

User Manual

Gemtek WiMAX Modem



Manual Version: 1.2

Manual Date: Apr. 30 2009

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

Software Date: Feb. 20 2009

CONTENTS

Chapter 1 Overview	1-1
1.1. Indoor CPE.....	1-1
1.2. Outdoor CPE.....	1-2
Chapter 2 WEB-GUI.....	2-3
2.1. System Configuration Login.....	2-3
2.2. System Logout	2-6
2.3. Account	2-7
2.4. Date	2-8
2.5. Language.....	2-9
2.6. Scanner.....	2-10
2.7. Authentication.....	2-12
2.8. Bridge Mode	2-14
2.9. NAT Mode	2-15
2.10. Firewall	2-16
2.11. DHCP Server.....	2-18
2.12. NAT ALG.....	2-20
2.13. Port Forwarding	2-21
2.14. Port Trigger	2-22
2.15. DDNS.....	2-23
2.16. TR-069.....	2-25
2.17. SNMP.....	2-27
2.18. Log	2-28
2.19. Upgrade.....	2-29
2.20. Recovery	2-31
2.21. Reboot.....	2-32

FIGURES

Figure 1-1	Indoor CPE Front Panel LED	1-1
Figure 1-2	Outdoor CPE installation	1-2
Figure 2-1	Login Page	2-3
Figure 2-2	WiMAX Status	2-4
Figure 2-3	WiMAX Status-Service Flow	2-4
Figure 2-4	Network Status	2-5
Figure 2-5	Device Status.....	2-5
Figure 2-6	Logout	2-6
Figure 2-7	Account	2-7
Figure 2-8	Date	2-8
Figure 2-9	Language	2-9
Figure 2-10	Scanner with Bandwidth range 6~10MHz.....	2-10
Figure 2-11	Scanner with Bandwidth range 3~5MHz	2-11
Figure 2-12	Authentication	2-12
Figure 2-13	Authentication-View Certificates.....	2-13
Figure 2-14	Bridge Mode.....	2-14
Figure 2-15	NAT Mode.....	2-15
Figure 2-16	Firewall	2-16
Figure 2-17	Firewall Filter.....	2-17
Figure 2-18	DHCP Server Enabled.....	2-18
Figure 2-19	DHCP Server Disabled.....	2-19
Figure 2-20	NAT ALG	2-20
Figure 2-21	Port Forwarding	2-21
Figure 2-22	Port Trigger	2-22
Figure 2-23	DDNS Enabled.....	2-23
Figure 2-24	DDNS Disabled.....	2-24
Figure 2-25	TR-069	2-26
Figure 2-26	TR-069-Certificate File Upload	2-26
Figure 2-27	SNMP enabled.....	2-27
Figure 2-28	SNMP disabled.....	2-27
Figure 2-29	Log	2-28
Figure 2-30	Web/FTP Upgrade.....	2-29
Figure 2-31	Web Upgrade Summary	2-30
Figure 2-32	TFTP Upgrade.....	2-30
Figure 2-33	Recovery	2-31

Figure 2-34 Reboot Button 2-32
Figure 2-35 Reboot Confirmation..... 2-33

CONFIDENTIAL

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. ($\text{CINR} < 8\text{dB}$)

Yellow LED is ON: the signal strength is medium. ($8\text{dB} \leq \text{CINR} < 15\text{dB}$)

Green LED is ON: the signal strength is good. ($15\text{dB} \leq \text{CINR}$)



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

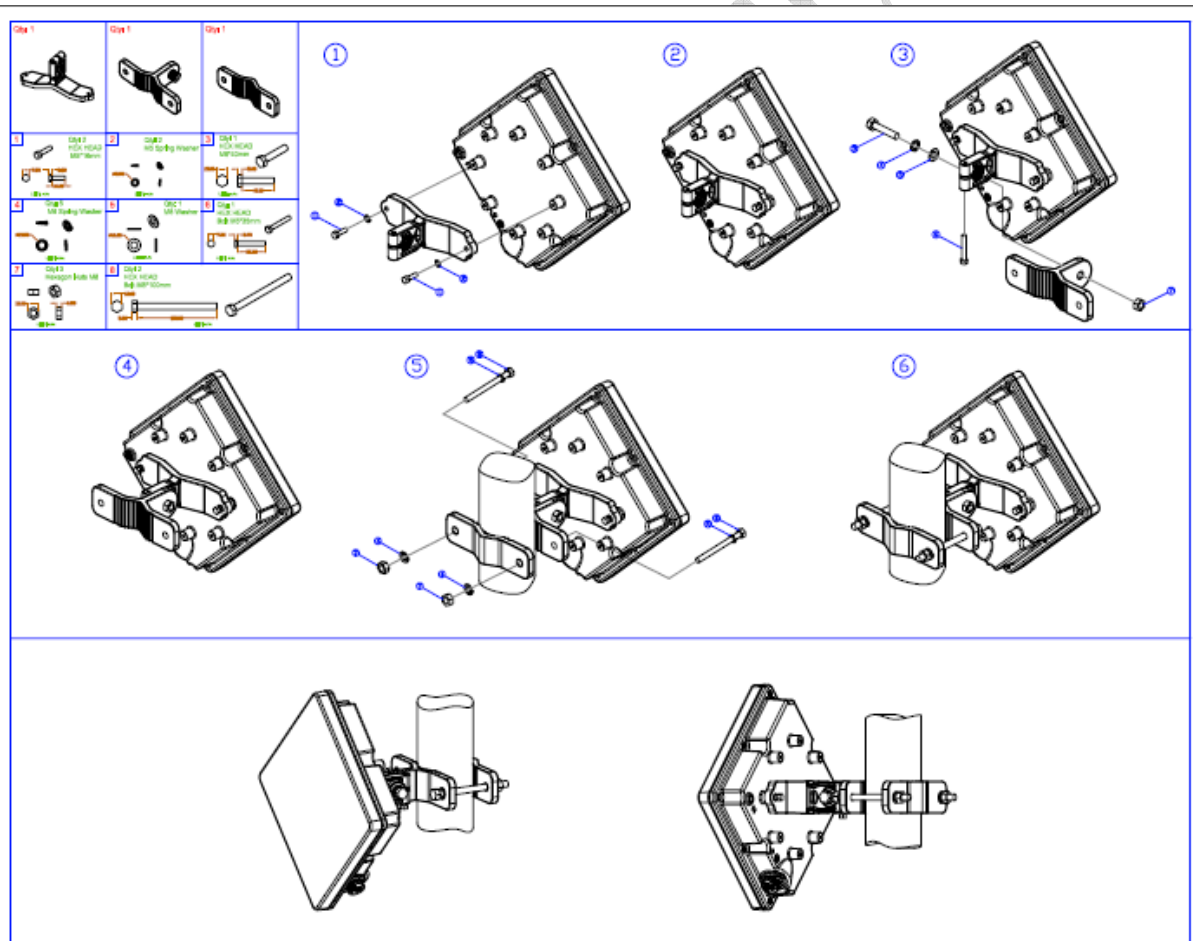


Figure 1-2 Outdoor CPE installation

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, netmask, and gateway as following.

IP address: 10.1.1.x, $1 \leq x \leq 253$

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

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

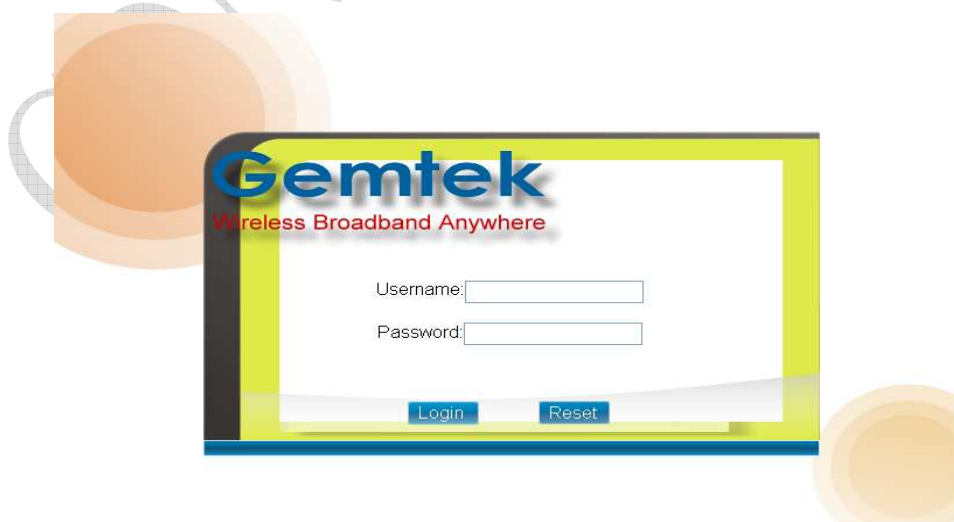


Figure 2-1 Login Page

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.



