WM5030M-OD WiMAX Outdoor Modem

User Manual

TECOM
Converging Your Networks

Version 1.3

TECOM CO., LTD

2010/5/5

Legal Rights

The material contained herein is proprietary, and owned by TECOM Co., Ltd or its third party licensors. TECOM Co., Ltd reserves the right to alter the specification and description in this document without prior notice.

Statement of Conditions

The information contained in this document is subject to change without prior notice. TECOM Co., Ltd shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Disclaimer

The software is sold on an “AS IS” basis. TECOM, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. TECOM SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE UNITS OF PRODUCT DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (“HIGH RISK ACTIVITIES”). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OR NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEM, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. TECOM SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT TECOM'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OF CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. TECOM WARRANTIES HEREIN RUN ONLY TO PURCHASER AND ARE NOT EXTENDED TO ANY THIRD PARTIES. TECOM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

TECOM SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OR THE POSSIBILITY OF SUCH DAMAGES.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OR ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY.

TABLE OF CONTENTS

LIST OF FIGURES

1 Configuration Using Web Page

1.1. Setup

Step 1: Connect WiMAX modem and PC with an Ethernet cable.

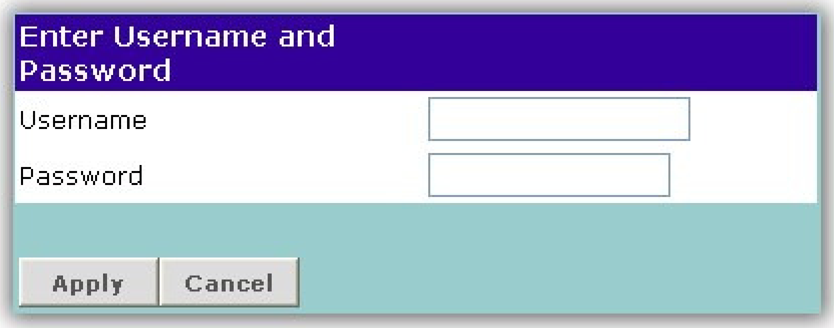
Step 2: Switch on WiMAX modem.

Step 3: The default IP of WiMAX modem is 192.168.111.113.

1.2. Establish Connection

Enter the IP address (default is 192.168.111.113) of WiMAX modem into Web Browser.

A Dialogue Box will pop out to request for user login information. (See Figure 1)



Enter Username and Password

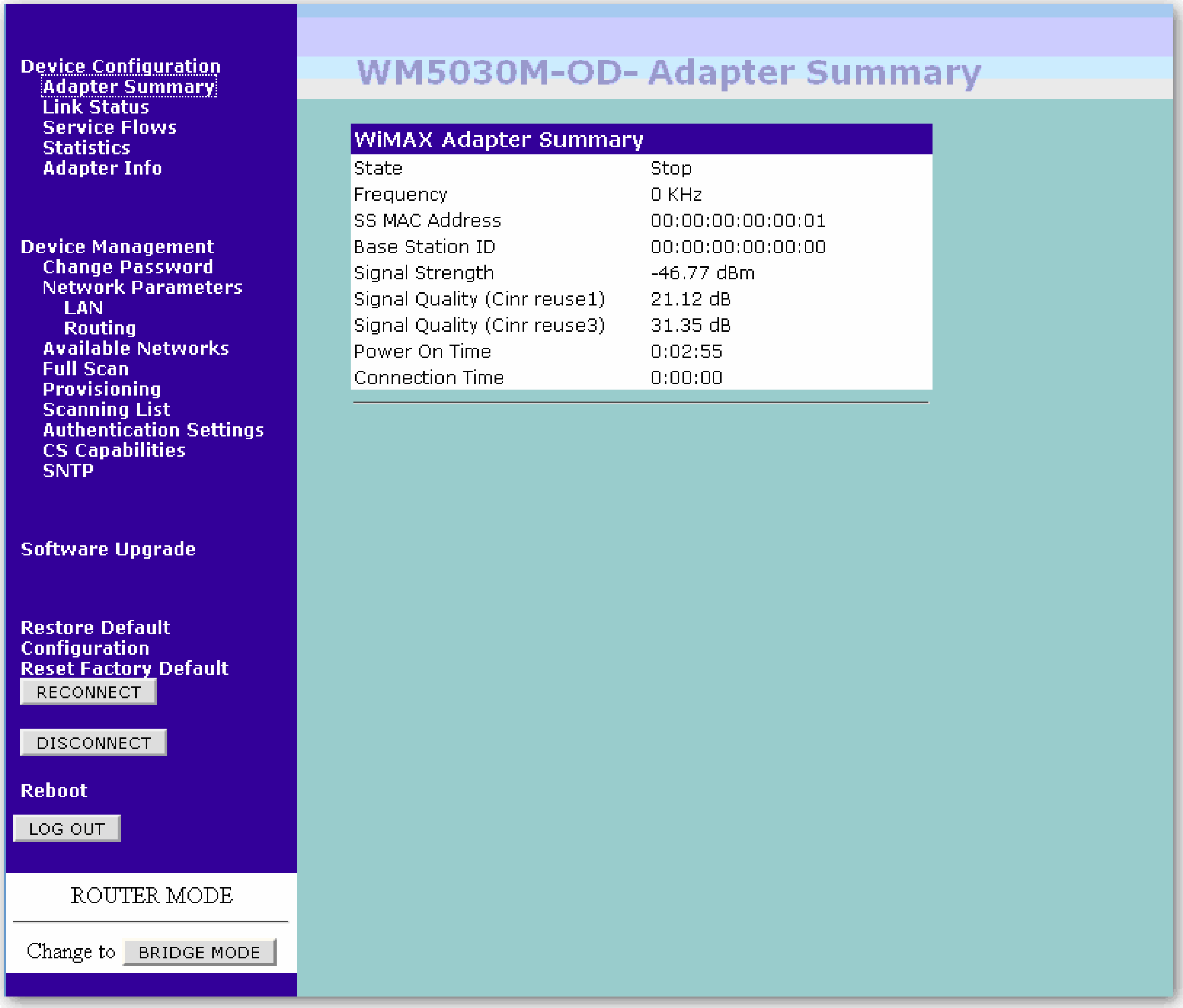
Username

Password

Figure 1. Login

Please enter management username/password into required fields, then click “OK” to continue. (Default username/password is **subscriber/subscriber**).

When user successfully logs in, the web page will lead user to Device Configuration – Adapter Summary as shown on Figure 2. The left frame is the main menu. The links on the main menu will pop up different information available on the right frame.



WM5030M-OD- Adapter Summary

WiMAX Adapter Summary	
State	Stop
Frequency	0 KHz
SS MAC Address	00:00:00:00:00:01
Base Station ID	00:00:00:00:00:00
Signal Strength	-46.77 dBm
Signal Quality (Cinr reuse1)	21.12 dB
Signal Quality (Cinr reuse3)	31.35 dB
Power On Time	0:02:55
Connection Time	0:00:00

Figure 2. Homepage

1.3. Device Configuration

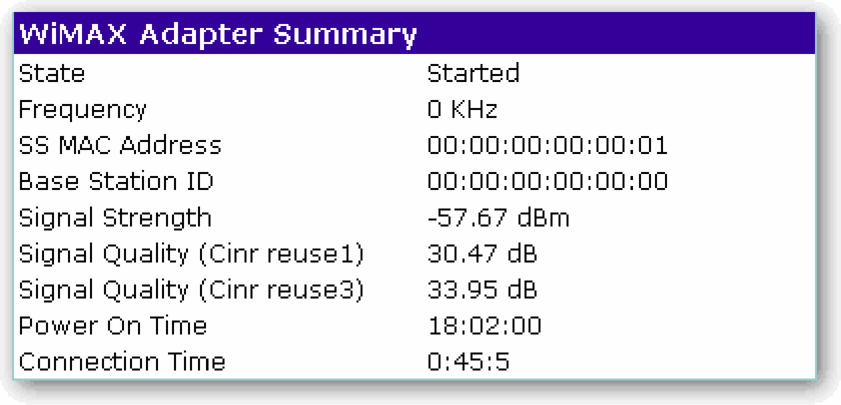
System administrator can configure WiMAX modem remotely or locally via a Web Browser. Network configuration must be planned and decided before starting the configuration procedure.

Under “Device Configuration”, all available functions are grouped in the following categories based on their nature:

- **Adapter Summary**
- **Link Status**
- **Service Flows**
- **Statistics**
- **Adapter Info**

1.3.1. Adapter Summary

Click “Adapter Summary” in the main menu (see Figure 3), its summary will appear as follows:



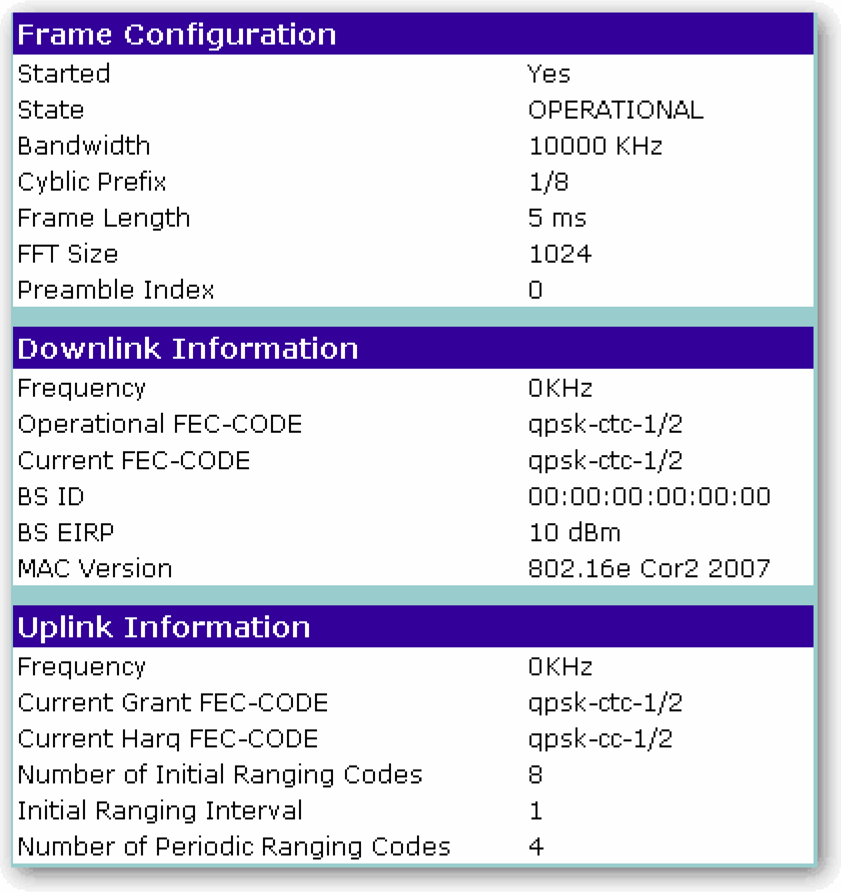
WiMAX Adapter Summary	
State	Started
Frequency	0 KHz
SS MAC Address	00:00:00:00:00:01
Base Station ID	00:00:00:00:00:00
Signal Strength	-57.67 dBm
Signal Quality (Cinr reuse1)	30.47 dB
Signal Quality (Cinr reuse3)	33.95 dB
Power On Time	18:02:00
Connection Time	0:45:5

Figure 3. Adapter Summary

- **State:** Connection status between CPE (i.e. WiMAX modem) and Base Station.
- **Frequency:** Downlink frequency status.
- **SS MAC Address:** Display WiMAX MAC address of this CPE
- **Base Station ID:** Display Base Station’s MAC address CPE is connected to.
- **Signal Strength:** Display strength of signal CPE is receiving.
- **Signal Quality (Cinr resue1):** Display quality of signal CPE is receiving.
- **Signal Quality (Cinr resue3):** Display quality of signal CPE is receiving.
- **Power On Time:** Display the time when the CPE is powered up.
- **Connection Time:** Display the duration that CPE has been connecting to Base Station.

1.3.2. Link Status

Figure 4 shows the following Link Status information:



Frame Configuration	
Started	Yes
State	OPERATIONAL
Bandwidth	10000 KHz
Cyblic Prefix	1/8
Frame Length	5 ms
FFT Size	1024
Preamble Index	0

Downlink Information	
Frequency	0KHz
Operational FEC-CODE	qpsk-ctc-1/2
Current FEC-CODE	qpsk-ctc-1/2
BS ID	00:00:00:00:00:00
BS EIRP	10 dBm
MAC Version	802.16e Cor2 2007

Uplink Information	
Frequency	0KHz
Current Grant FEC-CODE	qpsk-ctc-1/2
Current Harq FEC-CODE	qpsk-cc-1/2
Number of Initial Ranging Codes	8
Initial Ranging Interval	1
Number of Periodic Ranging Codes	4

Figure 4. Link Status

Frame Configuration

- **Started:** “Yes” indicates successful start-up.
- **State:** Display connection status
- **Bandwidth:** Display the existing Bandwidth.
- **Cyclic Prefix:** Display the existing Cyclic Prefix.
- **Frame Length:** Display the existing Frame Length.
- **FFT Size:** Displays the existing FFT size.
- **Preamble Index:** Display preamble index.

Downlink Information

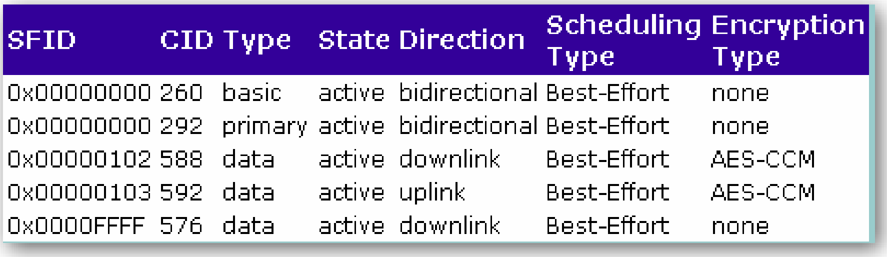
- **Frequency:** Display downlink frequency.
- **Operational FEC-CODE:** Display the Operational FEC-CODE type.
- **Current FEC-CODE:** Display the Current FEC-CODE type.
- **BS ID:** Display Base Station ID.
- **BS EIRP:** Display Base Station EIRP.
- **MAC Version:** Display MAC Version.

