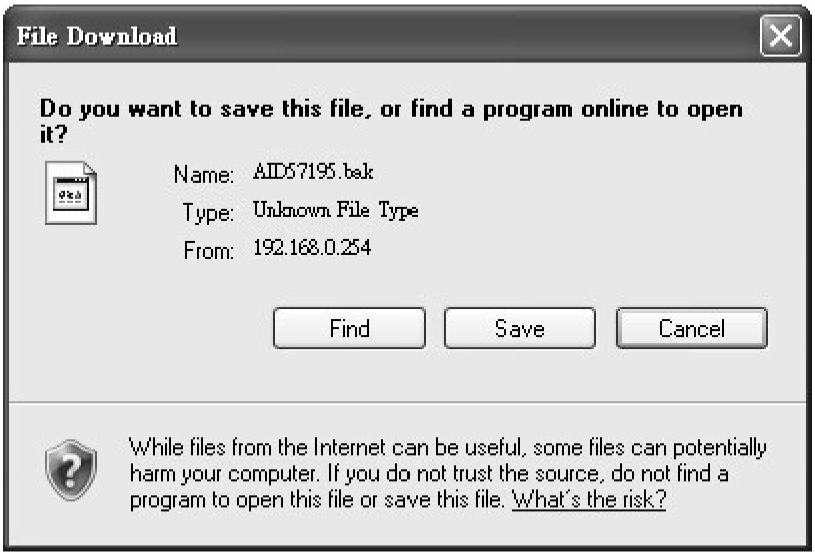
6.4.1. Configuration Backup



Backup Configuration

Save Current Configuration to File.

Figure 61 System>Backup/Restore>Backup



File Download

Do you want to save this file, or find a program online to open it?

