



MobileAccessVE WiMAX Instant Coverage Solution User Manual

**PN: 709C004001
REV: A01
Date: FEB 2010**

MobileAccess Worldwide Headquarters

8391 Old Courthouse Road Suite 300, Vienna, VA 22182

Tel: +1(866)436-9266, +1(703)848-0200 TAC: +1(800)787-1266, Fax: +1(703)848-0280

<http://www.MobileAccess.com>

Preface Material

© Copyright 2010, MobileAccess Networks Inc. All Rights Reserved.

This document contains confidential and proprietary information of MobileAccess and may not be copied, transmitted, stored in a retrieval system or reproduced in any format or media, in whole or in part, without the prior written consent of MobileAccess. Information contained in this document supersedes any previous manuals, guides, specifications, data sheets or other information that may have been provided or made available to the user.

This document is provided for informational purposes only, and MobileAccess does not warrant or guarantee the accuracy, adequacy, quality, validity, completeness or suitability for any purpose of the information contained in this document. MobileAccess reserves the right to make updates, improvements and enhancements to this document and the products to which it relates at any time without prior notice to the user. MOBILEACCESS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN.

Policy for Warrantee and Repair

MobileAccess tests and inspects all its products to verify their quality and reliability. MobileAccess uses every reasonable precaution to ensure that each unit meets their declared specifications before shipment. Customers should advise their incoming inspection, assembly, and test personnel about the precautions required in handling and testing our products. Many of these precautions can be found in this manual.

The products are covered by the following warranties:

General Warranty

MobileAccess warrants to the original purchaser all standard products sold by MobileAccess to be free of defects in material and workmanship for one (1) year from date of shipment from MobileAccess. During the warranty period, MobileAccess will repair or replace any product that MobileAccess proves to be defective. This warranty does not apply to any product that has been subject to alteration, abuse, improper installation or application, accident, electrical or environmental over-stress, negligence in use, storage, transportation or handling.

Specific Product Warranty Instructions

All MobileAccess products are warranted against defects in workmanship, materials and construction, and to no further extent. Any claim for repair or replacement of units found to be defective on incoming inspection by a customer must be made within 30 days of receipt of shipment, or within 30 days of discovery of a defect within the warranty period.

This warranty is the only warranty made by MobileAccess and is in lieu of all other warranties, expressed or implied. MobileAccess sales agents or representatives are not authorized to make commitments on warranty returns.

Returns

In the event that it is necessary to return any product against above warranty, the following procedure shall be followed:

1. Return authorization is to be received from MobileAccess prior to returning any unit. Advise MobileAccess of the model, serial number, and discrepancy. The unit may then be forwarded to MobileAccess, transportation prepaid. Devices returned collect or without authorization may not be accepted.
2. Prior to repair, MobileAccess will advise the customer of our test results and any charges for repairing customer-caused problems or out-of-warranty conditions etc.
3. Repaired products are warranted for the balance of the original warranty period, or at least 90 days from date of shipment.

Limitations of Liabilities

MobileAccess's liability on any claim, of any kind, including negligence for any loss or damage arising from, connected with, or resulting from the purchase order, contract, quotation, or from the performance or breach thereof, or from the design, manufacture, sale, delivery, installation, inspection, operation or use of any equipment covered by or furnished under this contact, shall in no case exceed the purchase price of the device which gives rise to the claim.

EXCEPT AS EXPRESSLY PROVIDED HEREIN, MOBILEACCESS MAKES NO WARRANTY, EXPRESSED OR IMPLIED, WITH RESPECT TO ANY GOODS, PARTS AND SERVICES PROVIDED IN CONNECTION WITH THIS AGREEMENT INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. MOBILEACCESS SHALL NOT BE LIABLE FOR ANY OTHER DAMAGE INCLUDING, BUT NOT LIMITED TO, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH FURNISHING OF GOODS, PARTS AND SERVICE HEREUNDER, OR THE PERFORMANCE, USE OF, OR INABILITY TO USE THE GOODS, PARTS AND SERVICE.

Reporting Defects

The units were inspected before shipment and found to be free of mechanical and electrical defects.

Examine the units for any damage that may have been caused in transit. If damage is discovered, file a claim with the freight carrier immediately. Notify MobileAccess as soon as possible.

