



UWB-D00142 Rev E

**MiMAX-Pro
V-Series
User Guide**

System Release 9.61



Acknowledgements

Airspan Networks Inc acknowledges the following trademarks used within this document:



© Microsoft Corporation <http://www.microsoft.com>



© SEQUANS COMMUNICATIONS <http://www.sequans.com>

Copyright

© Copyright by **Airspan Networks Inc.**, 2011. All rights reserved worldwide.

The information contained within this document is proprietary and is subject to all relevant copyright, patent and other laws protecting intellectual property, as well as any specific agreements protecting Airspan Networks Inc. rights in the aforesaid information. Neither this document nor the information contained herein may be published, reproduced or disclosed to third parties, in whole or in part, without the express, prior, written permission of Airspan Networks Inc. In addition, any use of this document or the information contained herein for the purposes other than those for which it is disclosed is strictly forbidden.

Airspan Networks Inc. reserves the right, without prior notice or liability, to make changes in equipment design or specifications.

Information supplied by Airspan Networks Inc. is believed to be accurate and reliable. However, no responsibility is assumed by Airspan Networks Inc. for the use thereof nor for the rights of third parties which may be effected in any way by the use of thereof.

Any representation(s) in this document concerning performance of Airspan Networks Inc. product(s) are for informational purposes only and are not warranties of future performance, either expressed or implied. Airspan Networks Inc. standard limited warranty, stated in its sales contract or order confirmation form, is the only warranty offered by Airspan Networks Inc. in relation thereto.

This document may contain flaws, omissions or typesetting errors; no warranty is granted nor liability assumed in relation thereto unless specifically undertaken in Airspan Networks Inc. sales contract or order confirmation. Information contained herein is periodically updated and changes will be incorporated into subsequent editions. If you have encountered an error, please notify Airspan Networks Inc. All specifications are subject to change without prior notice.

Product performance figures quoted within this document are indicative and for information purposes only.

Safety Notices

Safety Information

1. Read this user manual and follow all operating and safety instructions.
2. Keep all product information for future reference.
3. The power requirements are indicated on the product-marking label. Do not exceed the described limits.
4. Use only a damp cloth for cleaning. Do not use liquid or aerosol cleaners.
Disconnect the power before cleaning.
5. Disconnect power when unit is stored for long periods.

Human Exposure to Radio Frequencies

The MiMAX-Pro should be installed and operated from a minimum distance of 2 meters to your body.

Federal Communication Commission Interference Statement

FCC Part 15 Description

This equipment has been tested (on relevant frequencies) 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 (for relevant frequencies). 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 21 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 devices, 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).

R&TTE Directive 1999/5/EC Statements

Installation

The transceiver and antenna equipment must be installed by a qualified professional installer and must be installed in compliance with regional, national, and local regulations. It is the responsibility of the system installer and/or system operator to ensure the installed system does not exceed any operational constraints identified by local regulations. Refer to the sections in this product User Guide for detailed information about the correct installation steps to ensure power and frequency settings are set correctly before connecting the antenna.

National Interface documents may identify, among other parameters, a maximum output power for the system, expressed in terms of an EIRP level that must not be exceeded. Any use of a combination of output power and antenna resulting in an EIRP level above the national limit may be considered illegal and is outside the scope of the R&TTE Directive 1999/5/EC compliance declaration.

WEEE Product Return Process



In accordance with the WEEE (Waste from Electrical and Electronic Equipment) directive, 2002/96/EC, this equipment is marked with the logo shown. The WEEE directive seeks to increase recycling and re-use of electrical and electronic equipment. This symbol indicates that this product should not be disposed of as part of the local municipal waste program.

Important Service Information

1. Refer all repairs to qualified service personnel. Do not remove the covers or modify any part of this device, as this voids the warranty.
2. Disconnect the power to this product and return it for service if the following conditions apply:
 - The unit does not function after following the operating instructions out-lined in this manual.
 - The product has been dropped or the housing is damaged.
3. Record the unit's serial numbers for future reference.

Table of Contents

Acknowledgements	2
Copyright	2
Safety Notices.....	2
Safety Information.....	2
Human Exposure to Radio Frequencies	2
Federal Communication Commission Interference Statement.....	3
FCC Part 15 Description.....	3
R&TTE Directive 1999/5/EC Statements	3
WEEE Product Return Process.....	4
Important Service Information	4
Table of Contents	5
Summary of Figures	8
Summary of Tables	10
1 About this Guide.....	11
1.1 Purpose	11
1.2 Intended Audience	11
1.3 Conventions	11
2 System Overview	12
2.1 Local & Remote Management.....	12
2.2 MiMAX-Pro Frequency Ranges	12
2.3 Architecture	13
2.4 Main Features	14
2.5 MiMAX-Pro Unit.....	14
2.6 Block Diagram	15
3 Installation Prerequisites	16
3.1 Package Contents	16
3.2 Minimum PC Requirements	16
3.3 Required Tools	16
4 Physical Description.....	18
4.1 MiMAX-Pro	18
4.1.1 Port.....	18
4.2 PoE Adapter	18
4.2.1 Ports	18
4.2.2 LEDs.....	19
5 Mounting and Cabling	20
5.1 MiMAX-Pro	20
5.1.1 Mounting.....	20
5.1.2 Cabling	21
5.2 PoE Adapter	22
5.2.1 Cabling	22
5.3 Surge Protector (Optional)	22
5.3.1 Cabling	22
5.3.2 Cabling □ Cavity Filter	24
6 Initial Procedure	25
6.1 Browser Requirements.....	25

6.2	System Configuration and Login	25
6.3	Accessing the MiMAX-Pro	25
6.4	Navigating your MiMAX-Pro Management.....	27
6.4.1	Menus.....	27
6.4.2	Navigating	29
7	Status	30
7.1	WiMAX Status	30
7.2	Network Status	31
7.3	Device Status	33
8	Personalization.....	35
8.1	Account Management	35
8.1.1	Web Login Account Management.....	35
8.2	Date.....	36
8.3	Language	37
9	WiMAX	39
9.1	Scanner	39
9.1.1	Start/Stop WiMAX	39
9.1.2	Channel Table	39
9.2	Authentication.....	41
9.2.1	Authentication Selection.....	43
9.2.2	Certificate File Upload	43
10	Networking	45
10.1	Bridge/NAT Mode Configuration	45
10.1.1	Bridge Mode	45
10.1.2	NAT Mode	46
10.2	Firewall	47
10.2.1	CPE Access Control.....	47
10.2.2	DMZ access	47
10.2.3	Firewall Filter	47
10.3	DHCP Server.....	49
10.3.1	DHCP Server Configuration	49
10.3.2	Permanent Host Configuration	50
10.4	NAT ALG	50
10.5	Port Forwarding.....	51
10.6	Port Trigger	52
10.7	QinQ	53
10.7.1	Set QinQ Configuration	54
10.7.2	Show QinQ Setting.....	54
10.8	VLAN	54
11	Management	57
11.1	TR-069	57
11.1.1	TR-069 Configuration	57
11.1.2	TR-069 Certificate File Upload.....	58
11.2	Buzzer	59
11.3	Log	60
11.4	Upgrade.....	60



11.4.1	Web Upgrade	62
11.4.2	FTP Upgrade	62
11.4.3	TFTP Upgrade.....	62
11.5	Recovery	63
12	Logout	65
13	Reboot.....	66
14	Appendix	67
14.1	Glossary of Terms	67
14.2	Revision History	68
14.3	Contact Information	68

Summary of Figures

Figure 1 - MiMAX-Pro Frequency Ranges	12
Figure 2 - Architecture	14
Figure 3 - MiMAX-Pro	15
Figure 4 - MiMAX-Pro block diagram	15
Figure 5 MiMAX-Pro - orientation	20
Figure 6 - bracket to mounting holes	21
Figure 7 - mounting – pole.....	21
Figure 8 - cable connection	21
Figure 9 - cable and Cavity filter connections	22
Figure 10 - with optional surge suppressor	24
Figure 11 - Cavity Filter connections	24
Figure 12 - Login page	26
Figure 13 - Home page - Status	27
Figure 14 - WiMAX status.....	30
Figure 15 - Network status	32
Figure 16 - Device status.....	33
Figure 17 - Personalization – Account	35
Figure 18 - Personalization – date.....	36
Figure 19 - Personal – Language	37
Figure 20 - WiMAX – scanner	39
Figure 21 - WiMAX - Scanner - Channel table	40
Figure 22 - WiMAX – Authentication	41
Figure 23 - WiMAX – Authentication – TTLS	42
Figure 24 - WiMAX – Authentication – none	42
Figure 25 - Networking - Bridge mode	45
Figure 26 - Networking - NAT mode.....	46
Figure 27 - Firewall settings	47
Figure 28 - Firewall Filter – settings	48
Figure 29 - Networking - DHCP Server	49
Figure 30 - Networking - DHCP Server - Permanent Host Configuration	50
Figure 31 - Networking - NAT ALG.....	51
Figure 32 - Networking - Port Forwarding	52
Figure 33 - Networking - Port Trigger.....	53
Figure 34 - Networking – QinQ.....	54
Figure 35 - Networking VLAN.....	55
Figure 36 - Networking VLAN – configuration	55
Figure 37 - Management - TR-069 Configuration	57
Figure 38 - Management - TR-069 certification file upload	58
Figure 39 - Management – Buzzer	59
Figure 40 - Management - Log	60
Figure 41 - Management – Upgrades.....	61
Figure 42 - Management – Upgrade continued.....	61
Figure 43 - Management - Upgrade - confirm	62
Figure 44 - Management – Recovery	63
Figure 45 - Management - Rollback warning	63



Figure 46 - Management - Reset to default warning	64
Figure 47 - MiMAX-Pro - Logout.....	65
Figure 48 - MiMAX-Pro - Reboot	66

Summary of Tables

Table 1 - MiMAX-Pro Dimensions	18
Table 2 - PoE Dimensions	18
Table 3 - PoE Functional specifications	18
Table 4 - PoE ports.....	18
Table 5 - PoE LEDs	19
Table 6 - Surge protector - Pins	23
Table 7 - MiMAX-Pro Menu buttons	29
Table 8 - Navigation	29
Table 9 - WiMAX status	31
Table 10 - Network status.....	33
Table 11 - Device status	34
Table 12 - Personalization - date.....	37
Table 13 - WiMAX - Authentication	44
Table 14 - Firewall Filter	48
Table 15 - VLAN MGMT	56
Table 16 - Buzzer - beeps	60

1 About this Guide

This section discusses the purpose, intended audience, conventions, referenced documentation and organization for this document.

1.1 Purpose

This User Guide provides step-by-step instructions for setting up and installing the MiMAX-Pro. It also includes an overview with technical recommendations for implementation over Airspan's Base Stations using Airspan's unique MiMAX-Pro solution.






The MiMAX-Pro is part of Airspan's family of Mobile WiMAX-based products. This MiMAX-Pro user guide provides step-by-step instructions for configuring, and managing your MiMAX-Pro using a Web browser. These procedures include:

- Overview
- Installation Prerequisites
- Physical descriptions
- Mounting & Cabling
- Lightning and Surge Protection (optional)
- Initial Procedure
- Configuration
- Upgrade
- Diagnostics
- Logout

1.2 Intended Audience

This guide is intended for the technician who is qualified and authorized to install the MiMAX-Pro.

1.3 Conventions

Icon	Description
	Checkpoint: Marks a point in the workflow where there may be an exit or branch to some other procedure. At each Checkpoint the reason for an exit or branch is given along with specific directions to locate the entry point in the other procedure.
	Reference: Gives a resource in the workflow that may be needed to complete a procedure along with specific directions to use the resource.
	Caution: Describes a possible risk and how to lessen or avoid the risk.
	Advice: Provides a recommendation based on best practice.
	Note: Provides useful information.

2 System Overview

MiMAX-Pro is outdoor WiMAX customer premises equipment (CPE). The MiMAX-Pro connects IP-enabled devices directly to WiMAX networks. Designed for the residential and small enterprise markets, the device supports high-speed broadband Internet through a Fast Ethernet connection. The MiMAX-Pro ensures high service availability at enhanced ranges, operating in both LOS and NLOS propagation environments.

The MiMAX-Pro is an encased outdoor unit mounted outside on either a pole or the wall. MiMAX-Pro is available in numerous frequency bands, operating in TDD mode in numerous channel bandwidths see: [MiMAX-Pro Frequency Ranges](#).

Designed for the residential, SOHO, and small to medium enterprise (SME) markets, the device delivers over-the-air, high-speed broadband Internet from the Airspan WiMAX 802.16e certified base stations to the end-user. The MiMAX-Pro ensures high service availability at enhanced ranges, operating in both LOS and NLOS propagation environments.

MiMAX-Pro is powered through a single channel Power over Ethernet source (PoE) adapter which interfaces with the subscriber's PC or LAN. MiMAX-Pro connects to the PoE adapter (Data & Power) port by a standard 10/100BaseT CAT-5e cable. The PoE adapter provides the unit with 48 VDC power supply.

2.1 Local & Remote Management

MiMAX-Pro is designed for local and remote management via Web server or TR-069:

- Provisioning & Configuration: auto configuration and dynamic service activation
 - Initial CPE configuration
 - Remote CPE configuration - configuration of the device (including first time use), enabling and disabling features; Allowing changes to settings and parameters of the device
- Firmware upgrade & management
 - Version management
 - Update management
- Fault Management: Status and performance control
 - Log file analysis and dynamic messages
 - Diagnostics
 - Connectivity and service control.
 - Device error report, device status query

2.2 MiMAX-Pro Frequency Ranges

The table below lists the frequency range of MiMAX-Pro models currently available. This table will grow as more models become available.

Figure 1 - MiMAX-Pro Frequency Ranges

Frequency Band	Channel Bandwidth
2.3 – 2.4 in GHz TDD mode	<ul style="list-style-type: none">• 5 MHz• 10 MHz
2.496 – 2.690 GHz in TDD mode	<ul style="list-style-type: none">• 5 MHz• 10 MHz
3.300 – 3.600 GHz in TDD mode	<ul style="list-style-type: none">• 5 MHz• 7 MHz• 10 MHz

Frequency Band	Channel Bandwidth
3.600 – 3.800 GHz in TDD mode	<ul style="list-style-type: none"> • 3.5 MHz • 5 MHz • 7 MHz • 10 MHz

2.3 Architecture

The MiMAX-Pro is an outdoor unit requiring professional installation outdoors on a pole or wall, enabling optimal positioning for best reception with the BS.



Note: MiMAX-Pro must be properly grounded according with NEC and other local safety code requirements.



Note: (U.S.A. – WCS market only) A Cavity filter is required for the 2.3 GHz variant (ordered separately).

The MiMAX-Pro architecture includes the following components:

- Encased MiMAX-Pro outdoor unit
- Power over Ethernet (PoE) adapter (power supply) plugged into a standard electrical wall outlet (110/240 VAC, 60/50 Hz).

The figure below displays the MiMAX-Pro architecture:

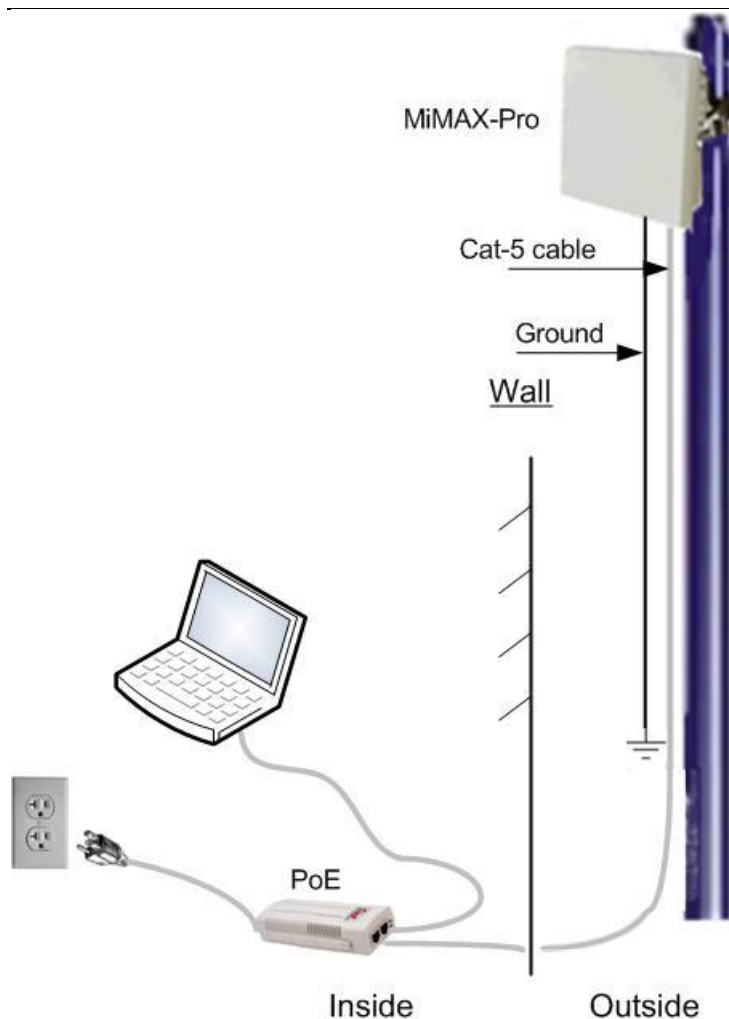


Figure 2 - Architecture

2.4 Main Features

MiMAX-Pro provides the following main features:

- IEEE 802.16e-2005 Wave 2 compliance
- OFDMA modulation, 512, 1024 FFT points QPSK, 16QAM, 64QAM
- Output power: 27 dBm
- Antenna - Integrated Directional Dual Polarization
- Security
 - 802.16e PKMv2 key management
 - X.509 digital certification for device authentication
 - EAP-TLS & EAP-TTLS (MD5, MSCHAPv2) device and user authentication methods
 - 3DES & AES(CCMP) encryption
- TR-069 for remote management
 - WEB-based interface for local management
- MIMO Matrix A and B on DL
- DL MRC
- Multi-language support

2.5 MiMAX-Pro Unit

The MiMAX-Pro V-Series with the integrated antenna is shown below:

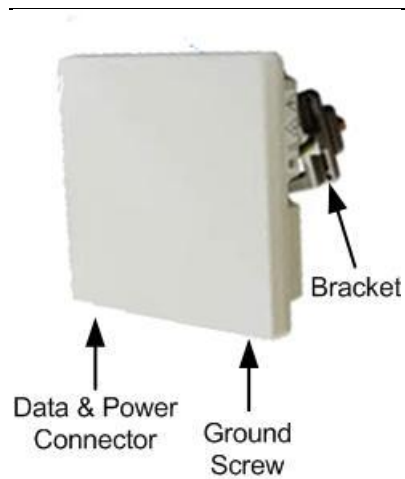


Figure 3 - MiMAX-Pro

2.6 Block Diagram

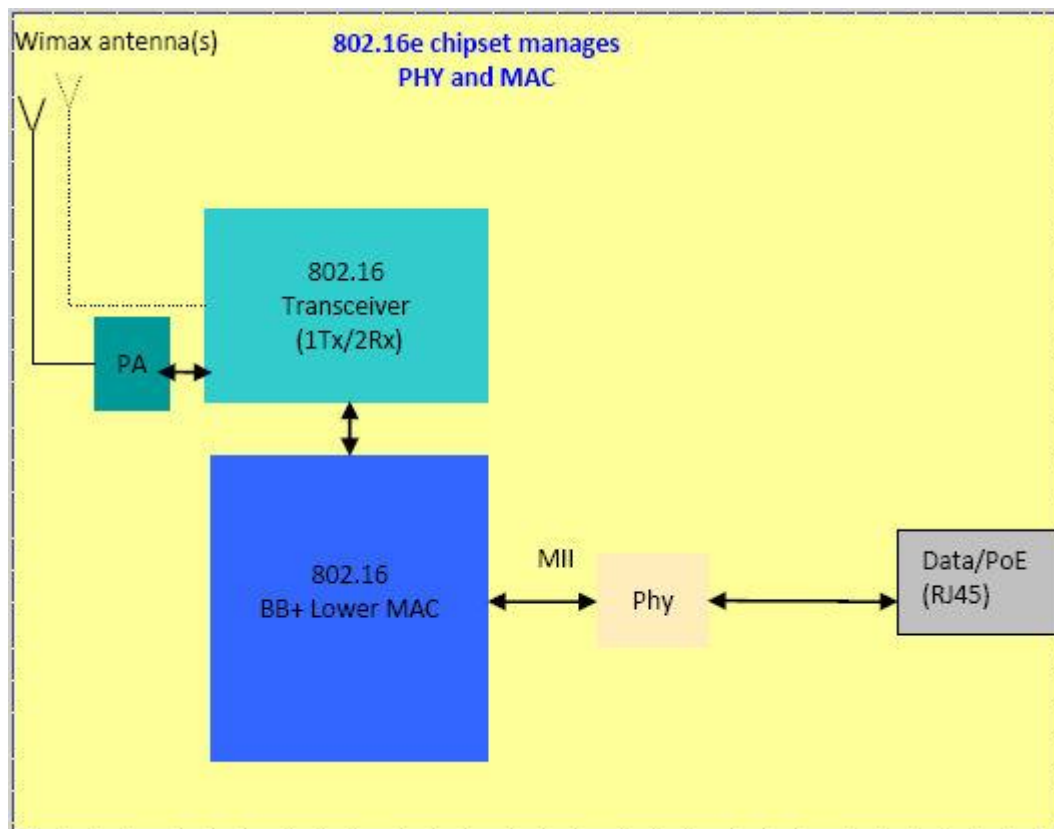


Figure 4 - MiMAX-Pro block diagram

3 Installation Prerequisites

Before installing your MiMAX-Pro, read the following to ensure that:

- [No items are missing from the package](#)
- [Minimum computer requirements are fulfilled](#)
- [You have the required installation tools](#)

3.1 Package Contents

Examine the MiMAX-Pro shipping container. If you notice any damage, or missing items as listed in the packing list, immediately notify the carrier that delivered the unit and contact an Airspan representative.