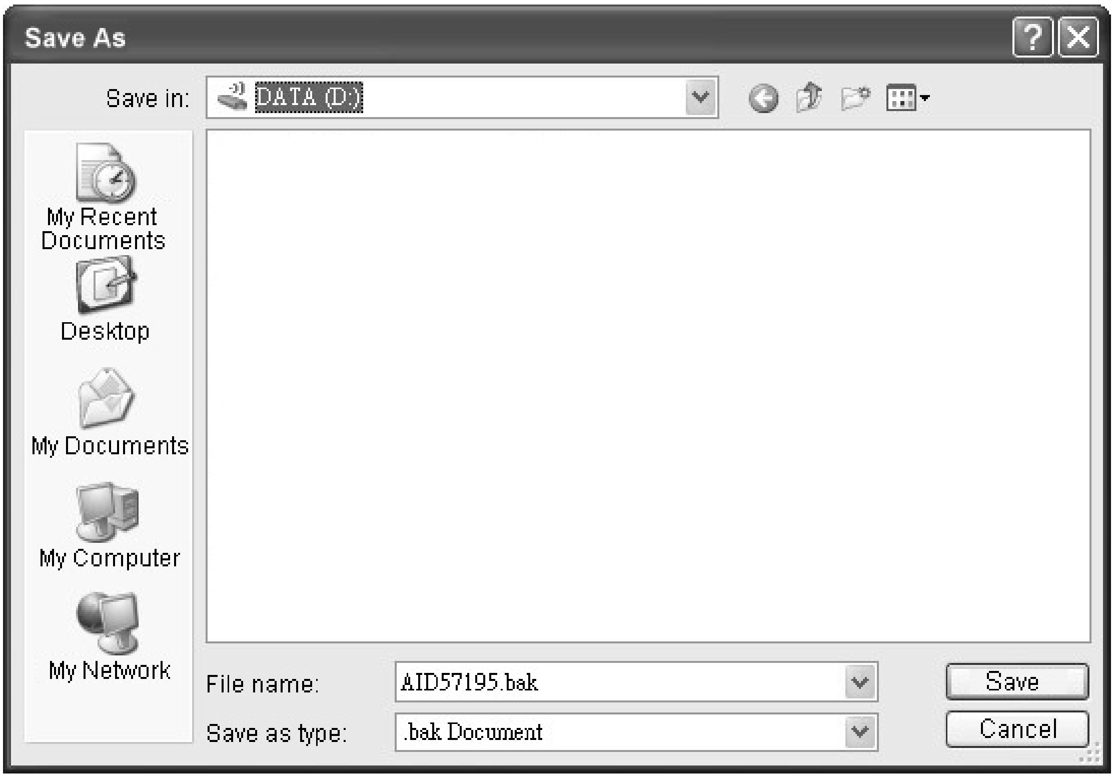
Name: AID57195.bak

Type: Unknown File Type

From: 192.168.0.254

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

Figure 62 File Download



Save As

Save in: DATA (D:)

File name: AID57195.bak

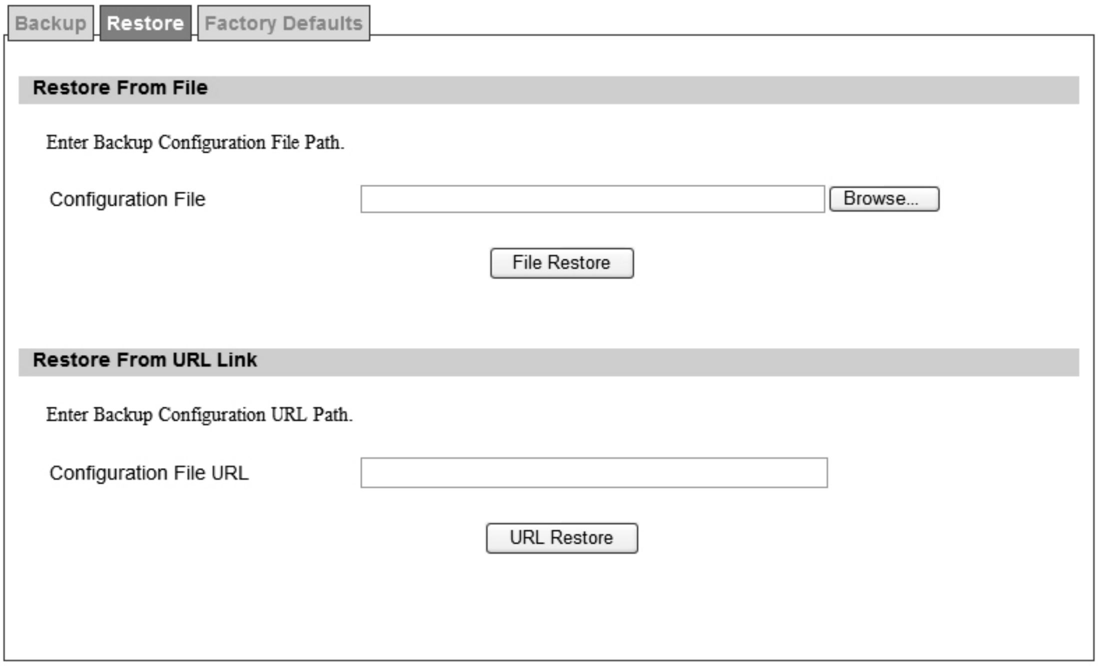
Save as type: .bak Document

Figure 63 Save File As

Name	Description
Backup	Click the "Backup" button o save the current configuration on the WiMAX outdoor CPE. After user clicks the "Backup" button "File Download" window will pop-up and prompt user to save the file. In the "Save As" window, enter the na me and location, where user wishs to download the file to.

Table 37 Field definition for System>Backup/Restore>Backup

6.4.2. Configuration Restore



Enter Backup Configuration File Path.

Configuration File

Enter Backup Configuration URL Path.