Uplink Information

- **Frequency:** Display uplink frequency.
- **Operational FEC-CODE:** Display the Operational FEC-CODE type.
- **Current FEC-CODE:** Display the current FEC-CODE type
- **Initial Ranging Interval:** Display the initial Ranging Interval.
- **Number of Periodic Ranging Codes:** Display the Number of Periodic Ranging Codes.

1.3.3. Service Flows

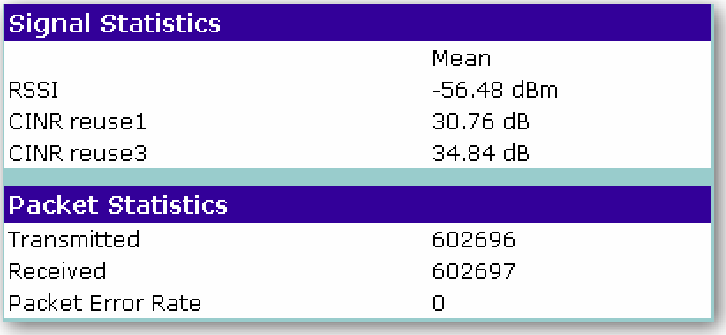
Figure 5 illustrates service flow information when Base Station and CPE are connected.



SFID	CID	Type	State	Direction	Scheduling Type	Encryption Type
0x00000000	260	basic	active	bidirectional	Best-Effort	none
0x00000000	292	primary	active	bidirectional	Best-Effort	none
0x00000102	588	data	active	downlink	Best-Effort	AES-CCM
0x00000103	592	data	active	uplink	Best-Effort	AES-CCM
0x0000FFFF	576	data	active	downlink	Best-Effort	none

Figure 5. Service Flows

1.3.4. Statistics



Signal Statistics	
	Mean
RSSI	-56.48 dBm
CINR reuse1	30.76 dB
CINR reuse3	34.84 dB

Packet Statistics	
Transmitted	602696
Received	602697
Packet Error Rate	0

Figure 6. Statistics

Signal Statistics

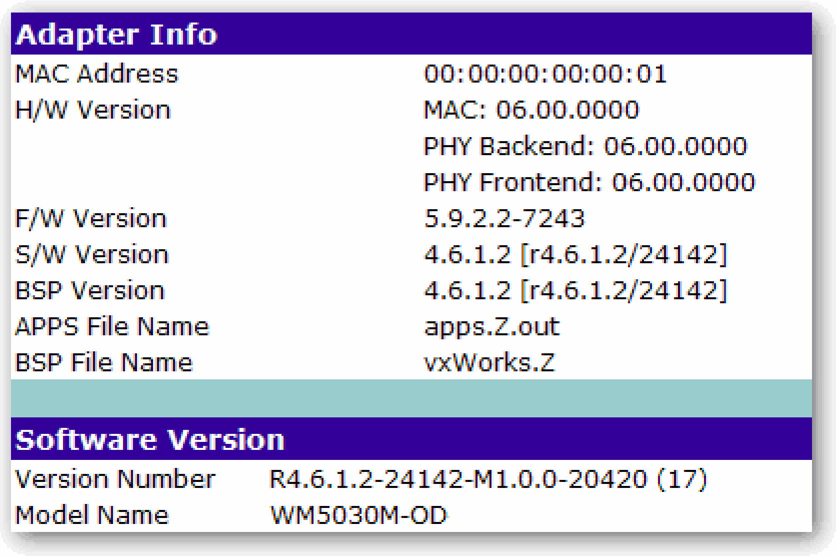
- **RSSI:** Display the average receiving signal strength value.
- **CINR resue1:** Display the average CINR resue1 signal quality value.
- **CINR resue3:** Display the average CINR resue3 signal quality value.

Packet Statistics

- **Transmitted:** Display the amount of transmitted packet.
- **Received:** Display the amount of received packet.
- **Packet Error Rate:** Display packet error rate.

1.3.5. Adapter Info

Figure 7 illustrates the following design related information in the device:



Adapter Info	
MAC Address	00:00:00:00:00:01
H/W Version	MAC: 06.00.0000 PHY Backend: 06.00.0000 PHY Frontend: 06.00.0000
F/W Version	5.9.2.2-7243
S/W Version	4.6.1.2 [r4.6.1.2/24142]
BSP Version	4.6.1.2 [r4.6.1.2/24142]
APPS File Name	apps.Z.out
BSP File Name	vxWorks.Z

Software Version	
Version Number	R4.6.1.2-24142-M1.0.0-20420 (17)
Model Name	WM5030M-OD

Figure 7. Adapter Information

Adapter Info

- **MAC Address:** Display CPE's MAC address.
- **H/W Version:** Display Hardware version.
- **F/W Version:** Display Firmware version.
- **S/W Version:** Display Software version.
- **BSP Version:** Display BSP version.
- **Apps File Name:** Display Apps File Name.
- **BSP File Name:** Display BSP File Name.

Software Version

- **Version Number:** Display software version.
- **Model Name:** Display device's model name.

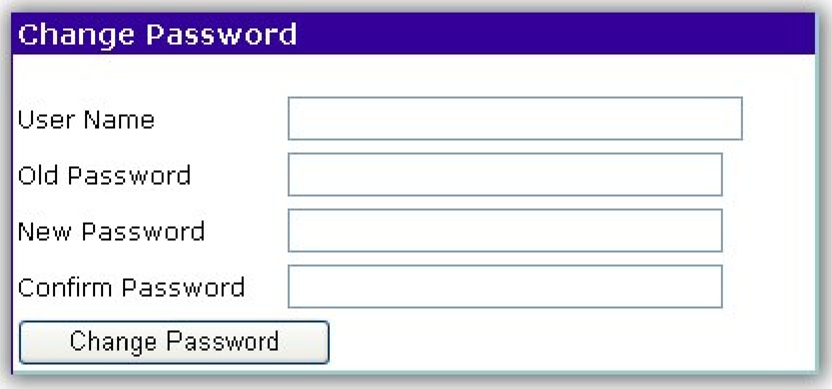
1.4. Device Management

In Device Management, user can configure WiMAX modem's settings. The main categories are as follows:

- **Change Password**
- **Network Parameters**
- **Available Networks**
- **Full Scan**
- **Provisioning**
- **Scanning List**
- **Authentication Settings**
- **CS Capabilities**
- **SNTP**

1.4.1. Change Password

User can change the login password when he or she logs in as administrator. As shown in Figure 8, user has to enter user name and the original password (**Old Password**), and new password (**New Password**), and then re-confirms the password (**Confirm Password**). Click "Change Password" to change password. If the information is correct, user can use the new password for subsequent login.



Change Password

User Name

Old Password

New Password

Confirm Password

Figure 8. Change Password

1.4.2. Network Parameters

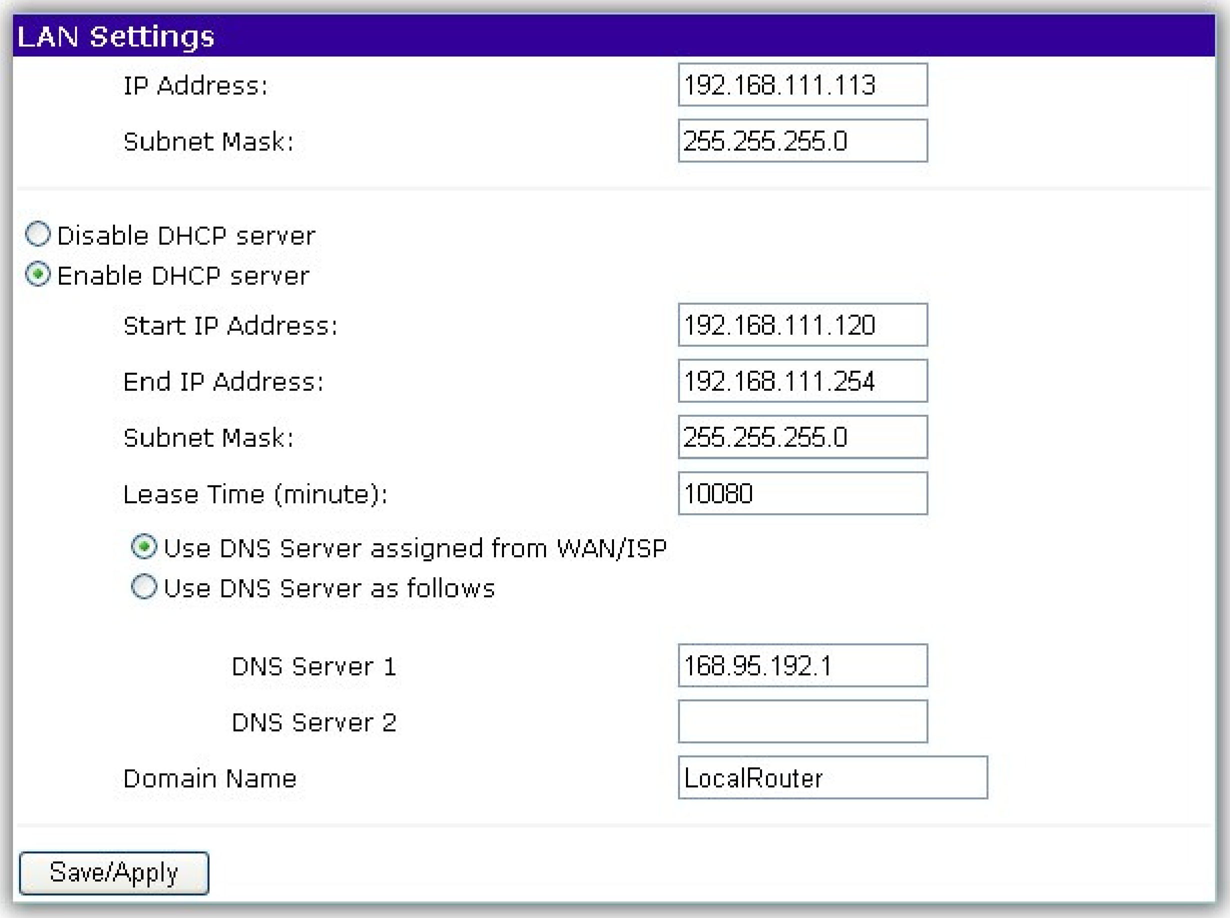
There are two sub-categories in Network Parameters:

- **LAN**
- Routing

1.4.2.1. LAN

Figure 9 displays LAN (Local Area Network) settings. User can feed IP address (LAN IP) and Subnet Mask into WiMAX modem.

User can select to Disable/Enable modem's DHCP Server function. When user enables the DHCP server function, he must also configure related settings for DHCP server. The Start IP Address and End IP address must be in the same subnet as the local IP Address of the LAN interface.



LAN Settings

IP Address:	192.168.111.113
Subnet Mask:	255.255.255.0

○ Disable DHCP server
● Enable DHCP server

Start IP Address:	192.168.111.120
End IP Address:	192.168.111.254
Subnet Mask:	255.255.255.0
Lease Time (minute):	10080

● Use DNS Server assigned from WAN/ISP
○ Use DNS Server as follows

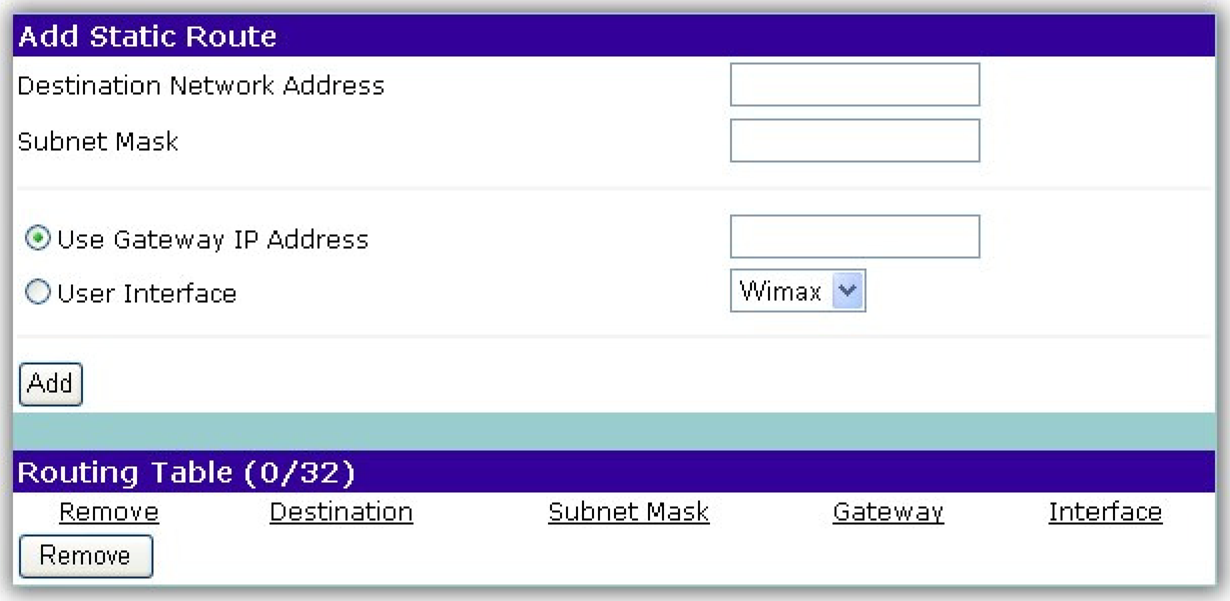
DNS Server 1	168.95.192.1
DNS Server 2	
Domain Name	LocalRouter

Figure 9. LAN

1.4.2.2. Routing

As shown in Figure 10, user can assign the Static Routing rule in this page.

Static Route Table can be configured with 32 entries maximum.