The MiMAX-Pro kit should contain the following items:

- MiMAX-Pro
- Cable Boot - Waterproof sealing cap for RJ 45 connector
- Power over Ethernet (PoE) power adapter.
- Wall/Pole-mounting kit:
 - 1 x back bracket (connects to MiMAX-Pro)
 - 1 x connecting bracket
 - 1 x mounting bracket for wall or pole (part 1)
 - 1 x clinch pole bracket for pole (part 2)
 - 2 x M5 hex head - 16mm length
 - 2 x M5 spring lock washers
 - 2 x M8 hex head - 40mm length
 - 6 x M8 spring lock washers
 - 2 x M8 flat washers
 - 2 x M5 hex head – 35 mm length
 - 4 x M8 hex nuts
 - 2 x M8 hex head – 100 mm length



Note: The standard MiMAX-Pro kit does not include a Surge Suppressor. For pricing and ordering of the Surge Suppressor, please contact your nearest Airspan dealer.

- Optional
 - Surge Suppressor
 - Filter (Cavity filter) Kit (for 2.3 GHz variant only) (U.S.A. – WCS market only) – includes Cavity Filter – (141-00-148) and 2 antenna cables – (689-000-47) – with stainless steel pole bands for mounting.

3.2 Minimum PC Requirements

Ensure that your computer provides an Ethernet interface such as a Network Interface Card (that provides an RJ-45 port).

3.3 Required Tools

The following tools are required to install the MiMAX-Pro unit:

- Wall Mounting:
 - appropriate drill bits (for wall anchors)
 - 2 x wall anchors
 - 4 x screws
 - appropriate screwdriver
- open ended spanners – for M5 & M8 hex head

Optional:

- Crimping tool for crimping CAT-5e cables to RJ-45 connectors.

➤ Cable stripping tool



Note: Airspan does not provide screws and wall anchors for mounting the MiMAX-Pro to the wall. The screw size depends on the structure of the building to which the MiMAX-Pro is to be attached. When selecting screw sizes, consideration must be given to the weight of the MiMAX-Pro and load that may be induced in windy conditions.

4 Physical Description

This section provides a description of the components of the MiMAX-Pro installation.

4.1 MiMAX-Pro

The MiMAX-Pro is an encased outdoor unit providing access to a power & communication port on its bottom panel. The MiMAX-Pro's back panel provides holes for MiMAX-Pro mounting.

The table below lists the physical dimensions of the MiMAX-Pro:

Parameter	Value
Dimensions (H x W x D)	205 X 205 X 55 mm
Weight	1.2 kg (approximate)

Table 1 - MiMAX-Pro Dimensions

4.1.1 Port

The MiMAX-Pro provides one (1) 10/100Base T Ethernet port (on the bottom) for interfacing with the PoE (LAN & power).

4.2 PoE Adapter

The PowerDsine-3001 is a single channel Power over Ethernet (PoE) source. The unit incorporates an Independent power controller, CPU controller and input (Data) and output (Data + Power) shielded RJ-45 connectors. The PoE is designed for use with a standard 10/100BaseT Ethernet network over a standard TIA/EIA-568 CAT-5e (or higher).

Parameter	Value
Dimensions (H x W x D)	31 X 58.5 X 145 mm
Weight	450 gram (approximate)

Table 2 - PoE Dimensions

Parameter	Value
AC Input Voltage	Main Input 47 to 63 Hz Vac
AC Input Current	110Vac, 60Hz 220Vac, 50Hz
Operating temperature	0 - +40 °C
Storage temperature	-20 - +70 °C
Weight	450 gram (approximate)

Table 3 - PoE Functional specifications

4.2.1 Ports

The PoE provides 2 RJ-45 ports for interfacing with the MiMAX-Pro, as defined in table below:

Port	Description
1 Input Shielded RJ-45	data from 10/100BaseTX
1 Output Shielded RJ-45	Data + Power to 10/100BaseTx terminal equipment
Universal 90-264Vac power receptacle	Input 47 to 63 Hz Vac – 110 – 220 Vac, 60Hz – 50Hz

Table 4 - PoE ports

4.2.2 LEDs

Port	Description		
Main Power Indications	Color	Status	Meaning
	Green	On	AC input active & main voltage is 44 to 57 V
		Off	AC input not active
		Blinking	Main voltage is under 46 or over 57V
Port Status Indications	Color	Status	Meaning
	Green	Off	Power is off or No-load is present
		On	Normal
		Blinking	Overload or short-circuit

Table 5 - PoE LEDs

5 Mounting and Cabling

This section describes the mounting procedures for the MiMAX-Pro, the PoE and the optional Surge Protector.

5.1 MiMAX-Pro



Caution: The MiMAX-Pro device is an outdoor radio unit and therefore, must only be mounted outdoors.



Caution: Mount the MiMAX-Pro in an orientation such that its 10/100Base T Ethernet port (located on the bottom) faces downwards. This prevents rain water from settling on the port, and thereby, avoiding damage to the unit such as corrosion and electrical short-circuiting.



Note: It is recommended to mount the MiMAX-Pro in an orientation with a corner facing down to position each antenna at a different angle, to obtain better signal coverage.

5.1.1 Mounting

The MiMAX-Pro offers two optional methods for outdoor mounting, either

- Wall mounting – in either orientation
- Pole Mounting – in either orientation

For either mounting method, the MiMAX-Pro provides mounting holes molded into its back panel for attaching the wall or pole-mounting brackets, as shown below:

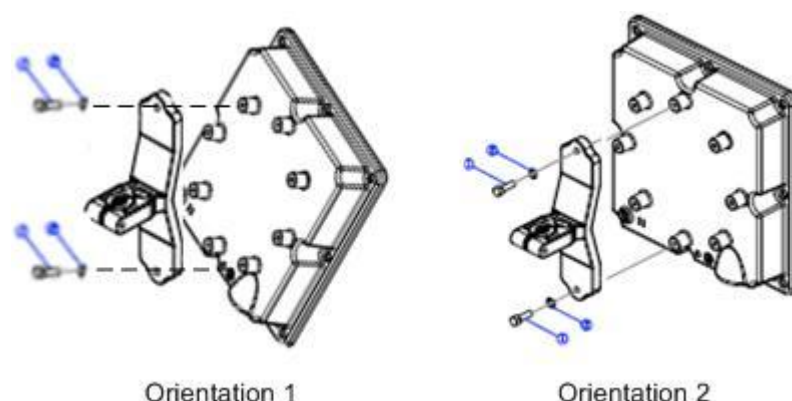


Figure 5 MiMAX-Pro - orientation

The MiMAX-Pro is mounted in the following steps:

1. Wall mounting - position the unassembled mounting bracket on the mounting surface (e.g. wall), and then use a pencil to mark the position of the two mounting holes.
Pole mounting - utilize the supplied pole-mounting bracket.
2. Attach the mounting bracket to the mounting holes located on the MiMAX-Pro's back panel mounting holes.

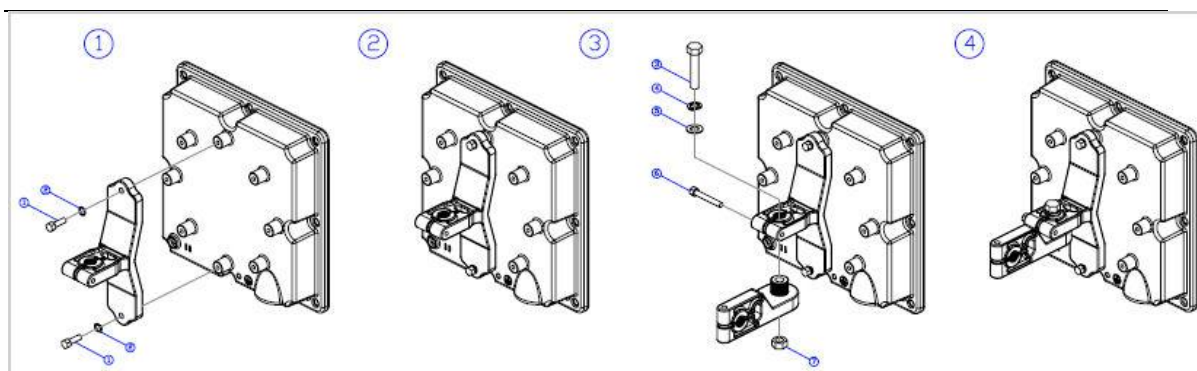


Figure 6 - bracket to mounting holes

3. Attaching the mounting bracket (now attached to the MiMAX-Pro) to the either the wall or to the pole. The mounting bracket allows the MiMAX-Pro to be easily adjusted in the horizontal (azimuth) and vertical (elevation) planes for antenna alignment, as displayed below:

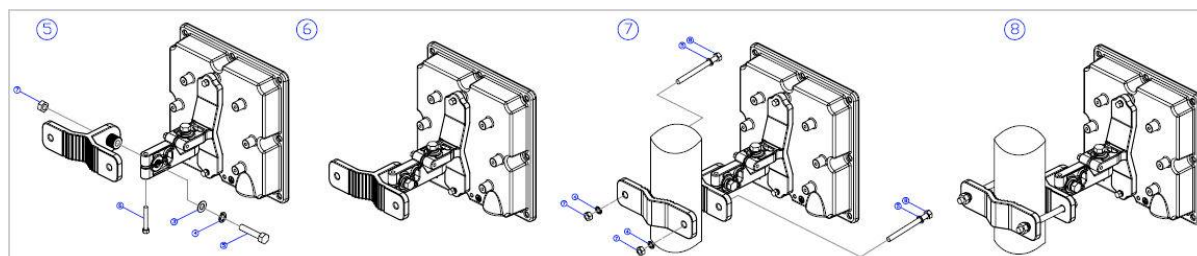


Figure 7 - mounting – pole

5.1.2 Cabling

To connect the MiMAX -> Surge Protector (if needed) -> PoE:

After properly mounting and grounding the encased MiMAX-Pro outdoor unit:

1. Strip the CAT-5e (recommended gauge = 24AWG) cable sheath to a length of approximately 7.7 mm.
2. Insert screw nut onto Cable Boot (supplied) housing and insert circular seal at the back end of the housing.
3. Insert the CAT-5e cable via the sealing nut through the housing.
4. Crimp the cable to the RJ-45 plug and insert the plug into the housing.
5. Secure the sealing nut on to the housing and stick the rubber gasket on the front end of the housing.
6. Connect and tighten to the 10/100BaseT Ethernet port located on the bottom panel of the CPE.



Note: It is important to provide strain relief and drip loop for CAT-5e cables. Create a drip loop and strain relief using cable tie, to tie cable to pole.

7. Connect CAT-5e cable Surge Protector (PIN-out defined below).
8. Connect CAT-5e cable from Surge Protector to PoE adapter (defined below).



Figure 8 - cable connection



Note: (U.S.A. – WCS market only) A Cavity filter is required for the 2.3 GHz variant (ordered separately).



Figure 9 - cable and Cavity filter connections

5.2 PoE Adapter

The Power over Ethernet adapter injects power into a standard Ethernet cable (e.g. standard CAT-5e), enabling power and data to run over a single cable. The PoE can be installed anywhere on the Ethernet cable run but is typically located near the corresponding data connection.

The PoE may be or wall/bench mounted using the rear side holes.



Note: Before mounting the PoE to a fixed location:

- Do not to cover the PoE or block the airflow to the PoE with any foreign objects. Keep the PoE away from excessive heat and humidity, and free from vibration and dust.
- Ensure that the cable length from the Ethernet network source to the terminal does not exceed 100 meters (333 Feet). The PoE is not a repeater and does not amplify the Ethernet data signal.

5.2.1 Cabling

To connect the Surge Protector (if needed) -> PoE:

1. Connect CAT-5e cable from Surge Protector to Data & Power (Out) port on PoE adapter.
2. Connect a straight through CAT-5e cable to Data (In) port from PoE to Ethernet connection on PC.
3. Plug the AC power chord into AC power socket and then into a standard electrical wall outlet (110/240 VAC, 60/50 Hz).

5.3 Surge Protector (Optional)

The optional third-party lightning and surge protector (Polyphaser) is implemented in the following deployment scenarios:

- ODU-to-IDU cable length of 40 meters or more (optional to use surge protector unless required by local law)
- Deployment of CPE in geographical areas that frequently experience severe lightning storms

The lightning and surge protector protects the ODU-to-IDU CAT-5e cable from any electrical surges due to lightning strikes.

The protector is installed outdoors on the CAT-5e cable that connects between the CPE and the PoE. In other words, two CAT-5e cables are required for the following connections:

- CPE-to-protector connection
- Protector-to-IDU connection

Mount and ground the Surge protector outdoors. The unit may be mounted/grounded on a nearby plate or bulkhead panel that is bonded to an earth-ground system.

5.3.1 Cabling



Caution: Do not install the lightning and surge protector during adverse weather conditions when the threat of lightning strike is possible.



Note: The protector unit must be grounded to a low-impedance (low R and low L) ground system to operate properly.



Note: For pricing and ordering of the Polyphaser lightning and surge protector, contact your Airspan representative.

To install the lightning protector:

1. Connect the protector in the direction according to the labels. The end labeled SURGE accepts the cable from the MiMAX-Pro; the end labeled PROTECTED accepts the cable from the PoE.
2. Feed the CAT-5e cable through the grommet (for each side). If the RJ-45 connector is already crimped to the other end, ensure that you have fed the cable through the gland nut beforehand. The gland nut secures the cable to the grommet.
3. Strip about 0.25" (6.35 mm) of the cable sheath and expose about 0.03" (0.8 mm) of the strands/wires.
4. Secure the wires to the protector's terminal block using the two spot ties. Each side of the data and DC assembly has + or – markings to ensure lines entering (surge side) match lines exiting (protected side).

Protected Pins	Function	Surge Pins
1 - 2	Data	pair #1
3 - 6	Data	pair #2
4 - 5	+48V	DC48 +/-
7 - 8	48V	DC48 +/-
Cable shield	Ground	GND or case

Table 6 - Surge protector - Pins

The figure below displays the MiMAX-Pro with optional Surge Suppressor:

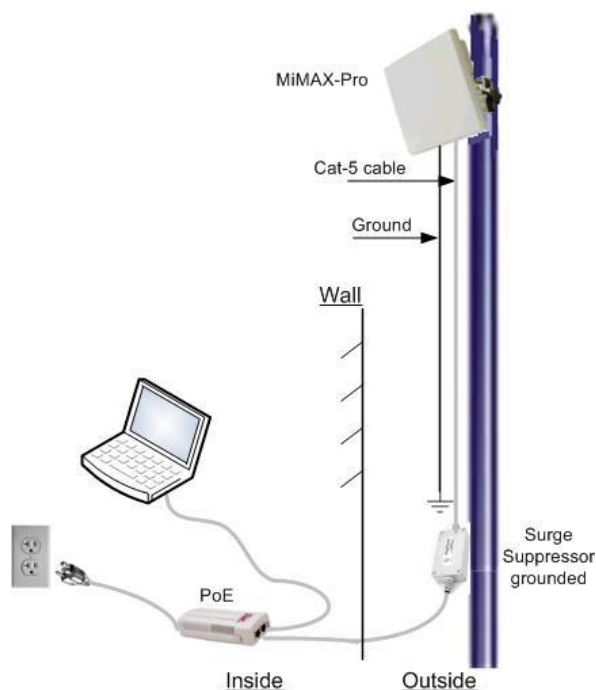


Figure 10 - with optional surge suppressor

5.3.2 Cabling – Cavity Filter

A Cavity filter is required for the 2.3 GHz variant for the USA market (WCS), the following demonstrates the connections.

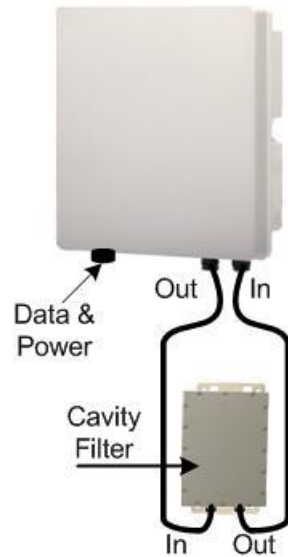


Figure 11 - Cavity Filter connections

6 Initial Procedure

This section discusses the following topics:

- [Browser Requirements](#)
- [Configure and Connect](#)
- [Accessing the MiMAX-Pro Web](#)
- [Navigating your Web Server](#)

6.1 Browser Requirements

Ensure that your Web browser with which you want to access the MiMAX-Pro is running Microsoft Internet Explorer 7, Firefox 2.0.0.6 and above.

This section describes the initial procedure for MiMAX-Pro operation and how to initially connect the CPE to the base station.

6.2 System Configuration and Login

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

The CPE enables a DHCP server by default. User computer can get IP address automatically from CPE. The CPE's DHCP server default login values are listed below:

- HTTP address:
 - 10.1.1.254 (subnet 255.255.255.0)
 - Gateway: 10.1.1.254
- User name: "admin"
- Password: "admin"



Note: The IP addresses shown in screen captures are for display purposes only.

6.3 Accessing the MiMAX-Pro

Proceed to login and connect to the MiMAX-Pro.

To access the MiMAX-Pro Web server:

1. Start your Web browser (e.g. Microsoft Internet Explorer).
2. In the **Address Bar** field, enter the IP address of the MiMAX-Pro (i.e. 10.1.1.254) subnet (255.255.255.0).



Note: To quickly enter the MiMAX-Pro server address, you can simply type the IP address without typing "http://". When you press <Enter> (see Step 3), the full address (i.e. "http://...") is automatically entered.

3. Press <Enter> on your keyboard.

The **Login** page of the MiMAX-Pro Web-based management opens, as displayed below:

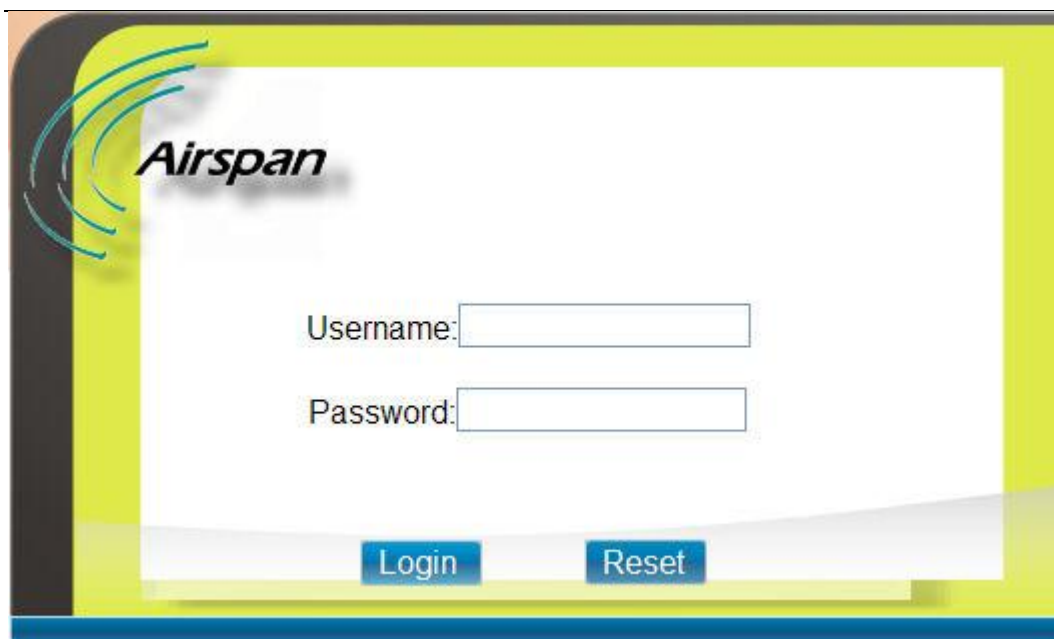


Figure 12 - Login page

4. In the **User Name** field, enter your user name, default = admin.
5. In the **Password** field, enter your password, default = admin.
6. Click **Login** to enter



Note: It is highly recommended to change your Password after initial login.



Note: The **User Name** and **Password** values are case-sensitive.

The MiMAX-Pro server home page opens, **Status**, displaying current information of the MiMAX-Pro System version and Network information, as displayed below.



Figure 13 - Home page - Status


6.4 Navigating your MiMAX-Pro Management

The MiMAX-Pro provides a user-friendly graphical user interface (GUI) that allows you to easily access commands for configuring MiMAX-Pro. The table below describes basic MiMAX-Pro navigation procedures.