Figure 2-2 WiMAX Status

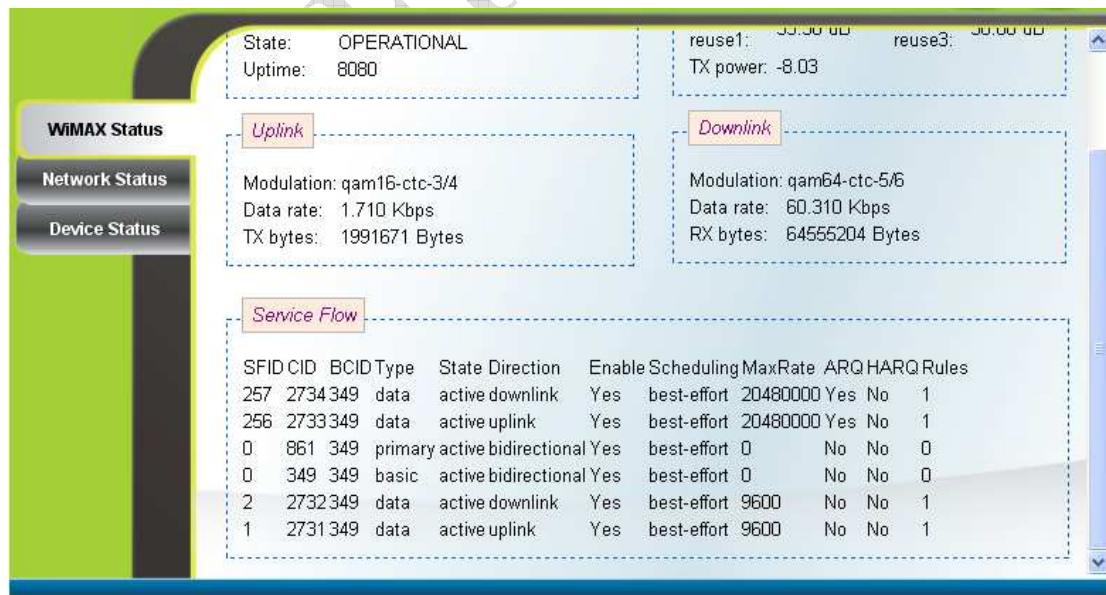


Figure 2-3 WiMAX Status-Service Flow

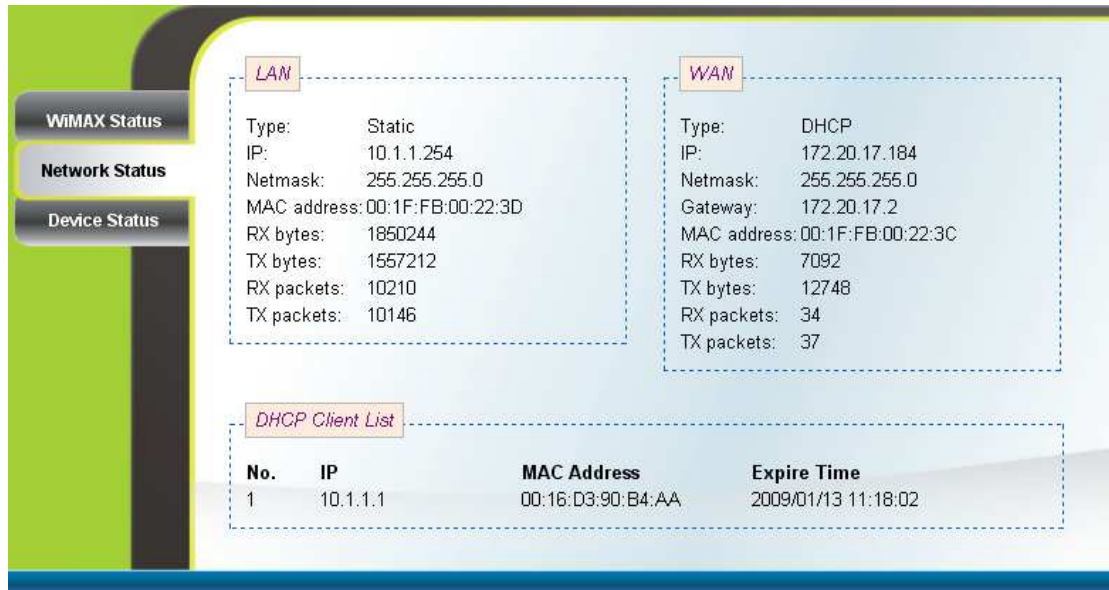


Figure 2-4 Network Status

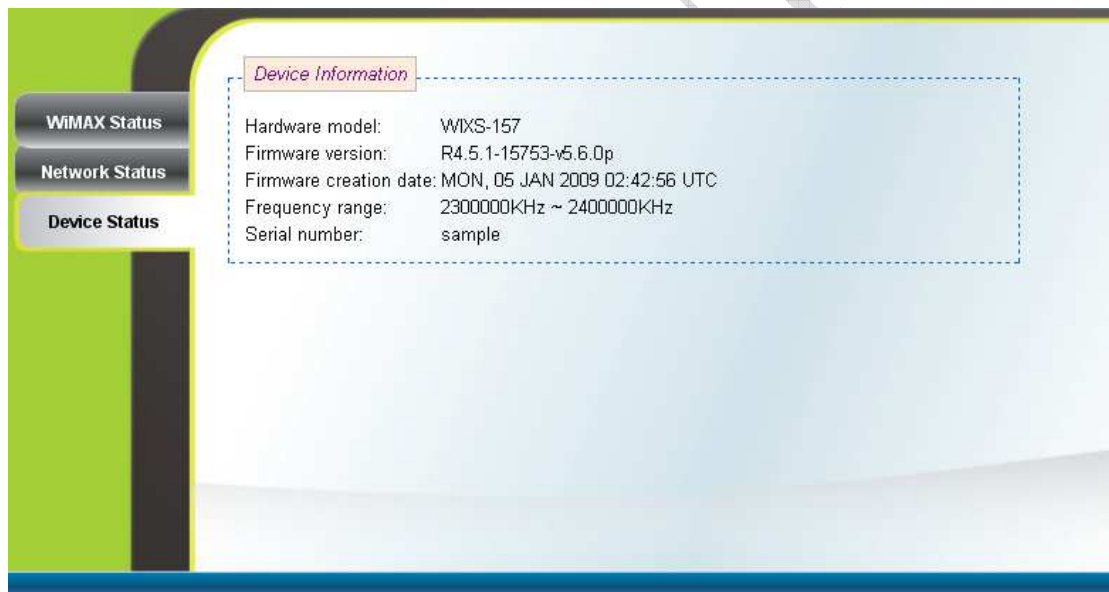


Figure 2-5 Device Status

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	unlink	Yes	best-effort	9600	No	No	1

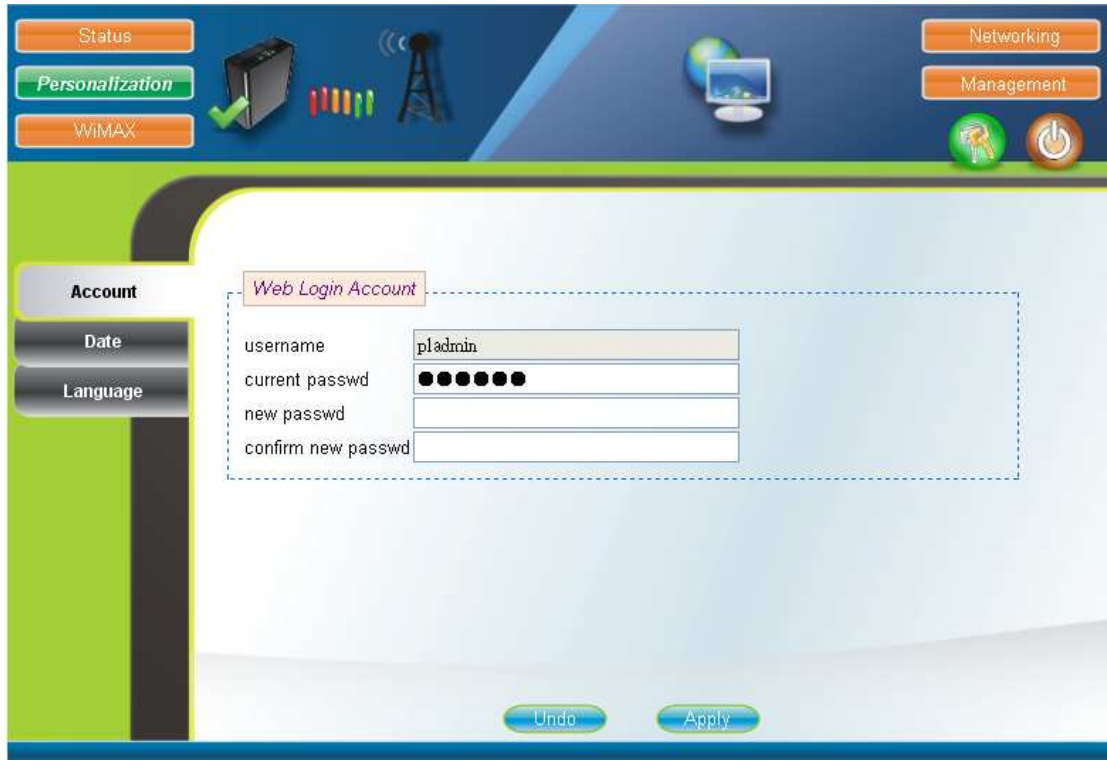
Figure 2-6 Logout

CONFIDENTIAL

2.3. Account

Personalization → Account

The Account page is used 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.