Add Static Route

Destination Network Address

Subnet Mask

● Use Gateway IP Address

○ User Interface: Wimax

Routing Table (0/32)

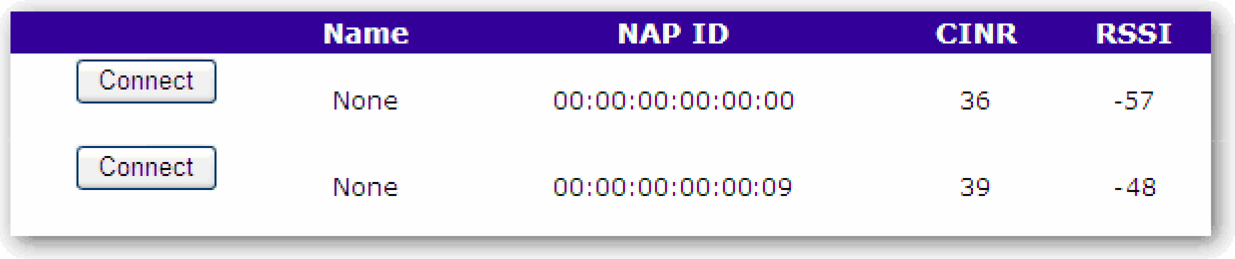
Remove	Destination	Subnet Mask	Gateway	Interface

Figure 10. Routing

Enter the destination network address, subnet mask, gateway IP address and/or interface, then click "Add" to add the entry to the routing table. Click “Remove” to remove a static routing rule from the Static Routing table.

1.4.3. Available Networks

The available networks are displayed in this table, with information about the NAP (Network Access Provider) ID, and the signal strength statistics CINR and RSSI. User can select the network that he want to connect to from this table and click the Connect button to connect to the network that he selects from the Available Networks table.

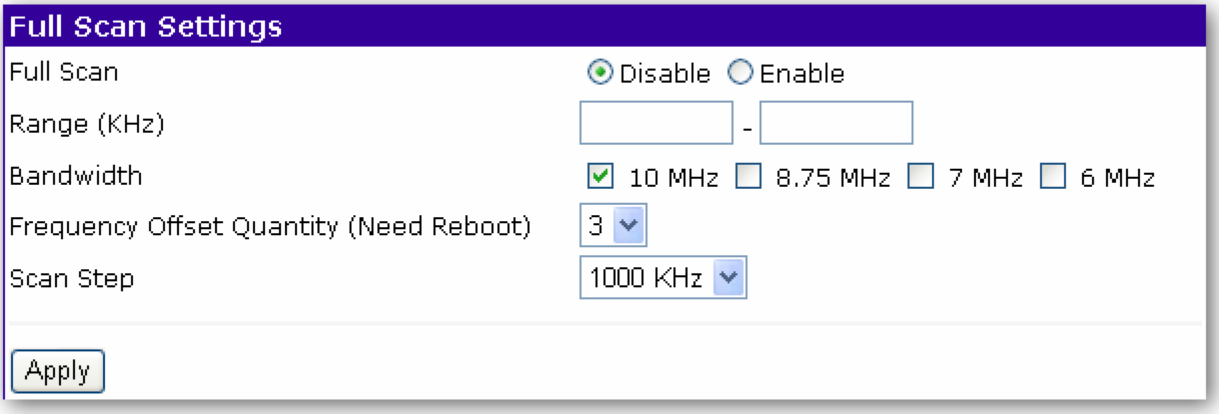


	Name	NAP ID	CINR	RSSI
Connect	None	00:00:00:00:00:00	36	-57
Connect	None	00:00:00:00:00:09	39	-48

Figure 11. Available Network Table

1.4.4. Full Scan

The Full Scan mode can be configured in the table. User can set the Range, Bandwidth and Scan Step from this table to enforce the CPE to do Full Scan for searching the WiMAX Base Stations in the configured Frequency Range, while the CPE can not connect to any frequency in the Scanning List. The Range is displayed min frequency to max frequency by user's device.



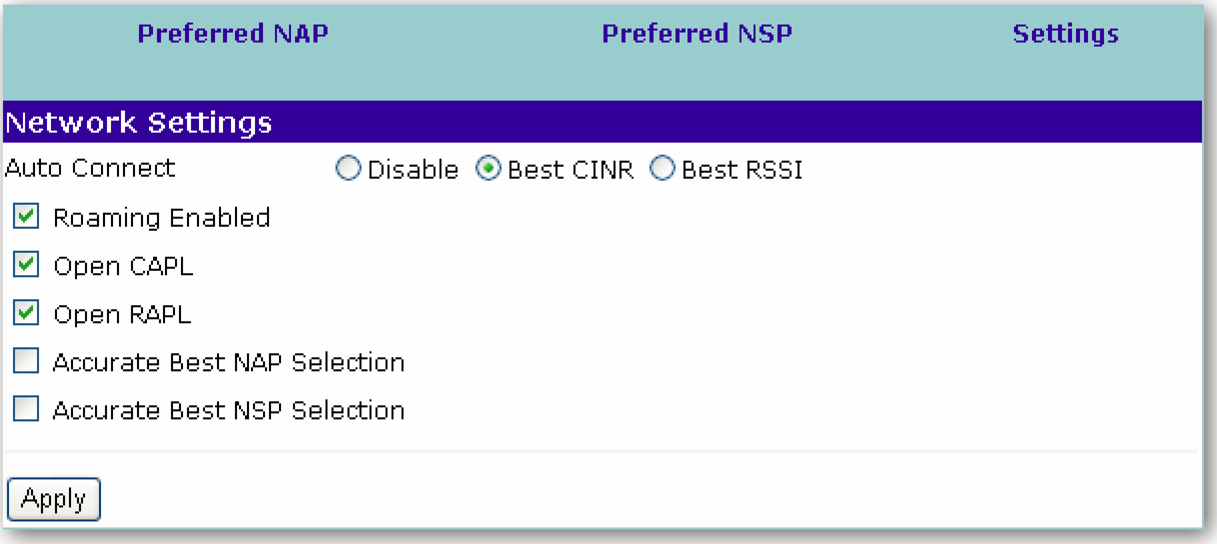
Full Scan Settings

Full Scan	● Disable ○ Enable
Range (KHz)	___ - ___
Bandwidth	☑ 10 MHz ☐ 8.75 MHz ☐ 7 MHz ☐ 6 MHz
Frequency Offset Quantity (Need Reboot)	3
Scan Step	1000 KHz

Figure 12. Full Scan Table

1.4.5. Provisioning

The Provisioning tab provides the following informational and interactive dialog elements:



Auto Connect ○ Disable ● Best CINR ○ Best RSSI

☑ Roaming Enabled

☑ Open CAPL

☑ Open RAPL

□ Accurate Best NAP Selection

□ Accurate Best NSP Selection

Figure 13. Provisioning Information

- **Preferred NAP**

This tab provides a display area for the contractual agreement preference list with information about the NAP ID, priority and channels.

- **Preferred NSP**

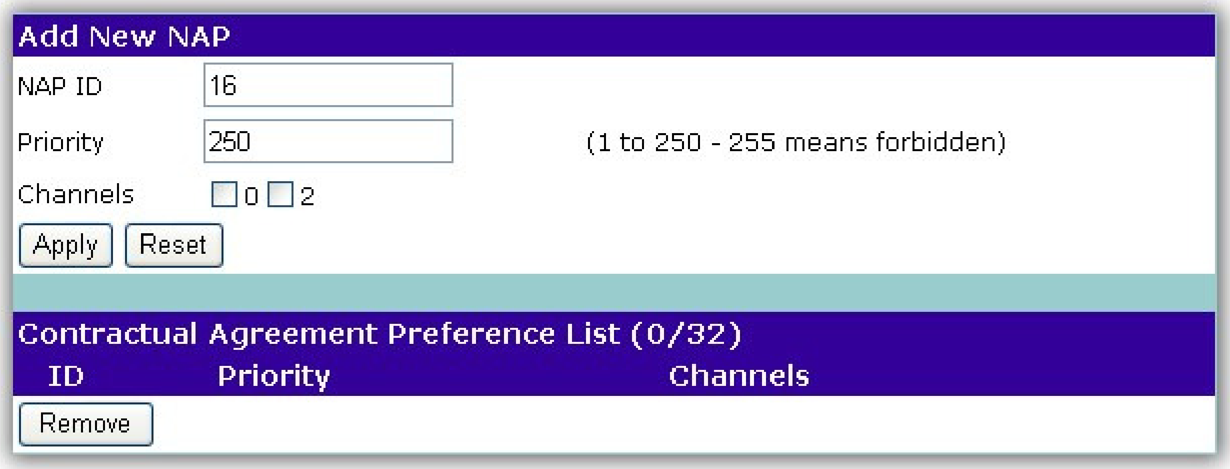
This tab provides a display area for the roaming agreement preference list with information about the NSP name, priority and IDs.

- **Settings**

This tab provides fields to select or configure the network settings.

1.4.5.1. Preferred NAP

This tab provides a display area for the contractual agreement preference list with information about the NAP ID, priority and channels. NAP is the network access provider. Each NAP is identified with an NAP ID and associated with a channel list. Contractual Agreement Preference List is a list of NAPs defined by NAP IDs that give access to the home NSP. The CAPL can be empty. Each NAP defined in the CAPL is associated with a channel list. The channel list can be empty, which indicates all provisioned channels.



Add New NAP

NAP ID: 16

Priority: 250 (1 to 250 - 255 means forbidden)

Channels: □ 0 □ 2

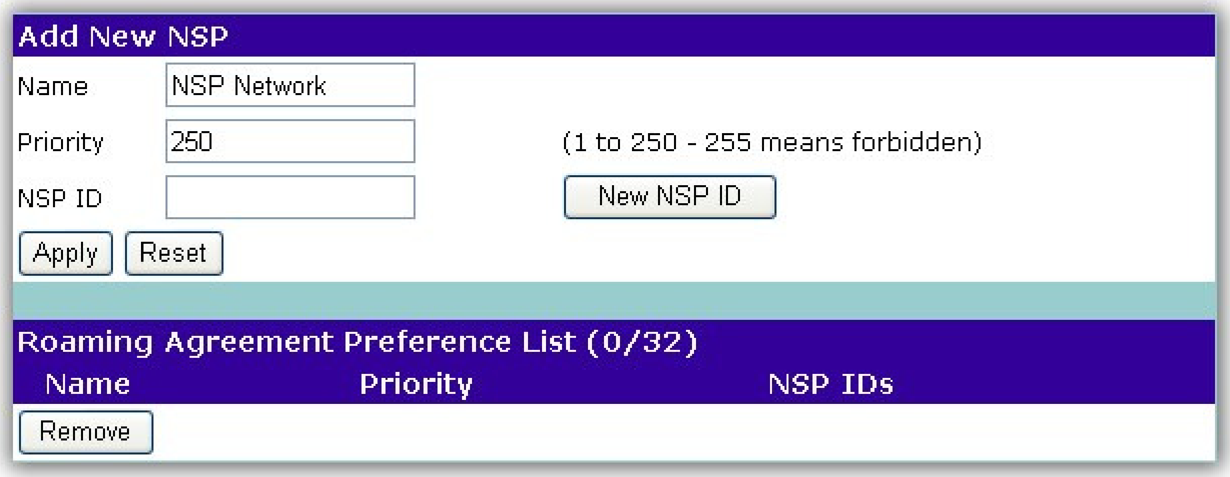
Contractual Agreement Preference List (0/32)

ID	Priority	Channels

Figure 14. Preferred NAP setting

1.4.5.2. Preferred NSP

This tab provides a display area for the roaming agreement preference list with information about the NSP name, priority and IDs. User can configure this parameter with the NSP names as character strings and NSP ID lists. An NSP ID list can be empty. Roaming Agreement Preference List is a list of NSPs defined by NSP IDs, to which the MS can connect if the home NSP is not found. The RAPL can be empty.


Add New NSP

Name: NSP Network

Priority: 250 (1 to 250 - 255 means forbidden)

NSP ID:

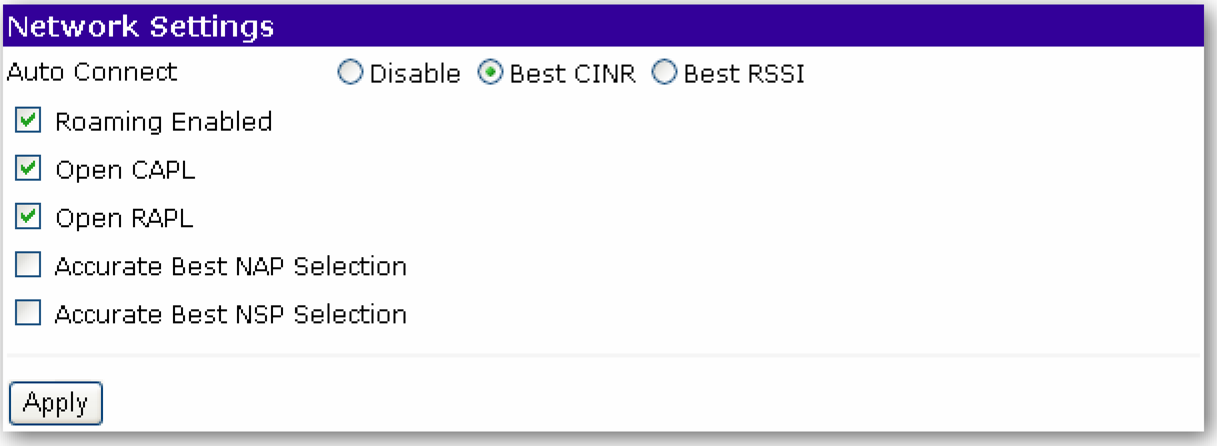
Roaming Agreement Preference List (0/32)

Name	Priority	NSP IDs

Figure 15. Preferred NSP Setting

1.4.5.3. Settings

This tab provides fields to select or configure the network settings


Network Settings

Auto Connect ○ Disable ● Best CINR ○ Best RSSI

☑ Roaming Enabled

☑ Open CAPL

☑ Open RAPL

□ Accurate Best NAP Selection

□ Accurate Best NSP Selection

Figure 16. NDSS Settings

Auto Connect

Disabled

MS performs a full round of scanning.

Best CINR

MS tries to perform network entry automatically as soon as a valid NAP or NSP is found. The MS connects to the channel with the best CINR, depending on the other scanning configuration parameters. The NDS state moves automatically from SCANNING to CONNECTING.

