User Manual

WiMAX Modem

Manual Version: 1.3

Manual Date: Feb. 20 2009

Software Version: R4.6.0.0-17743-v5.7.0

Software Date: Feb. 20 2009

CONTENTS

FIGURES

Chapter 1 Overview

This chapter describes the panel function and installation procedure for the CPE.

1.1. Indoor CPE

Front Panel LED

Power LED: ON: power on OFF: power fail
LAN LED: ON: connect OFF: disconnect Blinking: data transmit

When the CPE powers on, the LED indicates the CPE states as follow.
Only Red LED is Blinking: synchronization
Only Yellow LED is Blinking: authentication
Only Green LED is Blinking: DHCP client negotiation

After the CPE has connected to the base station, the signal strength LED are defined as follow.
Only Red LED is ON: the signal is weak. (CINR<8dB)
Yellow LED is ON: the signal strength is medium. (8dB≤CINR<15dB)
Green LED is ON: the signal strength is good. (15dB≤CINR)

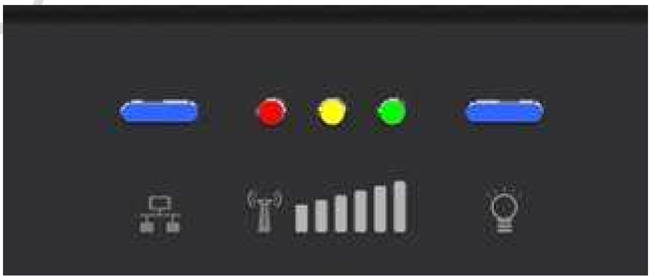


Figure 1-1 Indoor CPE Front Panel LED

Rear Panel

Power jack: DC 12V / 1.5A
LAN port: 10/100Base-TX
Reset button: To reboot the CPE

1.2. Outdoor CPE

Power Injector – Power Over Ethernet 802.3af compliant
LAN port: 10/100Base-TX

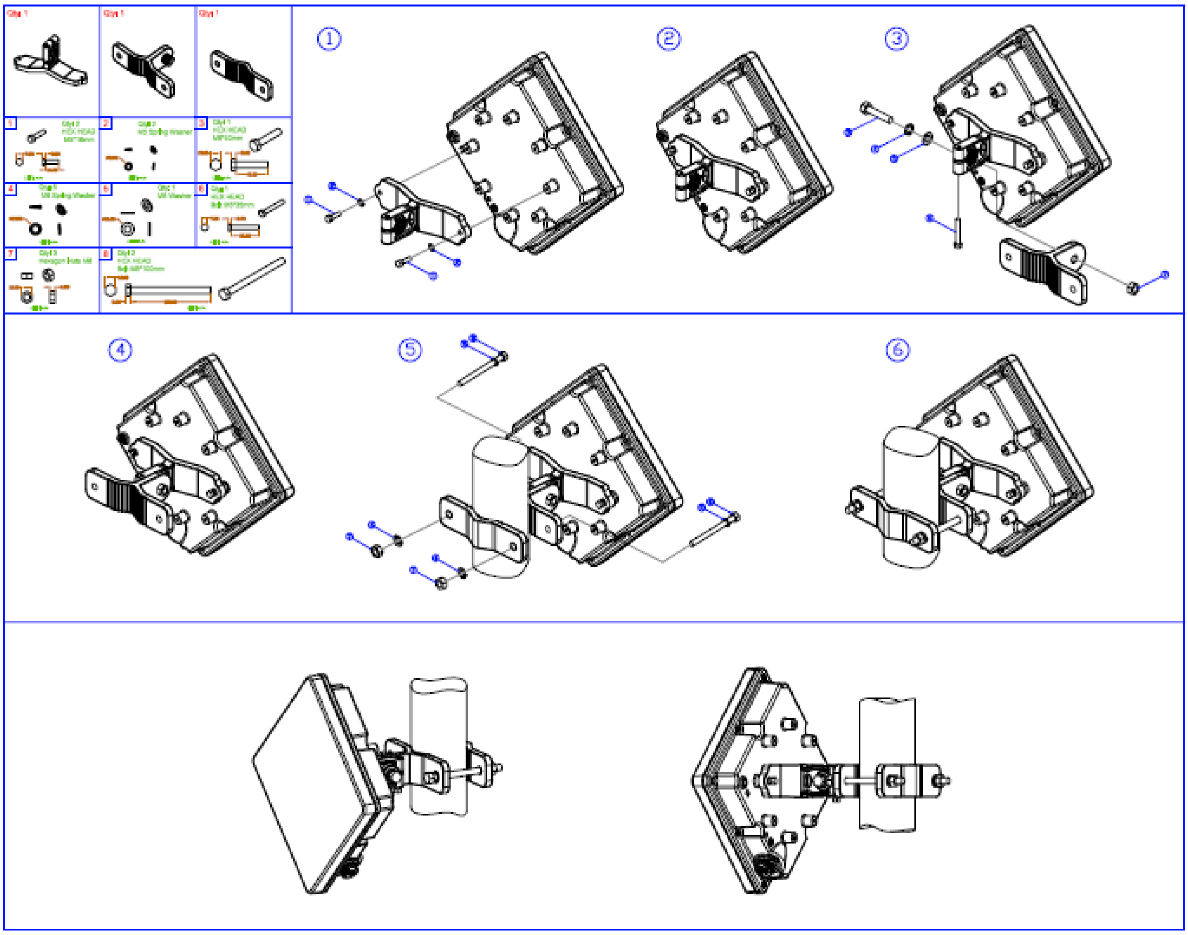


Figure 1-2 Outdoor CPE installation

Chapter 2 WEB-GUI

This chapter describes how to configure the CPE in order to connect to the base station.

2.1. System Configuration Login

The CPE will enable a DHCP server by default. Computers or network devices connected to its LAN side can get IP address automatically from CPE. If you disable CPE’s DHCP server by yourself, set the IP address, net mask, and gateway as following.

IP address: 10.1.1.x, 1 ≤ x ≤ 253
Netmask: 255.255.255.0
Gateway: 10.1.1.254

Connect to http://10.1.1.254/ with a browser, and you will see a webpage such as the one shown in Figure 2-1. The administrator username and password are as shown below:

Username: admin
Password: admin

WiMAX CPE also support multi-level user login. Please contact with us to define multi-user features.

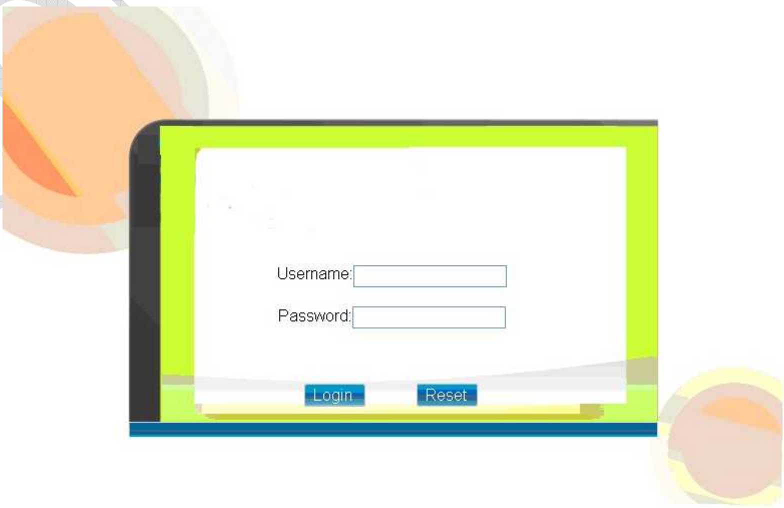
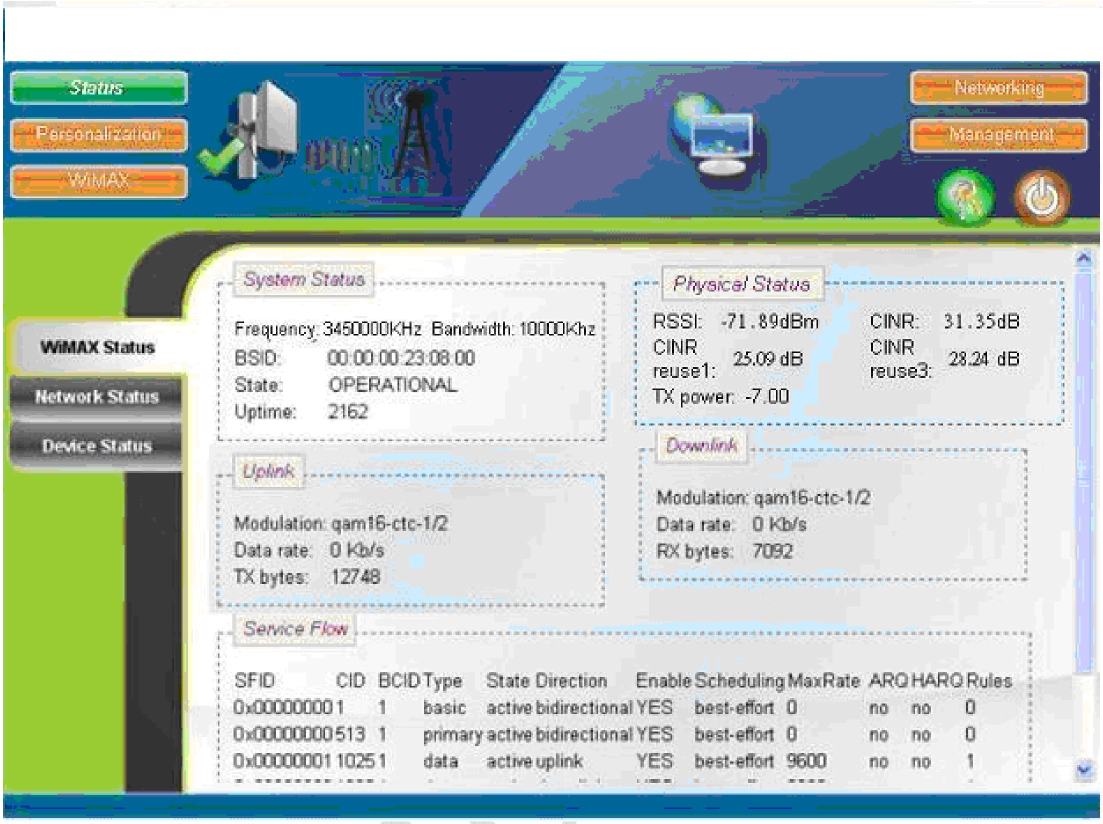


Figure 2-1 Login Page

If there is no error, the user can login into the Status Page, and WiMAX Status, Network Status, and Device Status are as shown in Figure 2-2, Figure 2-3, Figure 2-4, and Figure 2-5.



System Status

Frequency: 3450000KHz Bandwidth: 10000Khz
BSID: 00:00:00:23:08:00
State: OPERATIONAL
Uptime: 2162

Physical Status

RSSI: -71.89dBm
CINR: 31.35dB
CINR reuse1: 25.09 dB
CINR reuse3: 28.24 dB
TX power: -7.00

Uplink

Modulation: qam16-ctc-1/2
Data rate: 0 Kb/s
TX bytes: 12748

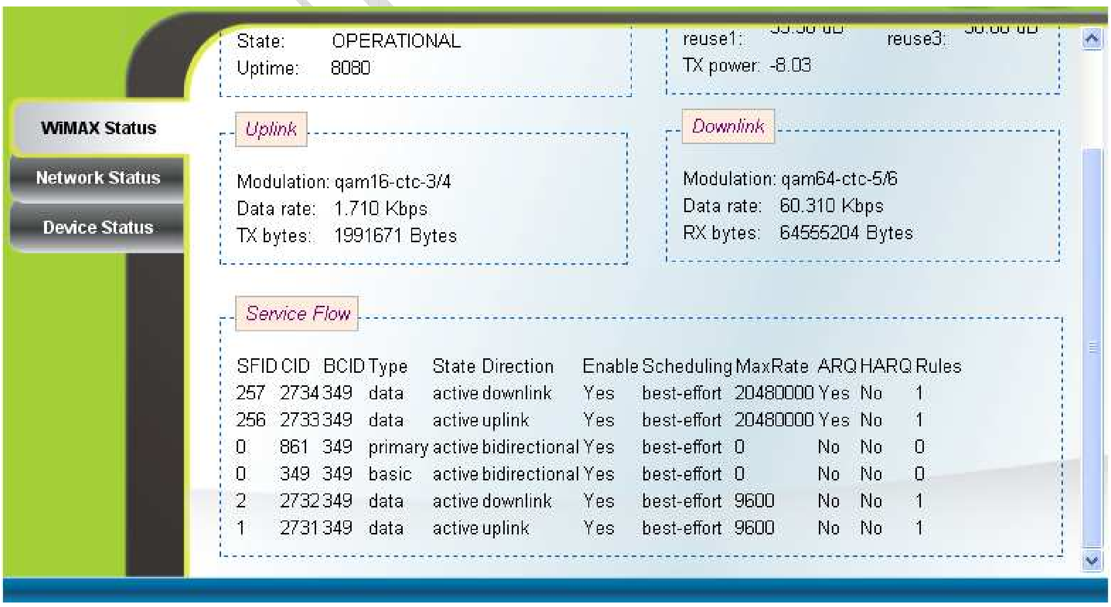
Downlink

Modulation: qam16-ctc-1/2
Data rate: 0 Kb/s
RX bytes: 7092

Service Flow

SFID	CID	BCID	Type	State	Direction	Enable	Scheduling	MaxRate	ARQ	HARQ	Rules
0x00000000	1	1	basic	active	bidirectional	YES	best-effort	0	no	no	0
0x00000000	513	1	primary	active	bidirectional	YES	best-effort	0	no	no	0
0x00000001	1025	1	data	active	uplink	YES	best-effort	9600	no	no	1