The screenshot shows a web management interface with a blue header and a green sidebar. The header contains navigation buttons for Status, Personalization, WIMAX, Networking, and Management, along with icons for a server, antenna, and computer. The sidebar has buttons for Account, Date, and Language. The main content area is titled "Web Login Account" and contains a form with the following fields:

username	<input type="text" value="pladmin"/>
current passwd	<input type="password" value="●●●●●●"/>
new passwd	<input type="password"/>
confirm new passwd	<input type="password"/>

At the bottom of the form area, there are two buttons: "Undo" and "Apply".

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 2-35, to reboot the system in order for the new configurations to take effect.

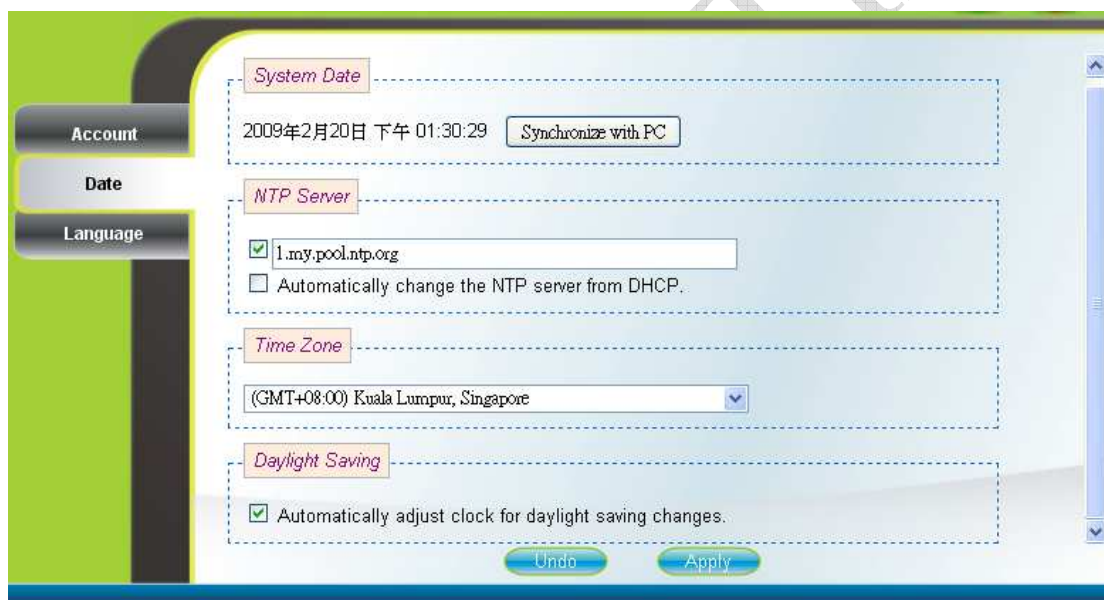


Figure 2-8 Date

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.

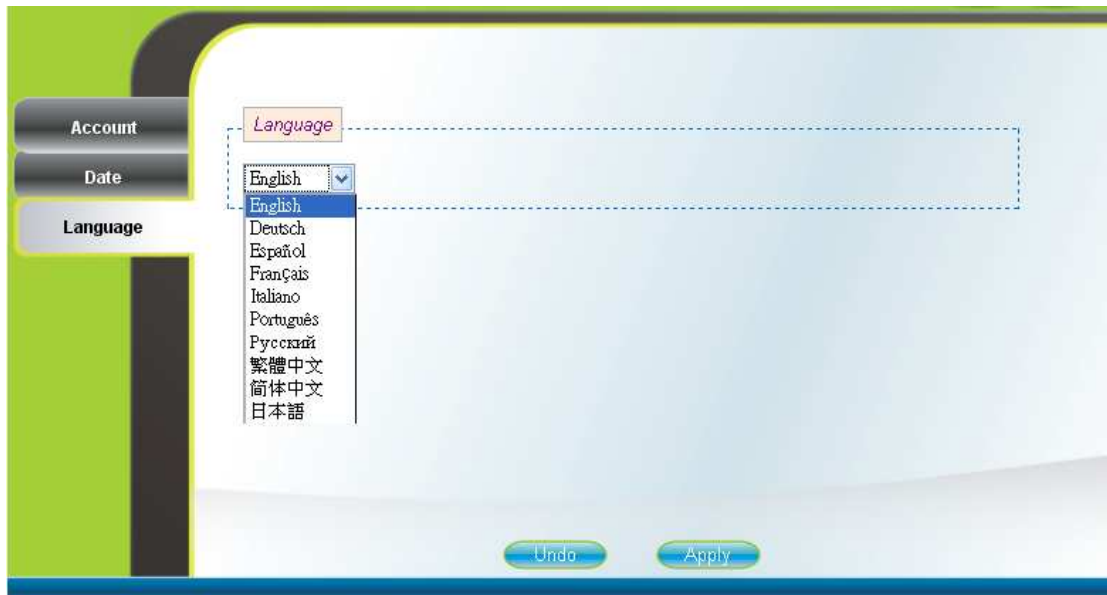


Figure 2-9 Language

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. Users are allowed to add, remove, and edit channels in the channel table. Please refer to Figure 2-10 and Figure 2-11 for 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 2-35, 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.



The screenshot displays the WiMAX Scanner interface. At the top, there are navigation buttons for Status, Personalization, WiMAX, Networking, and Management. The main content area is divided into two sections: "Start/Stop WiMAX" and "Channel Table".

The "Start/Stop WiMAX" section contains "Start" and "Stop" buttons.

The "Channel Table" section shows a "Bandwidth range" dropdown set to "6~10MHz". Below this is a table with the following data:

No.	Active	Name	Frequency	Bandwidth	RSSI	CINR	Enable	Delete
1	<input checked="" type="checkbox"/>		2385000	10MHz	-74.56	23.75	<input checked="" type="checkbox"/>	Delete
2	<input type="checkbox"/>		2365000	10MHz			<input checked="" type="checkbox"/>	Delete
3	<input type="checkbox"/>		2375000	10MHz			<input type="checkbox"/>	Delete

Below the table is an "Insert" button. At the bottom of the interface, there are "Undo" and "Apply" buttons.

Figure 2-10 Scanner with Bandwidth range 6~10MHz

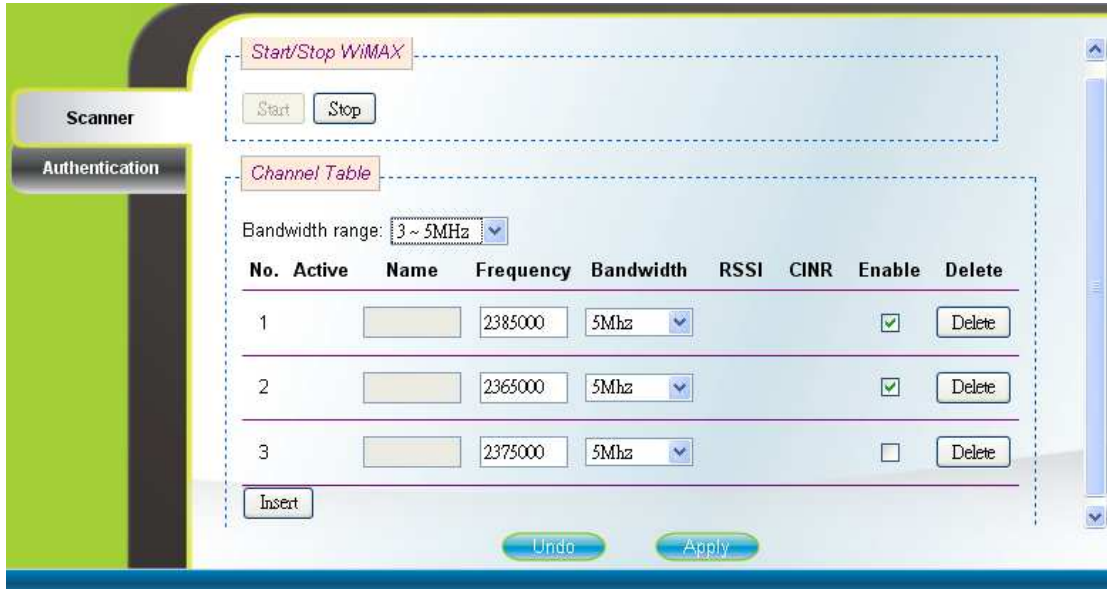


Figure 2-11 Scanner with Bandwidth range 3~5MHz

CONFIDENTIAL

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 2-35, 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 2-13. 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 2-12 for more details.