NOTE: Keep all packing material until you have completed the inspection

Safety Warnings

To comply with FCC RF exposure compliance requirement, adhere to the following warnings:

Warning! The Access Pod with its built-in antenna must be installed with a separation distance of at least 20cm from all persons and must not be located in conjunction with any other antenna.

Warning! The outside antenna must be installed with a separation of at least 20cm from all persons and must not be located in conjunction with any other antenna.

Warning! Use of this Access Pod with antennas other than those illustrated could be hazardous. Before using other antennas, contact Mobileaccess Support.

Caution: Double pole/neutral fusing (two fuses in the appliance inlet)

Approved Antennas for use with the MobileAccessVE Solution

The gain of external antennas connected to the VAPs should not exceed 10 dBi.

Compliance with RF Safety Requirements

MobileAccess products have no inherent significant RF radiation.

The RF level on the down link is very low at the downlink ports. Therefore, there is no dangerous RF radiation when the antenna is not connected.

Certification and Compliance to Standards

Category	Standards
Safety:	IEC 60950-1: 2003; UL-60950-1:2003; CAN/CSA – C22.2 No 60950-1-03
EMC:	EN 301489-8 V1.2.1:2002; EN 301489-1 V1.5.1:2004; EN 61000 V4.6:2005 EN 55022 V4.2:2001 / FCC Part 15; VCCI Class A for VCU and Class B for VAP
Radio:	FCC Part 27 ;EN 302 544
SAR:	EN 50385; FCC OET-65
ISO:	ISO 9001: 2000 and ISO 13485: 2003

About This Guide

This guide provides essential product functionality with all the information necessary to proper installation and configuration of the MobileAccess**VE** WiMAX system.

List of Acronyms

Term	Meaning
MIMO	Multi Input- Multi Output
PoE	Power Over Ethernet
PSE	Power Sourcing Equipment
SISO	Single Input-Single Output
SME	Small / Medium Enterprise
STP	Shielded Twisted Pair
UTP	Unshielded Twisted Pair
VAP	VE Access Pod
VCU	VE Control Unit
WiMAX	Worldwide Interoperability for Microwave Access

Table of Contents

1	Overview	1
1.1	System Architecture	2
1.2	System Elements	4
1.2.1	VE Control Unit (VCU)	4
1.2.1.1	VCU Front Panel	5
1.2.1.2	VCU Rear Panel	7
1.2.2	VE Access Pod (VAP)	8
1.2.2.1	VAP Antenna Options	9
1.3	System Monitoring and Management	10
1.3.1	Integration with an External Fault Management System	10
1.4	Overview of the Installation Procedure	11
2	Infrastructure Requirements and Layout Planning	12
2.1	Summary of Unit Locations and Connections	13
2.2	Infrastructure Requirements	13
2.3	Coverage and Installation Planning	15
2.3.1	Types of Environment	15
2.3.1.1	Open environment	16
2.3.1.2	Standard Environment	16
2.3.1.3	Dense Environment	16
2.3.1.4	Combination of Environments	16
2.4	Planning VAP Layout	17
2.4.1	RF Coverage Factors	17
2.4.2	Mapping Locations	17
2.4.3	Connecting Directional Antennas	17
2.4.4	Installation Plan Example	18
3	VCU Unit Installation and Configuration	20
3.1	Installation Kit Contents	21
3.2	Installing Master VCU	22
3.3	Auxiliary Alarm Output Connections	23
3.4	Installing Slave VCU	24
3.4.1	Connecting VAP Ethernet Cables	25
3.4.2	Operation with LAN utilizing Power over Ethernet (PoE)	26