Figure 2-2 WiMAX Status



State: OPERATIONAL
Uptime: 8080

reuse1:
reuse3:
TX power: -8.03

Uplink

Modulation: qam16-ctc-3/4
Data rate: 1.710 Kbps
TX bytes: 1991671 Bytes

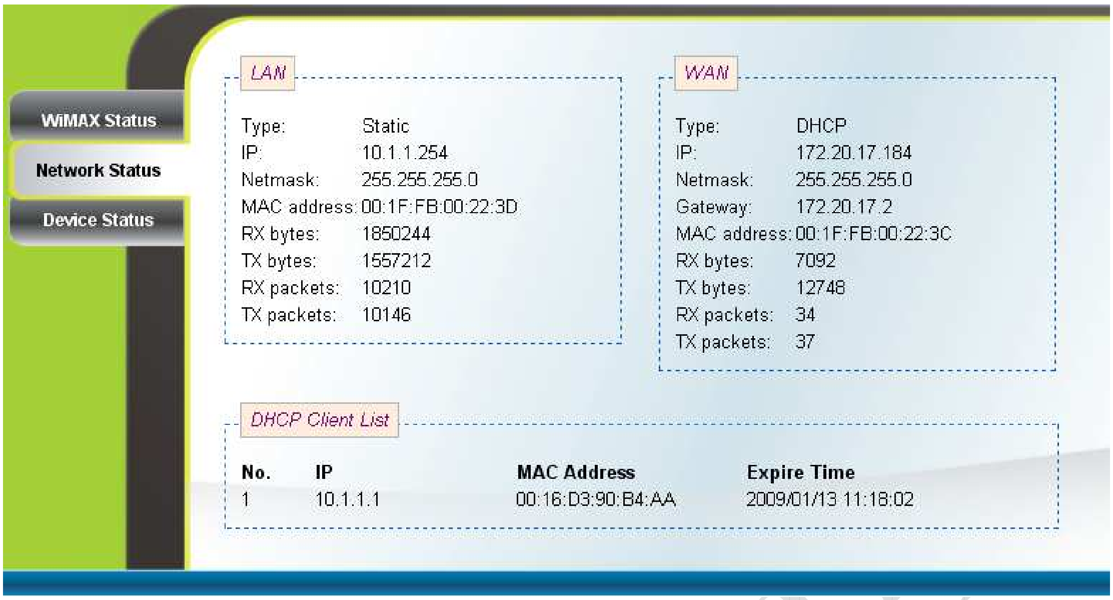
Downlink

Modulation: qam64-ctc-5/6
Data rate: 60.310 Kbps
RX bytes: 64555204 Bytes

Service Flow

SFID	CID	BCID	Type	State	Direction	Enable	Scheduling	MaxRate	ARQ	HARQ	Rules
257	2734	349	data	active	downlink	Yes	best-effort	20480000	Yes	No	1
256	2733	349	data	active	uplink	Yes	best-effort	20480000	Yes	No	1
0	861	349	primary	active	bidirectional	Yes	best-effort	0	No	No	0
0	349	349	basic	active	bidirectional	Yes	best-effort	0	No	No	0
2	2732	349	data	active	downlink	Yes	best-effort	9600	No	No	1
1	2731	349	data	active	uplink	Yes	best-effort	9600	No	No	1

Figure 2-3 WiMAX Status-Service Flow



LAN

```
Type:        Static
IP:          10.1.1.254
Netmask:     255.255.255.0
MAC address: 00:1F:FB:00:22:3D
RX bytes:    1850244
TX bytes:    1557212
RX packets:  10210
TX packets:  10146
```

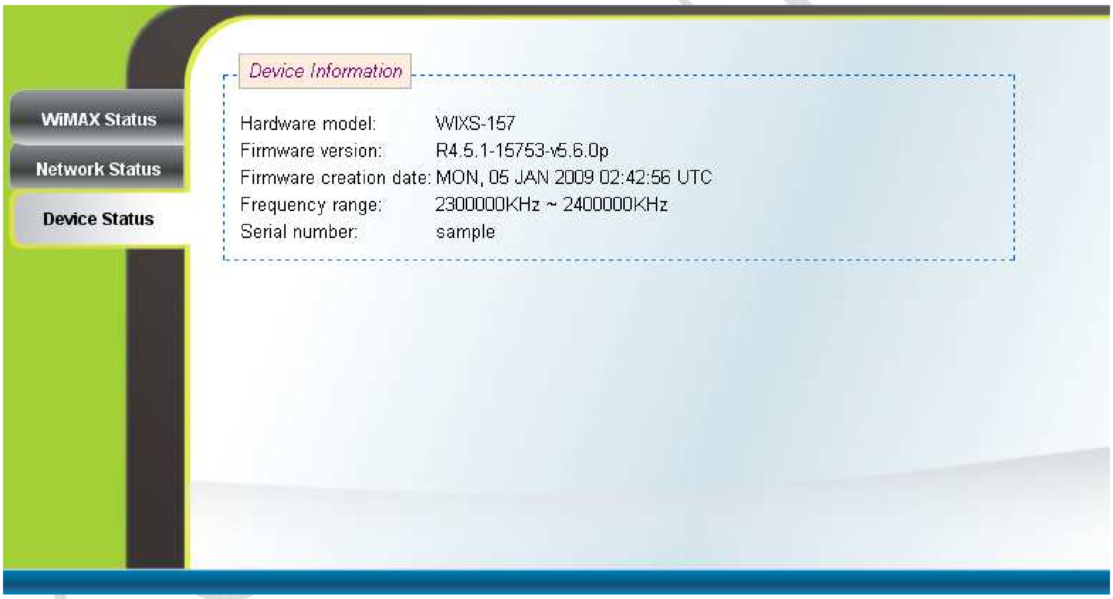
WAN

```
Type:        DHCP
IP:          172.20.17.184
Netmask:     255.255.255.0
Gateway:     172.20.17.2
MAC address: 00:1F:FB:00:22:3C
RX bytes:    7092
TX bytes:    12748
RX packets:  34
TX packets:  37
```

DHCP Client List

No.	IP	MAC Address	Expire Time
1	10.1.1.1	00:16:D3:90:B4:AA	2009/01/13 11:18:02

Figure 2-4 Network Status



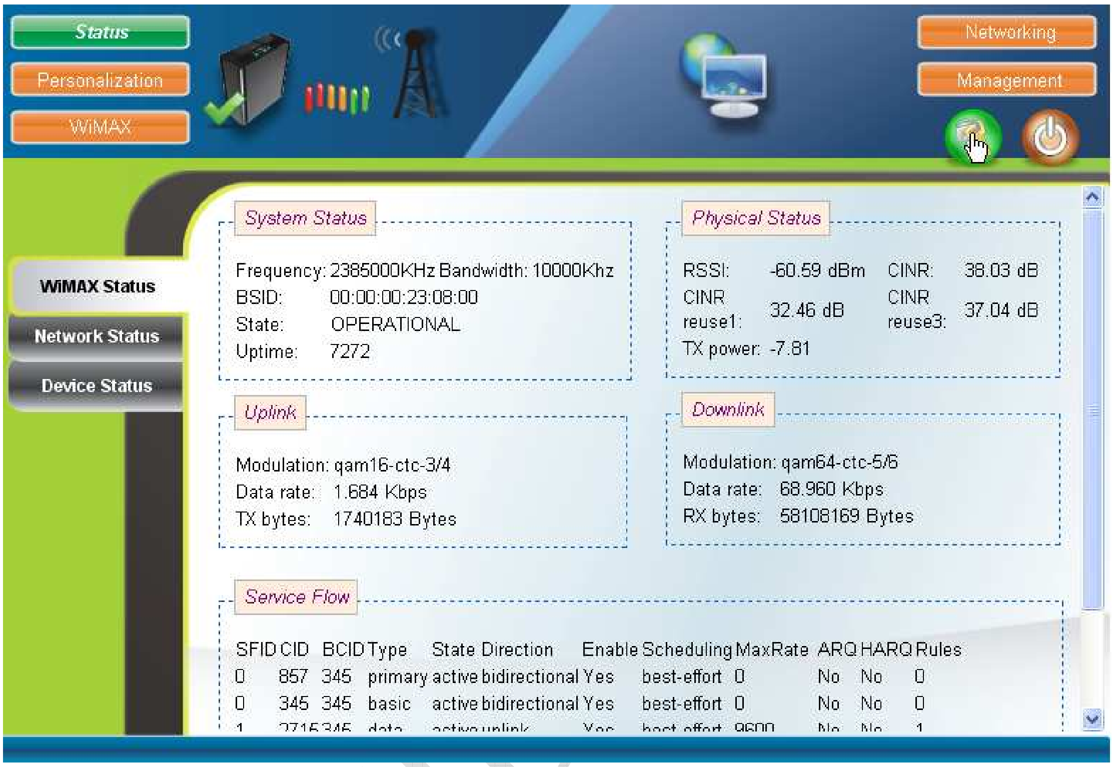
Device Information

```
Hardware model:          WIXS-157
Firmware version:        R4.5.1-15753-v5.6.0p
Firmware creation date:  MON, 05 JAN 2009 02:42:56 UTC
Frequency range:         2300000KHz ~ 2400000KHz
Serial number:           sample
```

Figure 2-5 Device Status

2.2. System Logout

Press the “Logout” button as shown in Figure 2-6 to logout of the system and go back to the “Login” page as shown in Figure 2-1.



System Status

Frequency: 2385000KHz Bandwidth: 10000Khz
BSID: 00:00:00:23:08:00
State: OPERATIONAL
Uptime: 7272

Physical Status

RSSI: -60.59 dBm CINR: 38.03 dB
CINR reuse1: 32.46 dB CINR reuse3: 37.04 dB
TX power: -7.81

Uplink

Modulation: qam16-ctc-3/4
Data rate: 1.684 Kbps
TX bytes: 1740183 Bytes

Downlink

Modulation: qam64-ctc-5/6
Data rate: 68.960 Kbps
RX bytes: 58108169 Bytes

Service Flow

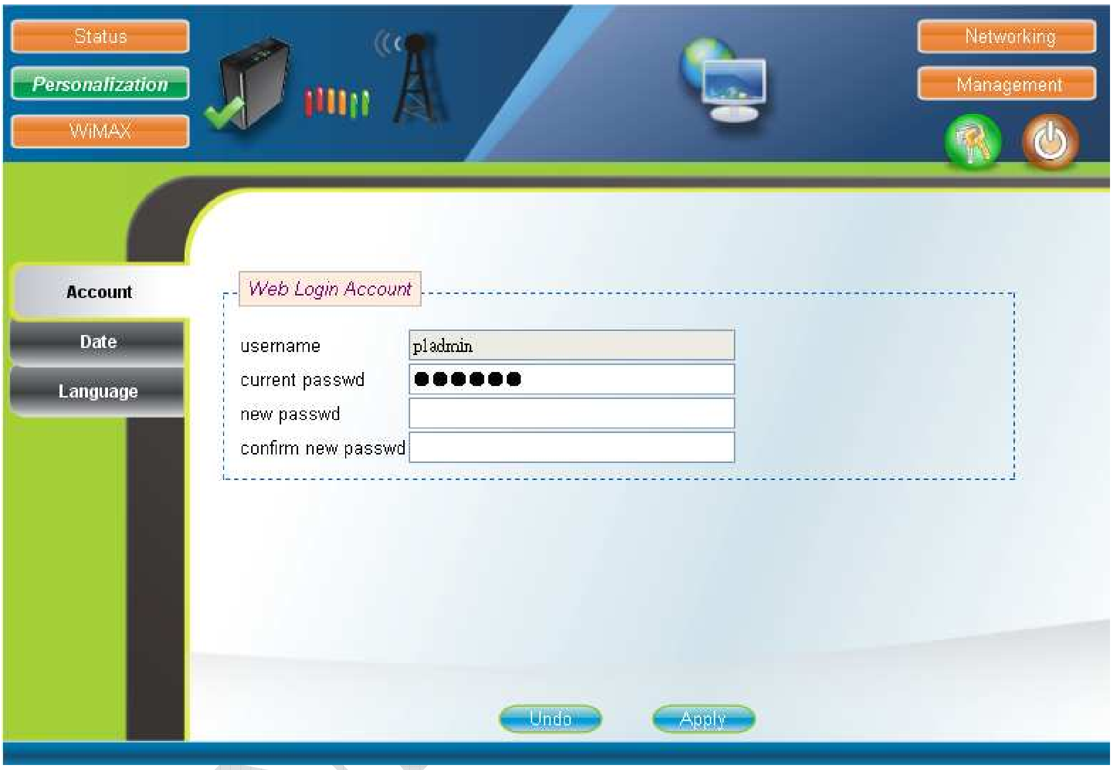
SFID	CID	BCID	Type	State	Direction	Enable	Scheduling	MaxRate	ARQ	HARQ	Rules
0	857	345	primary	active	bidirectional	Yes	best-effort	0	No	No	0
0	345	345	basic	active	bidirectional	Yes	best-effort	0	No	No	0
1	2715	345	data	active	uplink	Yes	best-effort	9600	No	No	1

Figure 2-6 Logout

2.3. Account

Personalization → Account

The Account page is for changing the password of the WEB-UI account as shown in Figure 2-7. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and the new configurations will take effect.