6.4.1 Menus

The menu buttons at the top of the page provides links (menus) to various configuration categories. These menu buttons are displayed throughout the MiMAX-Pro management pages to allow easy navigation between categories.

The menus on the MiMAX-Pro management menu buttons are described in the table below:

Menu	Description
Status	<p>Opens the Status page where the following system status information (read-only) is displayed:</p> <p>WiMAX Status:</p> <ul style="list-style-type: none"> ➤ System Status ➤ Physical Status ➤ Uplink ➤ Downlink ➤ Service Flow <p>Network Status:</p> <ul style="list-style-type: none"> ➤ LAN ➤ WAN ➤ DHCP Client List <p>Device Status:</p> <ul style="list-style-type: none"> ➤ Device Information <hr/> <div style="display: flex; align-items: center;">  <p>Note: Click Refresh to manually refresh the page. Click Auto to enable auto refresh every 4 seconds (displayed in red when activated). To cancel auto refresh click Refresh.</p> </div> <hr/>
Personalization	<p>Opens the Personalization page where the Account information is defined:</p> <ul style="list-style-type: none"> ➤ Account Management ➤ Date configuration ➤ Language
WiMAX	<p>Opens the WiMAX page where the following information is displayed and defined:</p> <ul style="list-style-type: none"> ➤ Scanner ➤ Authentication Selection
Networking	<p>Opens the Networking page where – mode configurations are performed:</p> <ul style="list-style-type: none"> ➤ Bridge Mode configuration ➤ NAT Router Mode configuration ➤ Firewall configuration ➤ QinQ ➤ VLAN ➤ DHCP Server settings ➤ NAT ALG configuration ➤ Port Forwarding - NAT ➤ Port Trigger ➤ DDNS configuration

Menu	Description
Management	<p>Opens the Management page where - remote management specifications are enabled and defined:</p> <ul style="list-style-type: none"> ➤ TR-069 configuration ➤ SNMP (for internal use only) ➤ Buzzer ➤ Log display ➤ Upgrade ➤ Recovery
Logout	Logs out of the system
Reboot	Reboots the device

Table 7 - MiMAX-Pro Menu buttons

6.4.2 Navigating

The table below describes basic MiMAX-Pro management navigation procedures:

To ...	Do this ...
Navigate to a specific category	Click the relevant menu tab.
Quit the Web-based tool	Close the Web tool window.

Table 8 - Navigation



Note: The following displayed screens shots are for illustration purposes only.

7 Status

The **Status** page is where to view system status information (read-only) related to the CPE and its related parameters and connections.

To return to Status page at anytime click the Status button.

To access the Status page:

1. Click the **Status** button to navigate to the Status page.
2. Click the desired sub-option on the on the left side column.

7.1 WiMAX Status

To view WiMAX status related parameters on the Status page:

1. Click **WiMAX Status** on the left side column, as displayed below:

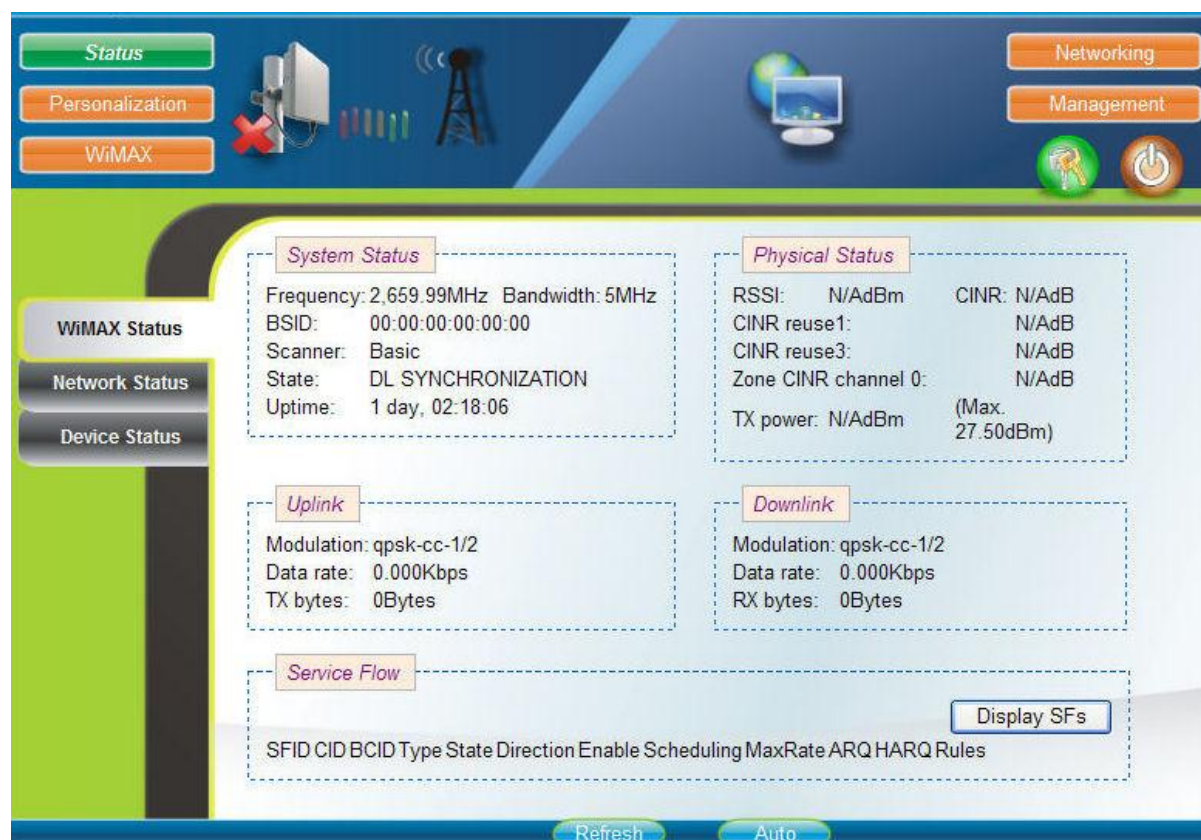


Figure 14 - WiMAX status

The parameters displayed (read only) on the WiMAX status page are described in the table below:

Parameter	Description
System Status	Displays System status information:
Frequency	Displays the current frequency being used. While scanning the frequency display will fluctuate until frequency is located.
Bandwidth	Displays the current bandwidth. When not connected to BS via radio link 00:00:00:00:00:00 is displayed.
BSID	Displays the Base Station ID
Scanner	Displays the

Parameter	Description
State	Displays the current state of the CPE.
Uptime	Displays the amount of time the system has been up and running.
Physical Status	Displays Physical status information:
RSSI	Displays the RSSI (Received Signal Strength Indicator) value.
CINR	Displays the CINR (Carrier to Interference Noise Ratio) value.
CINR reuse1	Displays the CINR (Carrier to Interference Noise Ratio) value for reuse1 zone.
CINR reuse3	Displays the CINR (Carrier to Interference Noise Ratio) value for reuse3 zone.
Zone CINR channel 0	Displays the CINR (Carrier to Interference Noise Ratio) value for zone channel 0.
TX power	Displays the current Tx power.
Uplink	Displays Uplink information:
Modulation	Displays the current uplink modulation.
Data rate	Displays the current uplink data rate.
TX bytes	Displays number of transmitted bytes.
Downlink	Displays Downlink information:
Modulation	Displays the current downlink modulation.
Data rate	Displays the current downlink data rate.
RX bytes	Displays number of received bytes.
Service Flow	Displays the service flow information.
Refresh (button)	Click to manually refresh this page.
Auto (button)	Click to enable auto refresh every 4 seconds (displayed in red when activated). To cancel auto refresh click Refresh .

Table 9 - WiMAX status

7.2 Network Status

To view Network status related parameters on the Status page:

1. Click the **Status** button to navigate to the Status page.
2. Click the **Network Status** on the left side column, as displayed below:

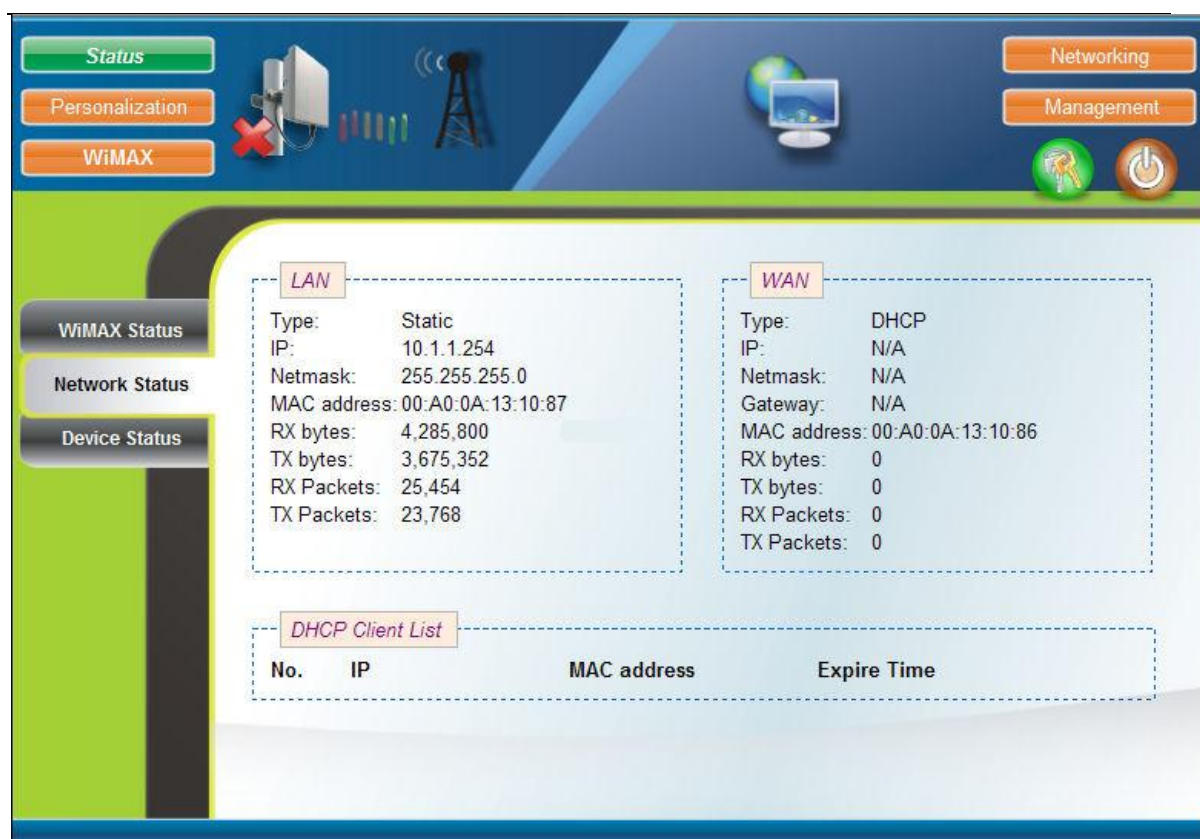


Figure 15 - Network status

The parameters displayed (read only) on the Network status page are described in the table below:

Parameter	Description
LAN	Displays current LAN status information:
Type	Displays the current network connection type.
IP	Displays the IP address assigned to the LAN port.
Netmask	Displays the subnet mask used that has been assigned to the device.
MAC address	Displays the MAC address of the LAN port's physical interface.
RX bytes	Displays number of received bytes.
TX bytes	Displays number of transmission bytes.
RX packets	Displays number of received packets.
TX packets	Displays number of transmission packets.
WAN	Displays the current WAN status information.
Type	Displays the current connection type, DHCP or Static
IP	Displays the IP address assigned by the WAN.
Netmask	Displays the subnet mask used that has been assigned to the device.

Parameter	Description
Gateway	Displays the IP address of the default gateway.
MAC address	Displays the .WAN MAC address assigned under DHCP.
RX bytes	Displays number of received bytes.
TX bytes	Displays number of transmission bytes.
RX packets	Displays number of received packets.
TX packets	Displays number of transmission packets.
DHCP Client List	Displays the current DHCP client list information.

Table 10 - Network status

7.3 Device Status

To view Device status related parameters on the Status page:

1. Click the **Status** button to navigate to the Status page.
2. Click **Device Status** on the left side column, as displayed below:

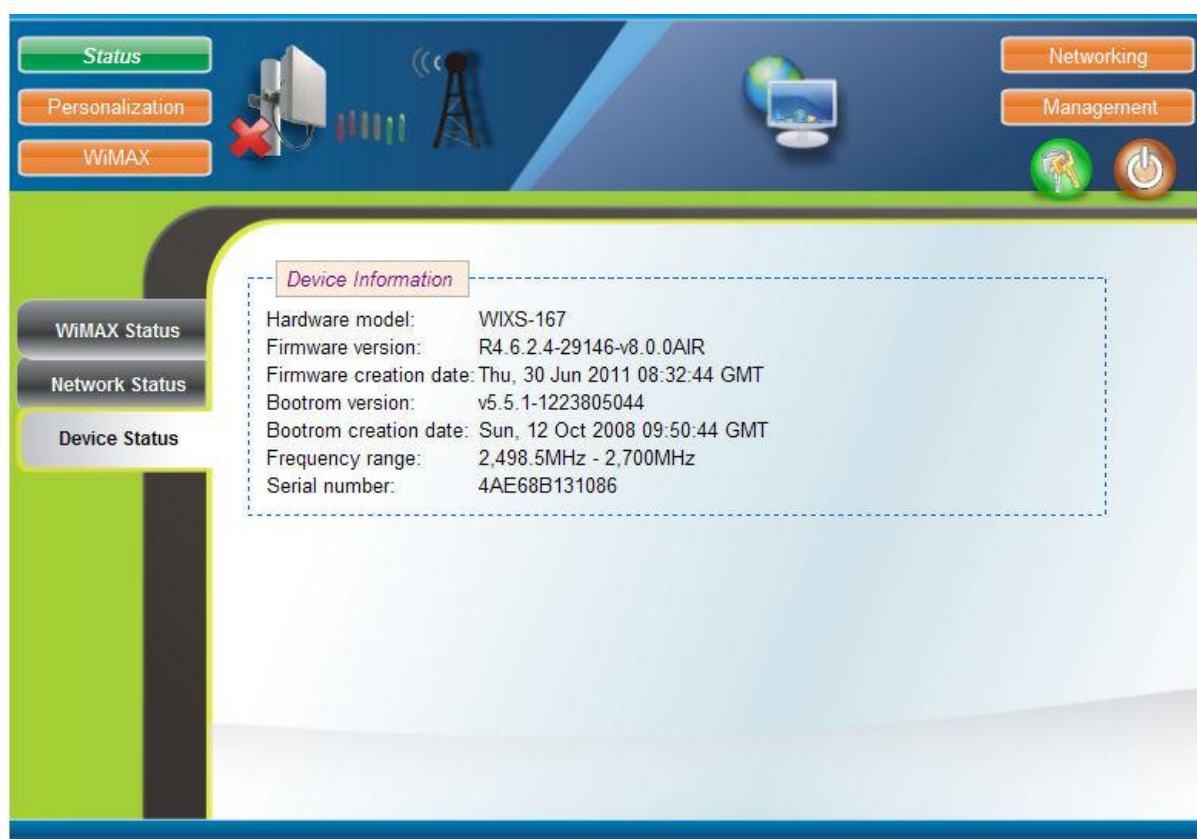


Figure 16 - Device status

The parameters displayed (read only) on the Device status page are described in the table below:

Parameter	Description
Device Information	Displays information on the device being used.
Hardware model	Displays the hardware model.
Firmware version	Displays the firmware version in use.
Firmware creation date	Displays the date the firmware was created.
Bootrom version	The bootrom version number.
Bootrom creation date	The bootrom creation date.
Frequency range	Displays the frequency range for the device.
Serial number	Displays serial number of the device.

Table 11 - Device status

8 Personalization

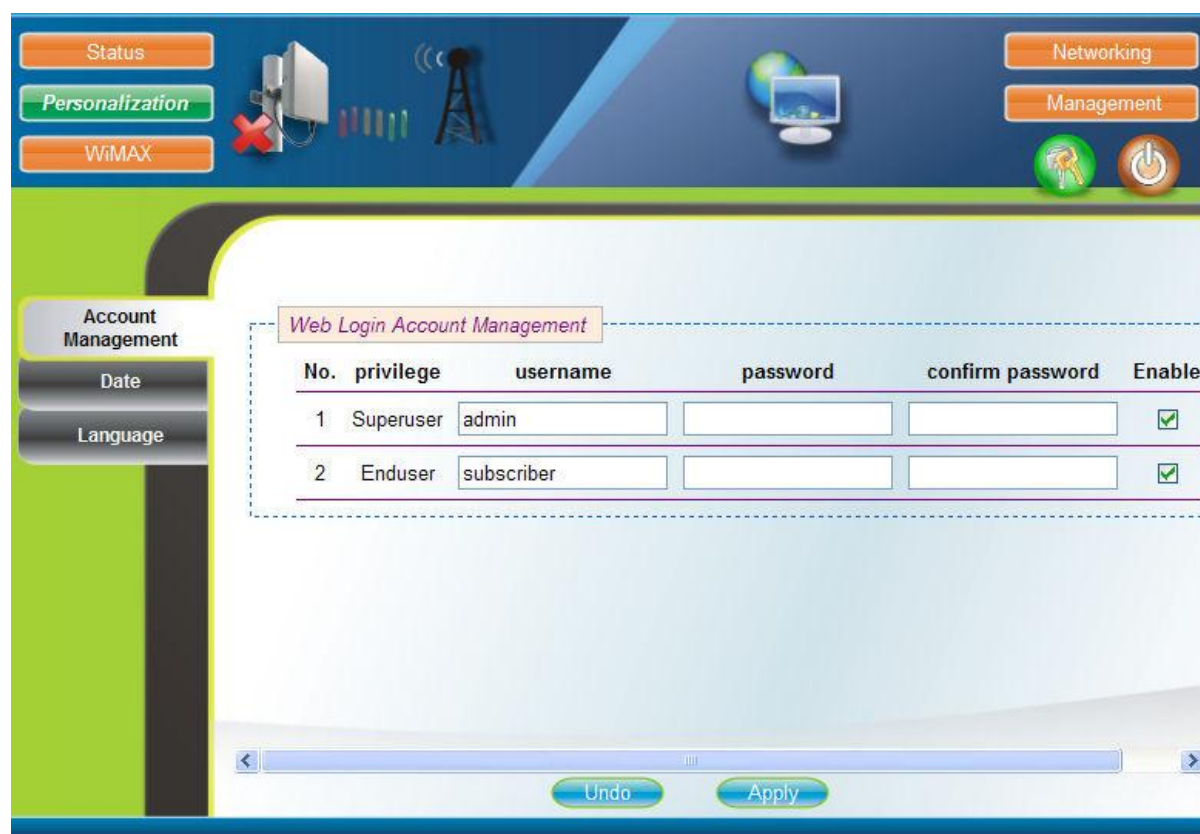
The Personalization page is where changes to account name and password are performed and where to configure date and time synchronization.

To access the Personalization page:

1. Click the **Personalization** button to navigate to the Personalization page.
2. Click the desired sub-option on the on the left side column.

8.1 Account Management

The Account Management page displays Account login parameters such as changing the username and password, as displayed below:



No.	privilege	username	password	confirm password	Enable
1	Superuser	admin			<input checked="" type="checkbox"/>
2	Enduser	subscriber			<input checked="" type="checkbox"/>

Figure 17 - Personalization – Account

8.1.1 Web Login Account Management

The following is valid for both Superuser (Administrator) and Enduser (subscriber). When logging in using Enduser, Administration is not displayed.

To change Account name & Password:

1. Click **Account Management** on the left side column.
2. Enter the **username** (admin = default) – for access to CPE - String
 - Modify the **username** – for subsequent access to CPE - String
3. Enter the current **password** (admin = default) – for access to CPE – String
 - Enter new **password** – for subsequent access to CPE - String
4. Re-enter **password** to confirm
5. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.



Note: Supports Multi-user login. To add additional users repeat steps 1-7.

6. After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

8.2 Date

The Date page is used to configure date and time synchronization, with available devices. In order for the CPE to pass the authentication from the base station the system date should be within the valid duration of the uploaded certificate file.