Configuration File URL

Figure 64 System>Backup/Restore>Restore

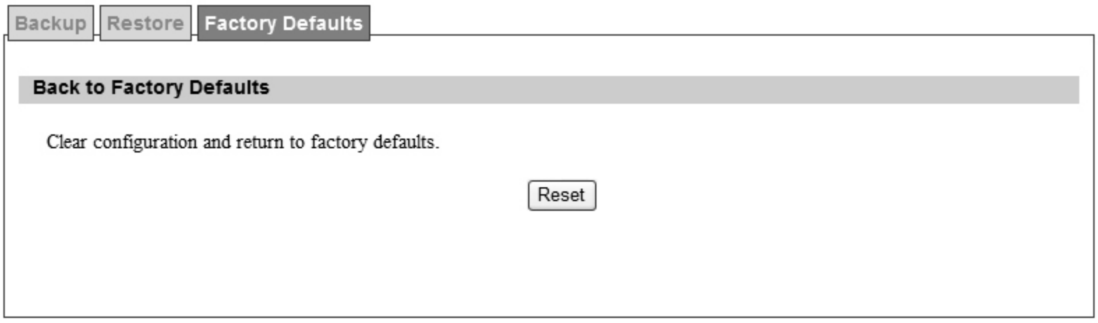
Name	Description
File Restore	Enter the path of the configuration file user wants to restore. Click on the "Browse" button to help user to navigate through directories and search for the file. After user enters the complete file path, click the "File Restore" button. It will begin restoring the configuration from the file specified.
URL Restore	Enter the configuration URL path user wants to restore from. After entering the complete URL path, click the "URL Restore" button. It will begin restoring the configuration from the URL location user specified.

Table 38 System>Backup/Restore>Restore

6.4.3. Factory Defaults

Factory default will set all the configurations back to factory defaults. Any configurations that user has made will be changed back to the factory default settings. After selecting “Reset” button, user will be prompted with a window to confirm or cancel the action.

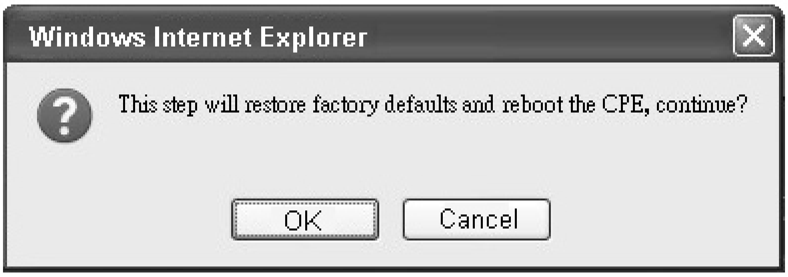
Warning: Restore factory defaults will clear any IP addresses and setting that may have been configured on the WiMAX outdoor CPE.



Back to Factory Defaults

Clear configuration and return to factory defaults.

Figure 65 System>Backup/Restore>Factory Defaults



This step will restore factory defaults and reboot the CPE, continue?

Figure 66 Restore to factory reset warning

7. Installing and grounding device

Before installing the Outdoor CPE Device

Before installing, it is important to comply with the precautions listed below.

- It must be installed by qualified service personnel who are well-trained in the correct procedures for handling and installing the equipment.
- Avoid installing or working on equipment in adverse weather conditions. Once it must be installed in adverse weather conditions, it's necessary to well protect the equipment.
- Do not install the device near overhead power lines or power circuits, or where the device can fall onto such power lines or circuits.
- Do not disassemble the product. Opening or removing covers may expose you to electric shock. Warranty void if seal is broken.
- Do not place or construct objects in close proximity to the device.
- Be sure to check the supplied mounting accessory is correct as listed in Figure 67. Please be noted that the mounting kits should be used for the pole with diameter between 34 ~ 49 mm.
- Under normal operating condition, it should be at least 50 cm away from the body of the user.

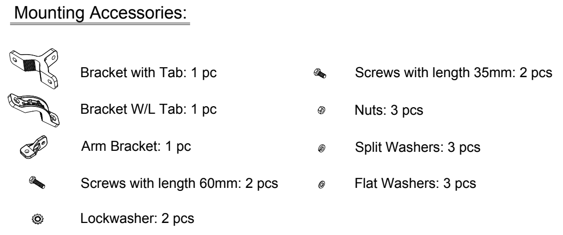


Figure 67 Mounting accessory list

An Overview of the Outdoor CPE Device Installation

Service personnel needs to follow the steps for installing Outdoor CPE Device

1. Pole-mounting or Wall-mounting the Outdoor CPE Device.
2. Grounding the Outdoor CPE Device
3. Connect the Outdoor CPE Device to PoE unit
4. Connect PC to PoE unit for configuring the Outdoor CPE Device
5. Connect the PoE unit to the power source to power up the Outdoor CPE Device
6. Use PC to configure the Outdoor CPE Device

Pole-Mounting the Outdoor CPE Device

In the following steps, it introduces how to pole-mounting the Outdoor CPE Device.