Web Login Account

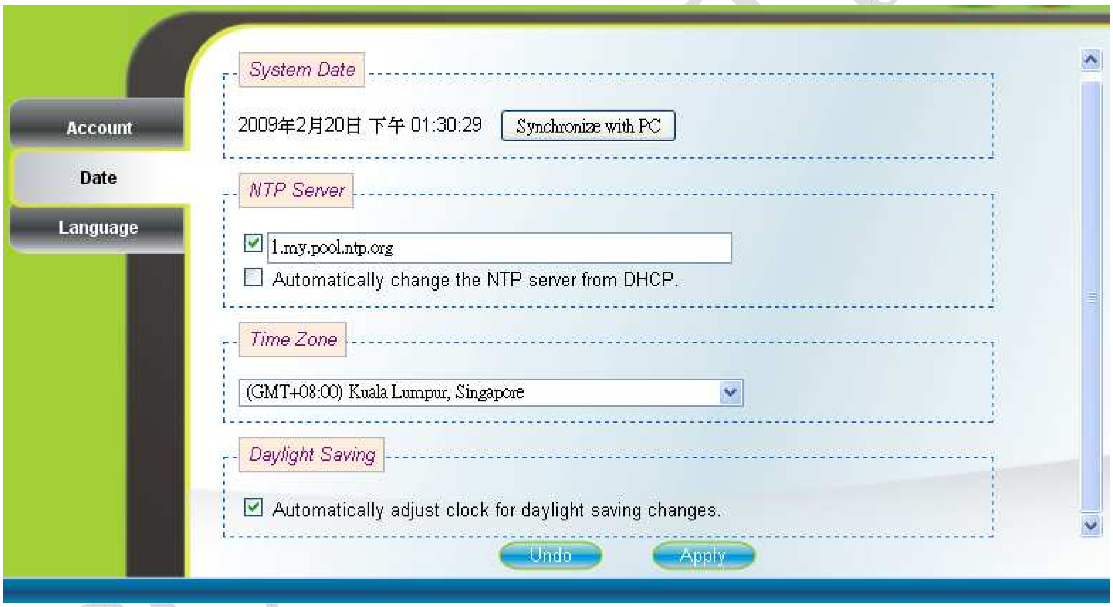
username pladmin
current passwd ●●●●●●
new passwd
confirm new passwd

Figure 2-7 Account

2.4. Date

Personalization → Date

If the system date is not in the valid duration of the uploaded certificate file, the CPE will not pass the authentication from the base station. The system date of a CPE can be synchronized with the PC that is connected to its LAN side by clicking the “Synchronize with PC” button. The system date of a CPE can also be automatically updated by synchronizing time with an NTP server assigned manually by the user or from the DHCP server. The selection of different time zone and daylight saving option are available as well for different regions. Please refer to Figure 2-8 for more detail. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and press “Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



System Date

2009年2月20日 下午 01:30:29

NTP Server

☑ 1.my.pool.ntp.org

□ Automatically change the NTP server from DHCP.

Time Zone

(GMT+08:00) Kuala Lumpur, Singapore

Daylight Saving

☑ Automatically adjust clock for daylight saving changes.

Figure 2-8 Date

2.5. Language

Personalization → Language

The Language page allows users to select one of the languages in the drop-down list for viewing the WEB-GUI as shown in Figure 2-9. After selecting the desired language, press the “Apply” button to view the WEB-GUI in the selected language.

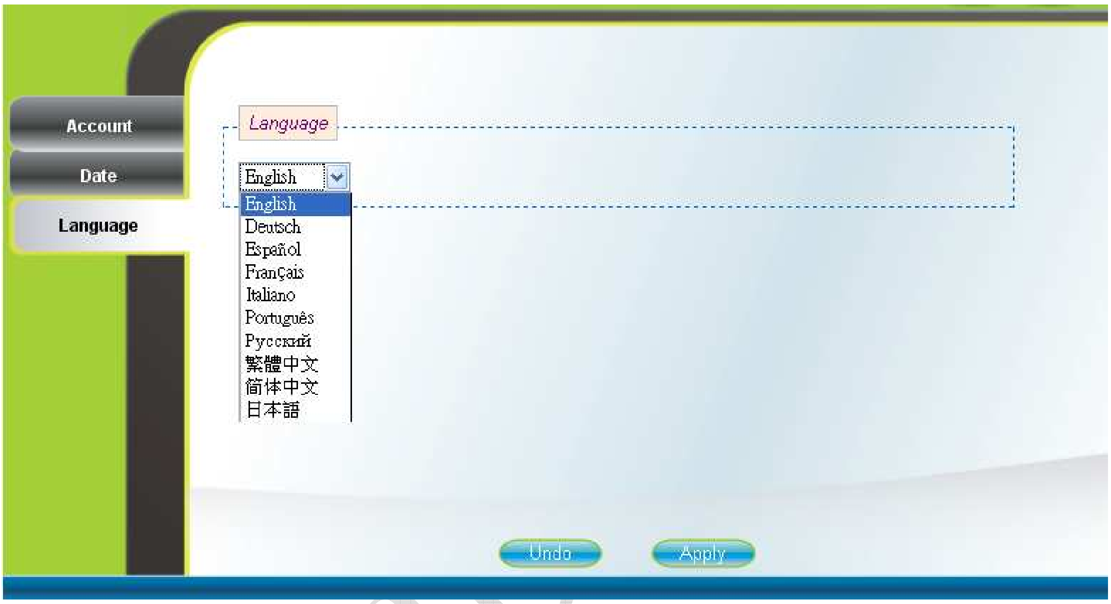
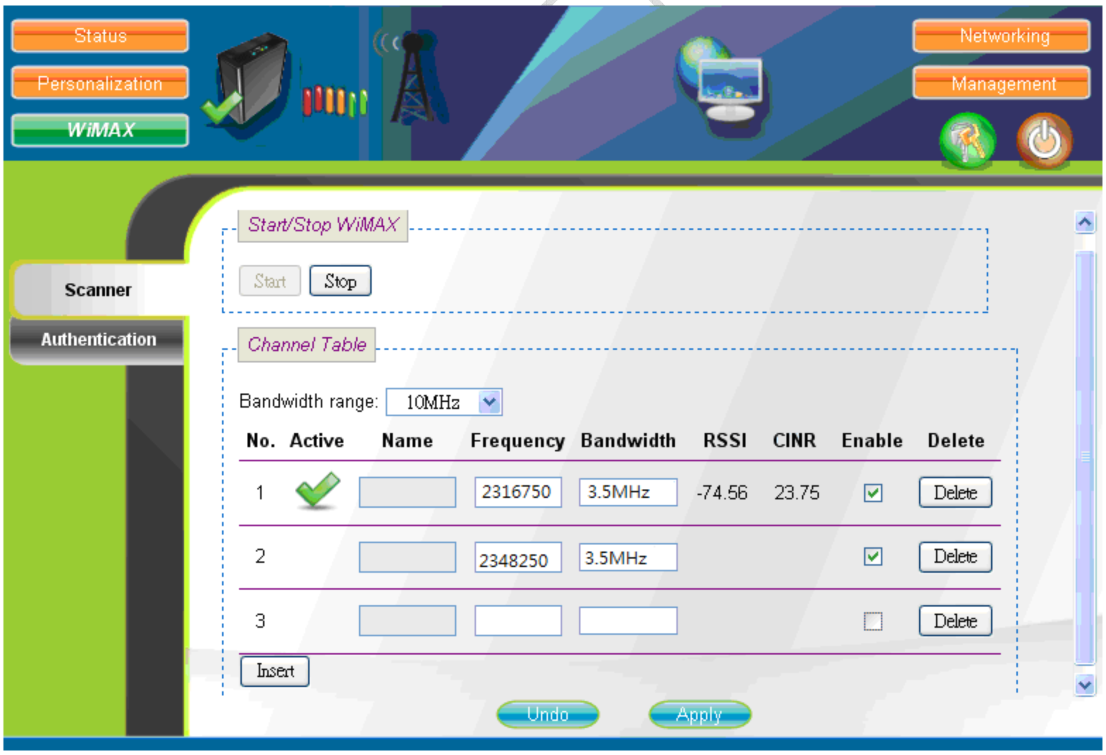


Figure 2-9 Language

2.6. Scanner

WiMAX → Scanner (can only be accessed by administrator)

The Scanner page allows users to stop or start WiMAX connection with a BS by simply clicking the “start” or “stop” button in the “Start/Stop WiMAX” section. The “Channel Table” section lists all the channels that are stored in the channel table along with channel status associated to the channel used to connect the CPE to a BS. Please refer to Figure 2-10 more detail. After changing the channel table, press the “Apply” button to write the new configurations into the CPE. If the “Bandwidth range” of the channel table is changed, then press “Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect; otherwise, just simply restart the system by using the “start” and “stop” button in the “Start/Stop WiMAX” section. Please note that when the CPE is connected to a BS, a green check will appear on the “Active” of the linked frequency in the “Channel Table” section as well as beside the small CPE icon on the top banner; otherwise, a red x will appear beside the small CPE icon on the top banner.



Bandwidth range: 10MHz

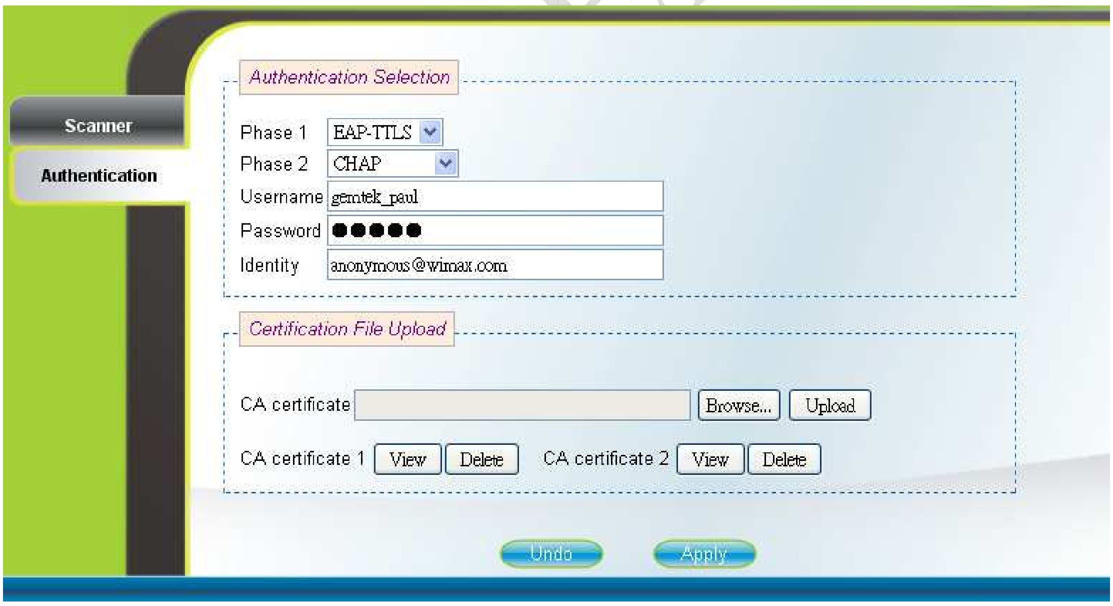
No.	Active	Name	Frequency	Bandwidth	RSSI	CINR	Enable	Delete
1	✓		2316750	3.5MHz	-74.56	23.75	☑	Delete
2			2348250	3.5MHz			☑	Delete
3							□	Delete

Figure 2-10 Scanner with Bandwidth range

2.7. Authentication

WiMAX → Authentication (can only be accessed by administrator)

Users can enable or disable the authentication by selecting one of the two methods supported, EAP-TLS and EAP-TTLS, or by selecting none in "Phase 1" field. Users can also choose one of five key encoding methods listed in "Phase 2". Identity, username, and password should be entered respectively as agreed upon with the BS, if authentication is required. After setting the configurations of these fields, press the "Apply" button to write the new configurations into the CPE and press "Reboot" as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect. Certificates required for authentication can be uploaded in the "Certificate File Upload" section. Contents of the certificates that are currently in the CPE can be viewed in details by clicking "View CA Certificate" as shown in Figure 2-12. Note that the only certificate format supported is PEM (Privacy Enhanced Mail, Base64 encoded DER certificate). Please confirm the format before uploading. Certificates in the CPE can also be deleted by pressing the "Delete" button. Please refer to Figure 2-11 for more details.