The Date page displays date and time synchronization parameters, as displayed below:

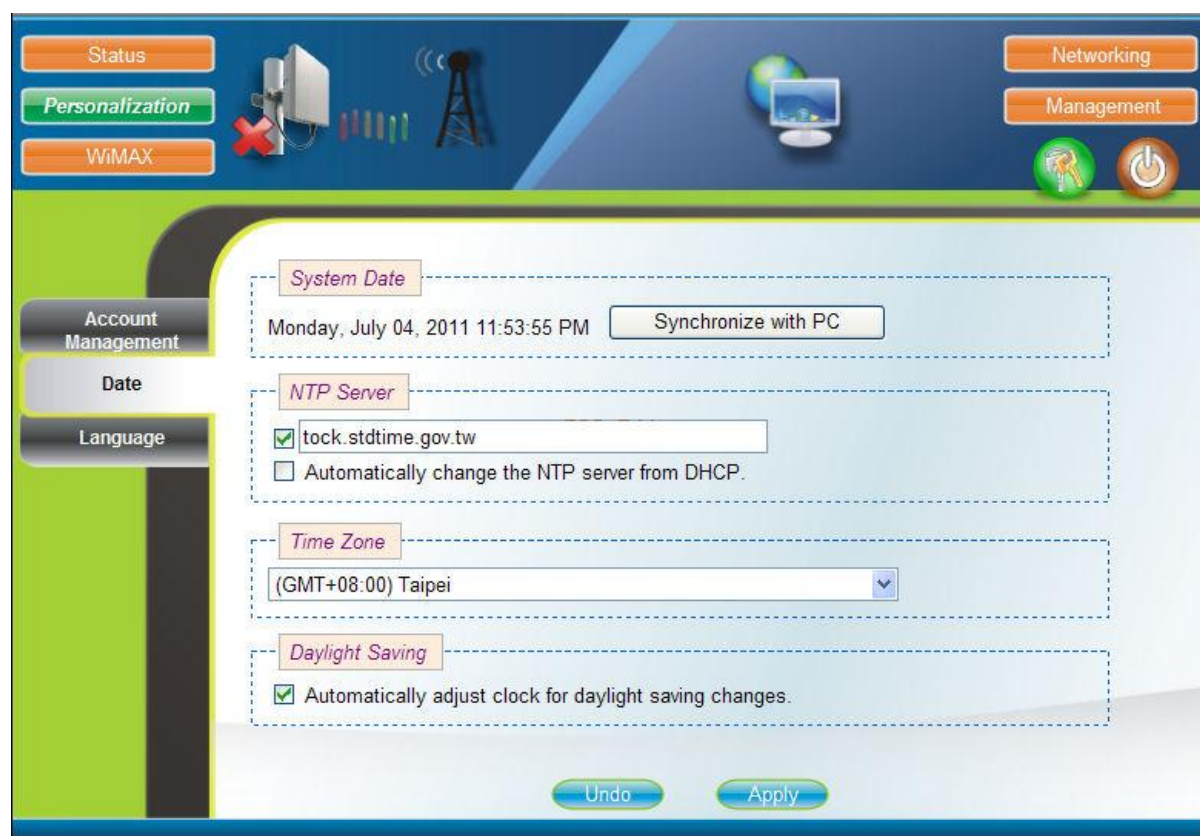


Figure 18 - Personalization – date

To configure Date and Time synchronization:

1. Click **Date** on the left side column.
2. Click **Synchronize with PC** (System Date) to synchronize the system date of a CPE with the PC that is connected to the LAN side.



Note: If the system date is not within the valid duration of the uploaded certificate file, the CPE will not pass the authentication from the base station.

3. Check and enter NTP URL manually.
Or
Check **Automatically change the NTP server from DHCP** to update the system date of the CPE automatically by synchronizing time with an NTP server.
4. Select the specific **Time Zone** required.
5. Check **Automatically adjust clock for daylight savings changes** to adjust automatically for daylight savings time.

6. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.
7. After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

The parameters displayed on the Date page are described in the table below:

Parameter	Description
System Date	To synchronize the system date of a CPE with the PC that is connected to the LAN side click Synchronize with PC button.
NTP Server	Update the system date of the CPE by synchronizing time with an NTP server either manually or automatically from the DHCP server.
Time Zone	The required time zone.
Daylight Savings	Whether or not to adjust clock for daylight savings time.

Table 12 - Personalization - date

8.3 Language

The Language page allows users to select one of the available languages from the drop-down list. After selecting the desired language, press the “Apply” button to view the WEB-GUI in the selected language.

The Language page displays the available languages, as displayed below:

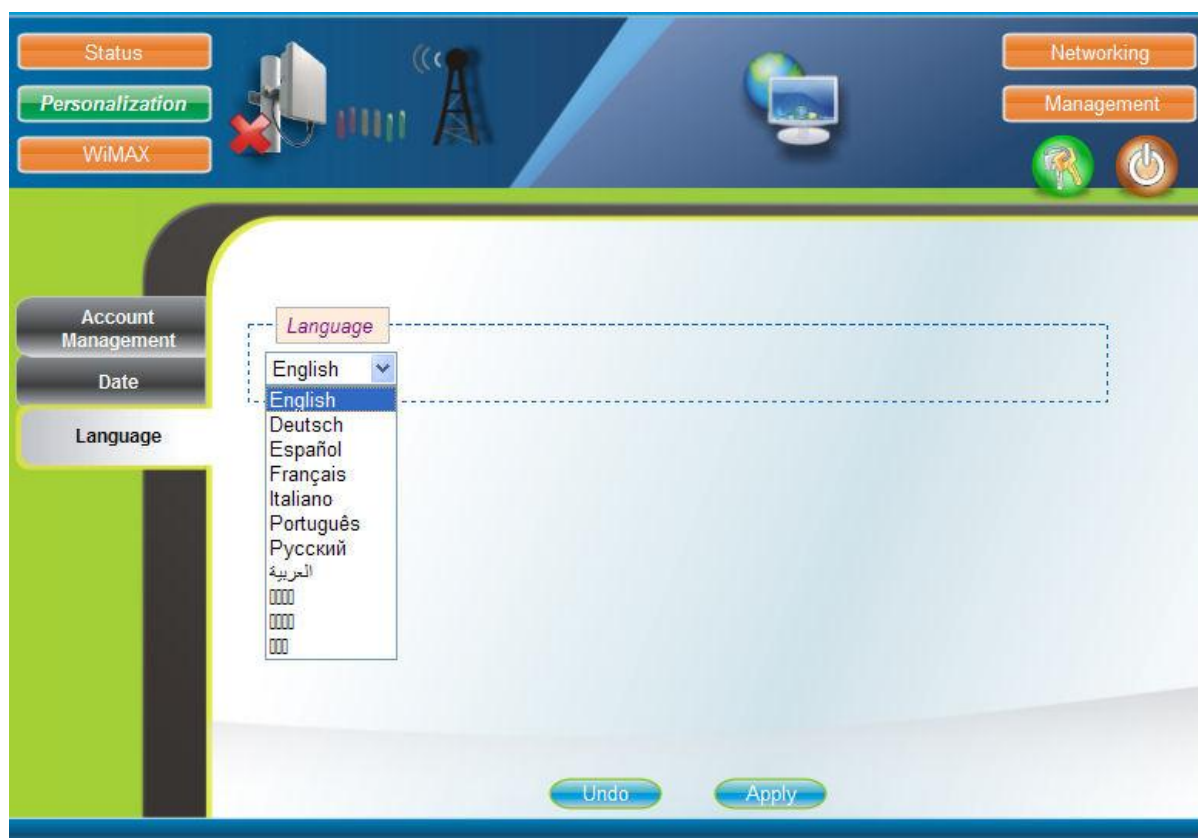


Figure 19 - Personal – Language

To configure the required language:

1. Click **Language** on the left side column.
2. Select the required language from the drop-down list.



-
3. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.
 4. After changes, reboot the system in order for the selected language to take effect, see [Reboot](#).

9 WiMAX

The WiMAX page is used to stop or start WiMAX scanning for a connection with a base station and enables you to add, delete and edit channels that device found during initial scanning.

To access the WiMAX page:

1. Click the **WiMAX** button to navigate to the WiMAX page.
2. Click the desired sub-option on the on the left side column.

9.1 Scanner



Note: Can only be accessed with Administrator privileges.

The Scanner page allows users to stop or start WiMAX connection with a BS, as displayed below:

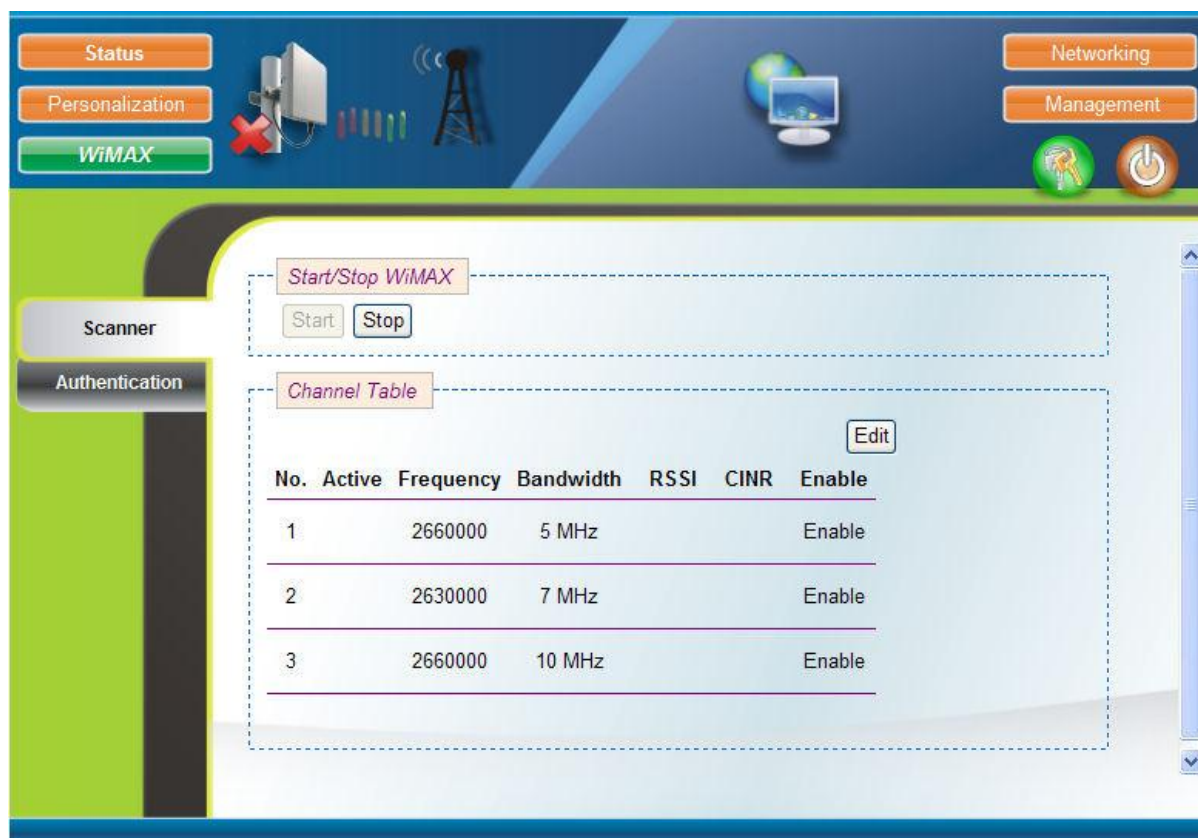


Figure 20 - WiMAX – scanner

9.1.1 Start/Stop WiMAX

To Start/Stop WiMAX:

1. Click **Scanner** on the left side column.
2. Click **Start** to start the WiMAX connection.
3. Click **Stop** to stop the WiMAX connection.



Note: When Bandwidth range is modified there is no need to reboot the system, just restart the system by using the “start” button in the “Start/Stop WiMAX” section.

9.1.2 Channel Table

The Channel Table setting page lists all the channels that are stored in the channel table along with channel status associated to the channel currently used to connect the CPE to a BS. Here one can add, remove, and edit channels in the channel table.

To add new Channel:

1. Click **Edit** the table expands as displayed below:



Figure 21 - WiMAX - Scanner - Channel table


2. **Active** - will display a check mark when the channel is active. This channel is used for the current wireless connection.
3. Enter the **Frequency** - the channel frequency in KHz.
4. Select the **Bandwidth** - the channel bandwidth from the available list. Channel bandwidth - values are: 3MHz 3.5MHz 4.375MHz 5MHz 6MHz 7MHz 8.75MHz 10MHz.



Note: Not all channel bandwidths fully supported. Please refer to latest Release note for current support.

5. Displays **RSSI** when functional.
 6. Displays **CINR** when functional.
 7. Check **Enable** - to enable scanning on this channel
 8. Click **Insert** to add an additional channel
 9. Click **Undo** to discard any changes.
- Or
Click **Apply** to save the changes.



Note: When the CPE is connected, a green check  will appear in the "Active" column of the linked frequency in the "Channel Table" section as well as beside the small CPE icon on the top banner; when not connected, a red x will appear beside the small CPE icon on the top banner.

To delete Channel:

1. Click **Delete** to remove a channel from the list.

After Bandwidth range changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

9.2 Authentication



Note: Can only be accessed with administrator privileges.

The Authentication settings page of the MiMAX-Pro management allows you to enable and define a method of authentication, mechanism and manage the certificates of the unit.



Note: Selecting either; EAP-TLS, EAP-TTLS or None will display different parameters, as shown below.

Additionally you can select one of five key encoding methods listed in “Phase 2”. Identity, username, and password should be entered with respect to the BS, if authentication is required. Upload the required certificates for authentication.



Note: PEM (Privacy Enhanced Mail, Base64 encoded DER certificate) is the only certificate format supported. Please confirm the format before uploading the certification.

To set Authentication:

1. Click **Authentication** on the left side column, as displayed below:

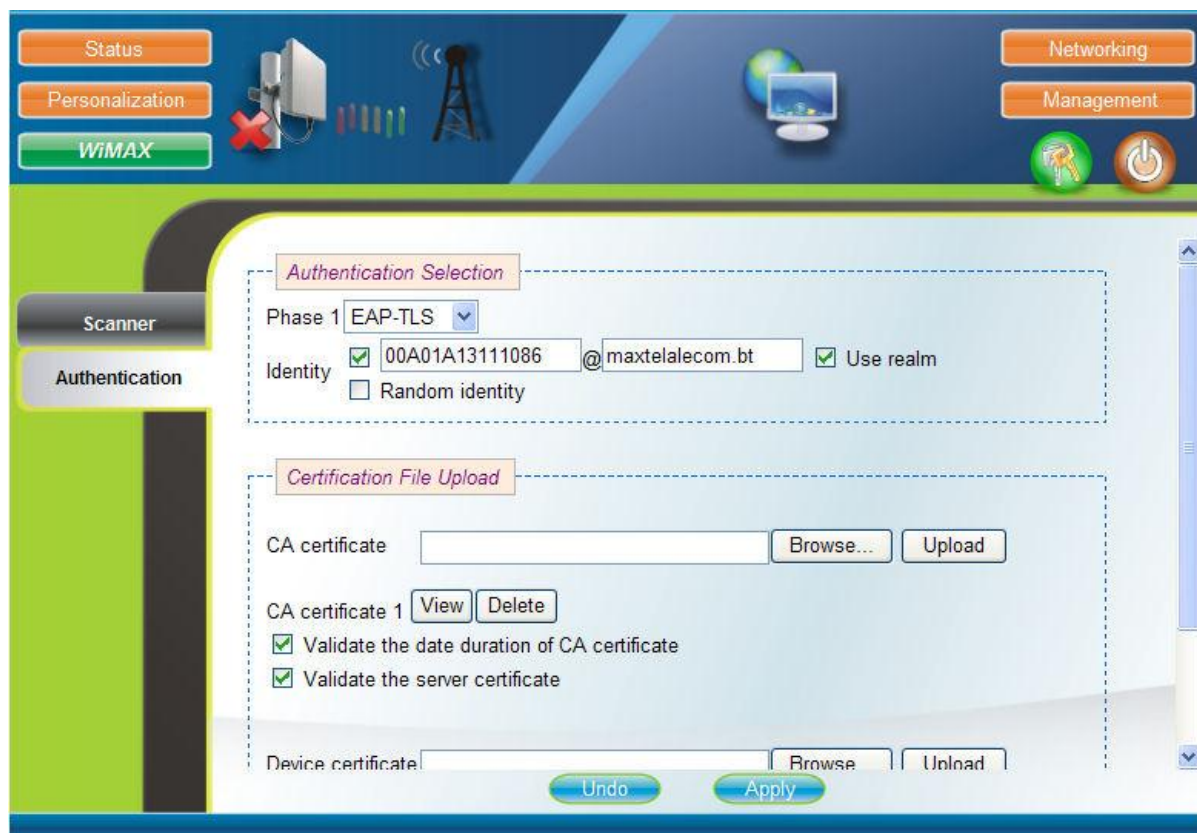
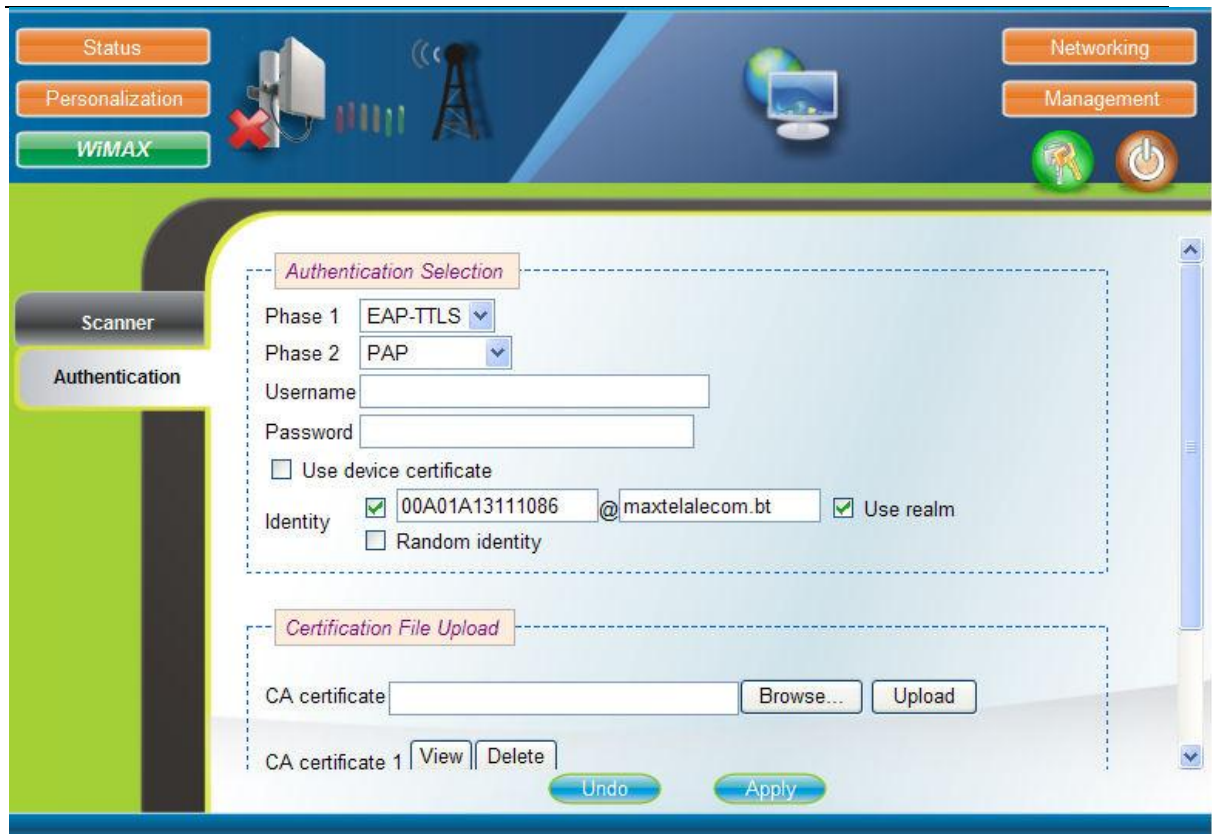


Figure 22 - WiMAX – Authentication

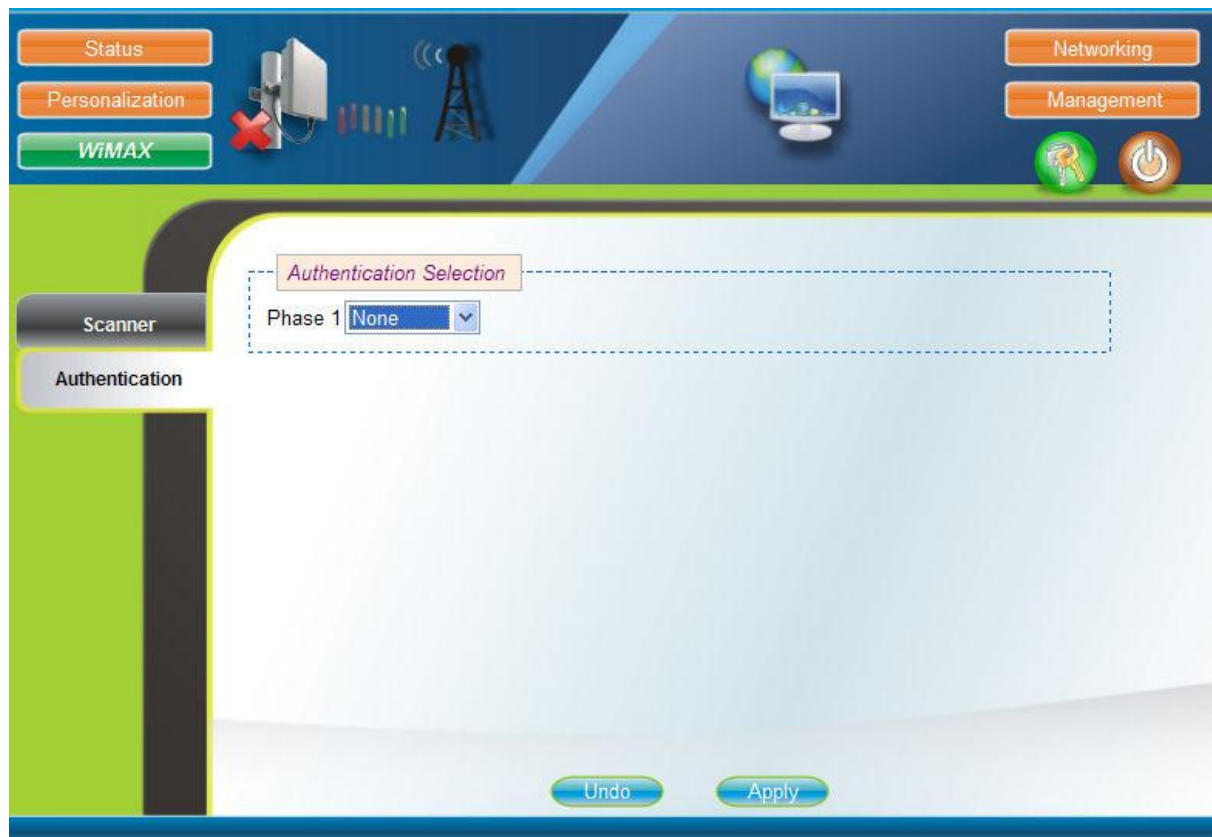


The screenshot shows the 'Authentication' configuration page in the MiMAX-Pro V-Series user interface. The page has a top navigation bar with buttons for 'Status', 'Personalization', 'WiMAX', 'Networking', and 'Management'. A left sidebar contains 'Scanner' and 'Authentication' tabs. The main content area is titled 'Authentication Selection' and includes the following fields and options:

- Phase 1:** A dropdown menu set to 'EAP-TTLS'.
- Phase 2:** A dropdown menu set to 'PAP'.
- Username:** A text input field.
- Password:** A text input field.
- Use device certificate:** An unchecked checkbox.
- Identity:** A section containing:
 - ☒ **00A01A13111086** @maxtelalecom.bt
 - ☐ **Random identity**
- Use realm:** A checked checkbox.