The screenshot shows a web-based configuration interface for WiMAX authentication. On the left, there is a sidebar with two tabs: "Scanner" and "Authentication", with "Authentication" currently selected. The main content area is titled "Authentication Selection" and contains the following fields:

- Phase 1: A dropdown menu set to "EAP-TTLS".
- Phase 2: A dropdown menu set to "CHAP".
- Username: A text input field containing "gemtek_paul".
- Password: A text input field with masked characters (dots).
- Identity: A text input field containing "anonymous@wimax.com".

Below this section is the "Certification File Upload" section, which includes:

- A file input field for "CA certificate" with "Browse..." and "Upload" buttons.
- Two existing certificates: "CA certificate 1" and "CA certificate 2", each with "View" and "Delete" buttons.

At the bottom of the form, there are "Undo" and "Apply" buttons.

Figure 2-12 Authentication

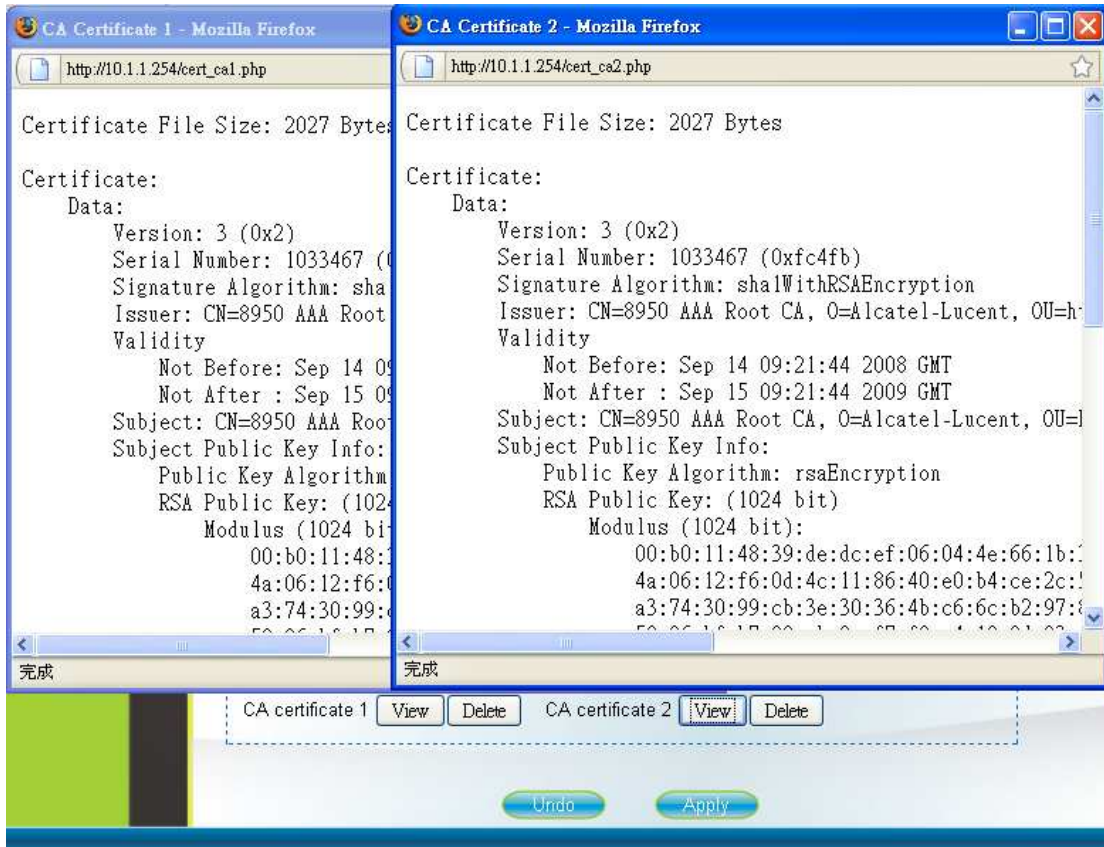


Figure 2-13 Authentication-View Certificates

CONFIDENTIAL

2.8. Bridge Mode

Networking → Bridge/NAT Mode

Bridge mode is enabled by simply selecting “Bridge Mode” as shown in Figure 2-14. 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 2-35, to reboot the system in order for the new configurations to take effect.

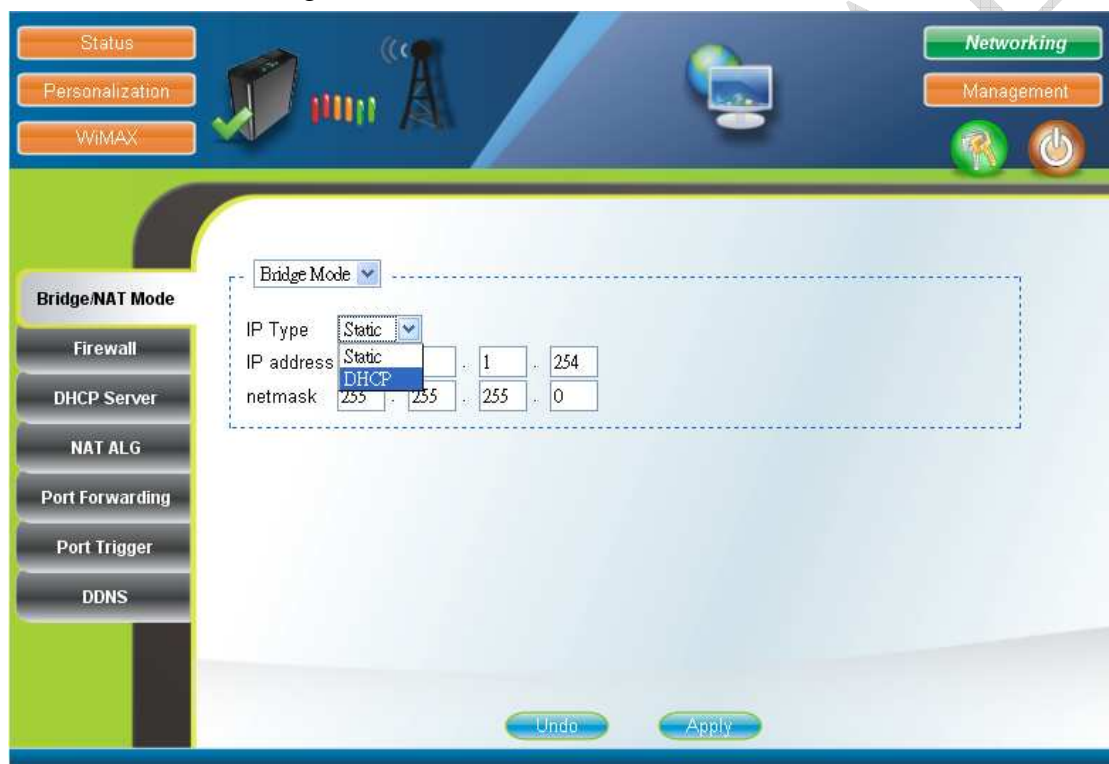


Figure 2-14 Bridge Mode

2.9. NAT Mode

Networking → Bridge/NAT Mode

NAT mode is enabled by simply selecting “NAT Mode” as shown in Figure 2-15. 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 2-35, to reboot the system in order for the new configurations to take effect.

NAT Mode	DHCP			
WAN IP type	DHCP			
WAN IP address	172	17	213	
WAN netmask	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 2-15 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 2-16 and Figure 2-17 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 2-35, to reboot the system in order for the new configurations to take effect.