Authentication Selection

Phase 1: EAP-TTLS

Phase 2: CHAP

Username: gemtek_paul

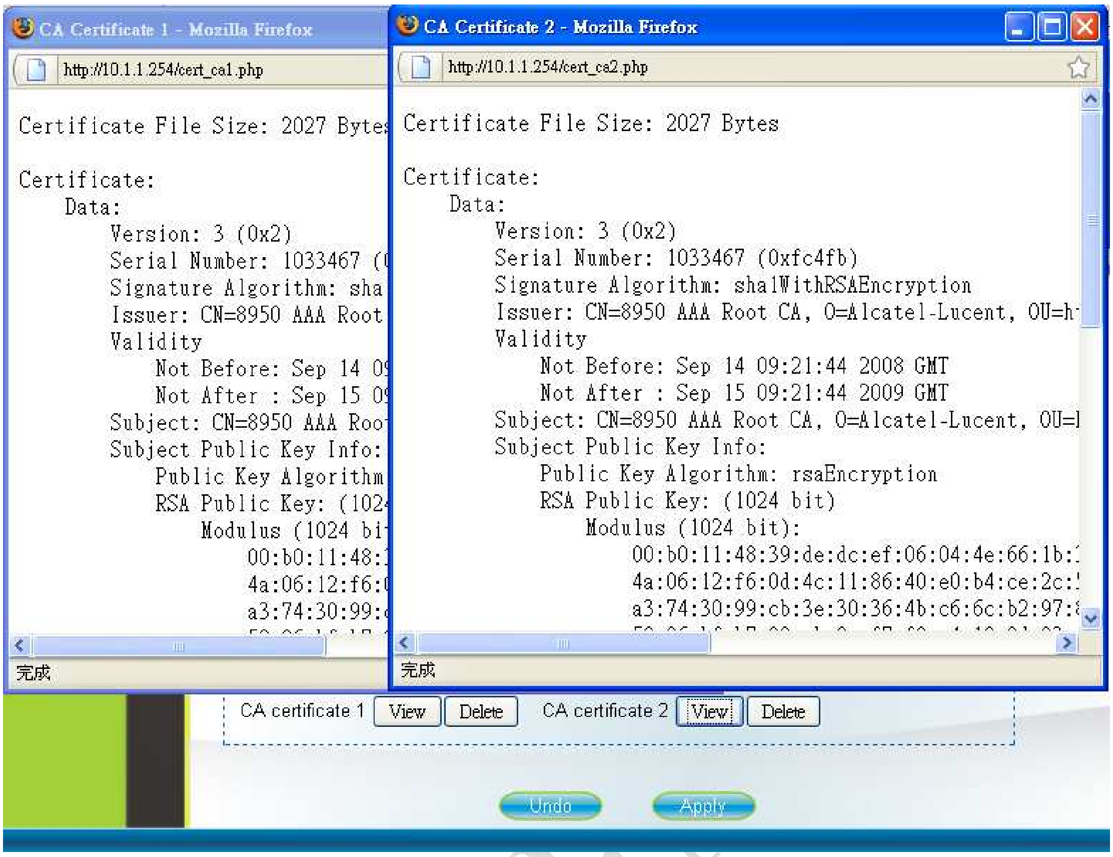
Password: ●●●●●

Identity: anonymous@wimax.com

Certification File Upload

CA certificate

Figure 2-11 Authentication


CA Certificate 1 - Mozilla Firefox
http://10.1.1.254/cert_ca1.php
完成
CA Certificate 2 - Mozilla Firefox
http://10.1.1.254/cert_ca2.php
完成
CA certificate 1
View
Delete
CA certificate 2
View
Delete
Undo
Apply

```
Certificate File Size: 2027 Byte

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1033467 (
        Signature Algorithm: sha
        Issuer: CN=8950 AAA Root
        Validity
            Not Before: Sep 14 0
            Not After : Sep 15 0
        Subject: CN=8950 AAA Roo
        Subject Public Key Info:
            Public Key Algorithm
            RSA Public Key: (102
                Modulus (1024 bi
                    00:b0:11:48:
                    4a:06:12:f6:
                    a3:74:30:99:
```

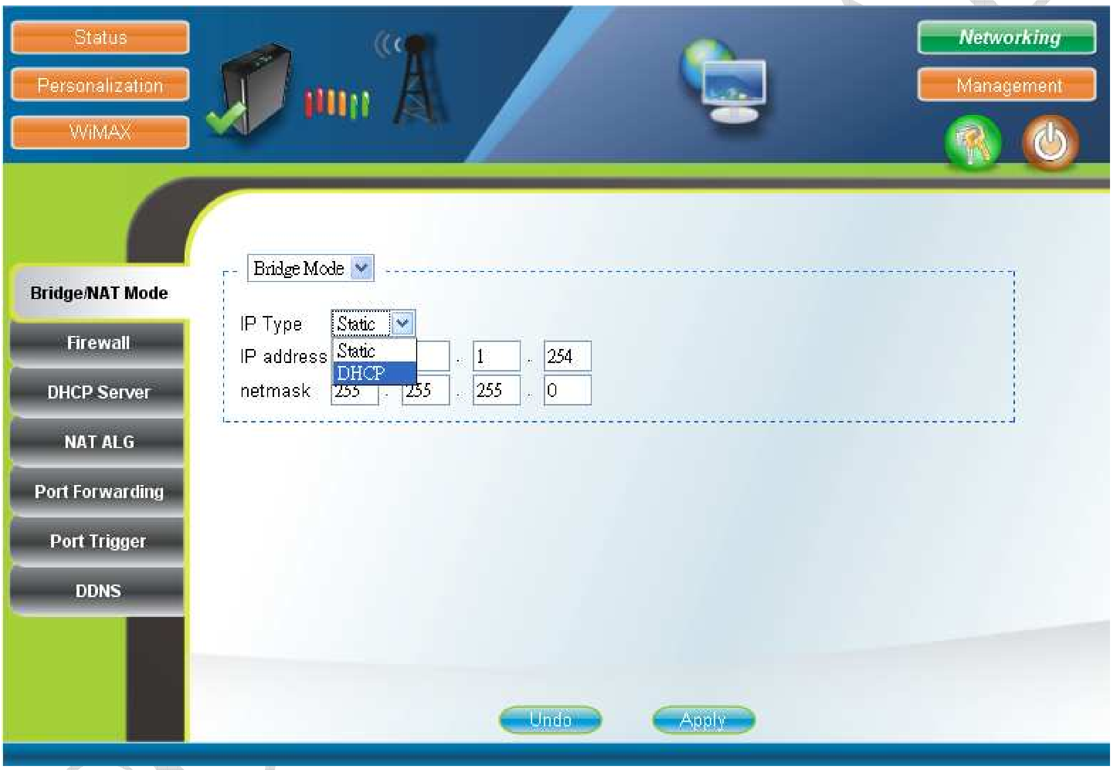
```
Certificate File Size: 2027 Bytes

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1033467 (0xfc4fb)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=8950 AAA Root CA, O=Alcatel-Lucent, OU=h
        Validity
            Not Before: Sep 14 09:21:44 2008 GMT
            Not After : Sep 15 09:21:44 2009 GMT
        Subject: CN=8950 AAA Root CA, O=Alcatel-Lucent, OU=
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b0:11:48:39:de:dc:ef:06:04:4e:66:1b:
                    4a:06:12:f6:0d:4c:11:86:40:e0:b4:ce:2c:
                    a3:74:30:99:cb:3e:30:36:4b:c6:6c:b2:97:
```

Figure 2-12 Authentication-View Certificates

2.8. Bridge Mode

Networking → Bridge/NAT Mode

Bridge mode is enabled by simply selecting “Bridge Mode” as shown in Figure 2-13. By selecting “Static” IP type, users can manually assign the “IP address” and “netmask”. The “IP address” and “netmask” can also be automatically assigned by the DHCP server by selecting “DHCP” IP type. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and go to “Management → Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



Bridge Mode

IP Type: Static

IP address: . . 1 . 254

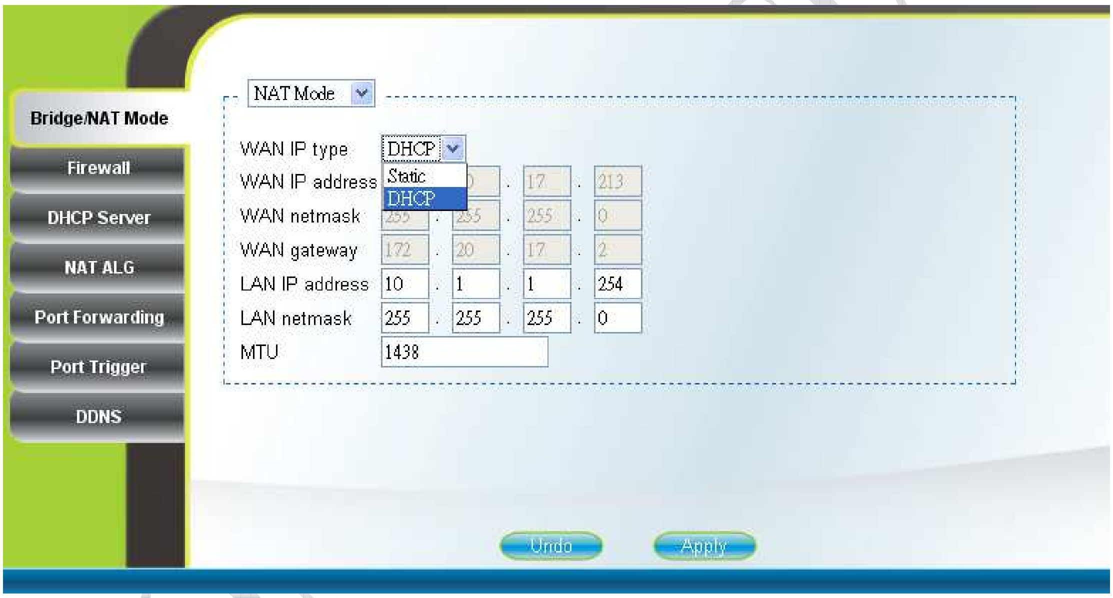
netmask: 255 . 255 . 255 . 0

Figure 2-13 Bridge Mode

2.9. NAT Mode

Networking → Bridge/NAT Mode

NAT mode is enabled by simply selecting “NAT Mode” as shown in Figure 2-14. By selecting “Static” WAN IP type, users can manually assign the “WAN IP address”, “WAN netmask”, and “WAN gateway”. The “WAN IP address”, “WAN netmask”, and “WAN gateway” can also be automatically assigned by the DHCP server by selecting “DHCP” WAN IP type. Users can also configure “LAN IP address”, “LAN netmask”, and “MTU”, which should be between 68 and 1500. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and go to “Management → Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



NAT Mode

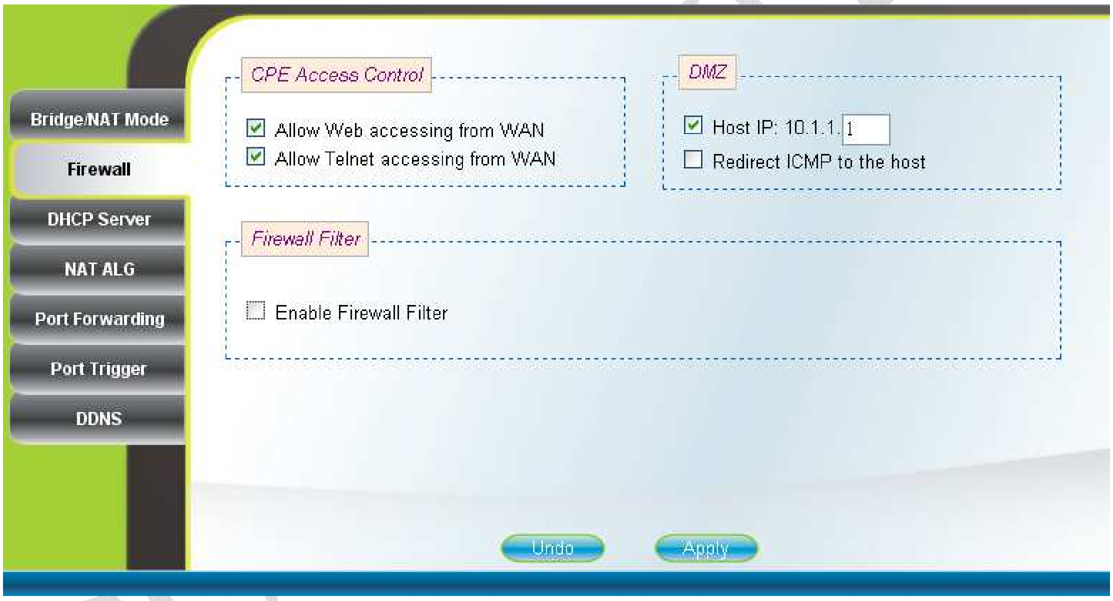
WAN IP type	DHCP			
WAN IP address		0	17	213
WAN netmask	255	255	255	0
WAN gateway	172	20	17	2
LAN IP address	10	1	1	254
LAN netmask	255	255	255	0
MTU	1438			

Figure 2-14 NAT Mode

2.10. Firewall

Networking → Firewall (can only be accessed by administrator)

The “CPE Access Control” section of this page gives users the ability to allow or deny web/telnet access from WAN. By enabling and identifying a DMZ host, an external attacker only has access to the DMZ host, rather than the entire private network at the CPE’s back end. Furthermore, the redirection of ICMP can also be enabled. The “Firewall Filter” section of this page is used to filter incoming network traffic based on MAC, IP, protocol, TCP/UDP port and interface. Please refer to Figure 2-15 and Figure 2-16 for more details. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and press “Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