Best RSSI

MS tries to perform network entry automatically as soon as a valid NAP or NSP is found. The MS connects to the channel with the best RSSI, depending on the other scanning configuration parameters. The NDS state moves automatically from SCANNING to CONNECTING.

Roaming Enabled

Enabled

MS can connect to NSPs other than the home NSP. All channels are scanned to retrieve all possible NSPs.

Disabled

MS only scans channels from the CAPL. If the CAPL is empty, then the MS scans all channels.

Open CAPL

Enabled

CAPL is semi-open. The MS considers BS from any NAP.

Disabled

CAPL is exclusive. The MS considers only BS from the CAPL.

Open RAPL

Enabled

RAPL is semi-open. MS considers BS from any NSP.

Disabled

RAPL is exclusive. MS considers only BS from the RAPL. This parameter is only valid if the roaming Enabled parameter is enabled.

Accurate Best NAP Selection

Enabled

MS looks for the highest priority NAP.

Disabled

MS connects to the first allowed NAP. This parameter is only valid if Auto Connect is enabled.

Accurate Best NSP Selection

Enabled

MS looks for the highest priority NSP.

Disabled

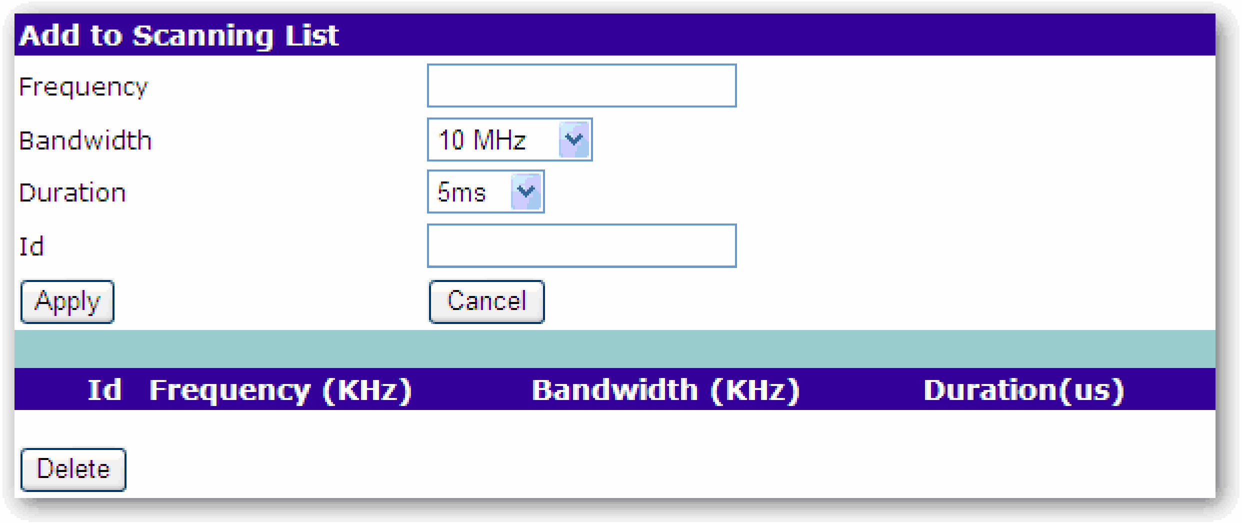
MS connects to the first allowed NSP in the CAPL. This parameter is only valid when Auto Connect is enabled.

Scanning Interval

After trying all the configured channels, the MS waits for certain interval time specified in this field before scanning again. This option can preserve battery power in battery-operated devices.

1.4.6. Scanning List

Figure 17 illustrates current channel setting. User can set the all bandwidth simultaneously. This setting affects the availabilities of each channel. The available state of each channel is shown on last column of the table.



Add to Scanning List

Frequency	
Bandwidth	10 MHz
Duration	5ms
Id	

Id	Frequency (KHz)	Bandwidth (KHz)	Duration(us)

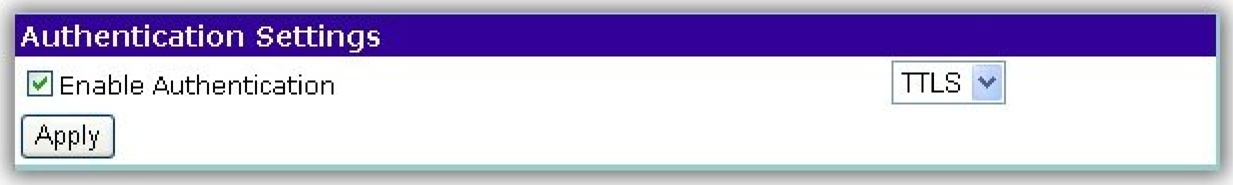
Figure 17. Scanning List

- Frequency: Input the required frequency.
- Bandwidth: Input the required Bandwidth, e.g. 3MHz / 4.375MHz / 5MHz / 6MHz / 7MHz / 8.75MHz / 10MHz.
- Duration: Choose the required Duration, e.g. 5ms / 10ms.
- ID: Input the required Identity

Note: A channel can not be added when WiMAX modem is scanning state. Press “Disconnect” to stop.

1.4.7. Authentication Setting

To use the authentication feature, user must provide security settings. Select “Authentication Settings” page to display dialog (see Figure 18). This section illustrates how to use the functions on the Authentication Settings page.



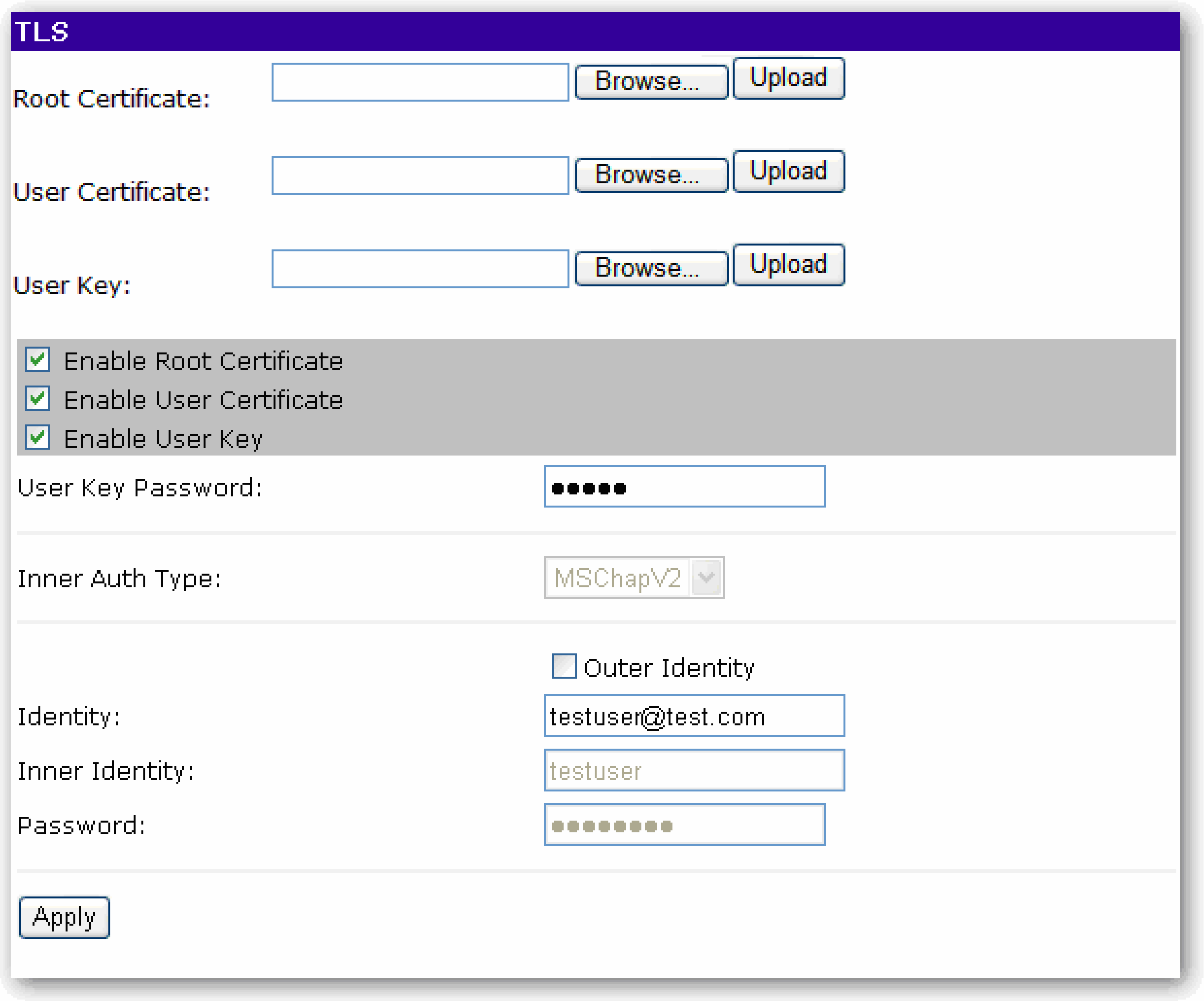
Authentication Settings

☑ Enable Authentication TTLS

Figure 18. Authentication Setting

Authentication type means EAP authentication method. The following methods are available:

- TLS
- TTLS



TLS

Root Certificate:

User Certificate:

User Key:

☑ Enable Root Certificate

☑ Enable User Certificate

☑ Enable User Key

User Key Password: ●●●●●

Inner Auth Type: MSChapV2

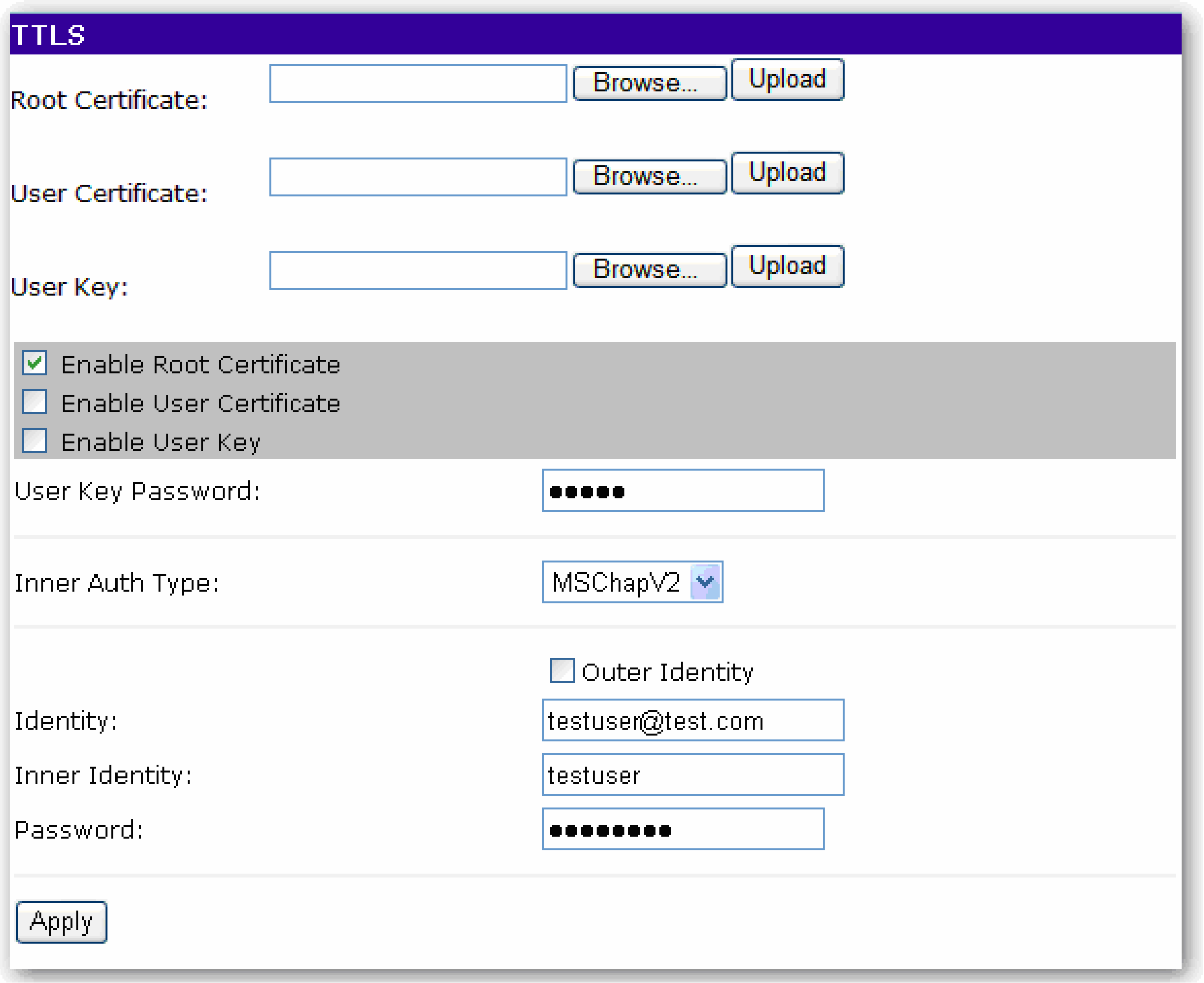
□ Outer Identity

Identity: testuser@test.com

Inner Identity: testuser

Password: ●●●●●●●●

Figure 19. TLS Settings



TTLS

Root Certificate:

User Certificate:

User Key:

☑ Enable Root Certificate

□ Enable User Certificate

□ Enable User Key

User Key Password: ●●●●●

Inner Auth Type: MSChapV2

□ Outer Identity

Identity: testuser@test.com

Inner Identity: testuser

Password: ●●●●●●●●●

Figure 20. TTLS Settings

Inner Auth type

The inner round of EAP authentication type only applies to EAP-TTLS. The following methods are available:

- CHAP
- MD5
- PAP
- MSCHAPV1
- MSCHAPV2

Identity

MS identity is for the outer EAP round.

Inner Identity

MS identity is for the inner EAP round which only applies to EAP-TTLS. To enhance privacy, an inner identity can be different from the outer identity, which is insecure.