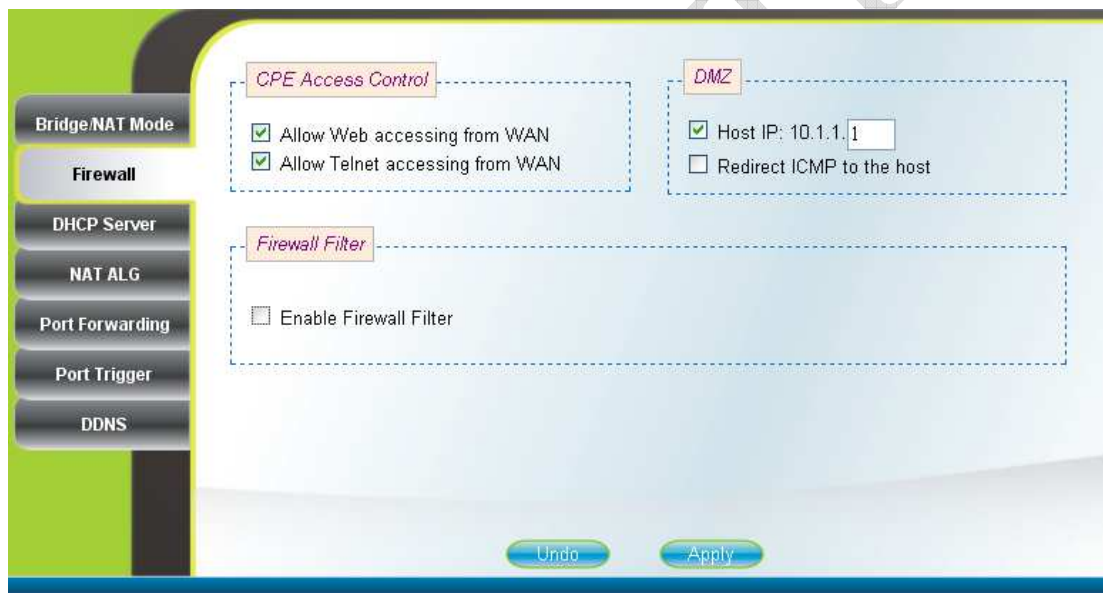


Figure 2-16 Firewall

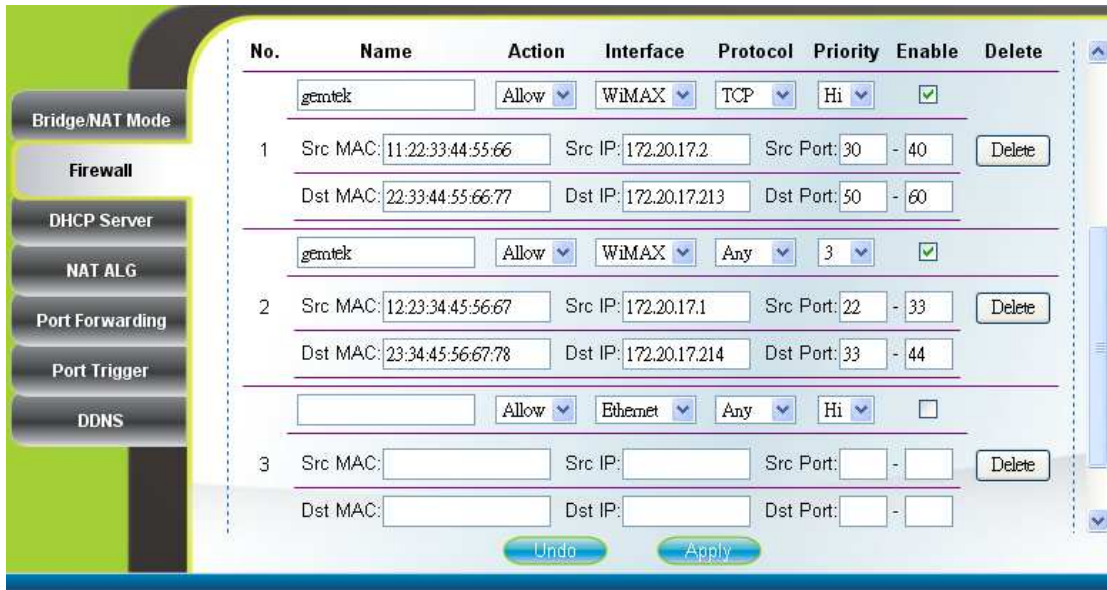


Figure 2-17 Firewall Filter

CONFIDENTIAL

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 2-18; otherwise, it shows that the DHCP server is disabled as shown in Figure 2-19. 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 2-18. 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 2-35, 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	<input checked="" type="checkbox"/>	Delete
2	12:23:34:45:56:67	10	.	1	.	1	.	7	<input checked="" type="checkbox"/>	Delete

Figure 2-18 DHCP Server Enabled

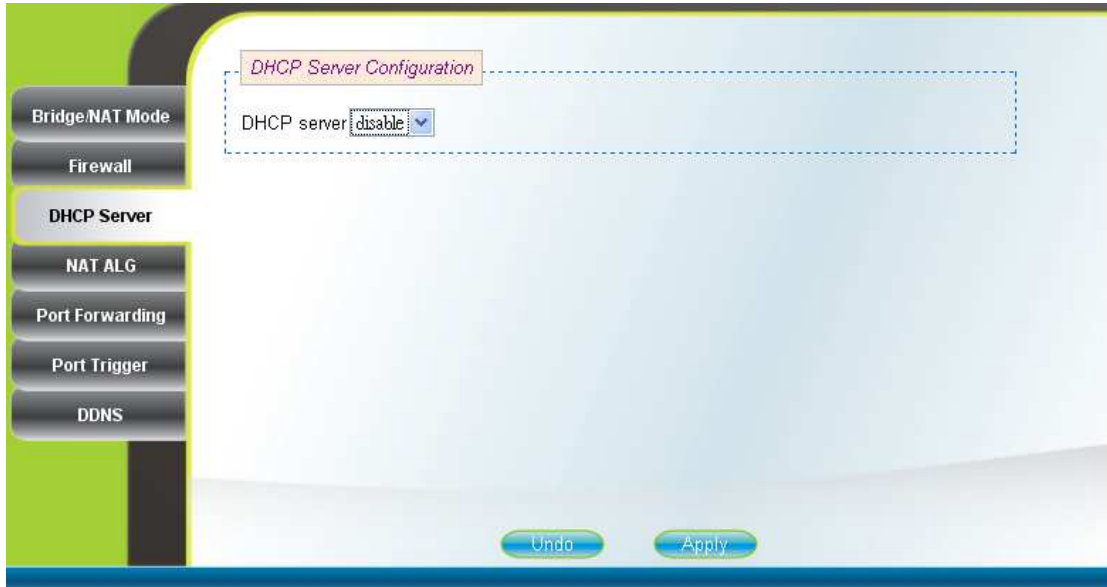


Figure 2-19 DHCP Server Disabled

CONFIDENTIAL

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 2-20. 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 2-35, to reboot the system in order for the new configurations to take effect.



Figure 2-20 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 2-21. 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 2-35, 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	<input checked="" type="checkbox"/>	Delete
2			10.1.1.			TCP	<input type="checkbox"/>	Delete

Figure 2-21 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 2-22. 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 2-35, 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	geratek	1000	1024	30	40	TCP	<input checked="" type="checkbox"/>	Delete
2	geratek	5600	5695	80	90	UDP	<input checked="" type="checkbox"/>	Delete
3						TCP	<input type="checkbox"/>	Delete

Figure 2-22 Port Trigger

2.15. DDNS

Networking → DDNS

By selecting or deselecting the checkbox, users can enable or disable DDNS as shown in Figure 2-23 and Figure 2-24. 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 2-35.



The screenshot displays the DDNS Configuration page in a web interface. On the left, a vertical sidebar contains navigation buttons for Bridge NAT Mode, Firewall, DHCP Server, NAT ALG, Port Forwarding, Port Trigger, and DDNS. The main content area is titled "DDNS Configuration" and contains the following settings:

- Enable DDNS:
- Service Provider: DynDNS.com (with a "Sign Up" link)
- Hostname: wits157.dyndns.org
- Username: pladmin
- Password: [masked with 8 dots]

At the bottom of the configuration area, there are "Undo" and "Apply" buttons.

Figure 2-23 DDNS Enabled



Figure 2-24 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 2-25 and Figure 2-26 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 2-35, to reboot the system in order for the new configurations to take effect.