CPE Access Control

☑ Allow Web accessing from WAN

☑ Allow Telnet accessing from WAN

DMZ

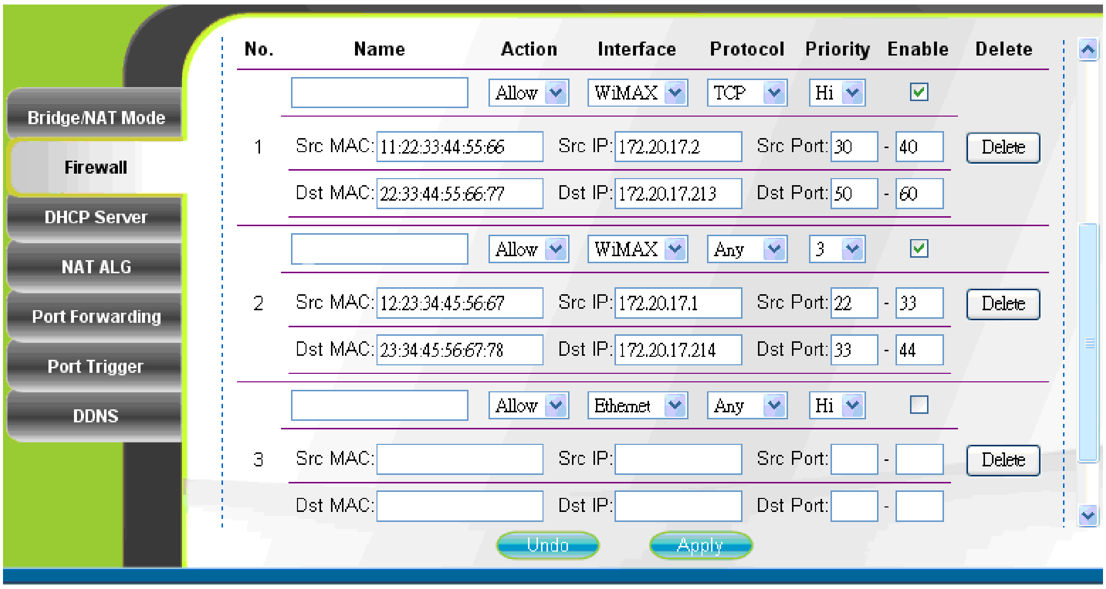
☑ Host IP: 10.1.1. 1

□ Redirect ICMP to the host

Firewall Filter

□ Enable Firewall Filter

Figure 2-15 Firewall



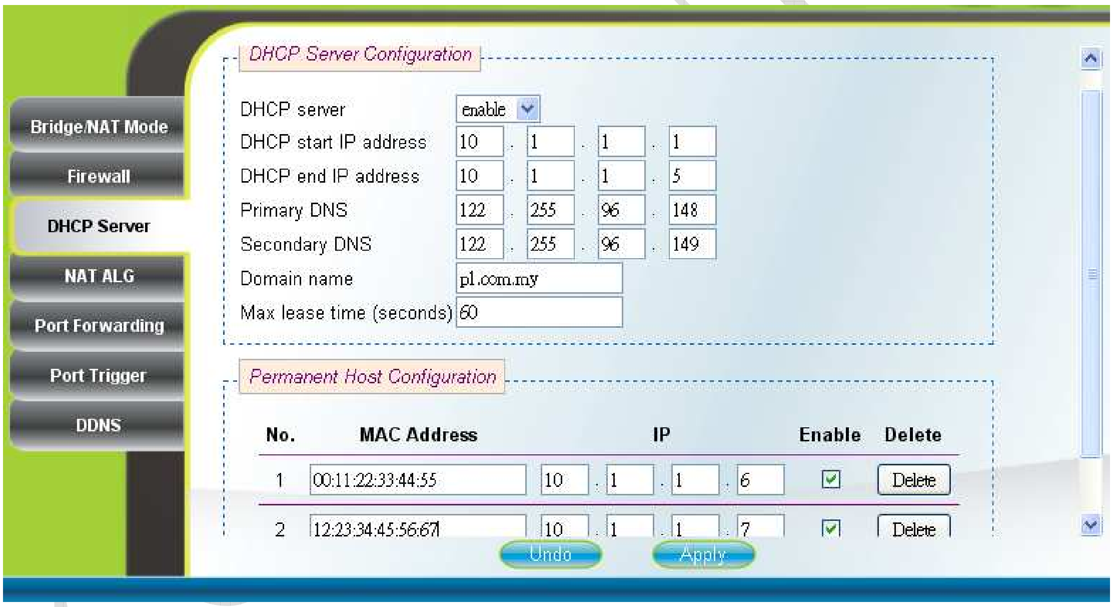
No.	Name	Action	Interface	Protocol	Priority	Enable	Delete
		Allow	WiMAX	TCP	Hi	☑	
1	Src MAC: 11:22:33:44:55:66	Src IP: 172.20.17.2	Src Port: 30 - 40				Delete
	Dst MAC: 22:33:44:55:66:77	Dst IP: 172.20.17.213	Dst Port: 50 - 60				
		Allow	WiMAX	Any	3	☑	
2	Src MAC: 12:23:34:45:56:67	Src IP: 172.20.17.1	Src Port: 22 - 33				Delete
	Dst MAC: 23:34:45:56:67:78	Dst IP: 172.20.17.214	Dst Port: 33 - 44				
		Allow	Ethernet	Any	Hi	□	
3	Src MAC:	Src IP:	Src Port: -				Delete
	Dst MAC:	Dst IP:	Dst Port: -				

Figure 2-16   Firewall Filter

2.11. DHCP Server

Networking → DHCP Server

DHCP server will automatically start up when the CPE is powered on if “DHCP server” is enabled. If enabled, this page shows the previous configuration of the DHCP server as shown in Figure 2-17; otherwise, it shows that the DHCP server is disabled as shown in Figure 2-18. Note that “Primary DNS” and “Domain Name” are required for DHCP server settings, and “Max lease time (seconds)” is between 1 and 99999999. Specific IP address can also be assigned to a specific MAC address in “Permanent Host Configuration” as shown in Figure 2-17. Please note that DHCP server is only applicable when the CPE is in NAT mode. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and press “Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



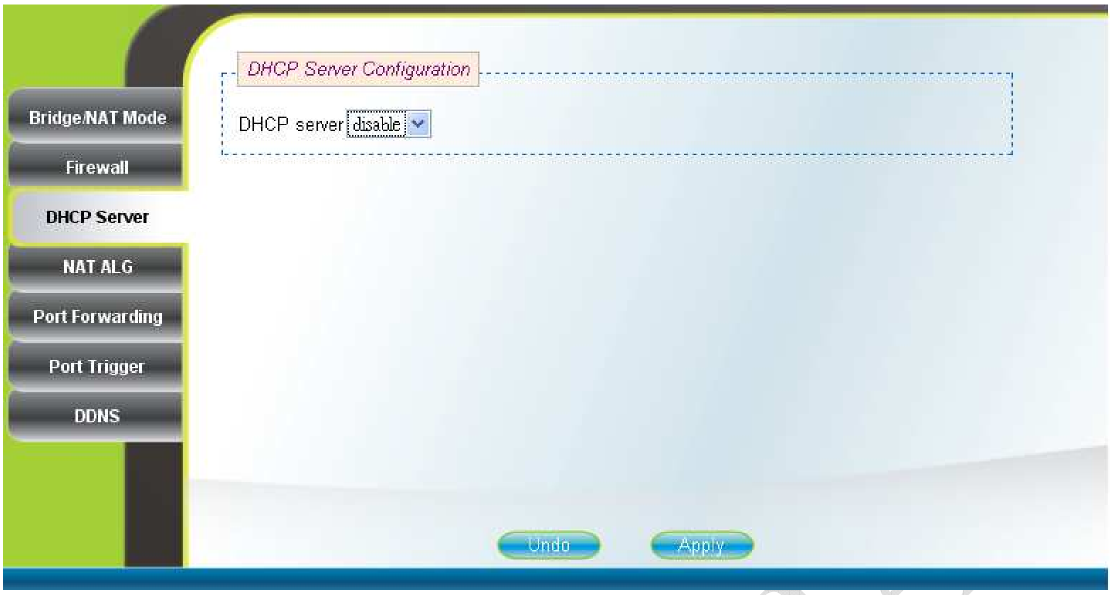
DHCP Server Configuration

DHCP server	enable
DHCP start IP address	10 . 1 . 1 . 1
DHCP end IP address	10 . 1 . 1 . 5
Primary DNS	122 . 255 . 96 . 148
Secondary DNS	122 . 255 . 96 . 149
Domain name	pl.com.my
Max lease time (seconds)	60

Permanent Host Configuration

No.	MAC Address	IP	Enable	Delete
1	00:11:22:33:44:55	10 . 1 . 1 . 6	☑	Delete
2	12:23:34:45:56:67	10 . 1 . 1 . 7	☑	Delete

Figure 2-17 DHCP Server Enabled



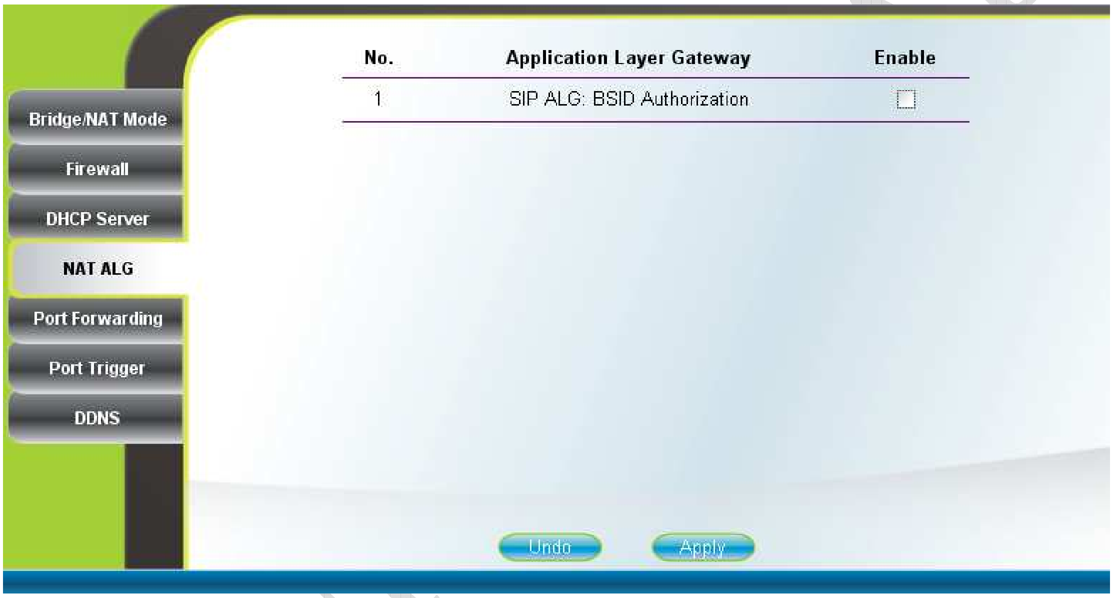
DHCP server disable

Figure 2-18 DHCP Server Disabled

2.12. NAT ALG

Networking → NAT ALG (can only be accessed by administrator)

By selecting or deselecting the checkbox, users can enable or disable BSID authorization of SIP ALG as shown in Figure 2-19. With it enabled, BSID can be used in SIP authentication to decide if the ATA is within the service area. Please note that NAT ALG is only applicable when the CPE is in NAT mode. After changing the configuration, press the "Apply" button to write the new configuration into the CPE and press "Reboot" as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



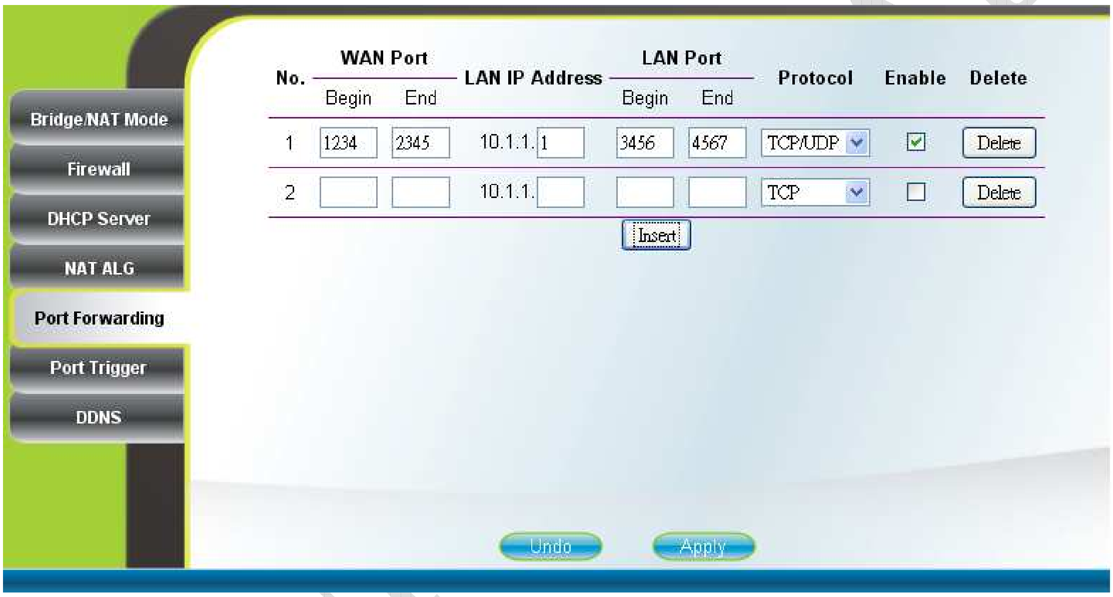
No.	Application Layer Gateway	Enable
1	SIP ALG: BSID Authorization	□

Figure 2-19 NAT ALG

2.13. Port Forwarding

Networking → Port Forwarding

Port forwarding redirects incoming network traffic from pre-defined "WAN Port" range to pre-defined "LAN IP Address" and "LAN Port" range. Users are allowed to add, remove, edit, enable, and disable port forwarding rules here as shown in Figure 2-20. Please note that port forwarding is only applicable when the CPE is in NAT mode. After setting the configurations of these fields, press the "Apply" button to write the new configurations into the CPE and press "Reboot" as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



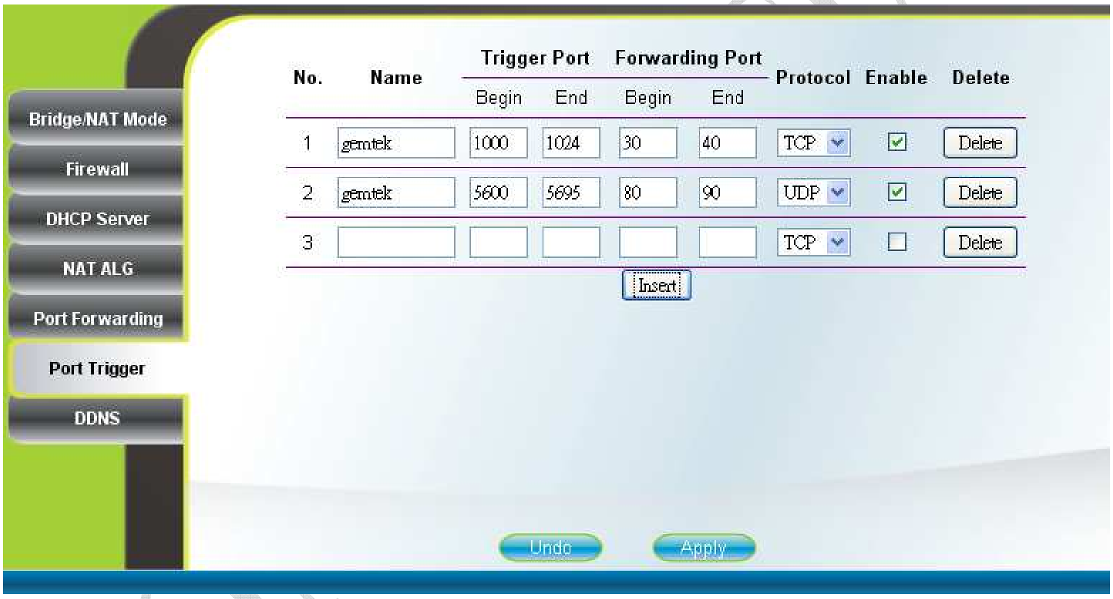
No.	WAN Port		LAN IP Address	LAN Port		Protocol	Enable	Delete
	Begin	End		Begin	End			
1	1234	2345	10.1.1.1	3456	4567	TCP/UDP	☑	Delete
2			10.1.1.			TCP	□	Delete