1. Assemble the mounting hardware brackets onto pole first: Take the Screws with 60mm length to pass through the Split washer and Flat washer in order, and then screw the Brackets together with nuts.
2. Use the Screw with 35mm length to attach the Outdoor CPE Device to the tab of the Bracket. Ensure the Lockwasher is located between the Bracket's tab and the Outdoor CPE Device's tab. Be sure to orient the Outdoor CPE Device with the connector towards the bottom. Remember to orderly add the Split washer, Flat washer and Nuts as shown in Figure 68. Do not over-tighten before finishing the Outdoor CPE Device alignment.
3. Adjust the azimuth and elevation of the Outdoor CPE Device toward the direction of WiMAX Base Station location.

4. Tighten the screws to secure the Outdoor CPE Device tightly.

It is not necessary to use Arm Bracket for pole-mounting. Arm Bracket is only used for wall-mounting.

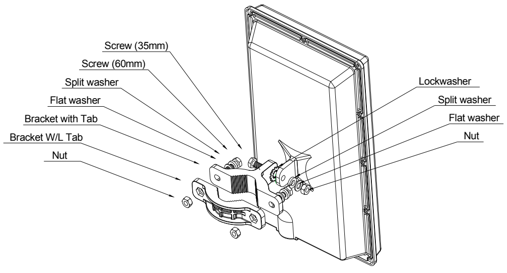


Figure 68 Pole-Mount the Outdoor CPE Device

Wall-Mounting the Outdoor CPE Device

In the following steps, it introduces how to wall-mounting the Outdoor CPE Device.

1. Install the Bracket with tab on a wall by using two mounting screws appropriate for the wall's construction material. The appropriate mounting hardware should be purchased directly from a local supplier.
2. Connect the Arm Bracket to Outdoor CPE Device with the 35mm length Screw, Lockwasher, Split washer, Flat washer, and Nut orderly as shown in Figure 69. Ensure the Lockwasher is located between the Bracket's tab and the Outdoor CPE Device's tab. Do not over-tighten before finishing the Outdoor CPE Device alignment.
3. Secure the other side of Arm Bracket along with Lockwasher to the Bracket's tab mounted on wall. Ensure that the bolt head is positioned in the socket of the Bracket. Do not over-tighten before finishing the Outdoor CPE Device alignment.
4. Adjust the azimuth and elevation of the Outdoor CPE Device toward the direction of WiMAX Base Station location.
5. Tighten the screws to secure the Outdoor CPE Device tightly.

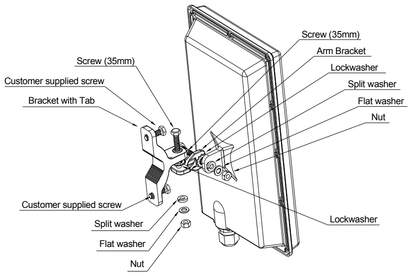


Figure 69 Wall-Mount the Outdoor CPE Device

Grounding the Outdoor CPE Device

Grounding the Outdoor CPE Device is essential to avoid serious injury to service personnel and damage to the Outdoor CPE Device. The following steps introduce how to ground the Outdoor CPE Device.

1. Remove the ground screw installed on the side of the Outdoor CPE Device, as shown in Figure 70.
2. Cut the required length of the ground wire, and then strip the insulation from the ground wire by using either a wire cutter/stripper or utility knife.
3. Crimp the ground wire to the copper cable lug, and then connect the cable lug to the grounding connection on the side of the Outdoor CPE Device. Please be noted that the thickness of the cable lug should be less than 0.85mm.
4. Tighten the screw by using the appropriate size and type of screw driver to secure the copper cable lug to the Outdoor CPE Device.
5. Strip the other end of the ground wire and connect to the main ground.