Password

It's a shared secret that can be used during the inner EAP round and only applies to EAP-TTLS.

CA Certificate

It's a certificate to authenticate BS, either directly or by chaining.

User certificate

It's MS public certificate. The User needs to duplicate user certificate if certificate and user key are in the same file.

Decryption Key

It's MS private key, if not included within MS user certificate. The key depends on the file format and only applies to EAP-TLS. User needs to duplicate user key if user certificate and key are in the same file. The user key field can not be empty.

Decryption Key File Password

Password: It's optional password protection for MS' private key.

Figure 19 and Figure 20 illustrate EAP's setting. User can select Enable Authentication to enable authentication, select authentication type, and then press "Apply" to save settings. To upload a certification file, user has to browse and select the file by pressing "Browse…", then press "Upload". Press "Apply" to save text input. Changes will take effect after pressing "Reconnect" button.

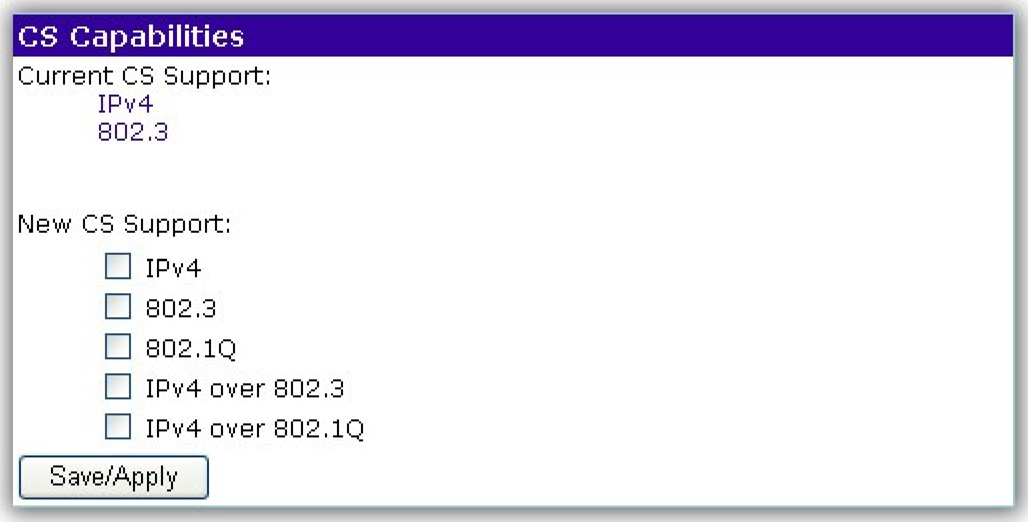
Note: The above figures are just for example. For using the WiMAX service, please use the correct authentication type and user information that ISP provides for the authentication setting.

1.4.8. CS Capabilities

The current CS (Convergence Sub-Layer) capabilities supported are listed in Figure 21. The supported CS types are:

- IPv4
- 802.3

If settings are changed, user has to reboot the device to enable CS support.



CS Capabilities

Current CS Support:
IPv4
802.3

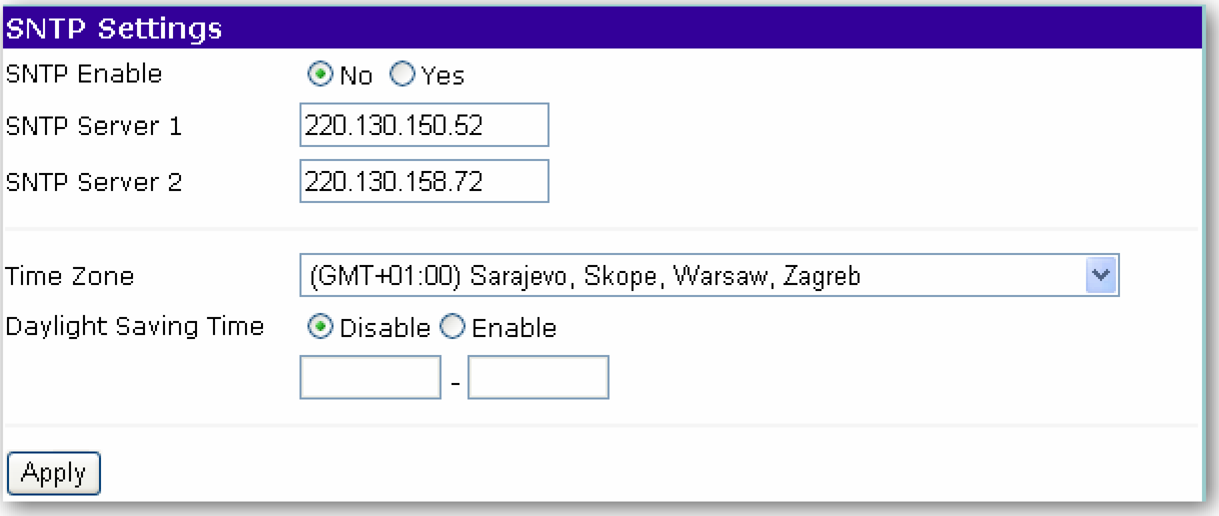
New CS Support:

□ IPv4
□ 802.3
□ 802.1Q
□ IPv4 over 802.3
□ IPv4 over 802.1Q

Figure 21. CS Capabilities

1.4.9. SNTP

SNTP (Simple Network Time Protocol) is a simplified version of the NTP (Network Time Protocol) protocol.



SNTP Settings

SNTP Enable ● No ○ Yes

SNTP Server 1 220.130.150.52

SNTP Server 2 220.130.158.72

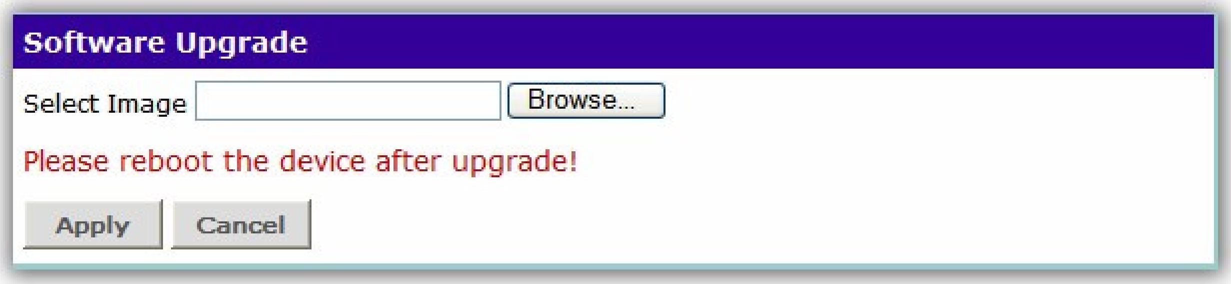
Time Zone (GMT+01:00) Sarajevo, Skope, Warsaw, Zagreb

Daylight Saving Time ● Disable ○ Enable

Figure 22. SNTP Settings

1.5. Software Upgrade

As Figure 23 illustrates, user can upgrade modem via the web. Click “Browse…” and select the upgrade file that has “.img” suffix in computer. Click “Apply” to start upgrade. Time spent depends on image size and modem usage status.



Please reboot the device after upgrade!

Figure 23. Software Upgrade

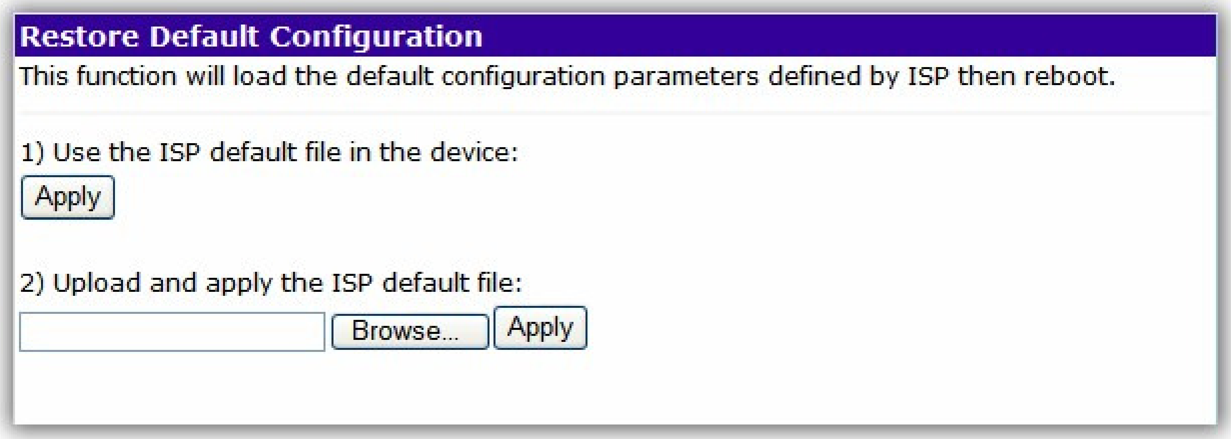
⚠

WARNING

Interrupting the update process may crash this Modem Image. Please Wait until the update process is finished before terminating the network or switching off the device.

1.6. Restore Default Configuration

This function can be used to load default configuration parameters by ISP (if provided). User needs to reboot device to make new settings take effect.



Restore Default Configuration

This function will load the default configuration parameters defined by ISP then reboot.

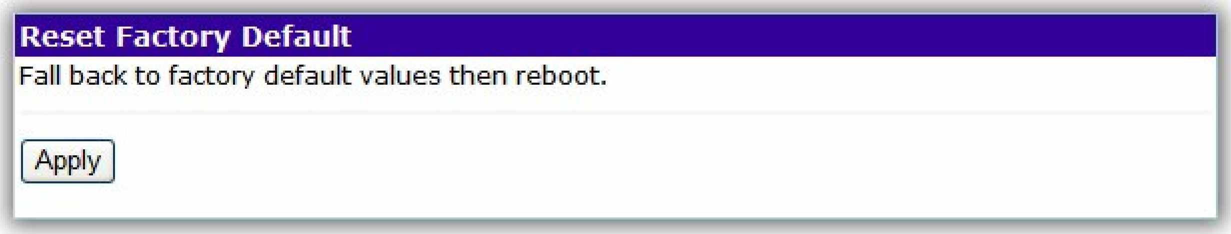
1) Use the ISP default file in the device:

2) Upload and apply the ISP default file:

Figure 24. Restore Default Configuration

1.7. Reset Factory Default

Press “Reset Factory Default” (see Figure 25) to reset to factory default settings. User needs to reboot device to make new settings take effect



Reset Factory Default

Fall back to factory default values then reboot.

Figure 25. Reset Factory Default

1.8. Reconnect/Disconnect

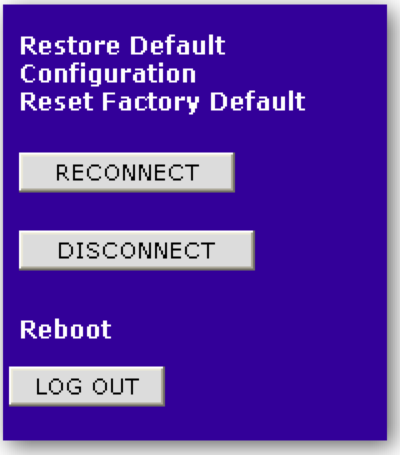


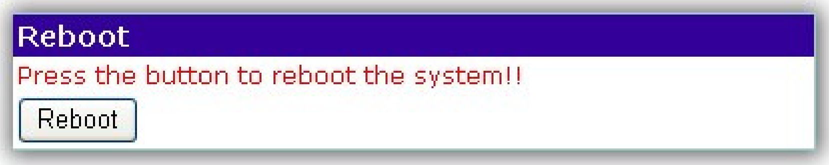
Figure 26. “RECONNECT” and “DISCONNECT” button

Press “Reconnect” to reconnect the CPE to the WIMAX Network.

Press “Disconnect” to disconnect the CPE from the WIMAX Network.

1.9. Reboot

Press “Reboot” to reboot device to make new settings take effect

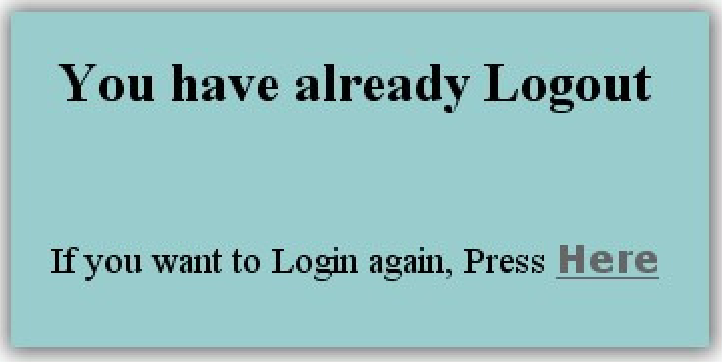

Reboot

Press the button to reboot the system!!

Figure 27. Reboot Button

1.10. Logout

Press “Logout” in the main menu, user will not be able to configure settings. To change device settings, access start-up page and login again.



You have already Logout

If you want to Login again, Press Here

Figure 28. Logout page

1.11. Change Mode

User can change mode between Router Mode and Bridge Mode. Press “BRIDGE MODE” button to change to bridge mode. User needs to reboot device to make new settings take effect.