Figure 2-20 Port Forwarding

2.14. Port Trigger

Networking → Port Trigger

Port trigger dynamically opens port forwarding from a pre-defined WAN “Forwarding Port” range to a pre-defined LAN “Forwarding Port” range when a client on the local network makes an outgoing connection to a predetermined “Trigger Port” range. Users are allowed to add, remove, edit, enable, and disable port trigger mappings here as shown in Figure 2-21. Please note that port trigger is only applicable when the CPE is in NAT mode. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and press “Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



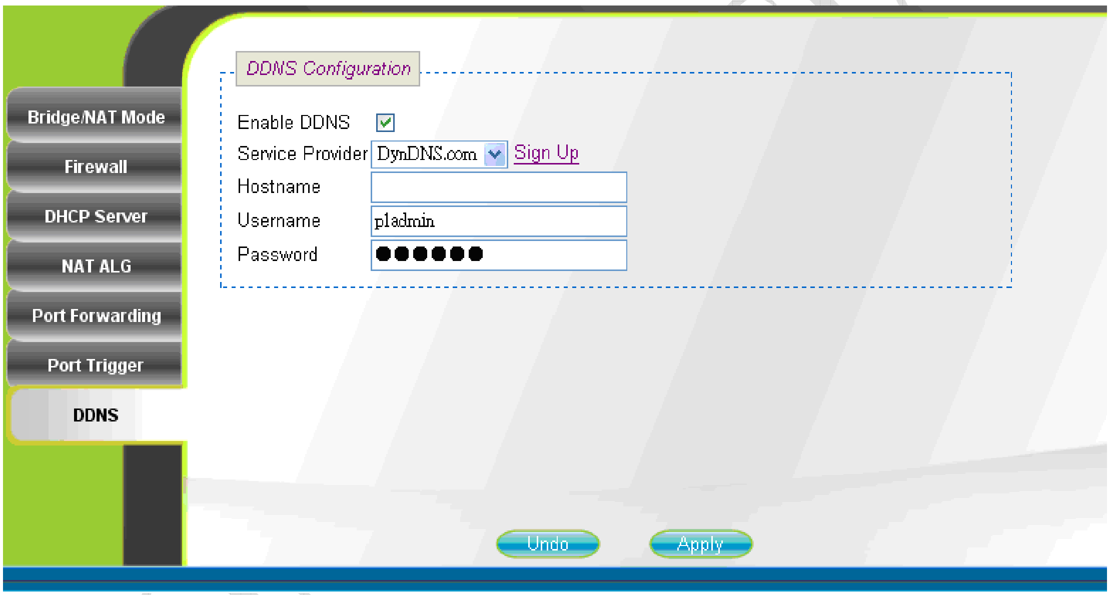
No.	Name	Trigger Port		Forwarding Port		Protocol	Enable	Delete
		Begin	End	Begin	End			
1	gemtek	1000	1024	30	40	TCP	☑	Delete
2	gemtek	5600	5695	80	90	UDP	☑	Delete
3						TCP	□	Delete

Figure 2-21 Port Trigger

2.15. DDNS

Networking → DDNS

By selecting or deselecting the checkbox, users can enable or disable DDNS as shown in Figure 2-22 and Figure 2-23. To enable DDNS, registration with at least one of the seven service providers is required, and can be done by clicking the "Sign Up" hyperlink and following the procedures. Enter the hostname, username, and password you have registered with the service provider and press the "Apply" button to save the changes into the CPE. The CPE will be able to notify the selected domain name server to change the active DNS configuration of its configured hostnames and addresses in real time by using the Internet Protocol Suite after pressing "Reboot" as shown in Figure 2-34.



DDNS Configuration

Enable DDNS ☑

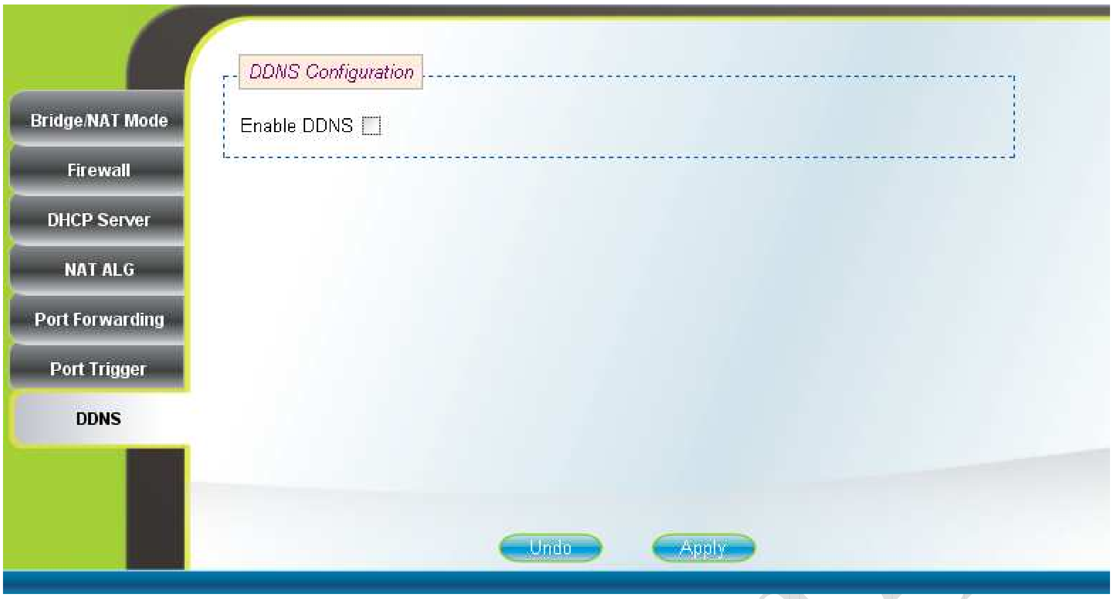
Service Provider DynDNS.com Sign Up

Hostname

Username pladmin

Password ●●●●●●

Figure 2-22 DDNS Enabled



DDNS Configuration

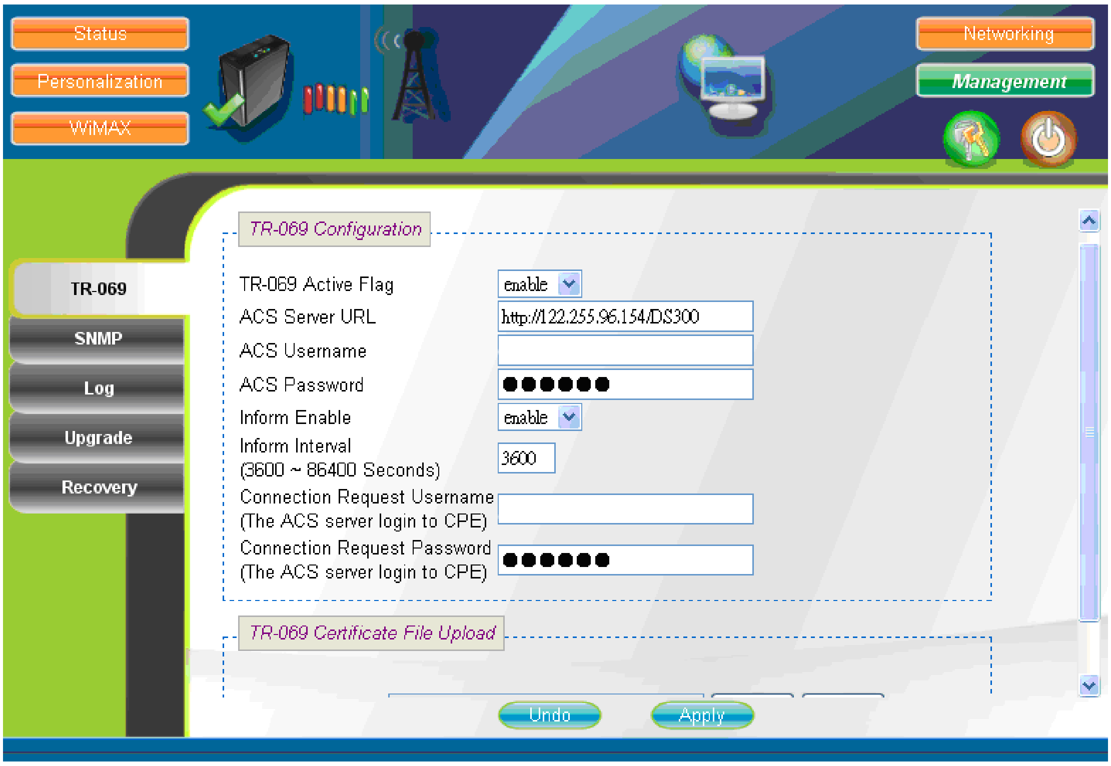
Enable DDNS □

Figure 2-23   DDNS Disabled

2.16. TR-069

Management → TR-069 (can only be accessed by administrator)

TR-069 client will automatically start up when the CPE is operational if the "TR-069 Active Flag" is enabled. The "ACS Server URL" is the URL used by TR-069 client to connect to the ACS server, and TR-069 client uses the "ACS Username" and "ACS Password" to login the ACS Server. When the "Inform Enable" is enabled, TR-069 client will periodically query the ACS server according to the "Inform Interval". The ACS server can also use the "Connection Request Username" and "Connection Request Password" to connect to the CPE and get/set parameter via connection request mechanism. Nevertheless, all of the above parameters will be overwritten if Option-43 is activated. However, the parameters changed by Option-43 will not be saved into the CPE. In other words, all of the above parameters will be restored when the CPE reboots. TR-069 certificates required for HTTPS protocol can be uploaded in the "TR-069 Certificate File Upload" section. Note that the only certificate format supported is PEM (Privacy Enhanced Mail, Base64 encoded DER certificate). Please confirm the format before uploading. Please refer to Figure 2-24 and Figure 2-25 for more details. After setting the configurations of these fields, press the "Apply" button to write the new configurations into the CPE. If only the "Inform Enable" and/or "Inform Interval" have been changed, then do nothing and the change will take effect in the next inform interval; otherwise press "Reboot" as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



TR-069 Configuration

TR-069 Active Flag: enable

ACS Server URL: http://122.255.96.154/DS300

ACS Username:

ACS Password: ●●●●●●

Inform Enable: enable

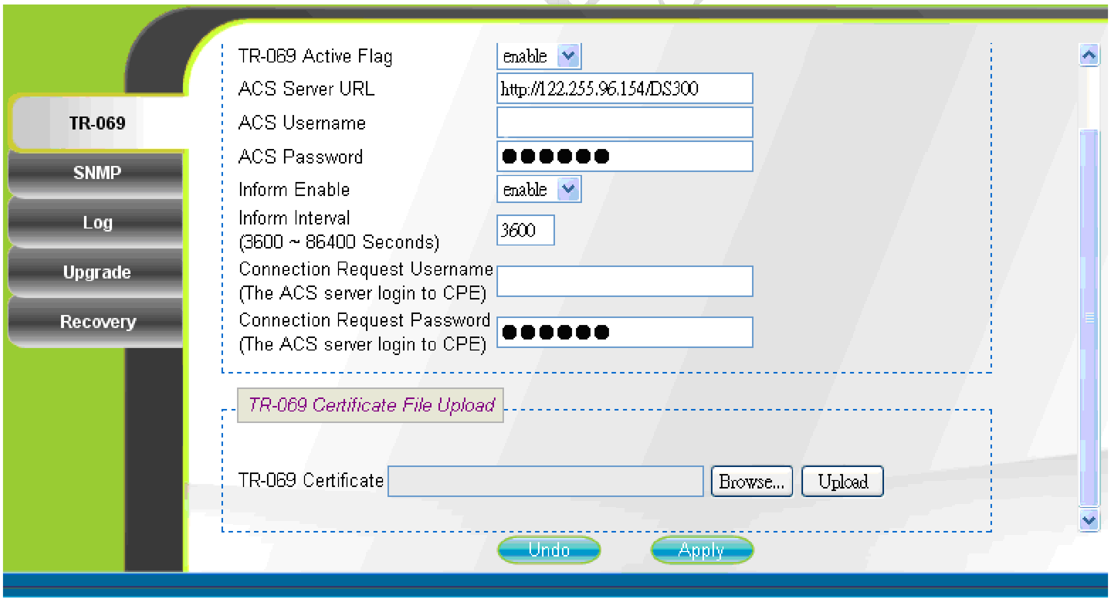
Inform Interval (3600 ~ 86400 Seconds): 3600

Connection Request Username (The ACS server login to CPE):

Connection Request Password (The ACS server login to CPE): ●●●●●●

TR-069 Certificate File Upload

Figure 2-24 TR-069



TR-069 Active Flag: enable

ACS Server URL: http://122.255.96.154/DS300

ACS Username:

ACS Password: ●●●●●●

Inform Enable: enable

Inform Interval (3600 ~ 86400 Seconds): 3600

Connection Request Username (The ACS server login to CPE):