Below the 'Authentication Selection' section is a 'Certification File Upload' section with a 'CA certificate' text input, 'Browse...' and 'Upload' buttons, and a 'CA certificate 1' section with 'View' and 'Delete' buttons. At the bottom of the main content area are 'Undo' and 'Apply' buttons.

Figure 23 - WiMAX – Authentication – TTLS



The screenshot shows the 'Authentication' configuration page in the MiMAX-Pro V-Series user interface, but with 'Phase 1' set to 'None'. The layout is identical to Figure 23, but the 'Phase 1' dropdown menu is now set to 'None'. The 'Phase 2' dropdown menu is not visible. The 'Authentication Selection' section only contains the 'Phase 1' dropdown. The 'Certification File Upload' section and the 'Undo' and 'Apply' buttons are still present at the bottom.

Figure 24 - WiMAX – Authentication – none

9.2.1 Authentication Selection

To select type of Authentication:

1. Define **Phase 1** – select either of the supported methods, None, EAP-TTLS or EAP-TLS.
2. Define the **Identity** - the WiMAX system identity



Note: Selecting either; EAP-TLS, EAP-TTLS or none will display different parameters, as shown above.

3. Define **Phase 2** - select one of the available key encoding methods listed, either, PAP, CHAP, MSCHAP, MSCHAPv2 or MD5.
4. Define the **Username**
5. Define the **Password**
6. Check to **Use device certificate**.
7. **Identity** can be either:
 - generated randomly
 - or
 - manually defined

9.2.2 Certificate File Upload



The Certification File Upload section enables uploading the CA certification files for the CPE.

To upload CA Certification Files:

1. Click **Browse** to choose the appropriate configuration file to upload.
2. Click **Upload** to upload the file to the CPE.
3. Click **View** to view the CA certificate (either 1 or 2)>
4. Click **Delete** to remove the CA certificate (either 1 or 2).
5. Check to **Validate the date duration** of the CA certificate.
6. Check to **Validate the server certificate**.
7. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

The parameters displayed on the Authentication page are described in the table below:

Parameter	Description
Authentication Selection – select supported methods either:	
	Phase 1 – either: <ul style="list-style-type: none"> ➤ None - No authentication <hr/> <div>  Note: When “none” is selected the following fields are not displayed. </div> <hr/> <ul style="list-style-type: none"> ➤ EAP-TLS - Extensible Authentication Protocol - Transport Layer Security. ➤ EAP-TTLS - Extensible Authentication Protocol -Tunneled Transport Layer Security. <hr/> <div>  Note: When “EAP-TLS” is selected fields are not displayed. </div> <hr/>

Parameter	Description
	Phase 2 – either: <ul style="list-style-type: none"> ➤ PAP ➤ CHAP ➤ MSCHAP ➤ MSCHAPV2 ➤ MD5
	Identity - WIMAX system identity
	Username – define username
	Password – define password
	User device certificate - to verify the authenticity
	Certification File Upload – to upload the certification files
	CA certificate - to verify the authenticity
	Validate the date duration - of the CA certificate.
	Validate the server certificate

Table 13 - WiMAX - Authentication



Note: The only certificate format supported is PEM (Privacy Enhanced Mail, Base64 encoded DER certificate).



Note: If the system date is not within the valid duration of the uploaded certificate file, the CPE will not pass the authentication from the base station. See [Personalization > Date](#) to set the system date.

10 Networking

The **Networking** page of the MiMAX-Pro management enables you to configure Bridge mode or NAT mode.

To access the Networking page:

1. Click the **Networking** button to navigate to the Networking page.
2. Click the desired sub-option on the on the left side column.

10.1 Bridge/NAT Mode Configuration

To access the Bridge/NAT Mode page:

1. Click **Bridge/NAT Mode** on the left side column, as displayed below:



Figure 25 - Networking - Bridge mode

10.1.1 Bridge Mode

To configure the Bridge Mode page:

1. Select **Bridge Mode** –to enable Bridge mode.
2. Select **WAN IP Type** (of the unit) - select **Static** to manually assign the IP address and subnet mask or **DHCP** to automatically assign the IP address and Subnet mask by the DHCP server.
3. **WAN IP address** – manually assign when in Static mode.
4. **WAN Netmask** - manually assign when in Static mode.
5. **WAN Gateway** – manually assign when in Static mode.
6. **Primary DNS** – the primary DNS
7. **Secondary DNS** – the secondary DNS
8. **LAN IP Address** – the LAN IP address of this device.
9. **LAN Netmask** – the LAN subnet mask address.

10. Click **Undo** to discard any changes.

Or

Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

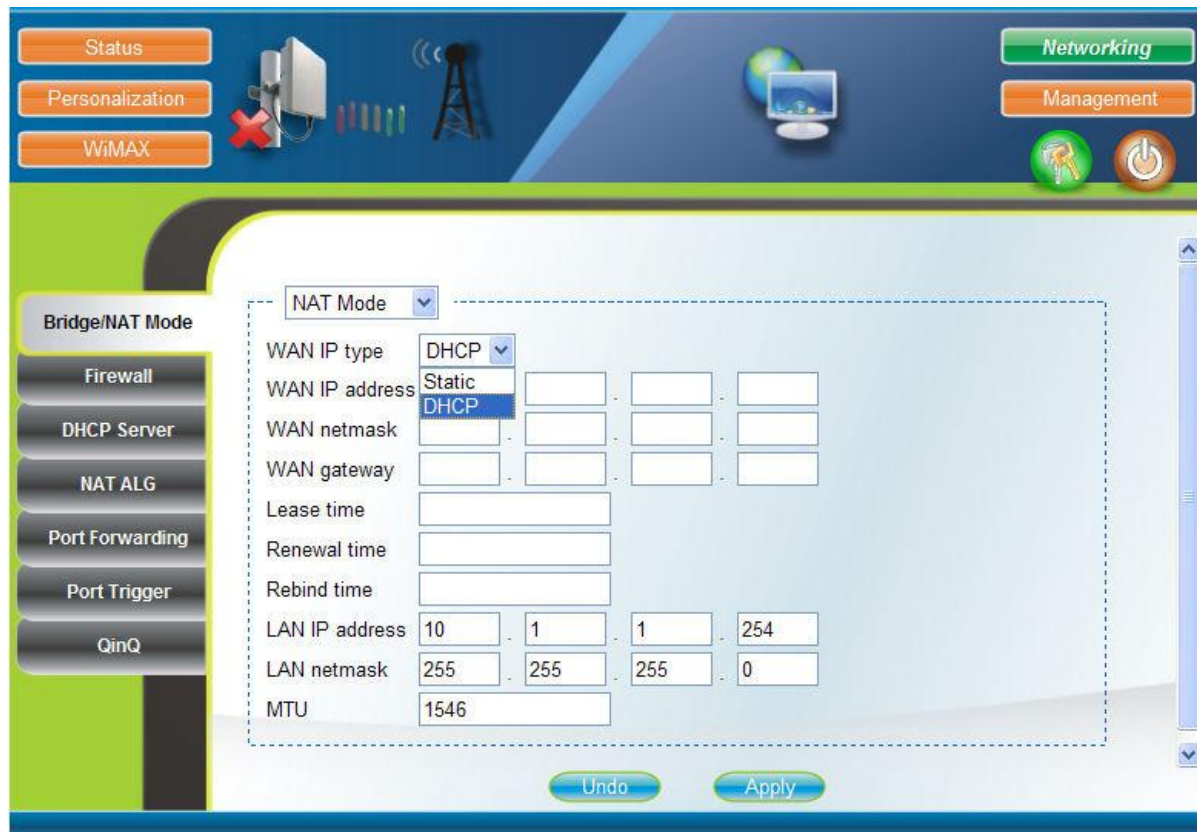


Figure 26 - Networking - NAT mode

10.1.2 NAT Mode

To configure the NAT Router Mode page:

2. Select **NAT Mode** - to enable NAT (Network Address Translation) mode
2. Select the **WAN IP type** - select **Static** to manually assign the WAN IP address and WAN subnet mask and WAN gateway or **DHCP** to automatically assign the WAN IP address and WAN Subnet mask and WAN gateway.
3. **WAN IP address** - WAN IP address.
4. **WAN netmask** - the WAN subnet mask, for example: 255.255.255.0.
5. **WAN gateway** - the gateway IP address in the WAN.
6. **Lease time** – the length of time that the DHCP server reserves IP addresses before recycling them.
7. **Renewal time** – the length of time till the lease time expires, that the client will attempt to *renew* the lease so it can keep using its IP address
8. **Rebind time** – amount of time the client will try to *rebind* to any active DHCP server if renewal fails.
9. **LAN IP address** - the LAN IP address of this device.
10. **LAN netmask** - the LAN subnet mask address.
11. **MTU** – the Maximum Transmission Unit, [68 -> 1500] default = 1476.

12. Click **Undo** to discard any changes.

Or

Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

10.2 Firewall



Note: Can only be accessed with Administrator privileges.

The Firewall page gives users the ability to allow or deny web/telnet access from WAN.

To configure Firewall settings:

1. Click **Firewall** on the left side column, as displayed below:

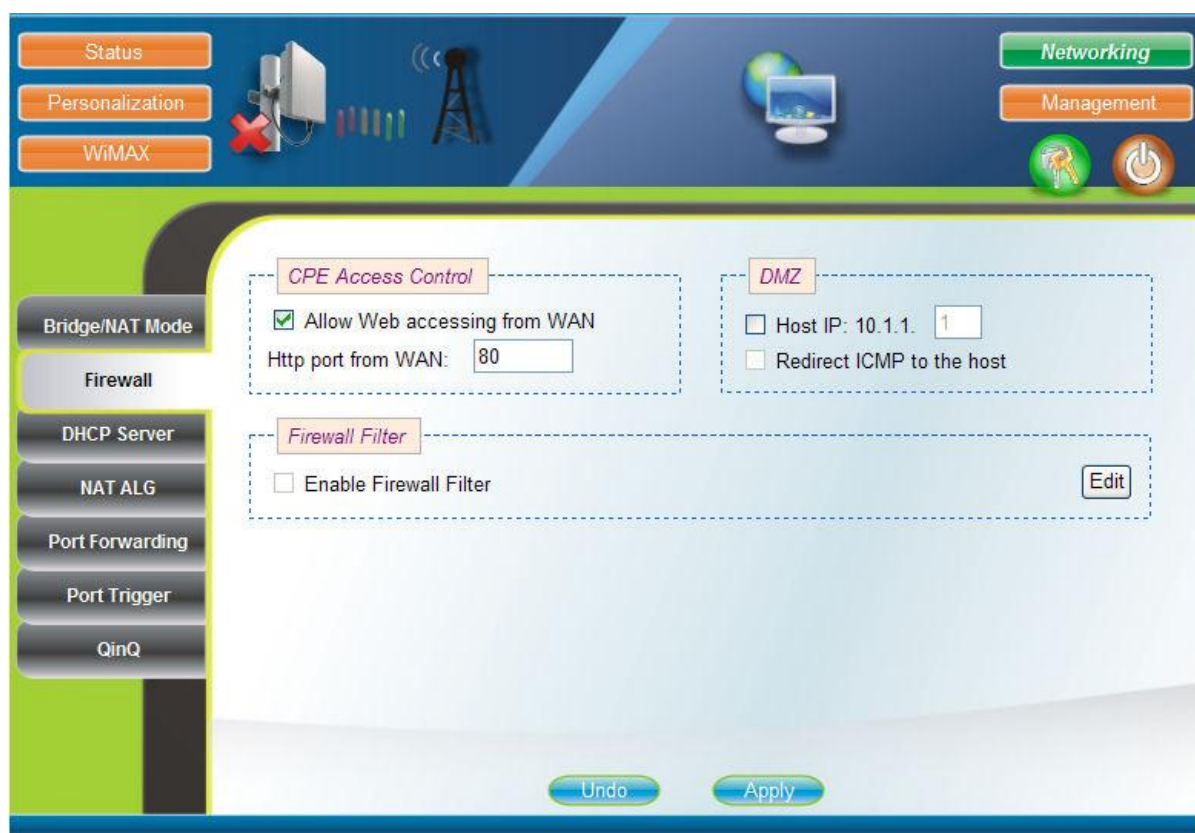


Figure 27 - Firewall settings

10.2.1 CPE Access Control

To enable CPE access:

1. Check **Allow WEB accessing from WAN** - to allow or deny WEB access from WAN.

10.2.2 DMZ access

To enable DMZ access:

1. Check **Host IP** & define IP address – to only allow access to the DMZ host, not to the entire private network at the CPE's back end.
2. Check **Redirect ICMP to the host** – to enable the redirection of ICMP.

10.2.3 Firewall Filter

To enable a Firewall Filter

1. Click **Edit** – to access Firewall Filter configuration.

2. Check **Enable Firewall Filter** – to filter incoming network traffic based on MAC, IP, protocol, TCP/UDP port and interface, as displayed below:



Figure 28 - Firewall Filter – settings

3. Define parameters as described in the table below:

Parameter	Description
Name	Define the device name
Action	Select either to Allow or Deny access
Interface	Select either Ethernet or WiMAX
Protocol	Select either: any, TCP, UDP or ICMP
Priority	Select : Hi, 2-9, Lo
Enable	Check to enable the filter
Src MAC	Define the source MAC address
Src IP	Define the source IP address
Src Port	Define the source port address
Dst MAC	Define the destination MAC address
Dst IP	Define the destination IP address
Dst Port	Define the destination port address

Table 14 - Firewall Filter

4. Click **Delete** - to remove from the list
5. Click **Insert** – to add another filter

6. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

10.3 DHCP Server

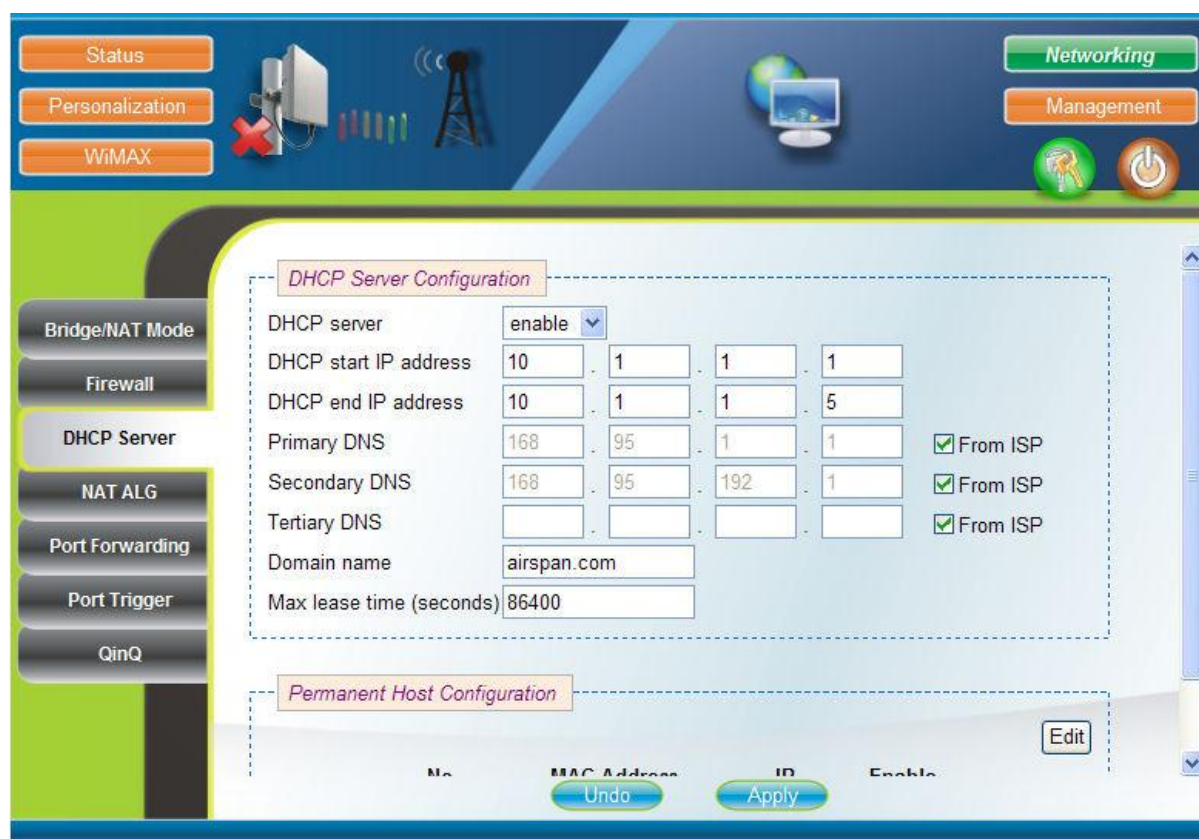
If **enabled** the DHCP server automatically starts when the CPE is powered on, and displays the current configuration.



Note: DHCP Server is only applicable when CPE is in NAT mode.

To access the DHCP Server configuration page:

1. Click **DHCP Server** on the left side column, as displayed below:



DHCP Server Configuration

DHCP server	enable				
DHCP start IP address	10	1	1	1	
DHCP end IP address	10	1	1	5	
Primary DNS	168	95	1	1	<input checked="" type="checkbox"/> From ISP
Secondary DNS	168	95	192	1	<input checked="" type="checkbox"/> From ISP
Tertiary DNS					<input checked="" type="checkbox"/> From ISP
Domain name	airspan.com				
Max lease time (seconds)	86400				

Permanent Host Configuration

No	MAC Address	IP	Enable

Undo Apply Edit

Figure 29 - Networking - DHCP Server

10.3.1 DHCP Server Configuration

To configure the DHCP Server Configuration page:

1. Select whether to enable the **DHCP server**, either: **enable** – default, or **disable**.

The following parameters are only available when DHCP server is enabled.

2. Define the **DHCP start IP address**.
3. Define the **DHCP end IP address**.
4. Enter the **Primary DNS** IP address. Check if to get **From ISP**.
5. Enter **Secondary DNS** IP address. Check if to get **From ISP**.
6. Enter **Tertiary DNS** IP address. Check if to get **From ISP**.
7. Enter **Domain name** of the local network.

8. Enter **Max lease time** - the maximum time for the IP lease, in seconds. [1 – 99999999]
9. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.

10.3.2 Permanent Host Configuration

Specific IP address can be assigned to a specific MAC address.