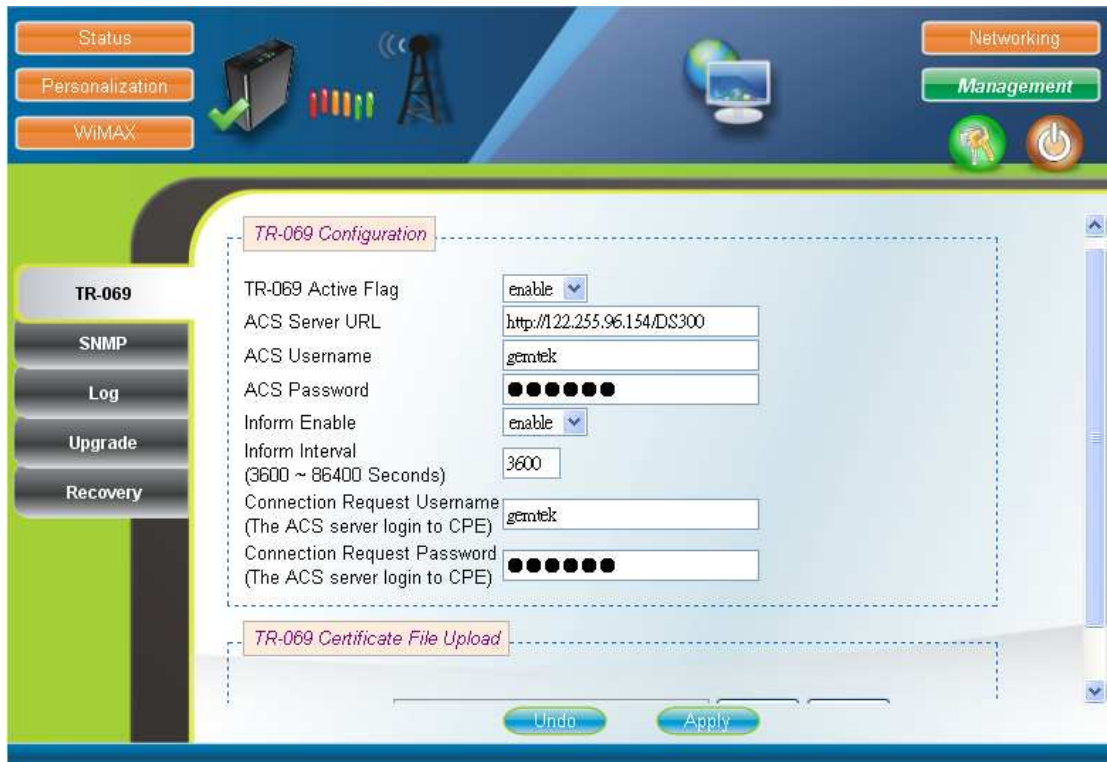


Figure 2-25 TR-069

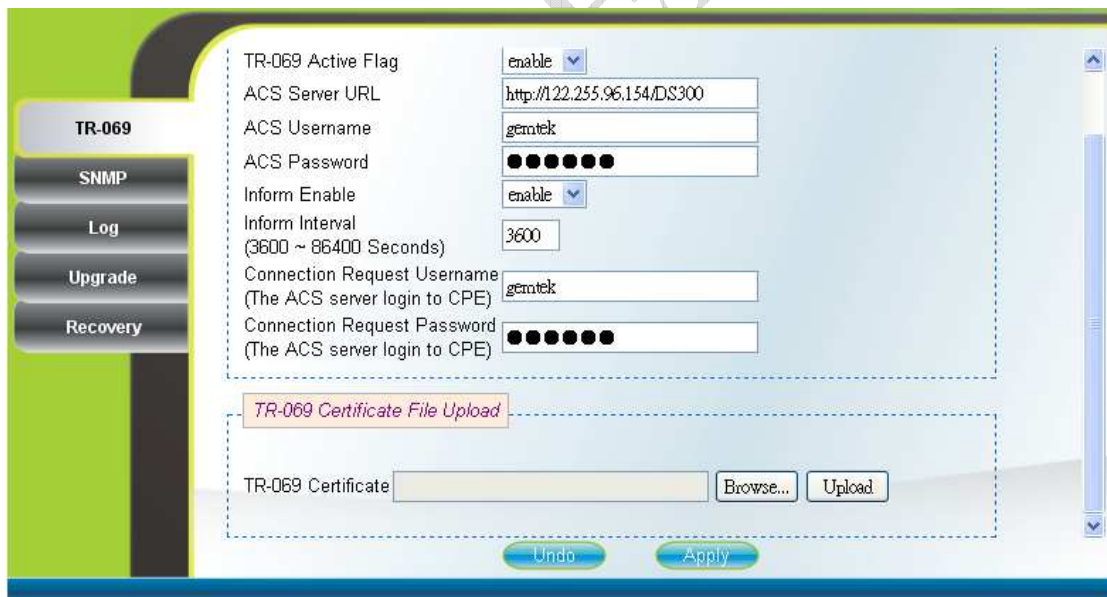


Figure 2-26 TR-069-Certificate File Upload

2.17. SNMP

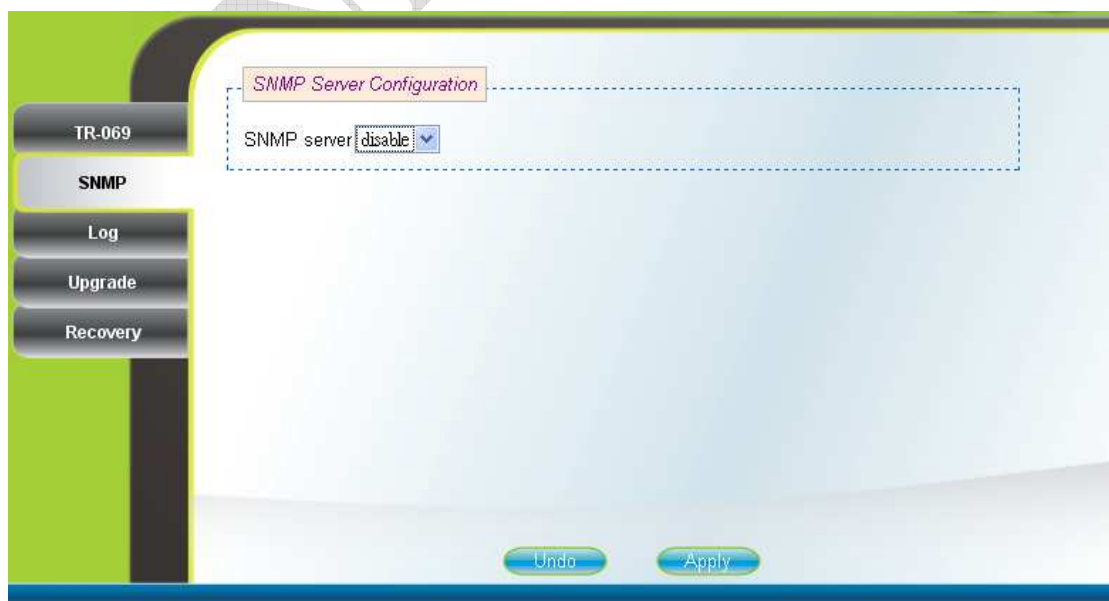
Management → SNMP (can only be accessed by administrator)

This page is used to enable/disable SNMP server as shown in Figure 2-27 and Figure 2-28. 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 2-35, to reboot the system in order for the new configurations to take effect.



The screenshot shows the 'SNMP Server Configuration' page. On the left, there is a navigation menu with buttons for 'TR-069', 'SNMP', 'Log', 'Upgrade', and 'Recovery'. The 'SNMP' button is highlighted. The main content area is titled 'SNMP Server Configuration' and contains three configuration fields: 'SNMP server' with a dropdown menu set to 'enable', 'SNMP read-only community' with a text input field containing 'public', and 'SNMP read-write community' with a text input field containing 'private'. At the bottom of the page, there are two buttons: 'Undo' and 'Apply'.

Figure 2-27 SNMP enabled



The screenshot shows the 'SNMP Server Configuration' page. On the left, there is a navigation menu with buttons for 'TR-069', 'SNMP', 'Log', 'Upgrade', and 'Recovery'. The 'SNMP' button is highlighted. The main content area is titled 'SNMP Server Configuration' and contains one configuration field: 'SNMP server' with a dropdown menu set to 'disable'. At the bottom of the page, there are two buttons: 'Undo' and 'Apply'.

Figure 2-28 SNMP disabled

2.18. Log

Management → Log (can only be accessed by administrator)

This page displays the system message log as shown in Figure 2-29.