Connection Request Password (The ACS server login to CPE): ●●●●●●

TR-069 Certificate File Upload

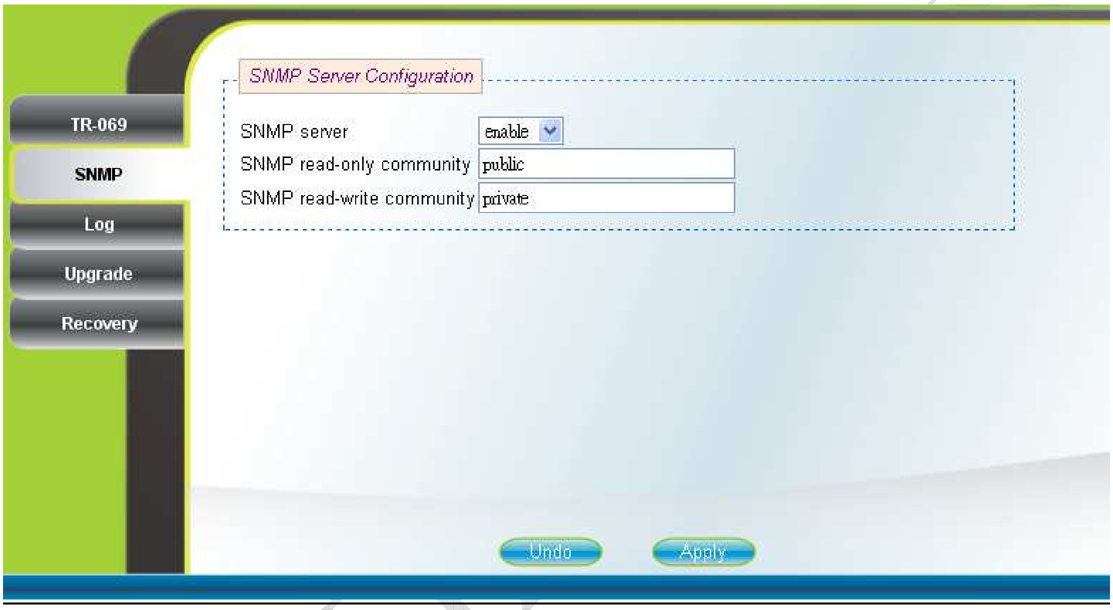
TR-069 Certificate:

Figure 2-25 TR-069-Certificate File Upload

2.17. SNMP

Management → SNMP (can only be accessed by administrator)

This page is used to enable disable SNMP server as shown in Figure 2-26 and Figure 2-27. When SNMP is enabled, the community string of the SNMP server can be changed. After setting the configurations of these fields, press the “Apply” button to write the new configurations into the CPE and press “Reboot” as shown in Figure 2-34, to reboot the system in order for the new configurations to take effect.



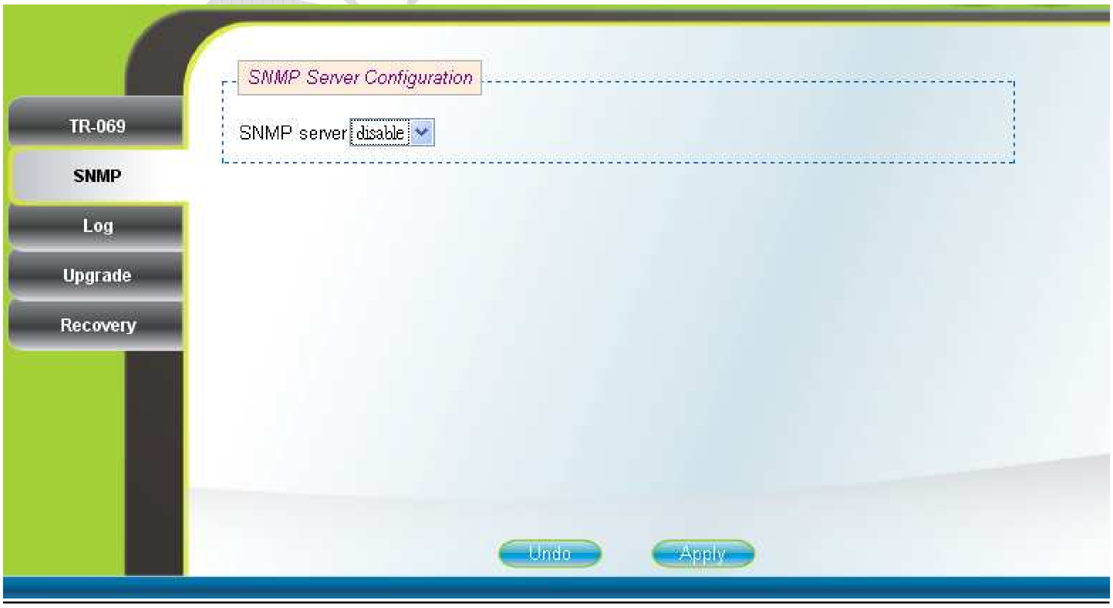
SNMP Server Configuration

SNMP server: enable

SNMP read-only community: public

SNMP read-write community: private

Figure 2-26 SNMP enabled



SNMP Server Configuration

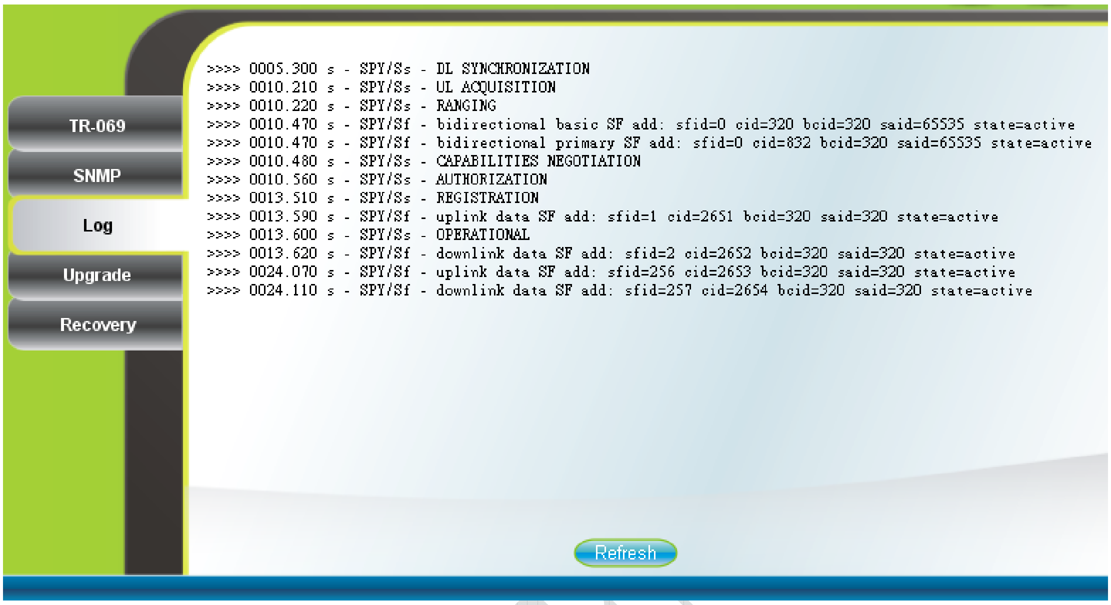
SNMP server: disable

Figure 2-27 SNMP disabled

2.18. Log

Management → Log (can only be accessed by administrator)

This page displays the system message log as shown in Figure 2-28.



```
>>>> 0005.300 s - SPY/Ss - DL SYNCHRONIZATION
>>>> 0010.210 s - SPY/Ss - UL ACQUISITION
>>>> 0010.220 s - SPY/Ss - RANGING
>>>> 0010.470 s - SPY/Sf - bidirectional basic SF add: sfid=0 cid=320 bcid=320 said=65535 state=active
>>>> 0010.470 s - SPY/Sf - bidirectional primary SF add: sfid=0 cid=832 bcid=320 said=65535 state=active
>>>> 0010.480 s - SPY/Ss - CAPABILITIES NEGOTIATION
>>>> 0010.560 s - SPY/Ss - AUTHORIZATION
>>>> 0013.510 s - SPY/Ss - REGISTRATION
>>>> 0013.590 s - SPY/Sf - uplink data SF add: sfid=1 cid=2651 bcid=320 said=320 state=active
>>>> 0013.600 s - SPY/Ss - OPERATIONAL
>>>> 0013.620 s - SPY/Sf - downlink data SF add: sfid=2 cid=2652 bcid=320 said=320 state=active
>>>> 0024.070 s - SPY/Sf - uplink data SF add: sfid=256 cid=2653 bcid=320 said=320 state=active
>>>> 0024.110 s - SPY/Sf - downlink data SF add: sfid=257 cid=2654 bcid=320 said=320 state=active
```

Figure 2-28 Log

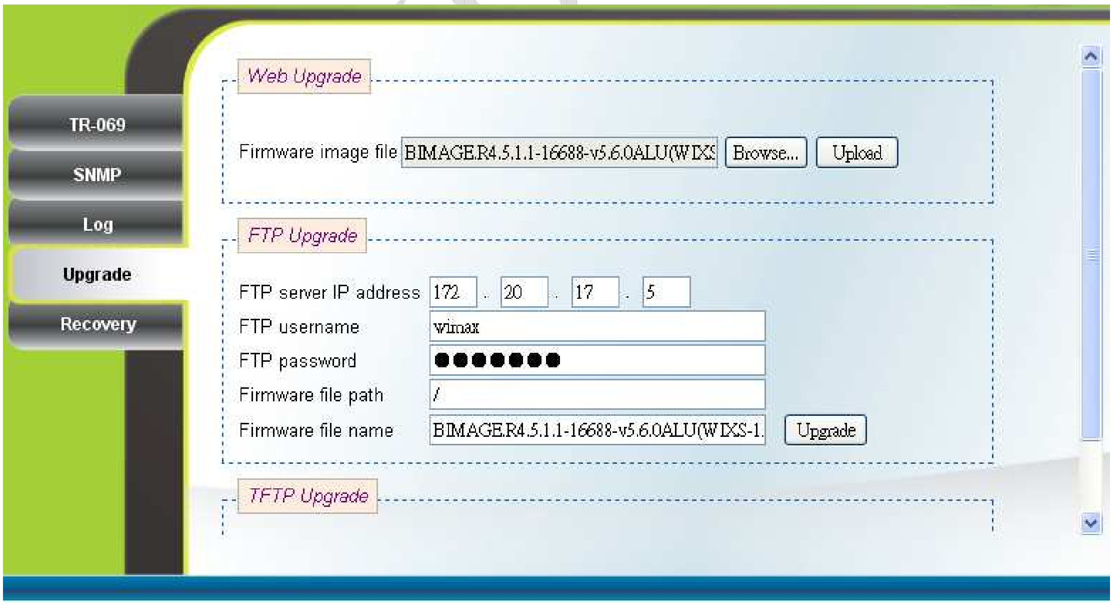
2.19. Upgrade

Management → Upgrade (can only be accessed by administrator)

To perform web upgrade, press the "Brows…" button to choose the firmware file in the computer in the "Web Upgrade" section, and press the "Upload" button to upload the file into the CPE. Please refer to Figure 2-29 for more details. After the firmware file is uploaded, the summary will be displayed as shown in Figure 2-30. Then press the "Apply" button to upgrade the firmware. This upgrade procedure takes about 3 minutes and reboots the CPE afterwards automatically.

To perform FTP upgrade, input the FTP server IP address, FTP username and password, firmware file path, and firmware file name. Press the "Upgrade" button in the "FTP Upgrade" section and the CPE will start to download the firmware from the FTP server and upgrade. The CPE will automatically reboot itself afterwards. Please refer to Figure 2-29 for more details.

To perform TFTP upgrade, input the TFTP server IP address and the firmware file path and press the "Upgrade" button in the "TFTP Upgrade" section. It takes about 3 minutes for a CPE to download the firmware from a TFTP server and upgrade it. The CPE automatically reboots itself afterwards. Please refer to Figure 2-31 for more details.