3.5	Provisioning the Master VCU	27
3.5.1	Configuring the Computer IP Parameters	27
3.5.2	Login	28
3.5.3	IP Settings	30
3.5.4	Assigning Identifying Information	31
3.5.5	Setting RF Parameters	32
3.5.6	Verifying System Operation	34
3.6	Assigning the Slave VCU an Identifiable Name	37
4	VAP Installation and Provisioning	38
4.1	VAP Installation	38
4.1.1	VAP Kit Contents	38
4.1.2	VAP Locations and Mounting	39
4.1.2.1	Desk Mount	39
4.1.2.2	Wall Mount	40
4.2	Verifying VAP Coverage Area	40
4.3	Provisioning the VAPs.....	40
4.3.1	Verifying Normal VAP Operation	41
4.3.2	Naming the VAP	42
4.3.3	Configuring VAP for External Antenna	43
5	Navigating the Web Access Application	44
5.1	Opening a Session and Authentication Levels	44
5.2	About the MobileAccessVE Web Access Window.....	45
5.3	Configuration Tab	46
5.3.1	Network Topology Tree	47
5.3.2	Management Tab	48
6	VCU Monitoring and Configuration.....	49
6.1	Viewing VCU General Information	49
6.2	Viewing VCU Alarms.....	50
6.3	Master VCU RF Parameters.....	52
7	VAP Monitoring and Configuration.....	53
7.1	Viewing VAP General Information	53
7.2	Viewing VAP Alarms	54
7.3	VAP RF Parameters	55

8	Administrative Operations.....	56
8.1	Changing Password.....	56
8.2	IP settings.....	57
8.3	SNMP Configuration Parameters	58
8.4	Upgrading (or Downgrading) VCU and VAP Software	59
8.4.1	Upgrading the VCU SW	60
8.4.2	Upgrading the VAP SW	61
9	Troubleshooting.....	63
9.1	Finding a Specific VAP in the Building.....	63
9.2	Wireless Service is Not Available	65
9.3	PoE is Not Working	65
9.4	Ethernet service is degraded.....	66
9.5	No Service from Connected Access Pod	66
9.6	VCU Cannot be Monitored via SNMP.....	68
	Appendices	69
	Traps	69
	MobileAccess VE Control Unit Traps	69
	MobileAccess VE Access Pod Traps	69
	VE Connections in Central Ethernet Source Topologies	70

1 Overview

MobileAccess**VE** WiMAX solution provides enhanced, cost effective in-building WiMAX coverage for enterprise environment. This solution is quickly and simply deployed using the existing cable infrastructure to provide instant MIMO or SISO WiMAX coverage without requiring the installation of new cables and without affecting existing LAN services. MobileAccess**VE** minimizes disruption while providing a scalable and flexible solution at a significantly lower total installation cost.

The VE solution distributes WiMAX wireless service from the service provider's equipment and Ethernet services from the corporate LAN, to Access Pods installed throughout the enterprise. The Access Pods distribute the WiMAX services via integrated internal antennas (or external antennas for additional coverage optimization), and also provide Ethernet connectivity to the LAN terminals. The MobileAccess**VE** solution seamlessly coexists with the Enterprise LAN and does not consume LAN capacity.

The VAPs are distributed on each floor and plug into standard Ethernet jacks already installed at the enterprise site. They are powered via PoE technology and managed via a VE Control Unit (VCU) located in the floor's communication shaft for site coverage that requires more than one VCU (each VCU supports up to 12 VAPs), several VCUs (up to 12) can be aggregated under a single VCU serving as Master. The Master VCU provides the interface to the capacity sources (the service provider's equipment) and for management of all units.

This enhanced WiMAX coverage solution can be easily and quickly installed with minimal disturbance to the enterprise. In less than a few hours, with no additional cables required, a scalable and flexible solution is provided at a significantly lower total installation cost.

The following figures illustrate *single-tier* and *multi-tier* VE installations.

In a single-tier installation, the VCU is connected to the service provider's equipment and to the Ethernet switch and distributes Ethernet and WiMAX services to up to 12 VAPs distributed over one more adjacent floors.