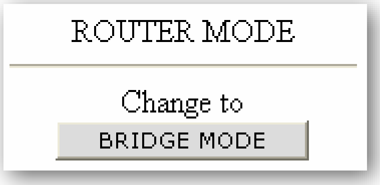


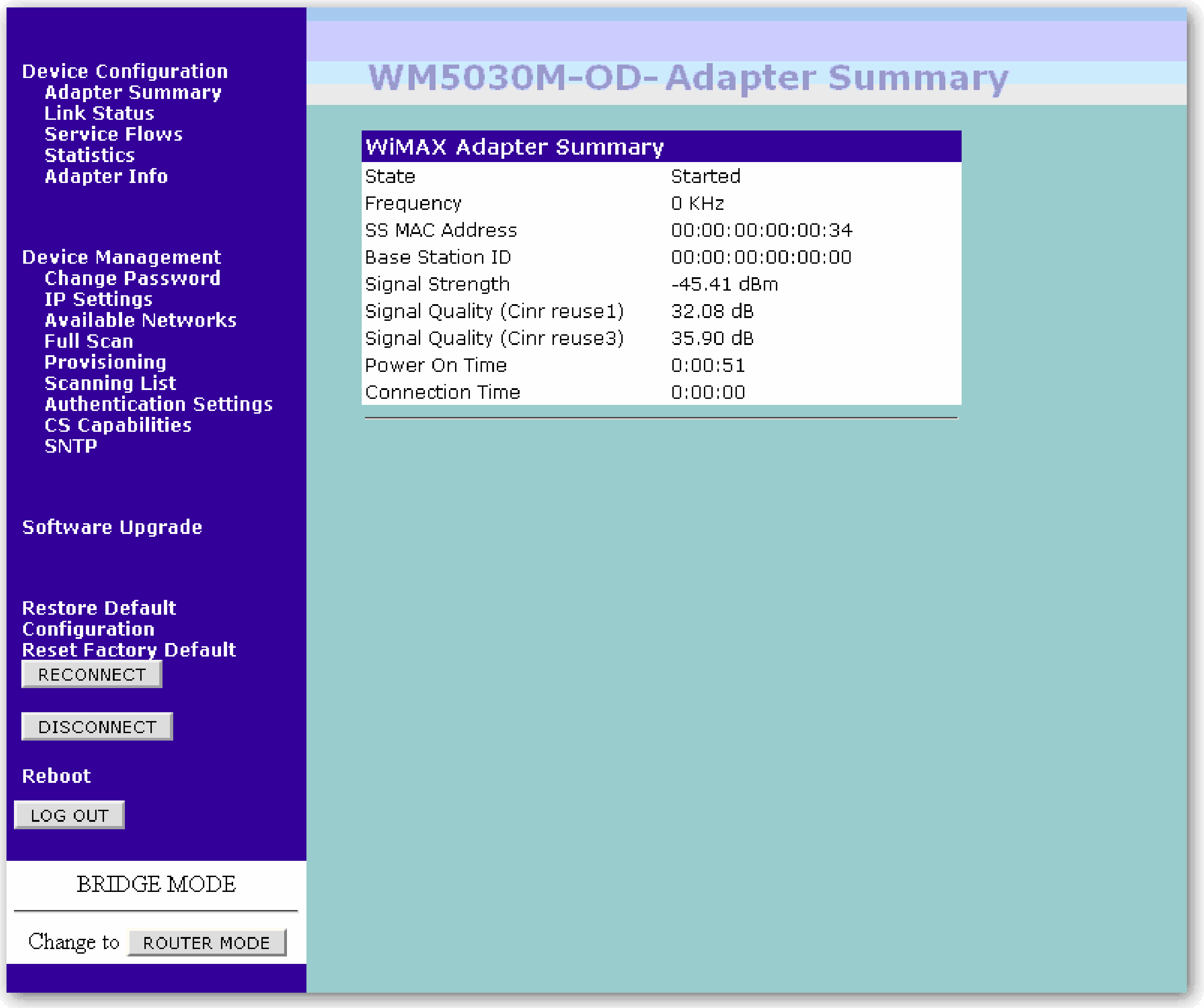
Figure 29. Change Mode Button

2 Bridge Mode

This chapter illustrates the configuration setting of the modem that supports bridge mode.

2.1. Router Mode and Bridge Mode

Other than supporting the Router mode to support IP Sharing for LAN network, this modem can be configured to work in bridge mode between WiMAX network and Ethernet LAN. User can switch operation modes according to his or her needs. Press the Button “BRIDGE MODE” or “ROUTER MODE” to choose the desired mode. Reboot the device to make new settings take effect.

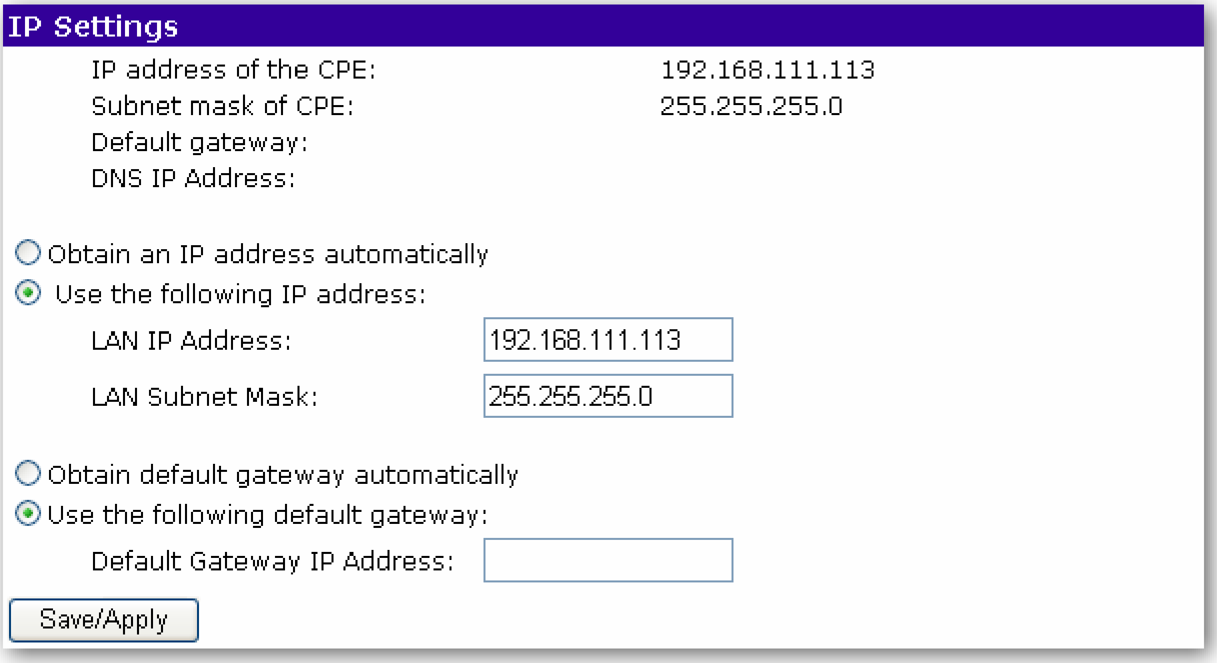


WiMAX Adapter Summary	
State	Started
Frequency	0 KHz
SS MAC Address	00:00:00:00:00:34
Base Station ID	00:00:00:00:00:00
Signal Strength	-45.41 dBm
Signal Quality (Cinr reuse1)	32.08 dB
Signal Quality (Cinr reuse3)	35.90 dB
Power On Time	0:00:51
Connection Time	0:00:00

Figure 30. Home Page of Bridge Mode

2.1.1. IP Setting

This page allows user to configure LAN IP Settings. Enter the ISP provided information to configure the LAN IP setting. User can configure the IP address and gateway with static value manually



IP Settings

IP address of the CPE: 192.168.111.113

Subnet mask of CPE: 255.255.255.0

Default gateway:

DNS IP Address:

○ Obtain an IP address automatically

● Use the following IP address:

LAN IP Address: 192.168.111.113

LAN Subnet Mask: 255.255.255.0

○ Obtain default gateway automatically

● Use the following default gateway:

Default Gateway IP Address:

Figure 31. IP Setting

User can enable “Obtain an IP address automatically” to obtain an IP address automatically. Or user can enable “Use the following IP address” to configure static IP address and subnet mask such as Figure 31.

Notice: Configuring the gateway with static value will disable the automatic assignment from DHCP or other connection.

Notice: Please use the Static IP assignment for bridge mode only. Otherwise you may lose the Ethernet connection of the CPE if the CPE can not obtain an IP from the ISP.

3 Software Upgrade from Web page

Recommendation:

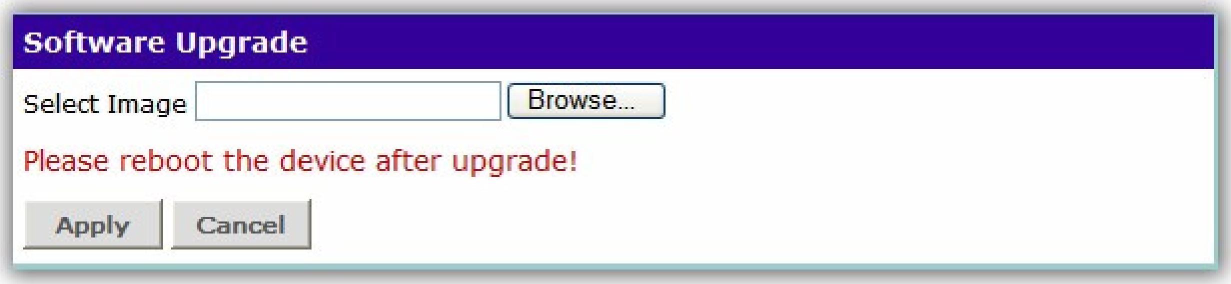
To speed up the upgrade procedure, it’s suggested to stop all network traffic before upgrading. Open “Scanning List” page, and click on “Disconnect” button.

Step 1 Connect the device to a PC or laptop. Configure IP address of network connection to be in the same subnet as default device IP Address. Enter IP address (default is 192.168.111.113) of device from the Web Browser. For example: 192.168.111.113.

A Dialogue Box will pop out and request user login.

Please enter the management username/password into the fields, then click on the OK button (default username/password is **subscriber/subscriber)**

Step 2 Obtain an updated software image file from your ISP. Go to Software Upgrade page and enter the path to the image file location in the box below or click the “Browse…" button to locate the image file which must be “.img” suffix in your computer. Click “Apply” to start upgrading the modem. Time spent is dependent on the image size and the usage status of modem.



Software Upgrade

Select Image

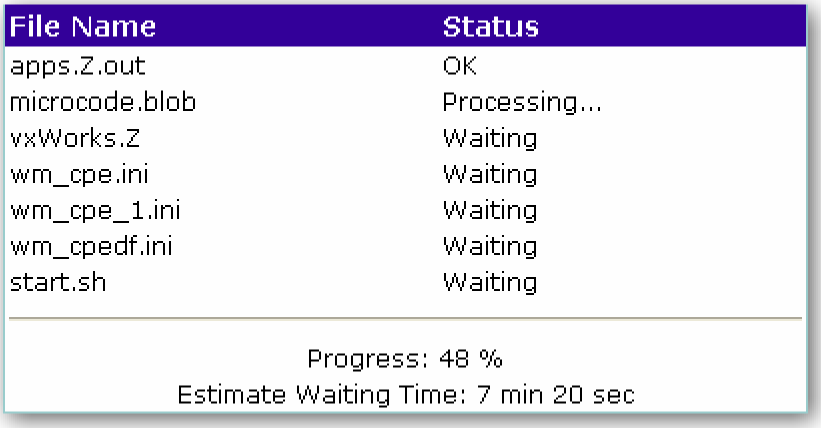
Please reboot the device after upgrade!

Figure 32. Software Upgrade Page

WARNING

Interrupt the updating process may crash this Modem Image. Please Wait until the updating process is finished before terminating the network or switching off the device.

Step 3 Wait for upgrading progress. "Estimate Waiting Time" is the remained estimate time for upgrade process finish, which is for reference only.

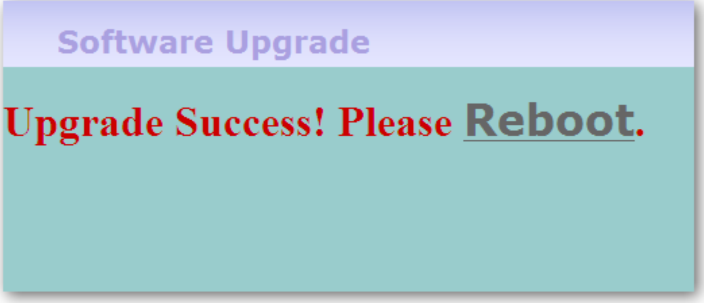


File Name	Status
apps.Z.out	OK
microcode.blob	Processing...
vxWorks.Z	Waiting
wm_cpe.ini	Waiting
wm_cpe_1.ini	Waiting
wm_cpedf.ini	Waiting
start.sh	Waiting

Progress: 48 %

Estimate Waiting Time: 7 min 20 sec

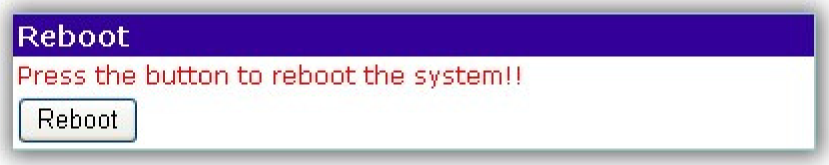
Step 4 "Upgrade Success" will be displayed when upgrading succeeds.



Software Upgrade

Upgrade Success! Please Reboot.

Step 5 Press "Reboot" button to reboot the system.



Reboot

Press the button to reboot the system!!