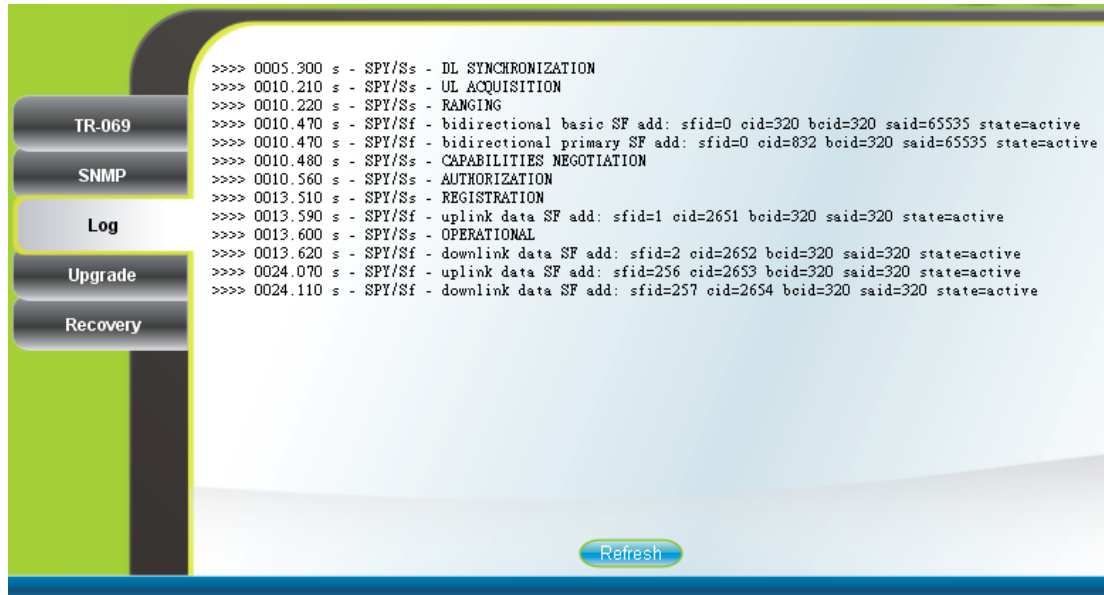


Figure 2-29 Log

CONFIDENTIAL

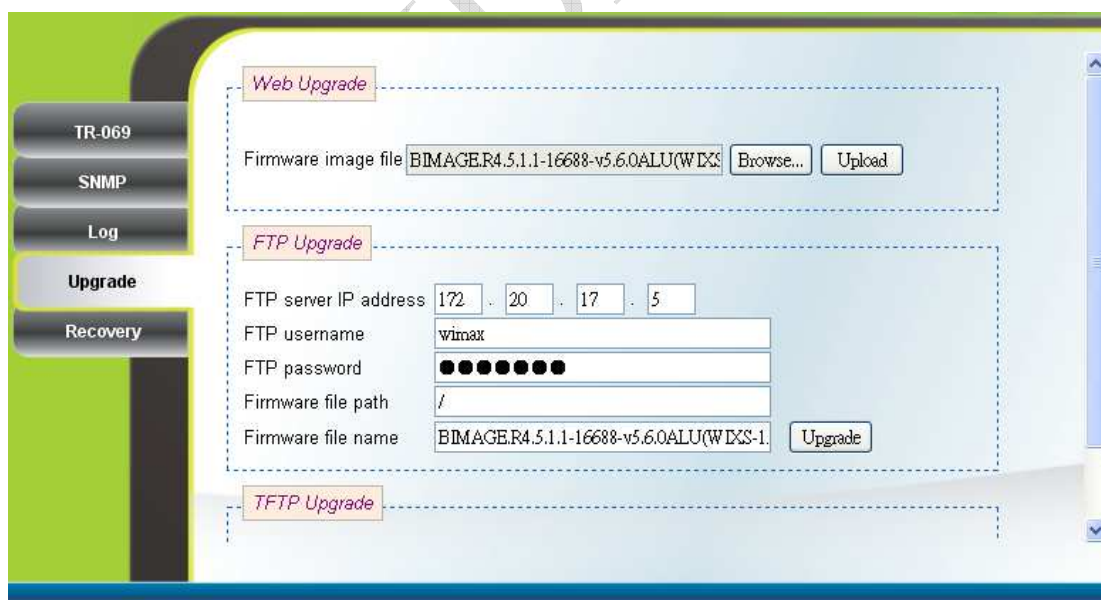
2.19. Upgrade

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 2-30 for more details. After the firmware file is uploaded, the summary will be displayed as shown in Figure 2-31. 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 2-30 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 2-32 for more details.



The screenshot displays a web-based configuration interface for upgrading the CPE firmware. On the left, a vertical navigation menu includes buttons for 'TR-069', 'SNMP', 'Log', 'Upgrade', and 'Recovery'. The main content area is divided into three sections:

- Web Upgrade:** Contains a text input field for 'Firmware image file' with the value 'BIMAGE.R4.5.1.1-16688-v5.6.0ALU(WIXS-1)'. To the right of this field are 'Browse...' and 'Upload' buttons.
- FTP Upgrade:** Contains several input fields: 'FTP server IP address' (172 . 20 . 17 . 5), 'FTP username' (winax), 'FTP password' (masked with dots), 'Firmware file path' (/), and 'Firmware file name' (BIMAGE.R4.5.1.1-16688-v5.6.0ALU(WIXS-1)). An 'Upgrade' button is located to the right of the file name field.
- TFTP Upgrade:** This section is currently empty.

Figure 2-30 Web/FTP Upgrade

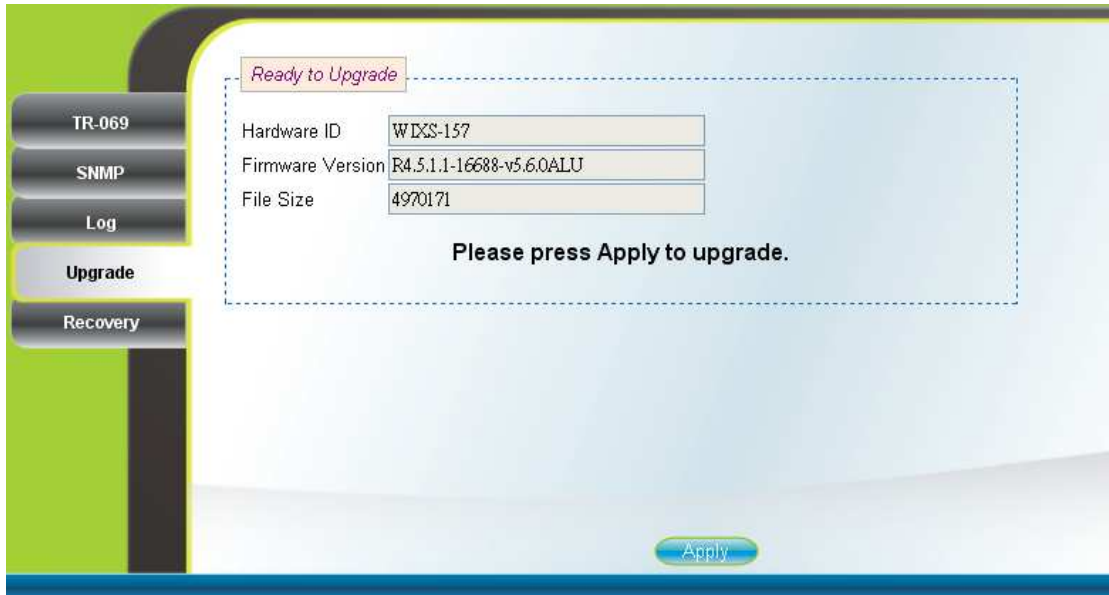


Figure 2-31 Web Upgrade Summary

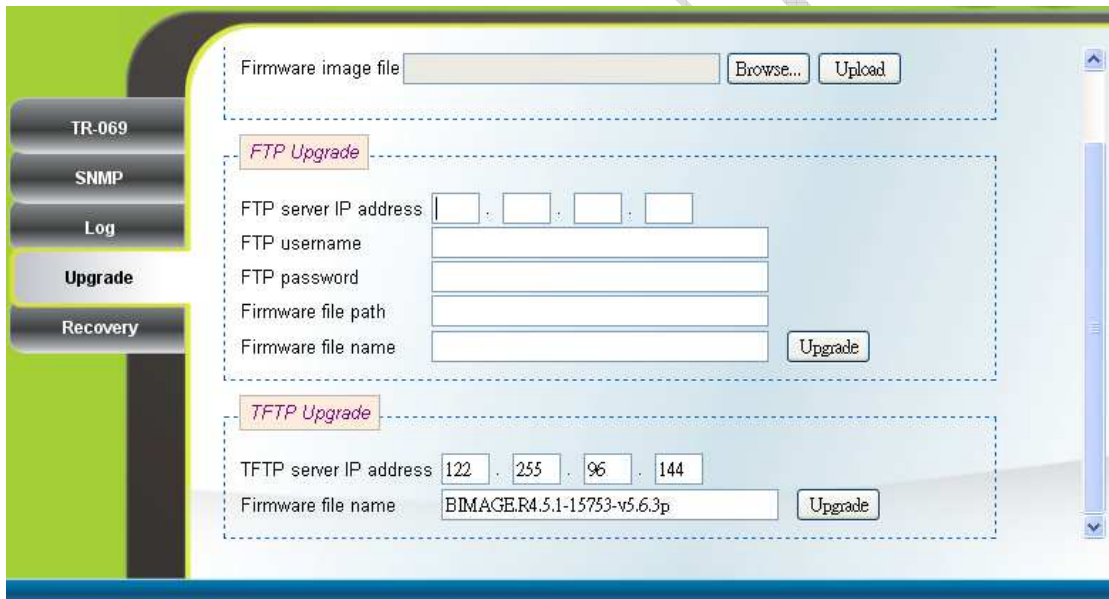


Figure 2-32 TFTP Upgrade

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 2-33 for more details.