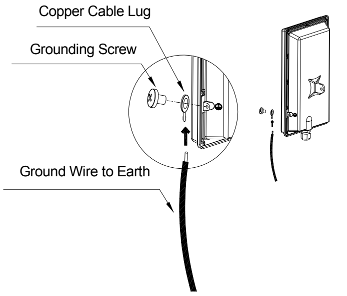


Figure 70 Connect the ground wire

Specification

Physical Standard	Description	XS-618-25MM
General Standard	PoE Standard- IEEE802.3af Compliant	●
	Wireless Standard - IEEE802.16e-2005	●
	Ethernet Interface - 10 /100 Base-T	●
WiMAX Specification		
Radio Frequency	2500MHz~2690MHz	●
Air Interface	Scalable OFDMA	●
RF Configuration	TX& RX Configuration	2T2R
Modulation - DL & UL	QPSK, 16QAM, 64QAM	●
Channel Bandwidth	5, 10 MHZ	●
Receiver Sensitivity	CTC-QPSK-1/2 @ 5MHz BW CTC-16QAM-3/4@ 5MHz BW CTC-64QAM-3/4@ 5MHz BW	- 95 dBm - 85 dBm - 80 dBm
	CTC-QPSK-1/2@10MHz BW CTC-16QAM-3/4@10MHz BW CTC-64QAM-3/4@10MHz BW	- 92 dBm - 83 dBm - 78 dBm
Firmware Feature		
Networking	Bridge /Gateway Switching Mode	●
	DDNS /DNS Relay	●
	Network Time Protocol	●
	IPv4	●
	Network Address Translation	●
	DHCP Client-WAN /DHCP Server-LAN	●
	Port Forwarding /Trigger Support	●
	NAT ALG -NAT FTP /PPTP /H.323 ALG	●
	UPnP, NAT-PMP & IGMP Proxy Support	●
Network Management	TR-069 /OMADM /SNMPv2 MIB II	●
	HTTP /HTTPS /SSH /Telnet	●
	BS Scanning- Auto /Manual Connection	●
	Web Access User Interface	●
	Web Link Status Display	●
	Web System Log Display	●
	User Account Permission Control	●
	Web Firmware Upgrade /Firmware Rollback	●
	Rest Factory Default Configuration &Settings	●
QoS Scheduling	UGS; RT-VR; NRT-VR; BE; ERT-VR	●
VLAN	VLAN packet pass through	●

VPN	PPTP Server /Client, L2TP Server /Client VPN Pass Through-IPSec, PPTP, and L2TP	●
Authentication	User /Device /User and Device Authentication	●
Security	AES-CCM /CBC /ECB /Key Wrap PKM v2, EAP TLS /TTLS / MSCHAPv2 /MS-CHAP /CHAP /MD5 /PAP X.509 Certificate	●
Firewall	IP Filter, DDOS, DMZ, NAT /NAPT Support	●
Mechanical Specification		
Hardware Specification	Dimension (L xW xH)	354 x 220 x 68 mm (Without Tab) 354 x 220 x 102 mm (With Tab)
	CPE Weight /without Accessories	< 2 Kg
	Power Requirements	100 ~ 240VAC /50 ~ 60Hz
	Power Input Voltage	+ 48VDC
	Power Consumption@Continue TX Mode	<=15 W
	Output Power @Antenna Port	>= 25 dBm
	Antenna /Internal Patch Antenna	>= 14 dBi
	LAN Port /RJ45 Connector	1xRJ45 Port
	Operating Temperature@Ambient Temp.	-40℃ ~ + 60℃
	Operation Humidity /Non-condensing	5 to 85%
	Storage Temperature@Ambient Temp.	- 40℃ ~ + 85℃
	Storage Humidity /Non-condensing	5 to 85%
	Grounding Design	●
	Surge Protection	+/- 4 KV
	Waterproof & Anti-Dust	IP67 Compliance