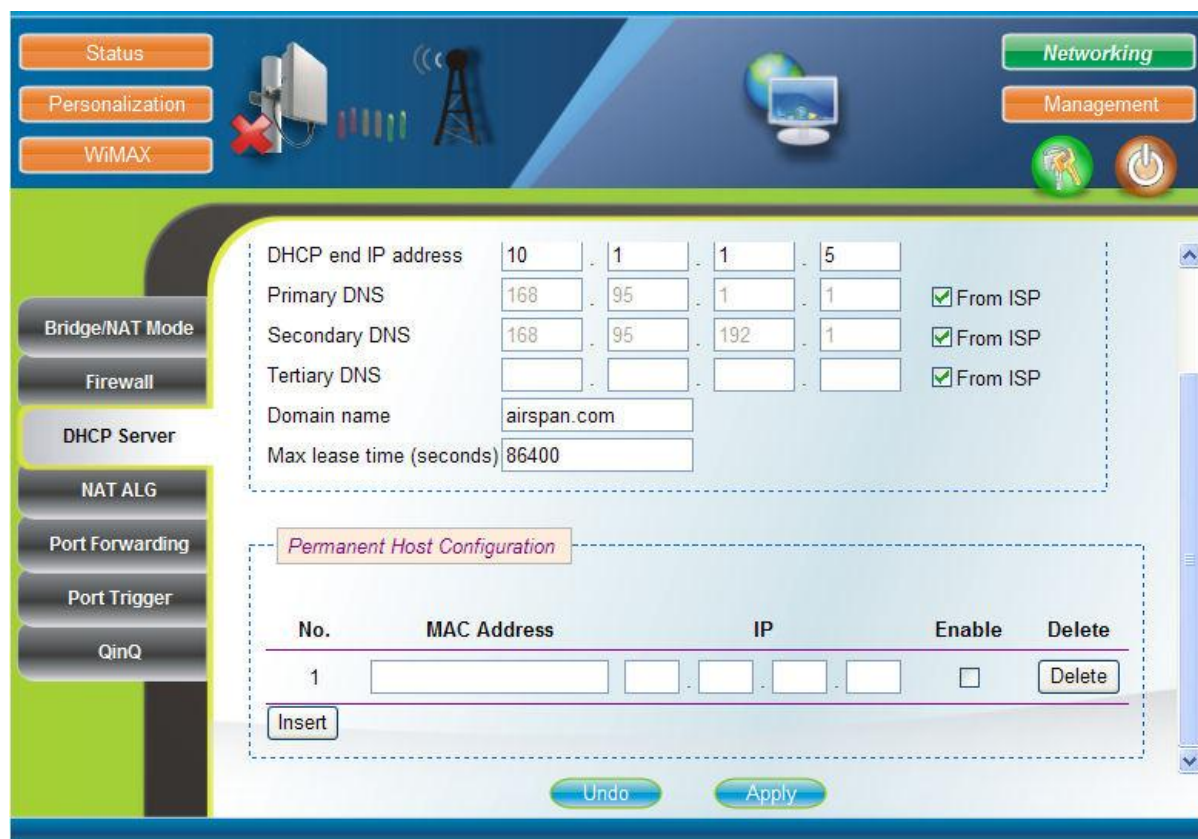


Figure 30 - Networking - DHCP Server - Permanent Host Configuration

To assign a specific MAC address:

1. Click **Edit** – to access Permanent Host Configuration.
2. Define **MAC address**.
3. Define **IP** address.
4. Check **Enable** – to assign specific IP address to a specific MAC address.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

10.4 NAT ALG

The NAT ALG page enables users to can enable or disable BSID authorization of FTP ALG, PPTP ALG, H323 ALG, SIP ALG, RTSP ALG, and IPsec ALG.



Note: NAT ALG is only applicable when CPE is in NAT mode.

To enable ALG:

1. Click **NAT ALG** on the left side column, as displayed below:



Figure 31 - Networking - NAT ALG

2. Check **Enable** – to enable BSID Authorization of FTP ALG, PPTP ALG, H323 ALG, SIP ALG, RTSP ALG, and IPsec ALG. The BSID can be used in SIP authentication to decide if the ATA is within the service area.
3. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

10.5 Port Forwarding

The Port Forwarding page enables users to add, remove, edit, enable, and disable port forwarding. Port forwarding redirects incoming network traffic from pre-defined a WAN Port range to pre-defined LAN IP Address and LAN Port range.



Note: Port Forwarding is only applicable when CPE is in NAT mode.

To access the Port Forwarding configuration page:

1. Click **Port Forwarding** on the left side column, as displayed below:



No.	WAN Port		LAN IP Address	LAN Port		Protocol	Enable	Delete
	Begin	End		Begin	End			
1	[]	[]	10.1.1.[]	[]	[]	TCP	<input type="checkbox"/>	[Delete]
2	[]	[]	10.1.1.[]	[]	[]	TCP	<input type="checkbox"/>	[Delete]

[Insert]

[Undo] [Apply]

Figure 32 - Networking - Port Forwarding

2. Click **Edit** – to access Port Forwarding configuration.
3. Click **Insert** to add additional port.
4. Define the WAN Port to **Begin** at and port to **End** at.
5. Define the **LAN IP Address**.
6. Define the LAN Port to **Begin** at and port to **End** at.
7. Select the **Protocol** – define the protocol to be used, either: TCP, UDP or TCP/UDP.
8. **Enable** the setting – check to enable the setting.
9. Click **Delete** - to remove from the list
10. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

10.6 Port Trigger

The Port trigger page 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. The Port trigger page enables users to add, remove, edit, enable, and disable port trigger mappings.



Note: Port Trigger is only applicable when CPE is in NAT mode.

To access the Port Trigger page:

1. Click **Port Trigger** on the left side column, as displayed below:

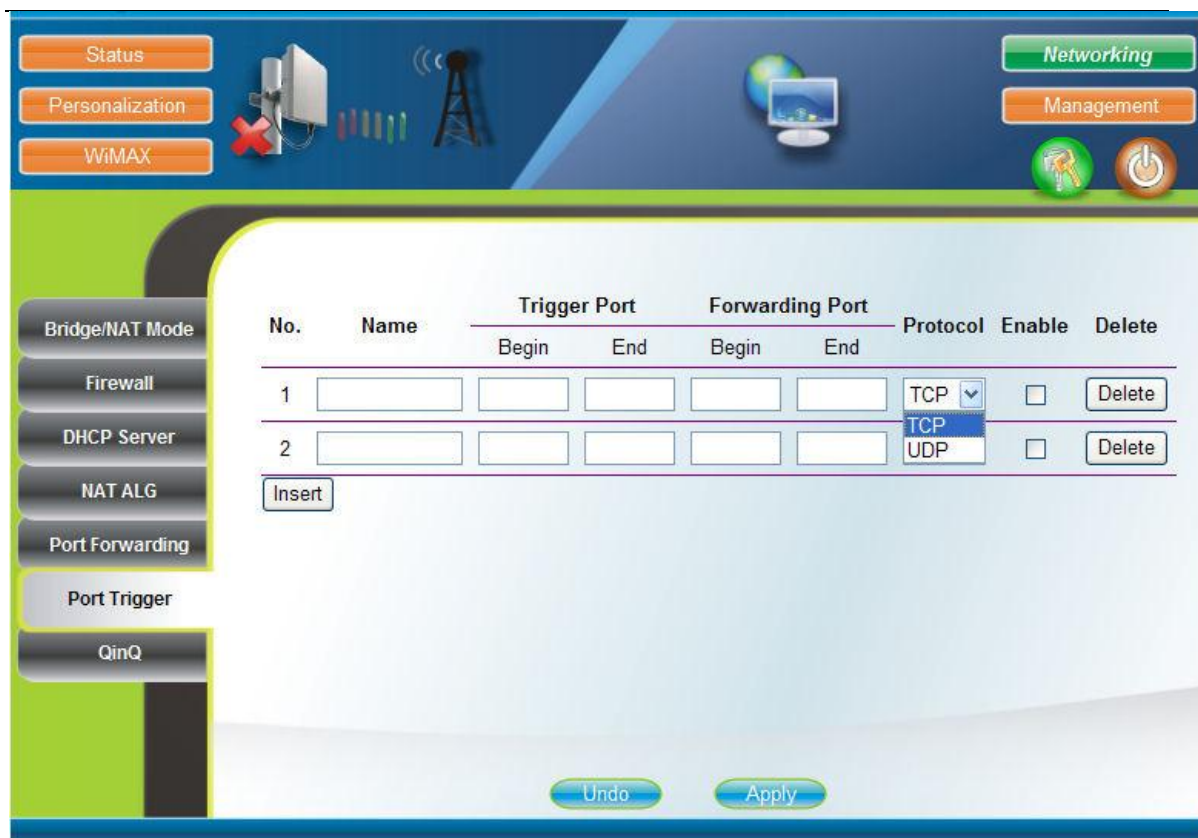


Figure 33 - Networking - Port Trigger

2. Click **Edit** – to access Port Trigger configuration.
3. Click **Insert** to add additional port.
4. Define the Trigger Port to **Begin** at and port to **End** at.
5. Define the Forwarding Port to **Begin** at and port to **End** at.
6. Select the **Protocol** – define the protocol to be used, either: TCP or UDP.
7. **Enable** the setting – check to enable the setting.
8. Click **Delete** - to remove from the list
9. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

10.7 QinQ

QinQ is a solution for large networks, to solve the limitation of maximum 4096 VLANs. This is done by adding another VLAN tag before the existing 802.1Q tag. When two 802.1Q tags are used, the first (or outer) tag is the Q-in-Q tag. The second (inner) tag is the VLAN tag.

To access the QinQ configuration page:

1. Click **QinQ** on the left side column, as displayed below:

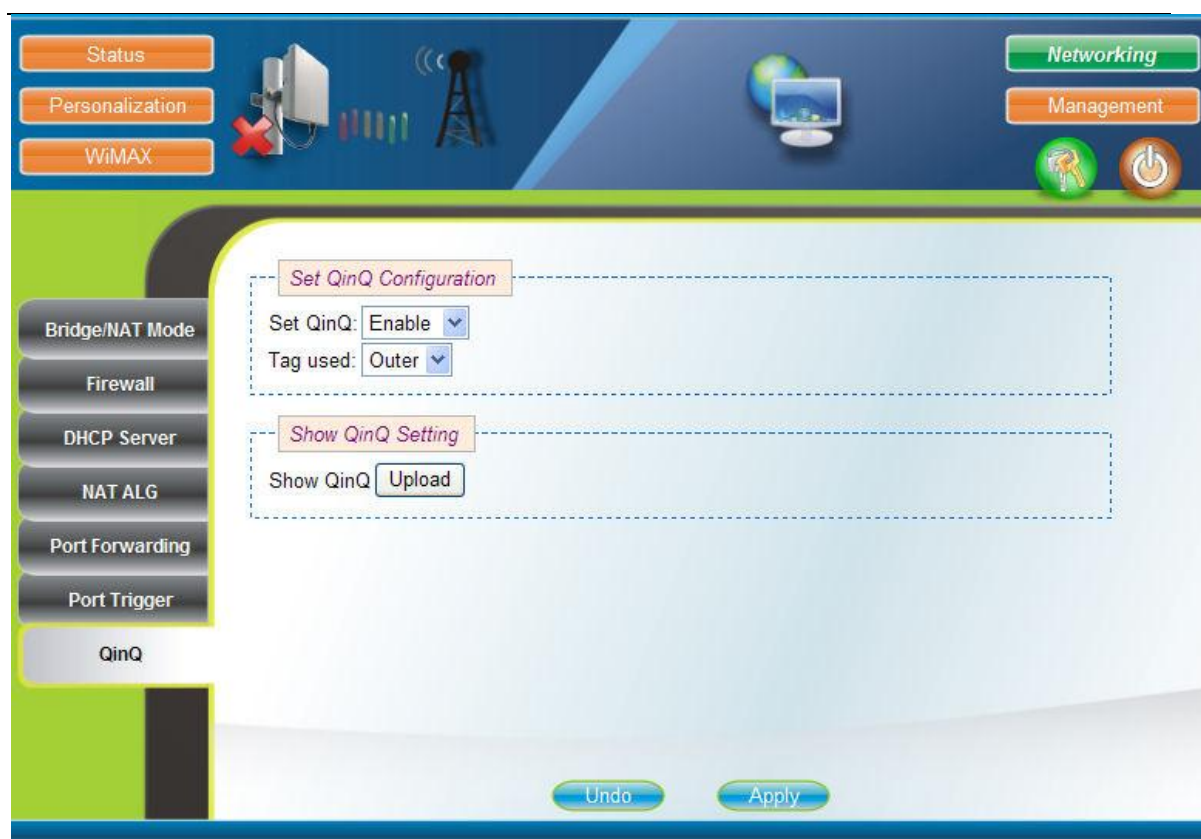


Figure 34 - Networking – Qinq

10.7.1 Set Qinq Configuration

2. Select whether to **Set Qinq**, either: **enable** – default, or **disable**.
3. Select **Tag used** - either: **Outer**, or **Inner**.

10.7.2 Show Qinq Setting

4. Show Qinq - click Upload to display Qinq settings
5. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

10.8 VLAN



Note: Changes to VLAN setting should be made only with appropriate authorization and consultation.

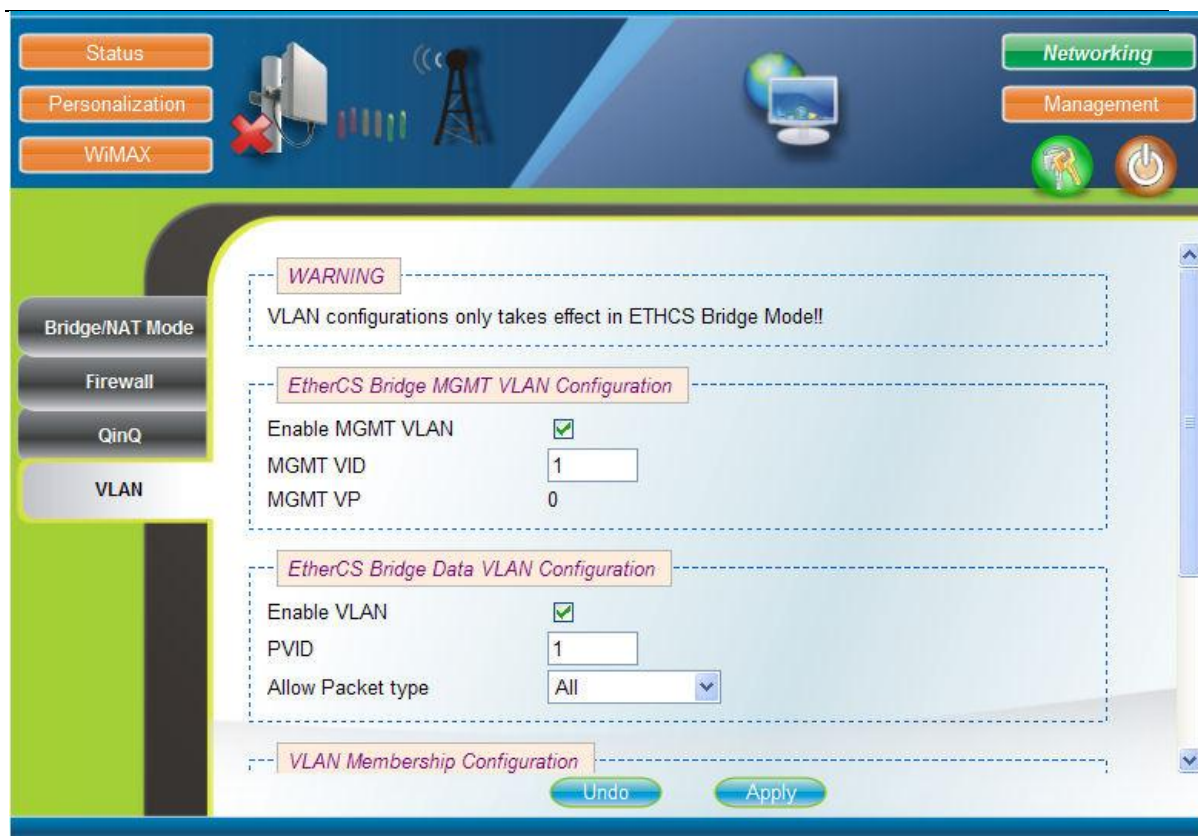


Note: VLAN is only available when in Bridge mode.

Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same network segment, when in fact they are located on a number of different LAN segments. MiMAX-Pro supports two (2) types of VLAN – MGMT VLAN and Data VLAN. When disabled the CPE functions in VLAN pass-through mode. The VLAN page allows you to enable support for VLANs, as displayed below:

To access the VLAN page:

Click **VLAN** on the left side column (when in Bridge mode), as displayed below:



WARNING
VLAN configurations only takes effect in ETHCS Bridge Mode!!

EtherCS Bridge MGMT VLAN Configuration

Enable MGMT VLAN ☒

MGMT VID

MGMT VP

EtherCS Bridge Data VLAN Configuration

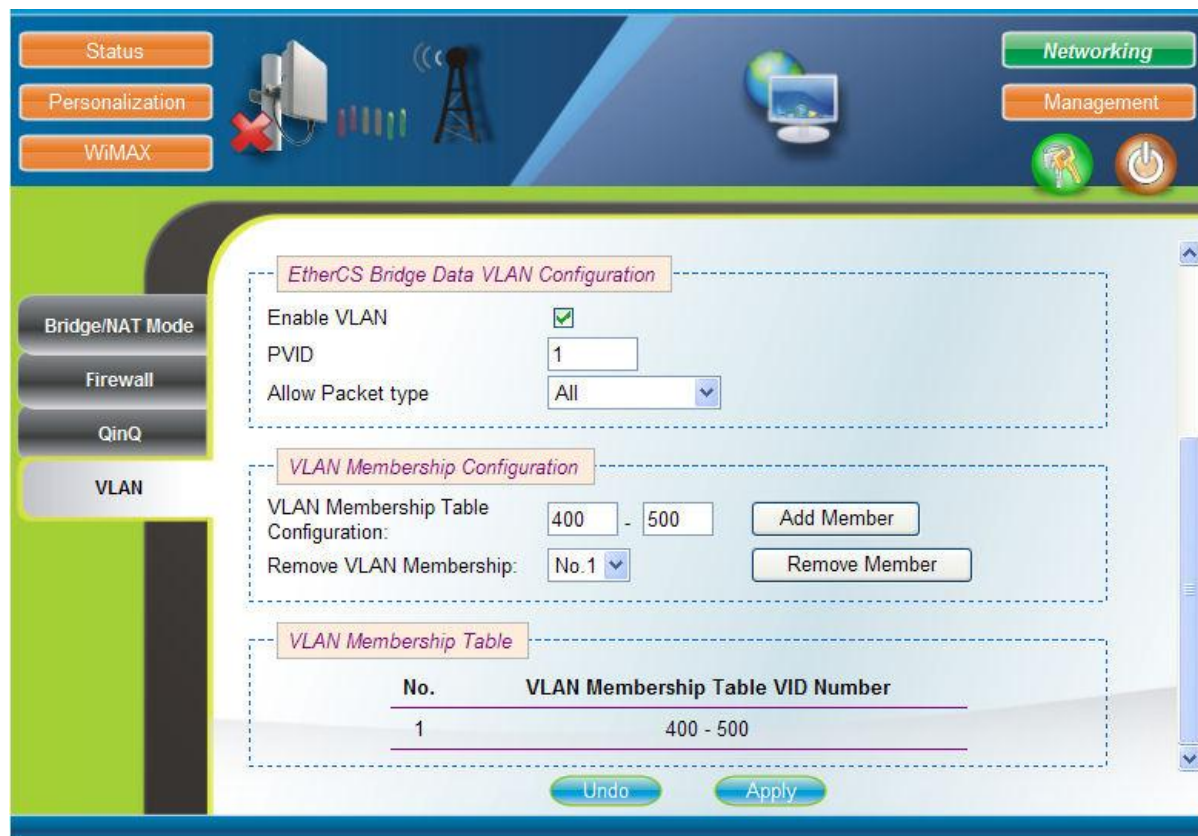
Enable VLAN ☒

PVID

Allow Packet type

VLAN Membership Configuration

Figure 35 - Networking VLAN



EtherCS Bridge Data VLAN Configuration

Enable VLAN ☒

PVID

Allow Packet type

VLAN Membership Configuration

VLAN Membership Table Configuration: -

Remove VLAN Membership:

VLAN Membership Table

No.	VLAN Membership Table VID Number
1	400 - 500

Figure 36 - Networking VLAN – configuration

Parameter	Description
EtherCS Bridge MGMT VLAN Configuration	
Enable MGMT VLAN	Check to enable the MGMT VLAN , either: check = enable , or uncheck = disable .
MGMT VID	Enter from 0 ~ 4095. Normal value = 1
MGMT VP	Displays the VLAN management Priority. Always "0".
EtherCS Bridge Data VLAN Configuration	
Enable VLAN	Check to enable (data) VLAN , either: check = enable , or uncheck = disable .
PVID	Define the PVID (Port VLAN Identifier), can be set from 0 ~ 4095
Allow Packet Types	Select the Packet type either:
	All – all packet type are passed, both Tagged and Untagged
	Tagged Only - users need to add member rule into "VLAN Membership Table". If the packet's VID is one of the values previously set in the membership table, the packet can pass. Otherwise, if not in the table, the packet will be dropped.
	Untagged Only – CPE will only allow packets without VLAN-Tag otherwise the packets are dropped. Once the packets are received "PVID" is added and packet is sent. Tagged packets with PVID (set by user) – PVID will be removed and sent.
VLAN Membership Configuration	
VLAN Membership Table Configuration	Define membership table configuration – 0~ 4095, click Add Member to add to table. Position number will be assigned automatically.
Remove VLAN Membership	Select Position number; click Remove Member to remove from table.
VLAN Membership Table – displays VLAN membership VID number.	
	No. – displays position number
	VID Number – displays VID number

Table 15 - VLAN MGMT

11 Management

The **Management** page of the MiMAX-Pro management enables configuration of the TR-069 client, viewing the Log page (read-only), perform a firmware upgrade, a firmware rollback or restore factory defaults and reboot the device.