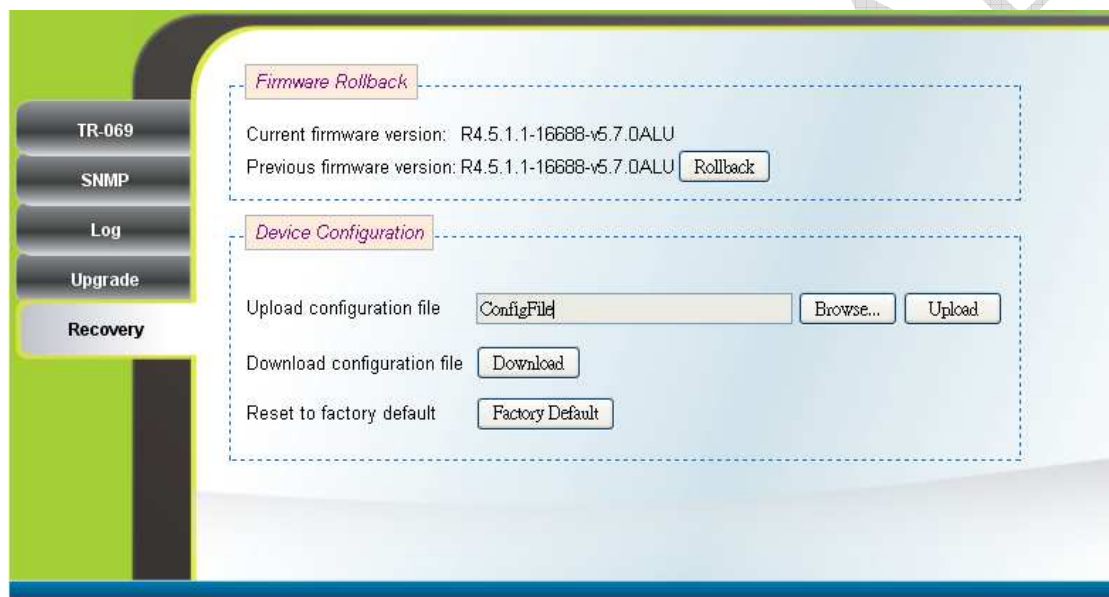


Figure 2-33 Recovery

2.21. Reboot

Press the “Reboot” and “Yes” buttons to reboot the system. Please refer to Figure 2-35 and Figure 2-35 for more details.

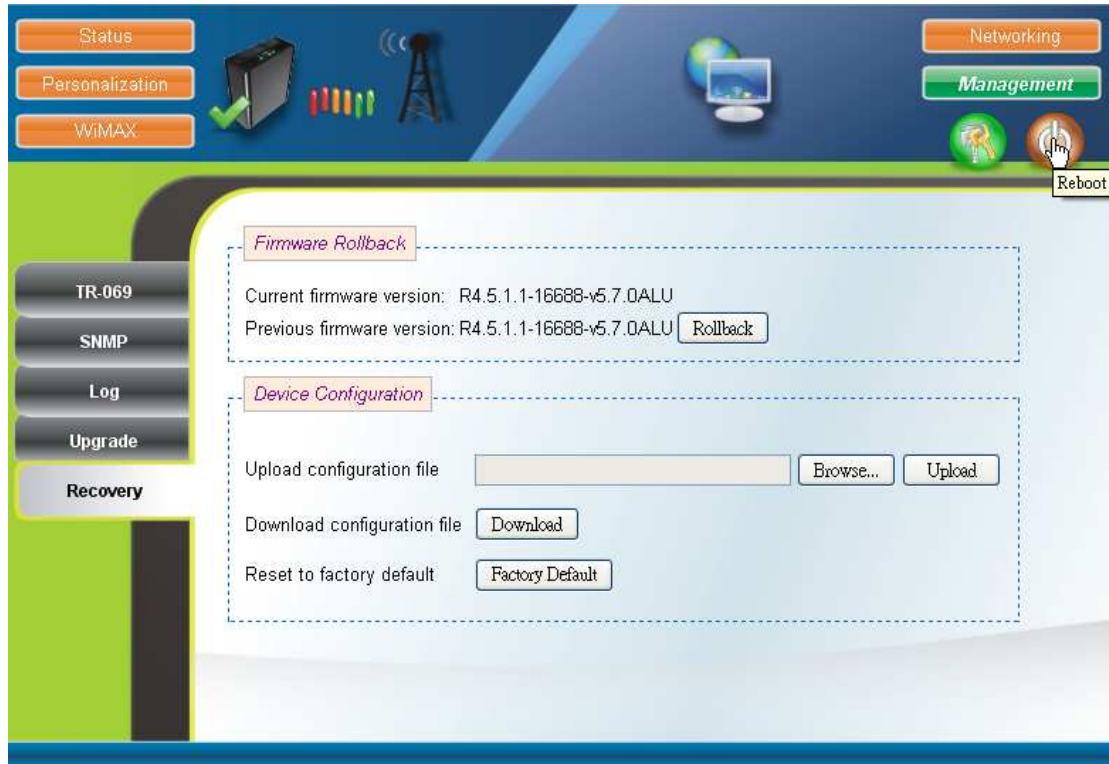


Figure 2-34 Reboot Button

CONFIDENTIAL



Figure 2-35 Reboot Confirmation



CONFIDENTIAL

1.3. Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN 60950-1: 2006+A11:2009**
Safety of Information Technology Equipment
- **EN50385 : (2002)**
- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
EN 301 489-1 V1.8.1 (2008-04)
- Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electro Magnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
EN 301 489-4 V1.4.1 (2009-05)
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 4: Specific conditions for fixed radio links, Broadband Data Transmission System Base stations, ancillary equipment and services.
EN 302 326-2 V1.2.2 (2007-06)
Fixed Radio Systems; Multipoint Equipment and Antennas; Part 2: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive for Digital Multipoint Radio Equipment
EN 302 326-3 V1.3.1 (2008-02)
Fixed Radio Systems; Multipoint Equipment and Antennas; Part 3: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive for Multipoint Radio Antennas

CE 0560

 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets</i>

[Danish]	<i>typebetegnelse</i>] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[de] Deutsch [German]	Hiermit erkl�rt [<i>Name des Herstellers</i>], dass sich das Ger�t [<i>Ger�tety</i>] in �bereinstimmung mit den grundlegenden Anforderungen und den �brigen einschl�gigen Bestimmungen der Richtlinie 1999/5/EG befindet.
[et] Eesti [Estonian]	K�esolevaga kinnitab [<i>tootja nimi = name of manufacturer</i>] seadme [<i>seadme t�iip = type of equipment</i>] vastavust direktiivi 1999/5/E� p�hin�uetele ja nimetatud direktiivist tulenevatele teistele asjakohastele s�tetele.
[en] English	Hereby, [<i>name of manufacturer</i>], declares that this [<i>type of equipment</i>] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[es] Espa�ol [Spanish]	Por medio de la presente [<i>nombre del fabricante</i>] declara que el [<i>clase de equipo</i>] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[el] Ελληνικ� [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [<i>name of manufacturer</i>] ΔΗΛΩΝΕΙ ΟΤΙ [<i>type of equipment</i>] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
[fr] Fran�ais [French]	Par la pr�sente [<i>nom du fabricant</i>] d�clare que l'appareil [<i>type d'appareil</i>] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
[it] Italiano [Italian]	Con la presente [<i>nome del costruttore</i>] dichiara che questo [<i>tipo di apparecchio</i>] � conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar �o [<i>name of manufacturer / izgatavot�ja nosaukums</i>] deklar�, ka [<i>type of equipment / iek�rtas tips</i>] atbilst Direkt�vas 1999/5/EK b�tiskaj�m pras�b�m un citiem ar to saist�tajiem noteikumiem.
Lietuvi� [Lithuanian]	�sio [<i>manufacturer name</i>] deklaruoja, kad �is [<i>equipment type</i>] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[nl] Nederlands [Dutch]	Hierbij verklaart [<i>naam van de fabrikant</i>] dat het toestel [<i>type van toestel</i>] in overeenstemming is met de essenti�le eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
[mt] Malti [Maltese]	Hawnhekk, [<i>isem tal-manifattur</i>], jiddikjara li dan [<i>il-mudel tal-prodott</i>] jikkonforma mal-htigijiet essenzjali u ma provvedimenti o�rajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[hu] Magyar [Hungarian]	Alul�rott, [<i>gy�rt� neve</i>] nyilatkozom, hogy a [<i>... t�pus</i>] megfelel a vonatkoz� alapvet� követelm�nyeknek �s az 1999/5/EC ir�nyelv egy�b el�r�sainak.
[pl] Polski [Polish]	Niniejszym [<i>nazwa producenta</i>] o�wiadcza, �e [<i>nazwa wyrobu</i>] jest zgodny z zasadniczymi wymogami oraz pozostalymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[pt] Portugu�s [Portuguese]	[<i>Nome do fabricante</i>] declara que este [<i>tipo de equipamento</i>] est� conforme com os requisitos essenciais e outras disposi��es da Directiva 1999/5/CE.
[sl] Slovensko	[<i>Ime proizvajalca</i>] izjavlja, da je ta [<i>tip opreme</i>] v skladu z bistvenimi zahtevami in ostalimi

[Slovenian]	relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[Meno výrobcu] týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
[fi]Suomi [Finnish]	[Valmistaja = manufacturer] vakuuttaa täten että [type of equipment = laitteen tyyppimerkintä] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[sv]Svenska [Swedish]	Härmed intygar [företag] att denna [utrustningstyp] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

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 **20** 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).

CONFIDENTIAL