Web Upgrade

Firmware image file BIMAGE.R4.5.1.1-16688-v5.6.0ALU(WIXS [Browse...] [Upload]

FTP Upgrade

FTP server IP address 172 . 20 . 17 . 5

FTP username wimax

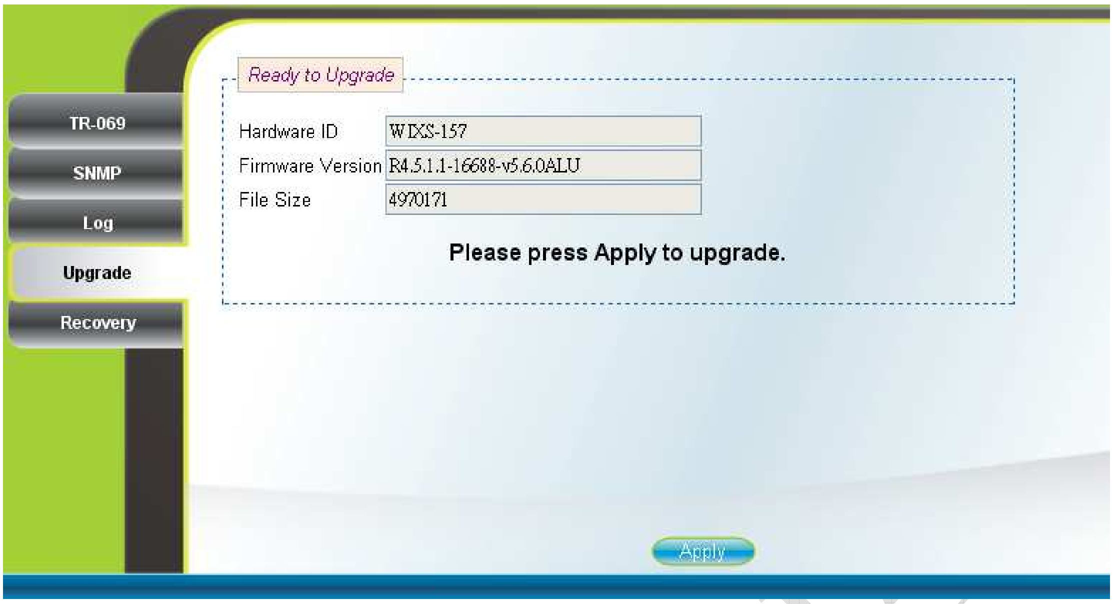
FTP password ●●●●●●●

Firmware file path /

Firmware file name BIMAGE.R4.5.1.1-16688-v5.6.0ALU(WIXS-1. [Upgrade]

TFTP Upgrade

Figure 2-29 Web/FTP Upgrade



Ready to Upgrade

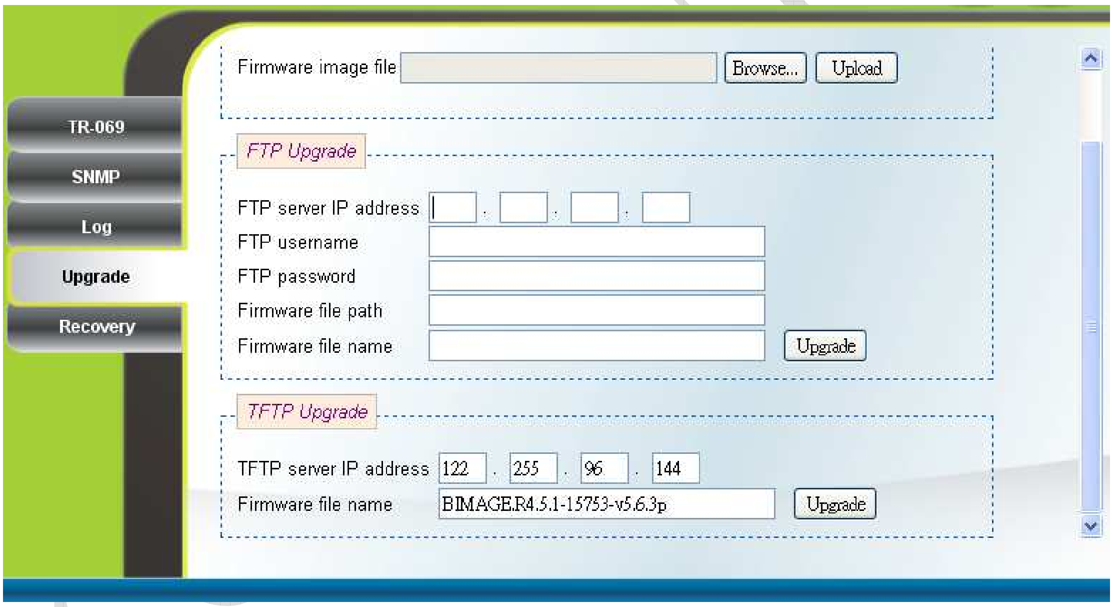
Hardware ID: WIXS-157

Firmware Version: R4.5.1.1-16688-v5.6.0ALU

File Size: 4970171

Please press Apply to upgrade.

Figure 2-30 Web Upgrade Summary



Firmware image file:

FTP Upgrade

FTP server IP address: . . .

FTP username:

FTP password:

Firmware file path:

Firmware file name:

TFTP Upgrade

TFTP server IP address: 122 . 255 . 96 . 144

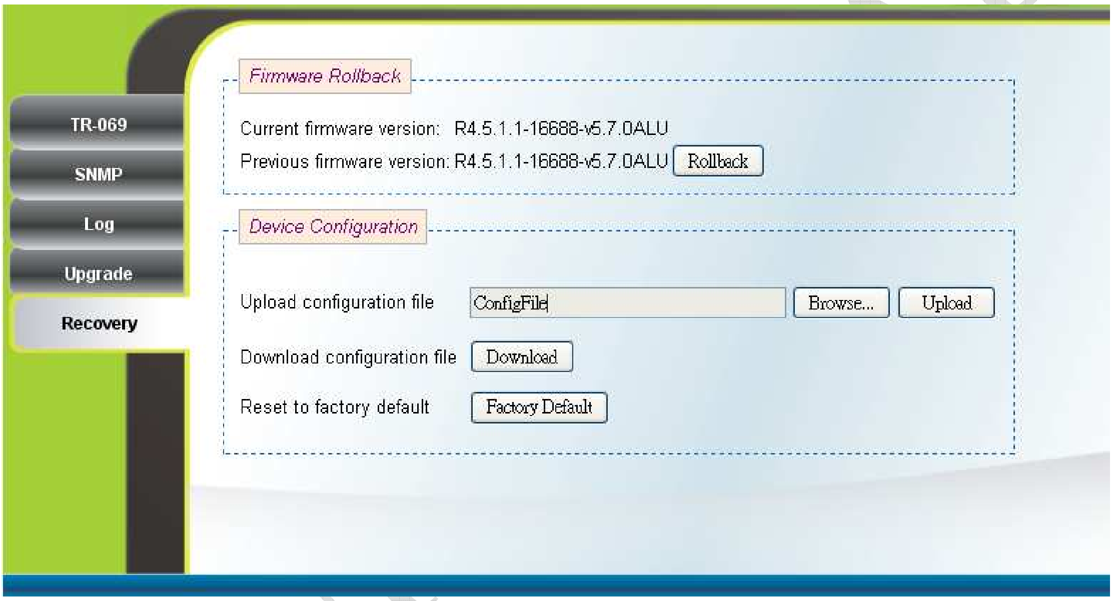
Firmware file name: BIMAGE.R4.5.1-15753-v5.6.3p

Figure 2-31 TFTP Upgrade

2.20. Recovery

Management → Recovery (can only be accessed by administrator)

Both current firmware version and previous firmware version are shown in the "Firmware Rollback" section. Firmware rollback can be performed by pressing the "Rollback" button. Device configuration file that includes files such as, .configdb and ddns.conf, can be uploaded from PC to CPE as well as downloaded from CPE to PC. To restore a CPE back to factory default settings, just press the "Factory Default" button in the "Factory Default Settings" section. Please refer to Figure 2-32 for more details.



Current firmware version: R4.5.1.1-16688-v5.7.0ALU

Previous firmware version: R4.5.1.1-16688-v5.7.0ALU

Upload configuration file: ConfigFile

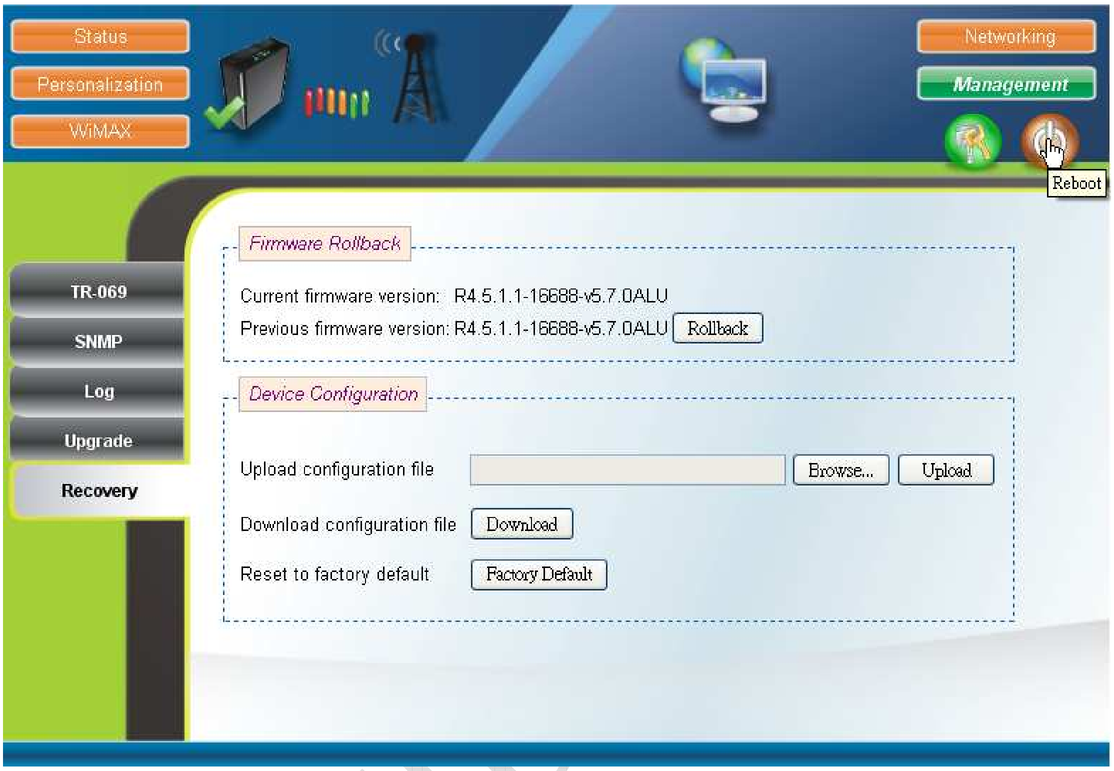
Download configuration file

Reset to factory default

Figure 2-32 Recovery

2.21. Reboot

Press the “Reboot” and “Yes” buttons to reboot the system. Please refer to Figure 2-34 and Figure 2-34 for more details.



Firmware Rollback

Current firmware version: R4.5.1.1-16688-v5.7.0ALU

Previous firmware version: R4.5.1.1-16688-v5.7.0ALU [Rollback]

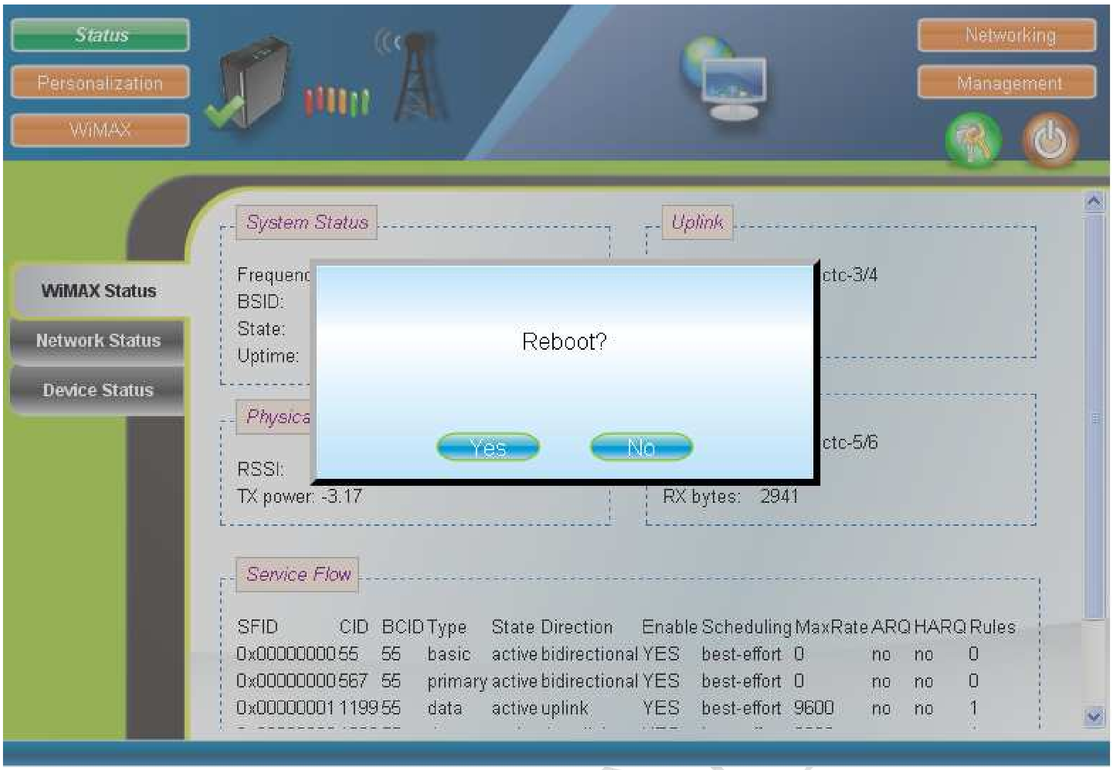
Device Configuration

Upload configuration file [Browse...] [Upload]

Download configuration file [Download]

Reset to factory default [Factory Default]

Figure 2-33 Reboot Button



Frequenc
BSID:
State:
Uptime:

ctc-3/4

RSSI:
TX power: -3.17

ctc-5/6
RX bytes: 2941

SFID	CID	BCID	Type	State	Direction	Enable	Scheduling	MaxRate	ARQ	HARQ	Rules
0x00000000	55	55	basic	active	bidirectional	YES	best-effort	0	no	no	0
0x00000000	567	55	primary	active	bidirectional	YES	best-effort	0	no	no	0
0x00000001	1199	55	data	active	uplink	YES	best-effort	9600	no	no	1

Figure 2-34 Reboot Confirmation

Industry Canada statement:

This device complies with RSS-192, RSS-195, and RSS-197 of the Industry Canada 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:

Radiation Exposure Statement:

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

Radio Frequency Interference Statement

This equipment has been tested and found to comply with RSS-197 and RSS-192 of the Industry Canada Rules (for 3.x GHz bandwidth) and the limits for a class B digital device, pursuant to ETSI EN 301 489-1 and Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment notwithstanding use in commercial, business and industrial environments. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Radiation Hazard Warning

To comply with FCC RF exposure requirements in Section 1.1307 and 2.1091 of FCC Rules, the antenna used for this transmitter must be kept at a separation distance of at least 50 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with the appropriate essential requirements

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:

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 **50** cm between the radiator & your body.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

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).