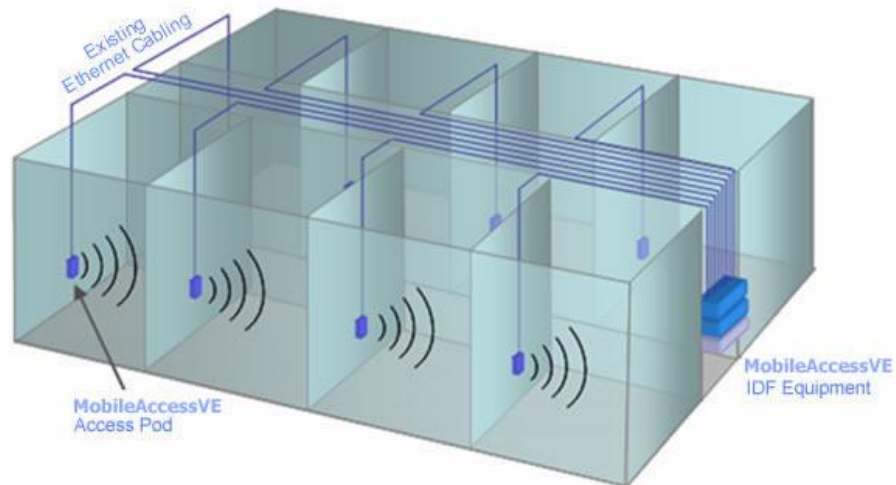


Figure 1-1. Single Tier MobileAccess**VE** Installation

Multi-tier installation includes the Master VCU that supports up to twelve Slave VCUs. In this type of installation the provider's services are fed to the Master VCU through which the Slave VCUs are controlled and managed.

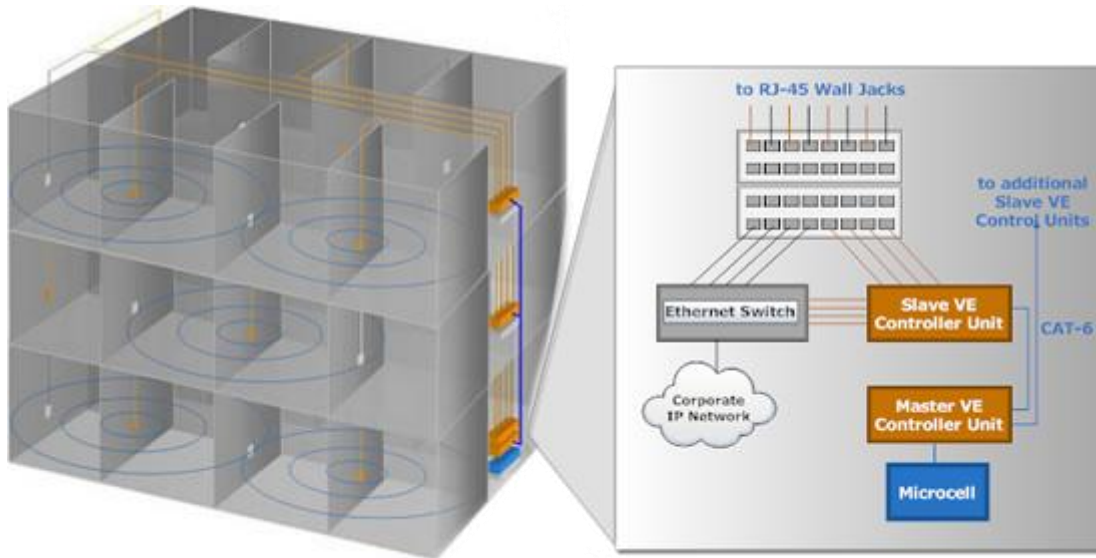


Figure 1-2. Multi Tier MobileAccessVE Installation

1.1 System Architecture

Main elements - The MobileAccessVE solution is based on the following main elements:

- **VE Control Unit (VCU)** – Control Unit that can serve either as a Master or a Slave and interfaces the other VCUs (in case of Master) or the VAPs (when serving as Slave). The Master or Slave mode is automatically detected according to the VCU's physical connection. If a connection to another VCU is detected the VCU will be identified as a Slave; otherwise it will assume the role of a Master.
- **Master VE Control Unit (Master VCU)** – installed in the main communication (IDF) closet, interfaces to the WiMAX BS and Ethernet switch and provides secure, central management to (up to twelve) VCUs and all connected VAPs. VAPs can also be connected to the Master VCU.
- **Slave VE Control Unit (Slave VCU)** – installed telco/IDF closet. Used to expand coverage to additional floors. Each VCU interfaces the Master VCU and up to twelve VAPs and twelve Ethernet connections.

The Slave VCUs distribute WiMAX MIMO or SISO signals to each VAP along with PoE and Ethernet signals from the Ethernet switch, throughout the existing CAT-5e infrastructure.