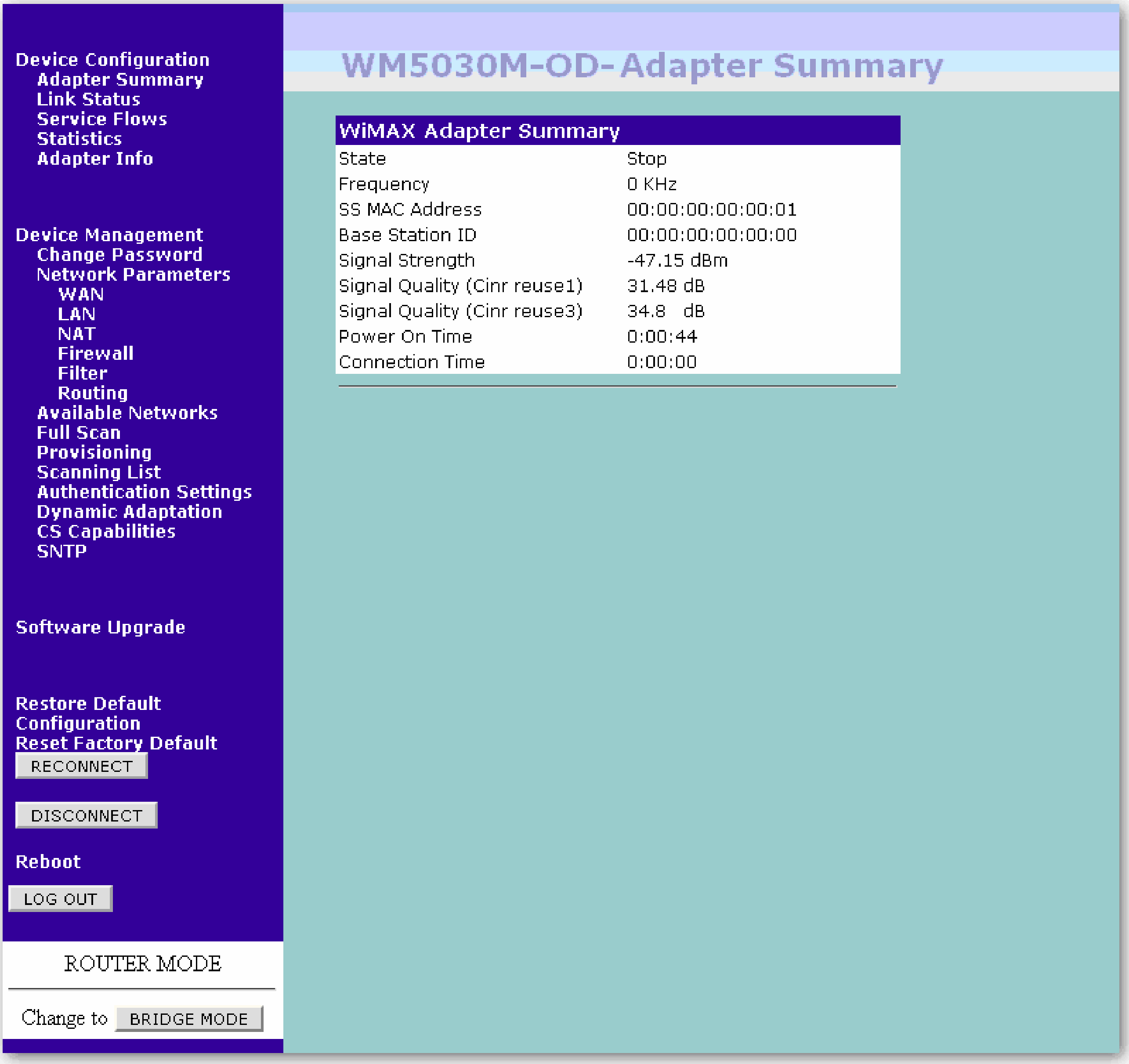
Step 6 After rebooting the system, user can check the latest software version.

4 Advance Setting for Service/ISP

4.1. Advance Setting

WiMAX modem web page configuration supports two administration levels. General users will use “subscriber” as login username. Through this account, user can’t configure Network Parameters, such as WAN, NAT, Firewall and Filter, as well as Dynamic Adaptation.

To enable advance settings in web page, user needs to use “isp” as username to login. The default password for “isp” account is “isp”.



WM5030M-OD-Adapter Summary

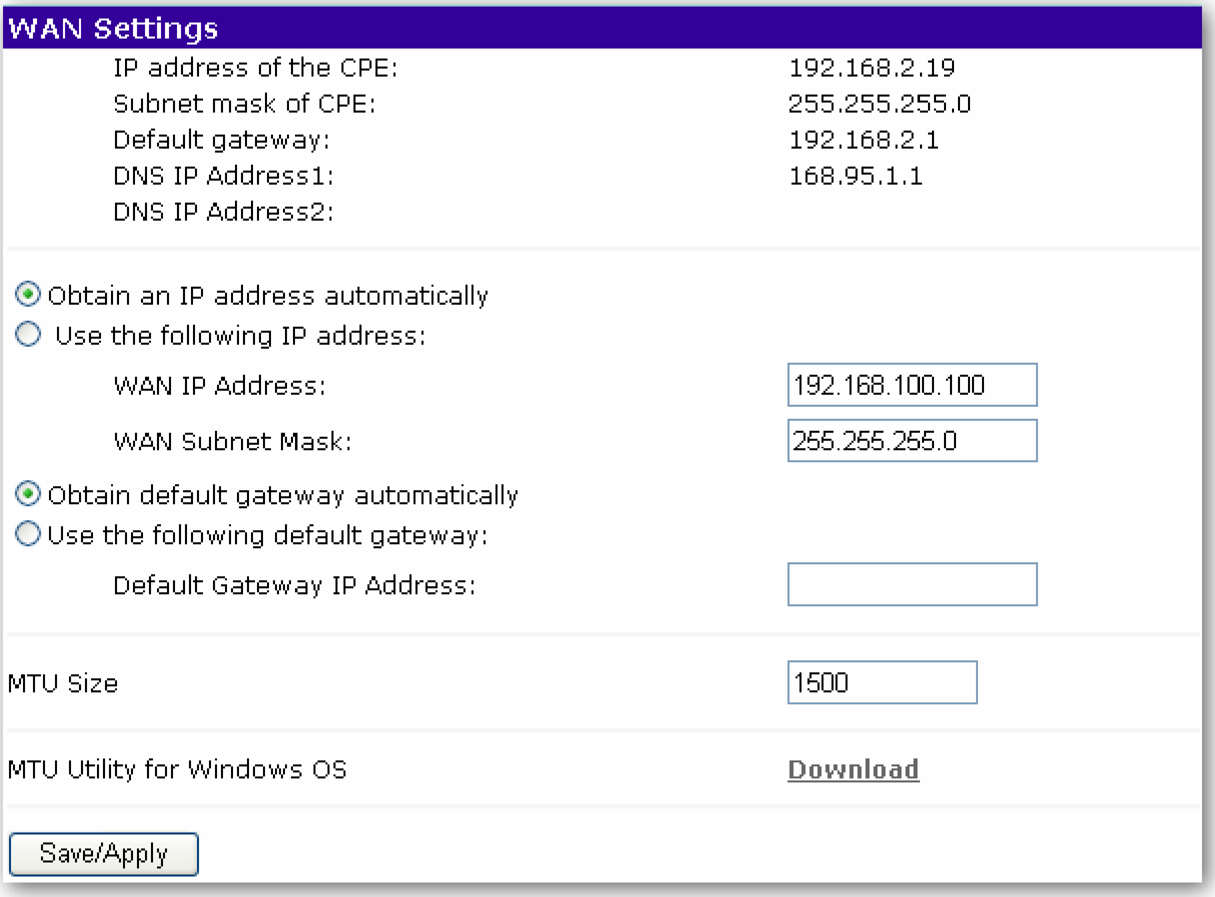
WiMAX Adapter Summary	
State	Stop
Frequency	0 KHz
SS MAC Address	00:00:00:00:00:01
Base Station ID	00:00:00:00:00:00
Signal Strength	-47.15 dBm
Signal Quality (Cinr reuse1)	31.48 dB
Signal Quality (Cinr reuse3)	34.8 dB
Power On Time	0:00:44
Connection Time	0:00:00

Figure 33. Home Page of Advance Settings for Router Mode

4.1.1. Network Parameters - WAN

WAN (Wide Area Network) displays IP address information and subnet mask getting from the ISP for the WiMAX Interface of this modem. (See Figure 34) User can configure WAN setting, e.g. **IP address**, **Default Gateway**, and **DNS**. All of them can be set to auto or manual. When user sets IP address manually, he has to configure the default gateway and DNS manually too.

MTU (Maximum Transfer Unit) can be set between 1300 and 2048.



WAN Settings

IP address of the CPE:	192.168.2.19
Subnet mask of CPE:	255.255.255.0
Default gateway:	192.168.2.1
DNS IP Address1:	168.95.1.1
DNS IP Address2:	

● Obtain an IP address automatically
○ Use the following IP address:

WAN IP Address: 192.168.100.100
WAN Subnet Mask: 255.255.255.0

● Obtain default gateway automatically
○ Use the following default gateway:

Default Gateway IP Address:

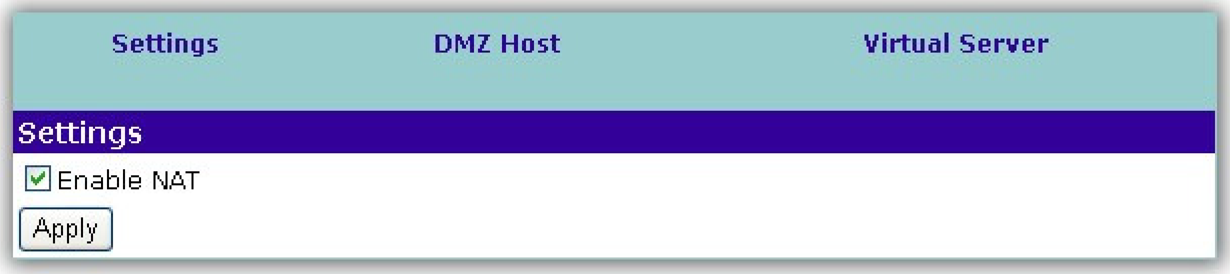
MTU Size: 1500

MTU Utility for Windows OS: Download

Figure 34. WAN

4.1.2. Network Parameters – NAT

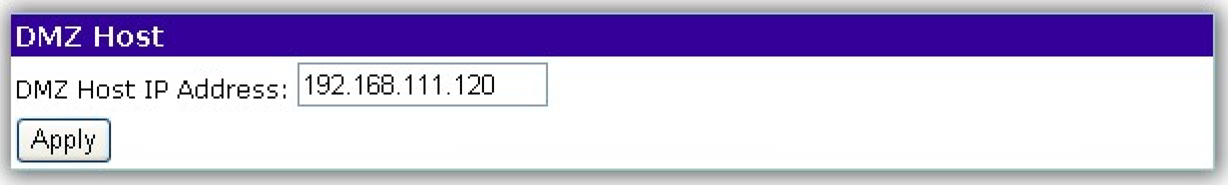
NAT (Network Address Translator) will translate the local IP address to global address and vice versa. In NAT setting, user can click check box to enable NAT settings. Figure 35 displays NAT setting which includes DMZ host and Virtual server.



☑ Enable NAT

Figure 35. NAT

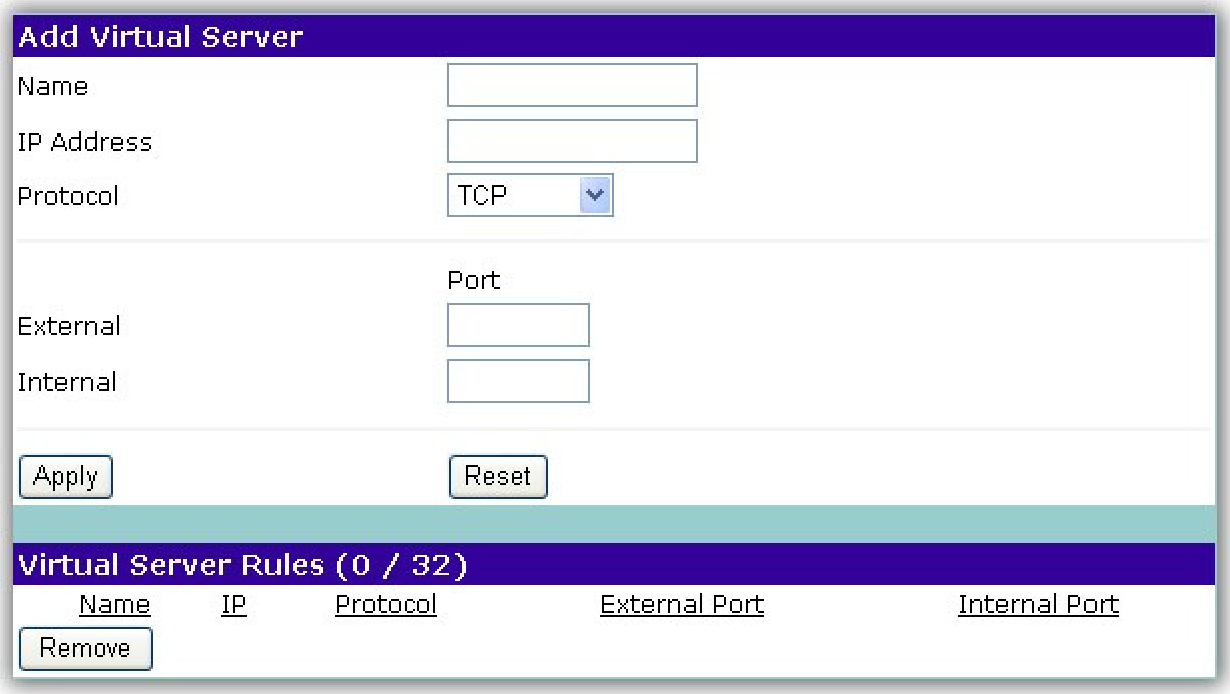
If user has a computer that can not run Internet applications properly from behind the device, then user can allow that computer unrestricted access to Internet, that is, to enter the IP address of that computer as a DMZ (Demilitarized Zone) host. Adding a client to the DMZ may expose that computer to a variety of security risks; so please use this option as the last resort.



DMZ Host IP Address: 192.168.111.120

Figure 36. DMZ Host

A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP. For example, if user has an FTP Server (port 21) at 192.168.111.1, a Web server (port 80) at 192.168.111.80, and a VPN (port 1723) server at 192.168.111.7, then user needs to specify the following virtual server.