To access the Management page:

1. Click the **Management** button to navigate to the Management page.
2. Click the desired sub-option on the on the left side column.

11.1 TR-069

The **TR-069** page enables you to configure TR-069 client (CPE WAN Management Protocol for communication with an Auto Configuration Server). When enabled, the TR-069 client will automatically start up when the CPE is operational.

11.1.1 TR-069 Configuration

To access the TR-069 Configuration:

1. Click **TR-069** on the left side column, as displayed below:

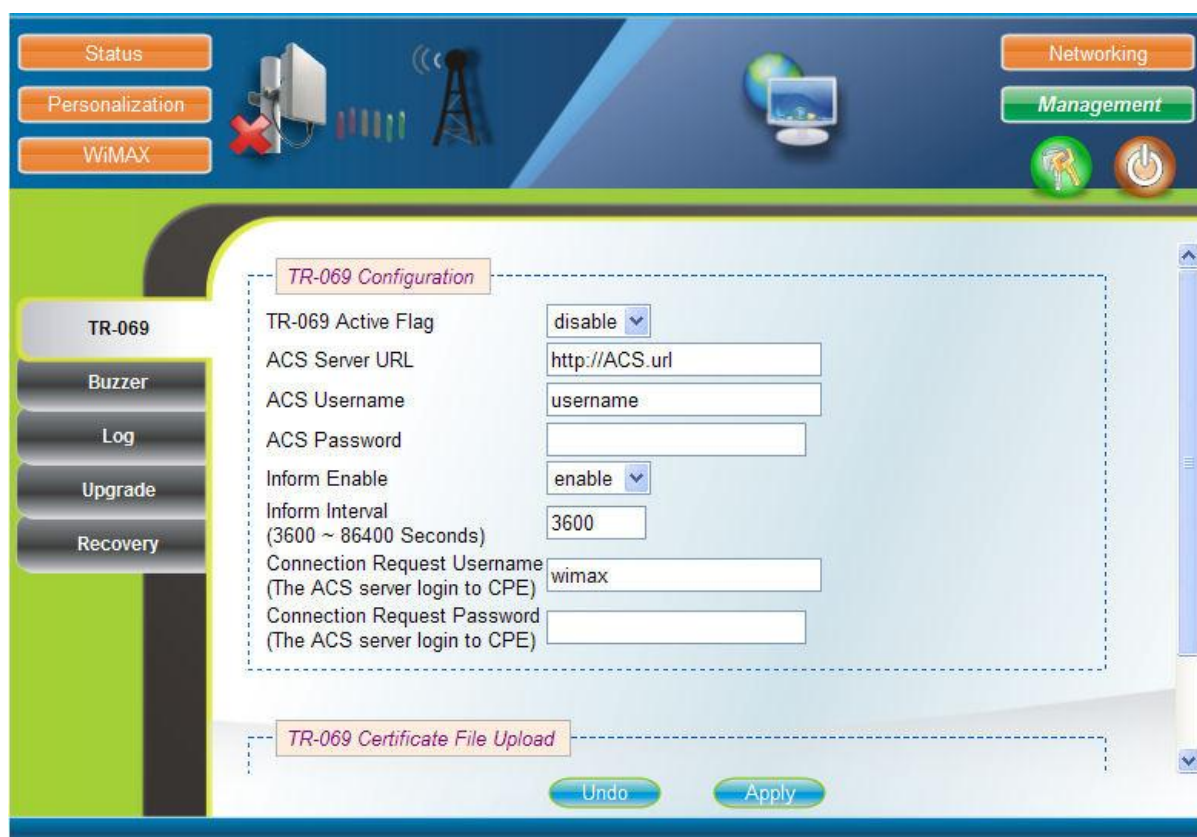


Figure 37 - Management - TR-069 Configuration

2. Select the **TR-069 Active Flag** – either; enable (activate) or disable.
3. Define the **ACS Server URL** – the URL of the ACS (Auto Configuration) server. Used by TR-069 client to connect to the ACS server.
4. Define the **ACS Username** – the username for access to the ACS server.
5. Define the **ACS Password** – the password for access to the ACS server
6. Select **Inform Enable** – either; enable or disable, the CPE will communicate with the ACS periodically (according to Inform Interval setting).
7. Define the **Inform Interval** – define Inform interval (in seconds), the interval between communicating with ACS server. [3600 – 86400] seconds.



Note: If only **Inform Enable** and/or **Inform Interval** have been modified, no reboot required, change will take effect in the next cycle.

8. Define **Connection Request Username** – the username for ACS access the CPE via Connection Request. ACS server can also use this to connect to the CPE and get/set parameter via connection request mechanism.
9. Define **Connection Request Password** – the password for ACS access to CPE. ACS server can also use this to connect to the CPE and get/set parameter via connection request mechanism.



Note: If utilizing DHCP server parameters will be changed but **not saved** to the CPE. The parameter settings will be restored when CPE is reset (unless modified by user).

11.1.2 TR-069 Certificate File Upload

The TR-069 Certification File Upload section enables uploading the TR-069 certification file, as displayed below:

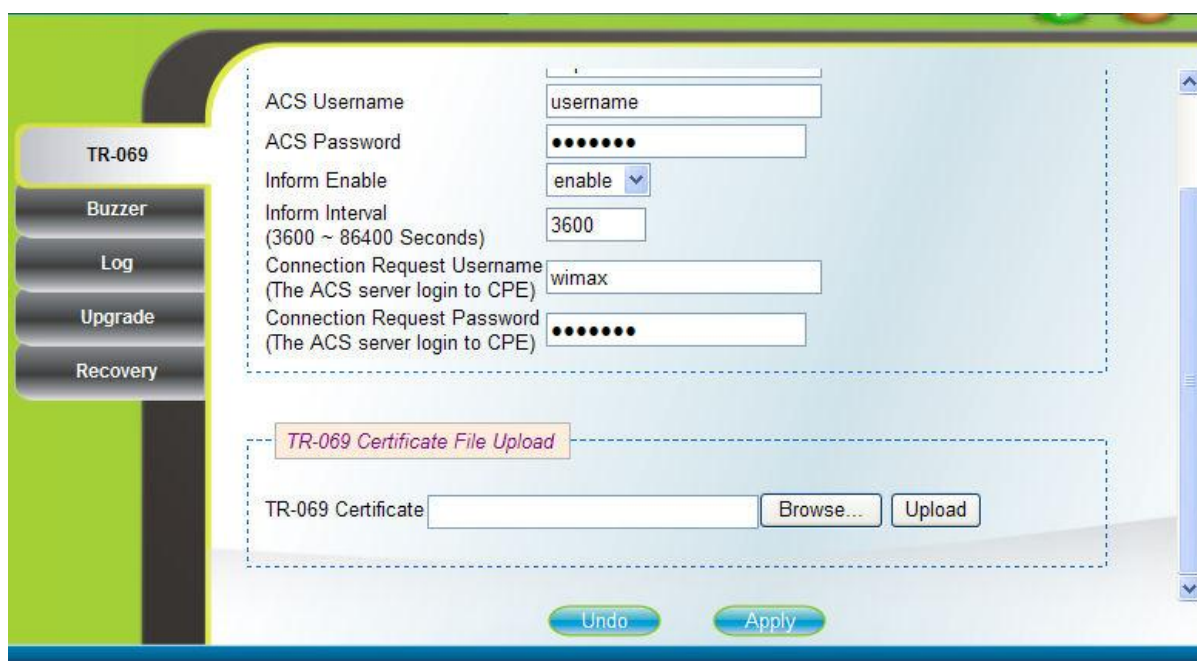


Figure 38 - Management - TR-069 certification file upload

To upload the TR-069 Certification file:

1. Click **Browse** to choose the appropriate configuration file to upload.
2. Click **Upload** to upload the file.
or
Click **Reset** to clear field.



Note: The certificate format, (CPE supports only) is PEM (Privacy Enhanced Mail, Base64 encoded DER certificate). Confirm the format prior to uploading.

The System responds “OK” if the certificate file has been successful uploaded into the CPE.

3. Click **Undo** to discard any changes.
Or
Click **Apply** to save the changes.



Note: CPE does not check the certificate file format even if the upload procedure is successful.

After changes, reboot the system in order for the new configurations to take effect, see [Reboot](#).

11.2 Buzzer

The Buzzer page is where to enable or disable the status indicator audible buzzer that will beep according to different CPE states and signal quality.

To access the Buzzer Configuration:

1. Click **Buzzer** on the left side column, as displayed below:

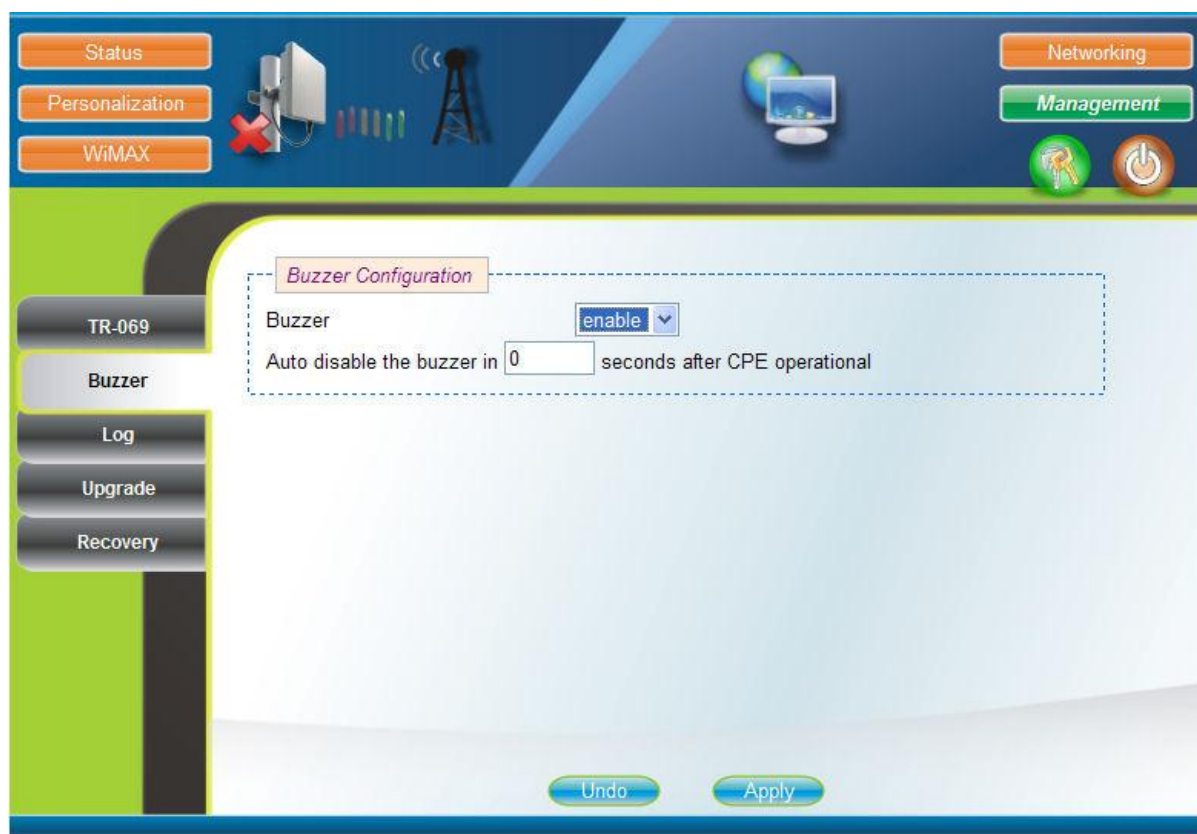


Figure 39 - Management – Buzzer

2. **Buzzer Configuration** – either; enable (activate), disable or demo (for demonstration).
3. Define the **Auto disable** ... interval (in seconds), the amount of time till the Buzzer is disabled after the CPE is operational.

The Buzzer beeps signify different states and signal quality as described in the table below:

Beeps per second	Description
Before the CPE is operational:	
1 short beep per sec.	CPE is in synchronization state
2 continuous beeps per sec.	CPE is in ranging state
3 continuous beeps per sec.	CPE is in DHCP negotiation state
After the CPE is operational:	
2 continuous beeps per sec.	CINR < 8

Beeps per second	Description
3 continuous beeps per sec.	15 > CINR > = 8
4 continuous beeps per sec.	24 > CINR > = 15
5 continuous beeps per sec.	CINR > = 24

Table 16 - Buzzer - beeps

11.3 Log

The **Log** page is where the MiMAX-Pro log information is displayed. The MiMAX-Pro management tool logs traps and events generated by and received from the device and displayed on the Log page.

To display Log page:

1. Click **Log** on the left side column to display the system log, as displayed below:

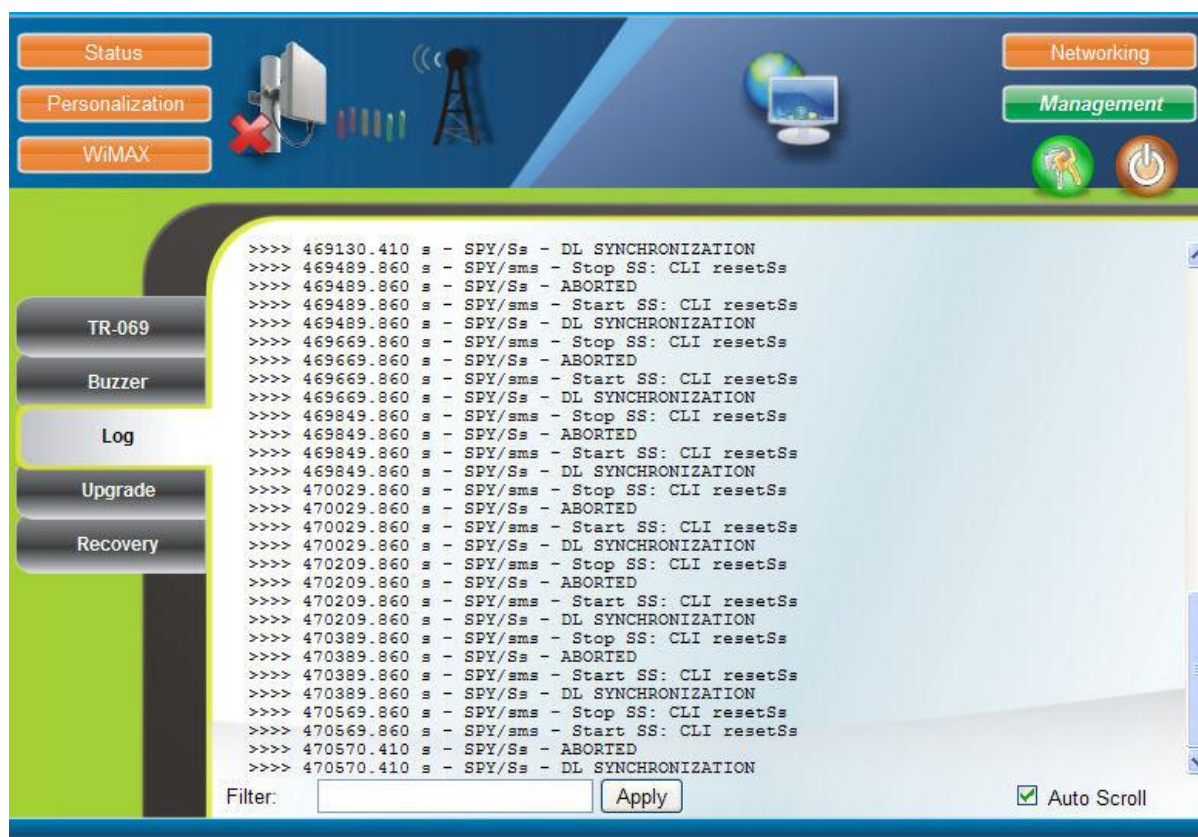


Figure 40 - Management - Log

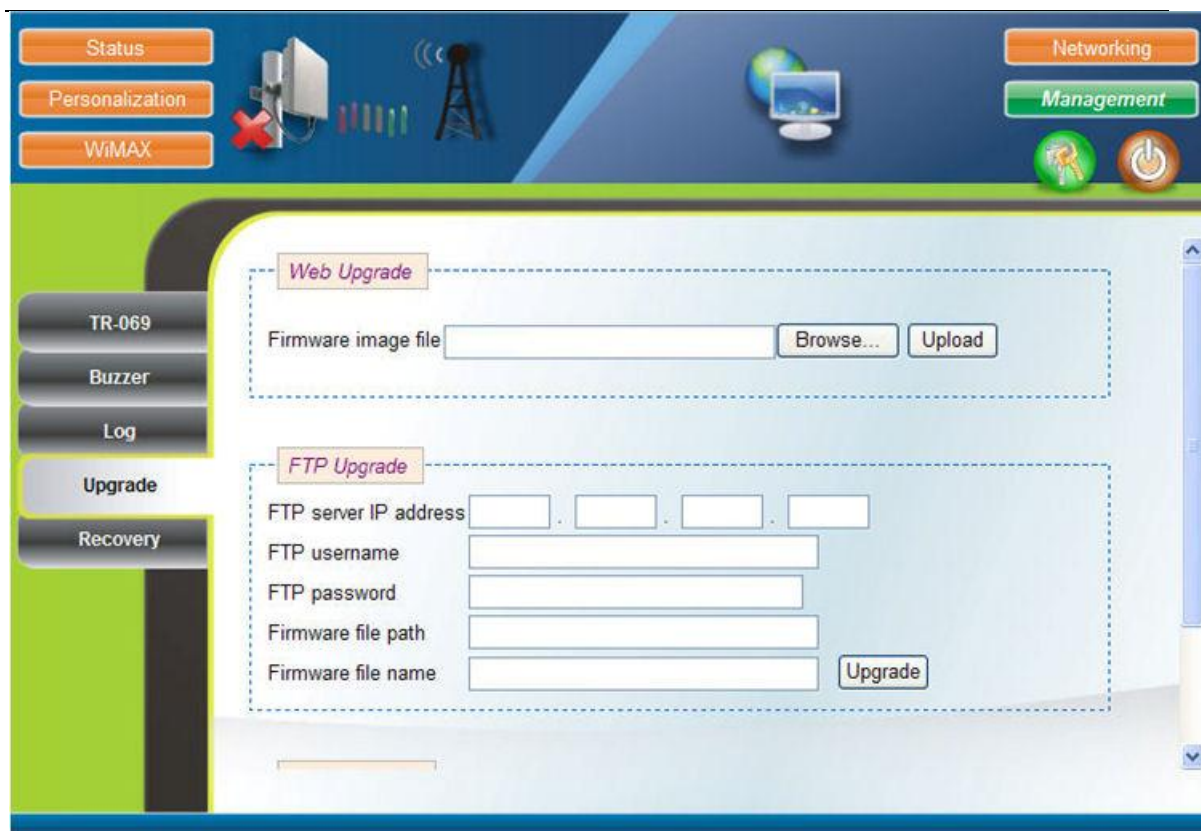
2. **Filter** – Open, close, and filter logs using this field.
3. Click **Apply** – to utilize filter.
4. Click **Auto Scroll** – to activate auto-scrolling.

11.4 Upgrade

This section describes how to upgrade the device's firmware by downloading a new firmware version file via either the Web browser or the FTP/TFTP server. To upgrade the device, you need to define the FTP/TFTP parameters and the name of the software version file that you want downloaded. New firmware releases can be downloaded periodically as they become available.