The Slave VCUs are connected to the Master VCU using CAT-6 or CAT-7 cables.

- **VAP (VE Access Pod)** – These are pluggable antennas distributed at strategic locations on the floor to provide maximum WiMAX coverage. VAPs provide RF coverage via integrated, internal antennas. VAPs are also equipped with interfaces for external antennas that can be used for special coverage requirements. VAPs are remotely powered from the VCU using Power over Ethernet (PoE) – no local power required.

Up to twelve VAPs can be connected to a single VCU using LAN cables (CAT-5e or higher).

Note: When the total number of VAPs in the deployment exceeds 72 VAPs, consult with MobileAccess support.

The following figure shows the MobileAccess**VE** solution architecture (multi-tier).

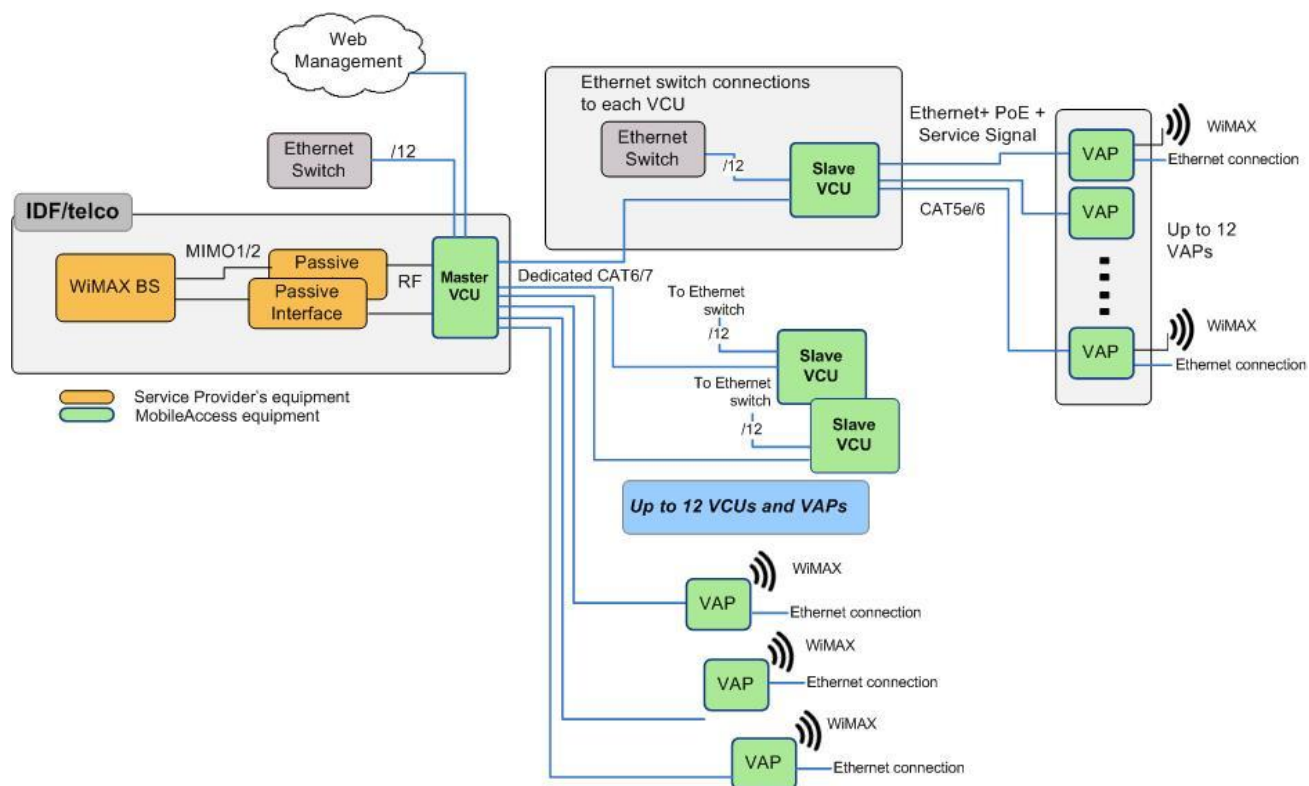


Figure 1-3. MobileAccessVE Basic Architecture

The Master VCU distributes the converged WiMAX services from the service provider's equipment to the Slave VCUs. At the Slave VCUs, the wireless services are converged with Ethernet service and routed to the VAPs via the Ethernet LAN CAT-5e/6 cabling infrastructure.