Add Virtual Server

Name

IP Address

Protocol: TCP

Port

External

Internal

Virtual Server Rules (0 / 32)

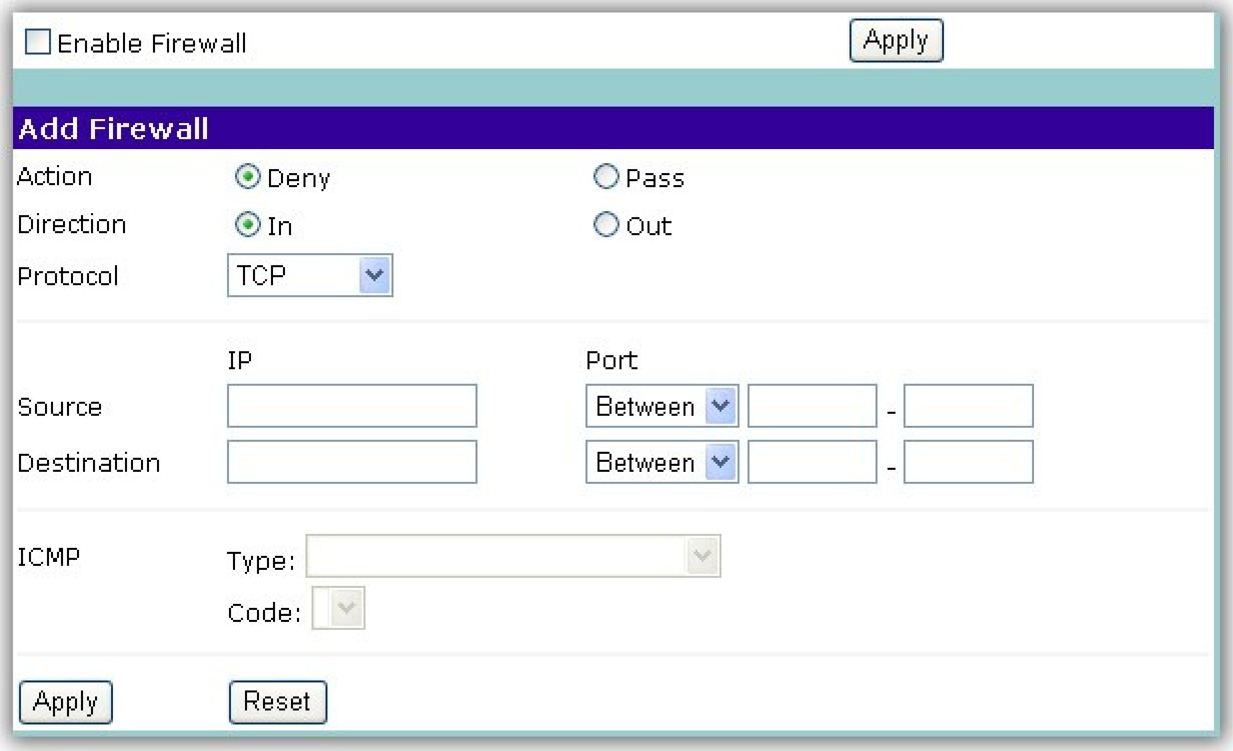
Name	IP	Protocol	External Port	Internal Port

Figure 37. Virtual Server

- **IP Address:** The server computer in the LAN network that will be providing the virtual services.
- **Protocol:** The protocol used for the virtual service.
- **External Port:** The port number on the WAN side that will be used to access the virtual service.
- **Internal Port:** The port number of the service used by the Private IP computer.

4.1.3. Network Parameters – Firewall

Firewall setting is used to pass or deny traffic through the device as show in Figure 38 displays. Click check box to enable the desired firewall settings. Un-checking “Enable Firewall” will also disable Firewall function (see Figure 38 and Figure 39). The maximum quantity of each filter is 32.



□ Enable Firewall

Add Firewall

Action ● Deny ○ Pass

Direction ● In ○ Out

Protocol: TCP

	IP	Port		
Source		Between		-
Destination		Between		-

ICMP Type: Code:

Figure 38. Firewall

- **Action**

Select Deny and Pass to allow or deny the traffic through the device.

- **Direction**

Selecting “In” indicates the traffic direction is inward into device, and selecting “out” indicates the traffic direction is outward from the device.

- **Protocol**

Select one of the following protocols, including TCP, UDP, ICMP, TCP/UDP and ALL.

- **IP address**

Enter the IP address range from source IP to destination IP.

- **Port**

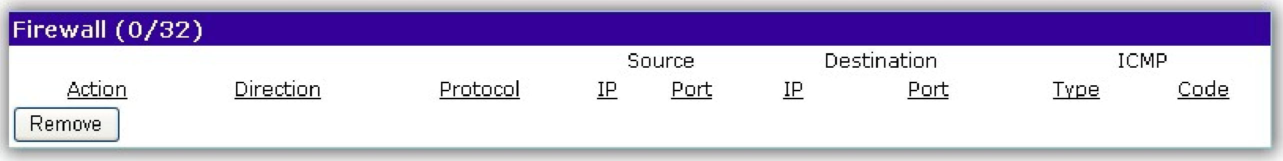
User can enter a single port, port range, excluded port range or all port range.

- **ICMP**

When selecting ICMP protocol, user can decide the type and the code of ICMP.

Press “Apply” at end of table to add a new firewall rule. (See Figure 38). If “Pass” in Action filed is selected, only user-specified source IP addresses are allowed to access the Destination IP addresses and the specified port. If “Deny” in Action field is selected, only user-specified source IP addresses are not allowed to access to the Destination IP addresses and the specified port.

To remove a selected firewall rule, select the desired rule, then press “Remove” at the end of the table



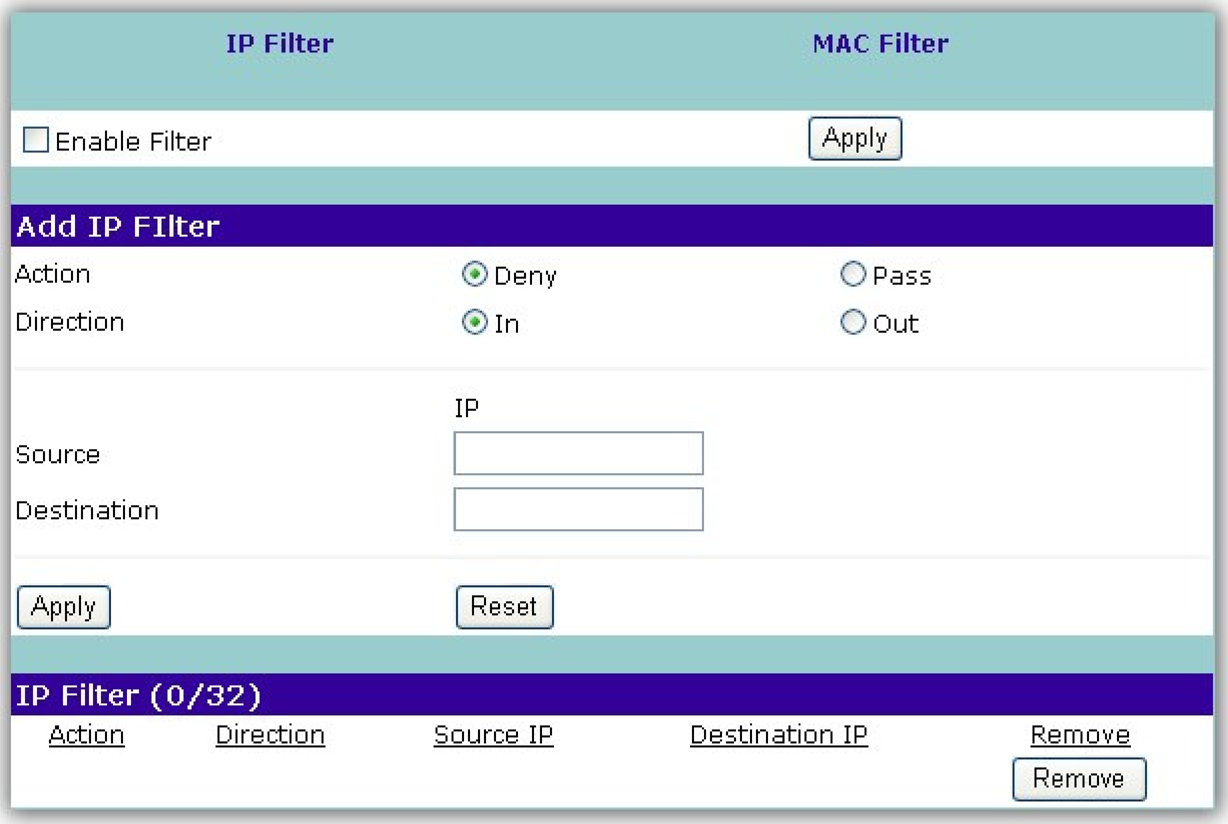
Firewall (0/32)

			Source		Destination		ICMP	
Action	Direction	Protocol	IP	Port	IP	Port	Type	Code

Figure 39. Firewall Rules Table

4.1.4. Network Parameters – Filter

Figure 40 displays Filter setting which include IP filter and MAC filter. It works in the same way as Firewall with simple setting. On this page, user can set two kinds of filters: IP Filter and MAC Filter. Click check box to enable desired filter settings.



IP Filter | MAC Filter

□ Enable Filter

Add IP FIlter

Action: ● Deny ○ Pass

Direction: ● In ○ Out

	IP
Source	
Destination	

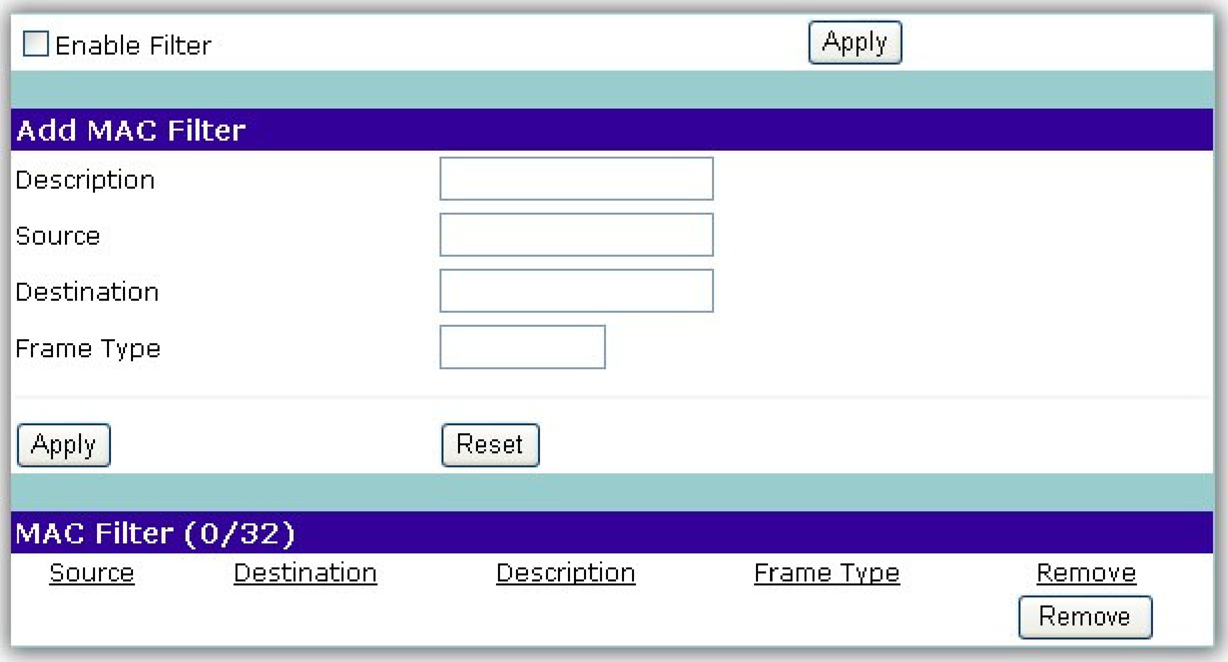
IP Filter (0/32)

Action	Direction	Source IP	Destination IP	Remove

Figure 40. IP Filter Table

Press “Apply” at end of table to add a new IP Filter. (See Figure 40 and Figure 41 for setting details). If “Pass” in Action field is selected, only user-specified IP addresses are allowed to access the wireless network. If “Deny” in Action field is selected, only user-specified IP addresses are not allowed to access the wireless network.

To remove a selected IP filter rule, select the desired rule, then press “Remove” at the end of the table (see Figure 41).



□ Enable Filter [Apply]

Add MAC Filter

Description □

Source □

Destination □

Frame Type □

[Apply] [Reset]

MAC Filter (0/32)

Source	Destination	Description	Frame Type	Remove
				[Remove]

Figure 41. MAC Filter Table

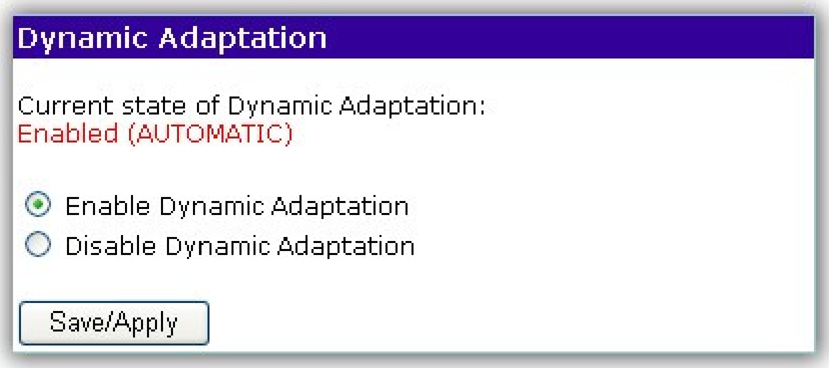
User can enter any description in Description block. Press “Apply” at end of table to add a new MAC Filter. (See Figure 41). User-specified source MAC addresses are not allowed to access the destination MAC address.

To remove a selected MAC filter rule, select the desired rule, then press “Remove” at the end of the table (see Figure 41).

4.1.5. Dynamic Adaptation

The goal of dynamic modulation is to optimize the downlink capacity of a mobile WiMAX network for each mobile station (MS) This optimization is done by selecting the most suitable Modulation and Coding Scheme (MCS), in other words, from QPSK-1/2 to 64QAM-5/6, in accordance with the signal quality measured by MS.

Select Enable / Disable Dynamic Adaptation (see Figure 42), and press “Save/Apply” to save settings.



Dynamic Adaptation

Current state of Dynamic Adaptation:
Enabled (AUTOMATIC)

● Enable Dynamic Adaptation
○ Disable Dynamic Adaptation

Figure 42. Dynamic Adaptation