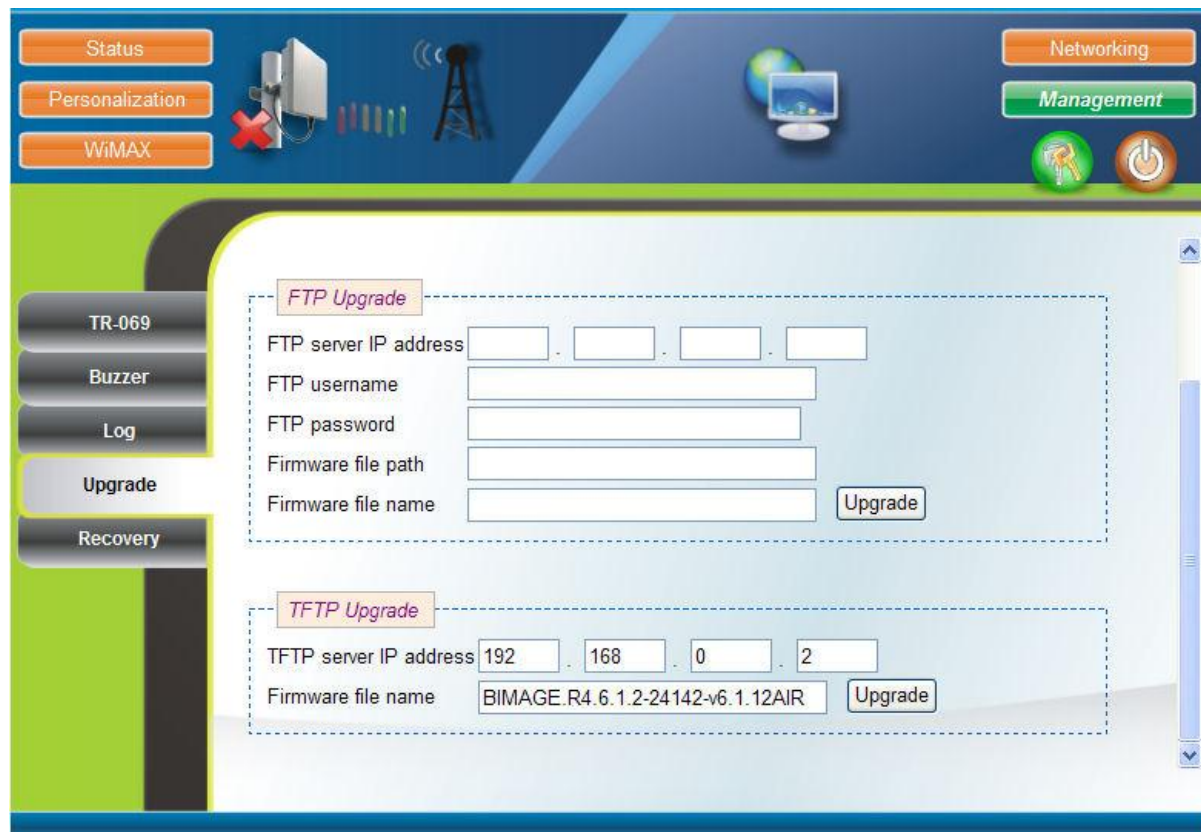
To access the Upgrade page:

1. Click **Upgrade** on the left side column to display the Upgrade page, as displayed below:



The screenshot shows the 'Management - Upgrades' page. On the left, there is a sidebar with buttons: Status, Personalization, WiMAX, TR-069, Buzzer, Log, Upgrade, and Recovery. The main content area has two sections: 'Web Upgrade' and 'FTP Upgrade'. The 'Web Upgrade' section has a 'Firmware image file' input field with 'Browse...' and 'Upload' buttons. The 'FTP Upgrade' section has fields for 'FTP server IP address', 'FTP username', 'FTP password', 'Firmware file path', and 'Firmware file name', with an 'Upgrade' button.

Figure 41 - Management – Upgrades



The screenshot shows the 'Management - Upgrade continued' page. It features the same sidebar as Figure 41. The main content area has two sections: 'FTP Upgrade' and 'TFTP Upgrade'. The 'FTP Upgrade' section is identical to the one in Figure 41. The 'TFTP Upgrade' section has fields for 'TFTP server IP address' (with pre-filled values 192, 168, 0, 2) and 'Firmware file name' (with pre-filled value BIMAGE.R4.6.1.2-24142-v6.1.12AIR), with an 'Upgrade' button.

Figure 42 - Management – Upgrade continued

11.4.1 Web Upgrade

Web Upgrade enables upgrade of the device's firmware by downloading a new firmware version file via the web browser.

To perform an upgrade via the Web:

1. Click **Browse** to choose the appropriate **Firmware image file** to upload.
2. Click **Upload** to upload the file. After the firmware file is uploaded, a summary will be displayed, as shown below:

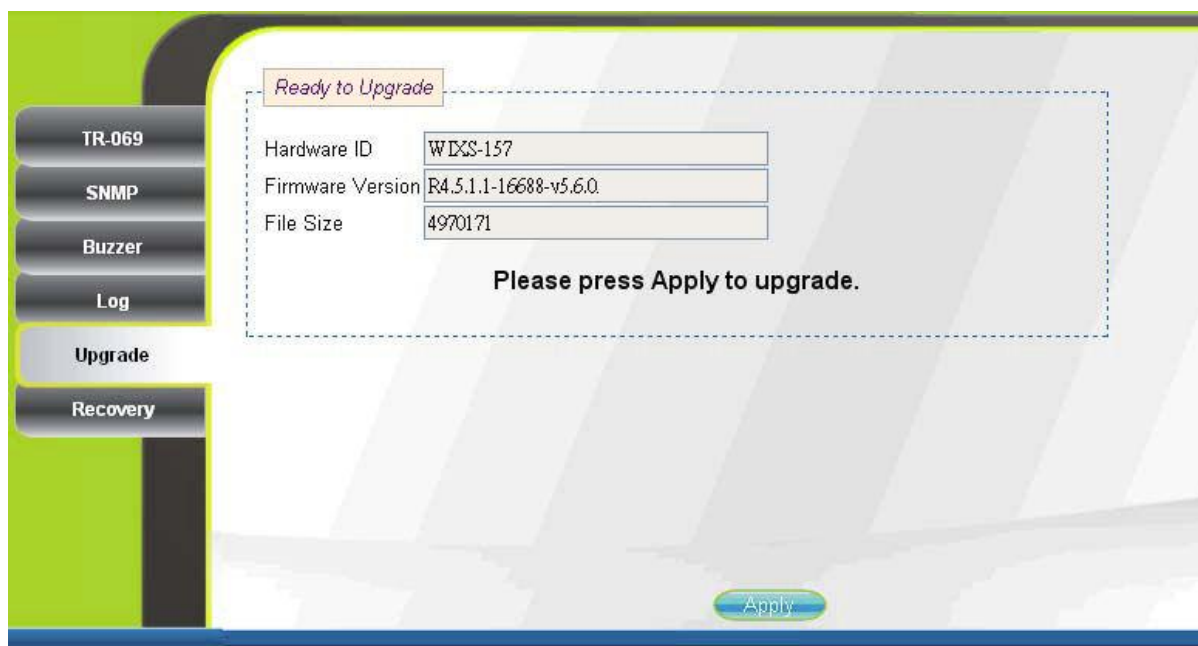


Figure 43 - Management - Upgrade - confirm

3. Click **Apply** to upgrade the firmware. The upgrade procedure takes approximately 3 minutes and automatically reboots the CPE.

11.4.2 FTP Upgrade

FTP Upgrade enables upgrade the device's firmware by downloading a new firmware version file via the FTP server.

1. Define the **FTP server IP address** – FTP server's IP address.
2. Define the **FTP username** – for access to the FTP server.
3. Define the **FTP password** – for access to the FTP server.
4. Define **Firmware file path** – define the path where the upgrade file is located.
5. Define **Firmware file name** – define the name of file.
6. Click **Upgrade** to upgrade the firmware. The upgrade procedure takes approximately 3 minutes and automatically reboots the CPE.

11.4.3 TFTP Upgrade

TFTP Upgrade enables upgrade the device's firmware by downloading a new firmware version file via the TFTP server.

1. Define the **TFTP server IP address** – TFTP server's IP address.
2. Define **Firmware file name** – define the name of file and path where the upgrade file is located.
3. Click **Upgrade** to upgrade the firmware. The upgrade procedure takes approximately 3 minutes and automatically reboots the CPE.

11.5 Recovery

The **Recovery** page enables you to rollback (Firmware Rollback) the firmware version file via the Web browser. Factory Default Settings enable you to restore a CPE back to factory default settings, as shown below:

To access the Recovery page:

1. Click **Recovery** on the left side column to display the recovery page, as displayed below:

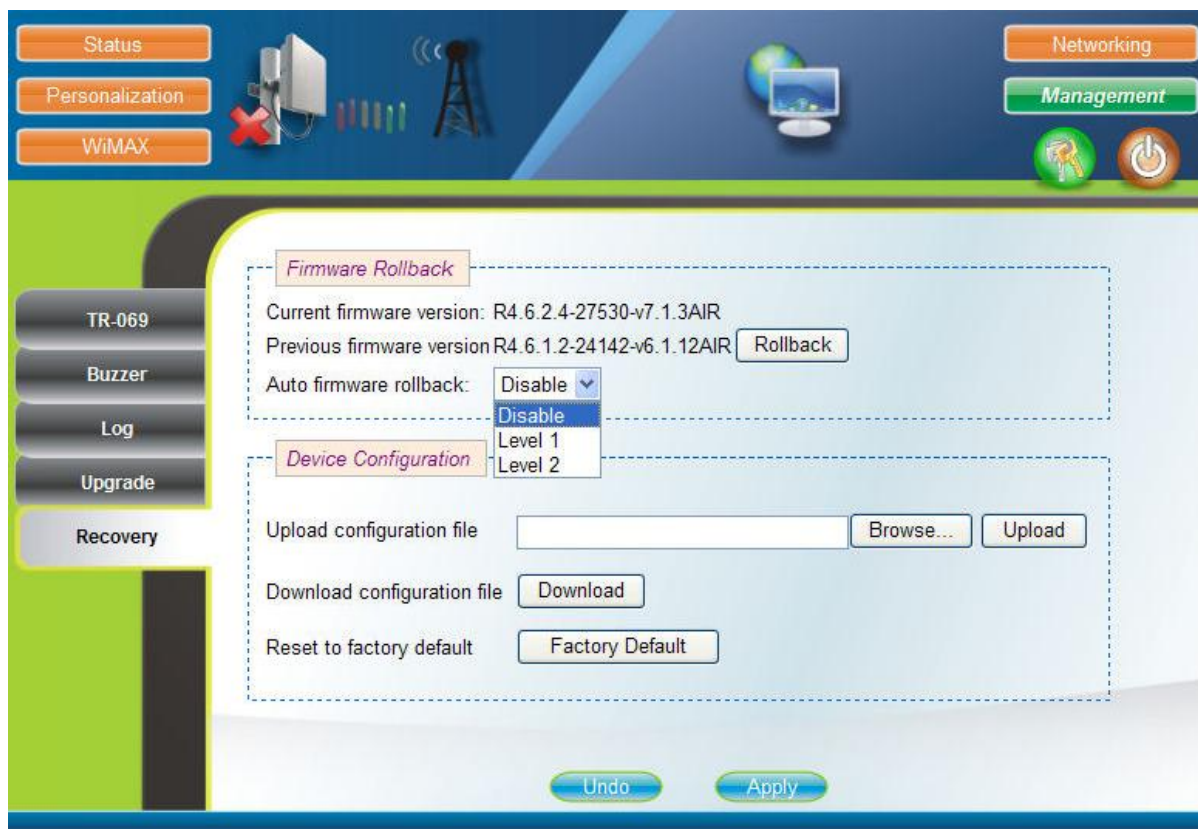


Figure 44 - Management – Recovery

To perform Firmware Rollback:

1. Click **Rollback** to return the firmware to the previous version. A conformation warning is displayed (as shown below).

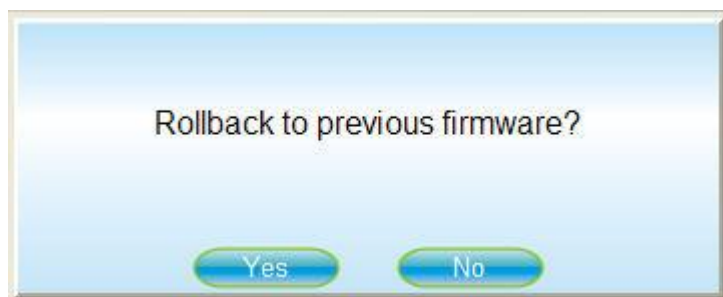


Figure 45 - Management - Rollback warning

2. Click **Yes** to rollback, **No** to cancel.



Note: Momentarily you will be required to Login again after device reboots.

To Reset to Factory Default:

-
1. Click **Reset to Factory Default Settings** to set the product parameters to factory default settings. A conformation warning is displayed (as shown below).

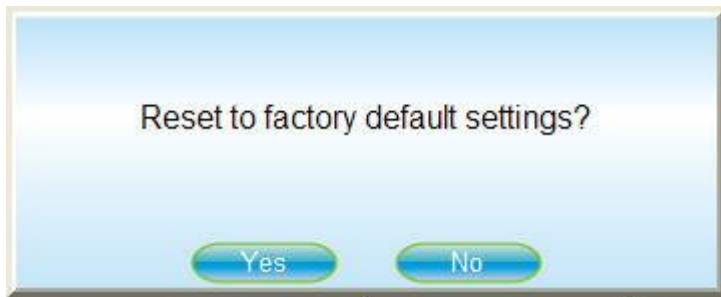


Figure 46 - Management - Reset to default warning

2. Click **Yes** to reset to factory defaults, No to cancel.



Note: Momentarily you will be required to Login again after device reboots.

12 Logout

To quit the MiMAX-Pro Web Server at the end of a session or for maintenance, as shown below:

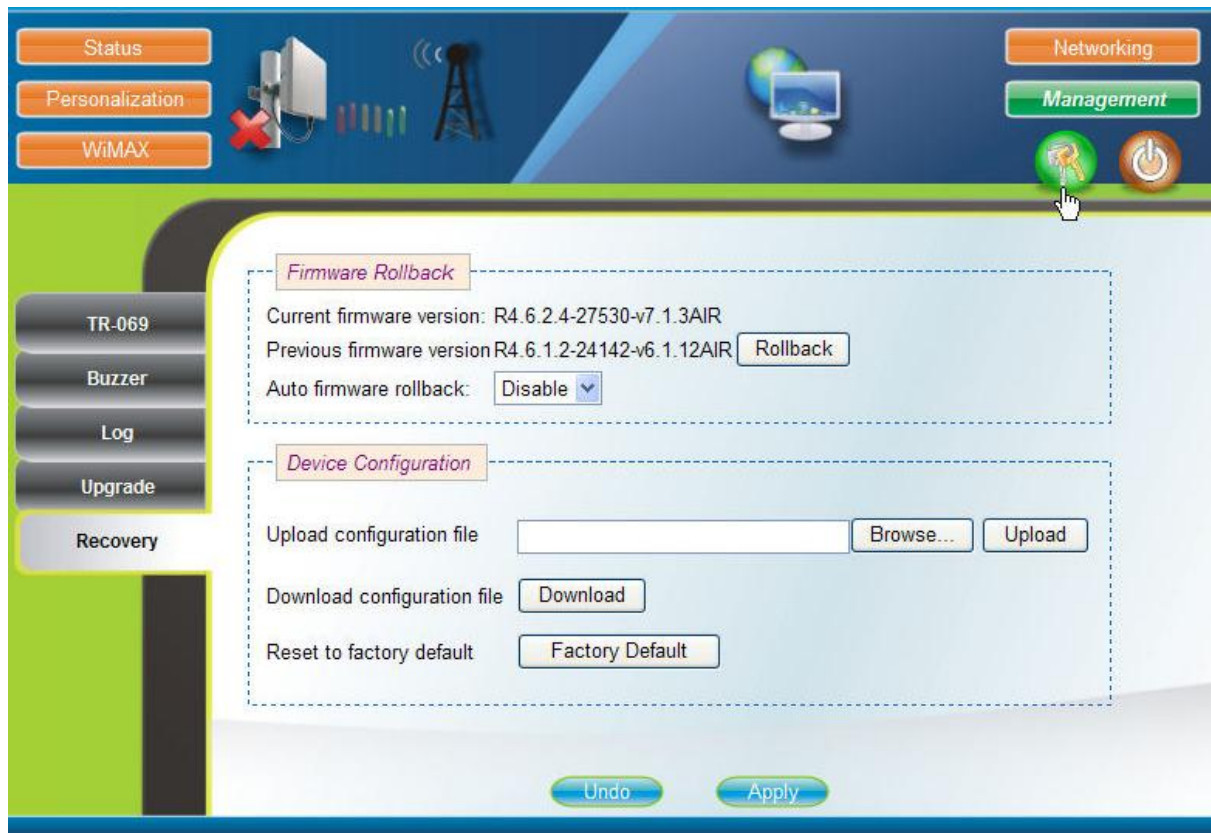


Figure 47 - MiMAX-Pro - Logout

To quit the MiMAX-Pro

1. Click the **Logout** button. You will be re-directed to the Login page.

13 Reboot

Some configuration settings require that you restart the unit to apply new parameter settings to the device, such as upgrading the software version. In order for upgrades and/or other changes to take effect the CPE must be rebooted, as shown below:

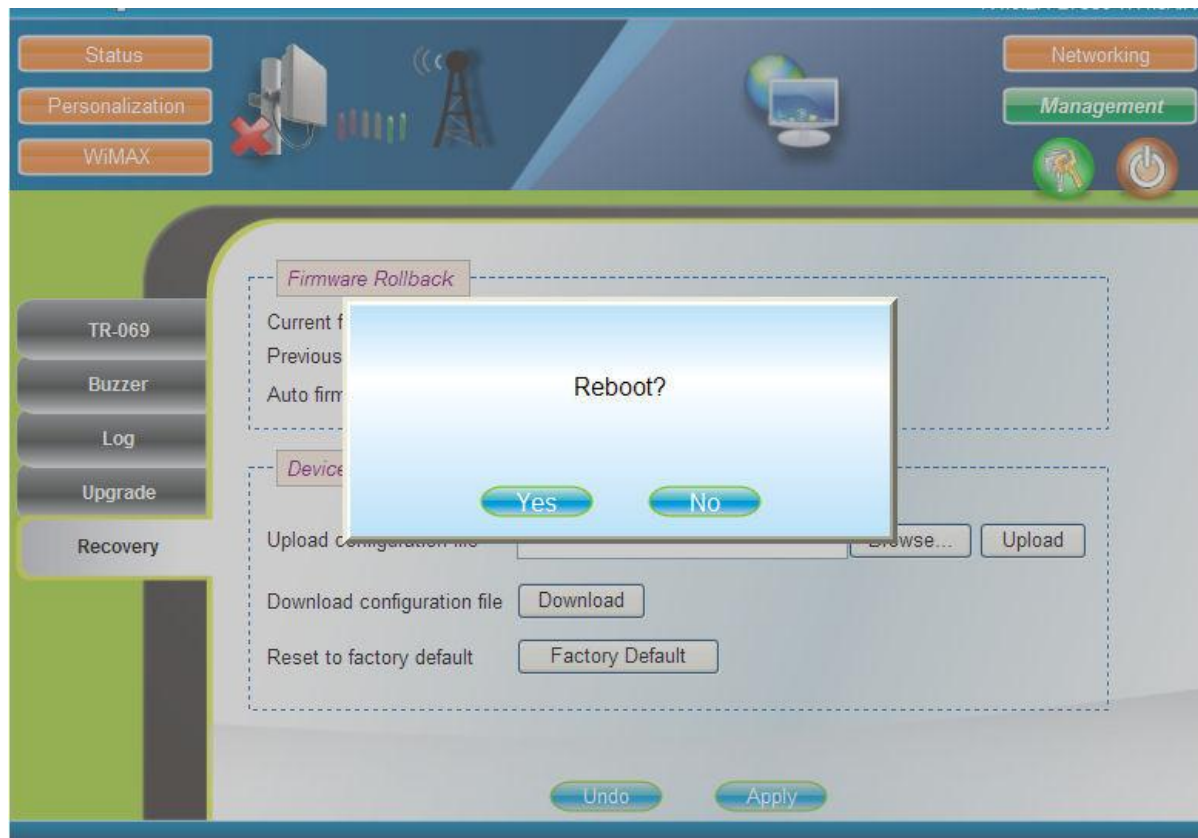


Figure 48 - MiMAX-Pro - Reboot

To perform a Reboot

1. Click the **Reboot** button. A conformation warning is displayed (as shown above).
2. Click **Yes** to reboot CPE, No to cancel.



Note: Momentarily you will be required to Login again after device reboots.

14 Appendix

14.1 Glossary of Terms

ALG	Application Layered Gateway
ATA	Analog Terminal Adapter
BS	Base station
CPE	Customer premises equipment (interchangeable with ST)
DDNS	Dynamic Domain Name System (networking)
DHCP	Dynamic Host Configuration Protocol. Protocol for assigning dynamic IP addresses to devices on a network.
DL	Downlink
IP	Internet protocol
ISP	Internet Service Provider
MAC	The next layer up from the PHY, known as the media access controller
MIMO	Multiple-in, multiple-out
NAT	Network Address Translation
PHY	The physical layer associated with the WiMAX interconnection stack.
Rx	Receiver
SIP	Session Initiation Protocol
SNMP	Simple network management protocol
SS	Subscriber station (interchangeable with CPE or ST)
STC	Space time coding
SW	Software
T1	North American standard 1.56Mb/s pulse code modulated transmission link
TDD	Time division duplex
Tx	Transmitter
URL	Uniform Resource Locator
VoIP	Voice over Internet protocol
WBM	Web-based management
WiMAX	WiMAX is a wireless industry coalition whose members are organized to advance IEEE 802.16 standards for broadband wireless access (BWA) networks.

14.2 Revision History

Revision	Originator	Date	Description
A	M. Falik	11-2008	Initial document
B	M.Falik	01-2009	Mounting instructions and additional content
C	M. Falik	01-2010	Modifications
C1	M. Falik	05-2010	Minor Modification
C2	M. Falik	07-2010	Language support and additions
D	M. Falik	06-2011	SW Update
E	M. Falik	09-2011	SW Update – added VLAN MGMT

14.3 Contact Information

Customer Service Help-Desk for customer service emergency

Airspan Networks have introduced the [Airspan Tracker](#) application to enable prompt and efficient Customer Support services.

If you do not have an Airspan Tracker account, please obtain login credentials by filling-in the form in the main page ["Register New Account"](#).

Worldwide Headquarters:

Airspan Networks Inc.
777, Yamato Road, Suite 310,
Boca Raton, FL 33431, USA
Tel: +1 561 893 8670

www.airspan.com

Feedback:

To provide feedback on this document, please send comments to the following email address:
documentfeedback@airspan.com