The VAPs distribute the WiMAX services via integrated internal antennas or external antennas and provide Ethernet connectivity to the LAN terminals.

1.2 System Elements

This chapter describes the interfaces of the VE Control Units and Access Pods.

1.2.1 VE Control Unit (VCU)

Capabilities and interfaces

The VE Control Unit can operate as a Master VCU, managing up to twelve slave VCUs and/or VAPs, **OR** as a Slave VCU connected to up to twelve VAPs

While operating as a Master VCU:

- Interfaces to WiMAX BS, Ethernet switch, slave VCUs and (optionally) to VAPs.
- Converges WiMAX, Ethernet and PoE and interfaces to VAPs/VCUs.
- VAPs and Slave VCUs management and control
- Remote management of the entire deployment

While operating as a Slave VCU:

- Interfaces to Master VCU
- Converges Wireless services, Ethernet and PoE and interfaces to VAPs
- Management and control of connected VAPs

1.2.1.1 VCU Front Panel

The front panel includes the connections to two WiMAX MIMO channels (when supporting SISO service – only **MIMO 1** connector is relevant), interfaces to VAPs and to other VCUs according to the configuration, and to management.

This section describes the front panel interfaces and LEDs.

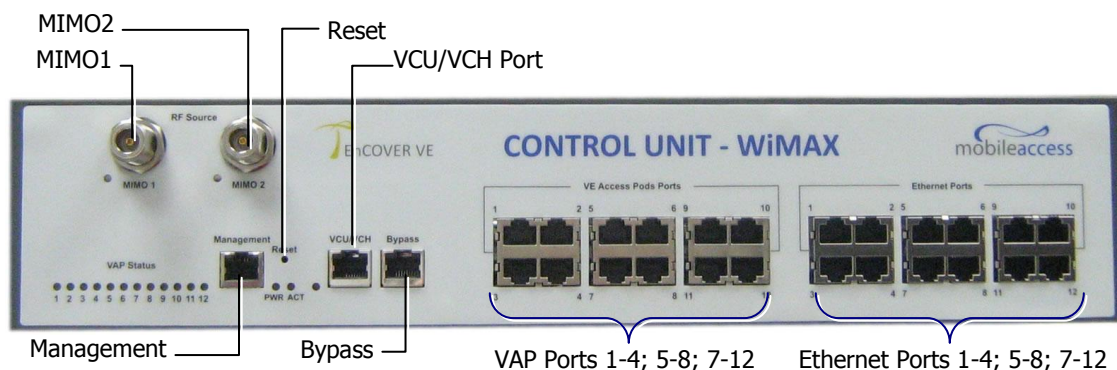


Figure 1-4. VCU Front Panel Ports

Table 1-1: VCU Ports Description

Ports	Description
MIMO1 MIMO2	RF connections (two TDD MIMO channels) to the service provider WiMAX BS equipment. Coax cables. <i>Note: When supporting SISO service – only MIMO 1 connector is relevant.</i>
Management	RJ45 WEB management connection.
VE Access Pod Ports 1-4; 5-8; 7-12	VAP/VCU port connections. RJ-45 connection to VAP/VCU through the LAN infrastructure. CAT-5e/6 cables. If VCU is connected as Master – these are connections to the Slave VCUs (and optionally also to VAPs). If VCU is connected as Slave – these are connections to VAPs.
Ethernet Ports 1-4; 5-8; 7-12	Ethernet port connections to Ethernet Switch. Ethernet cables.
VCU/VCH	Used for connecting a Slave VCU to the Master VCU in a multi-tier deployment (connects to one of the VAP ports of the Master VCU).
Bypass	Relevant for Slave controllers in topologies in which the connection to the Master VCU is also used to transport Ethernet signals to the switch – the Ethernet signals are separated from the WiMAX signals and flow through the Bypass port to the switch. See the Appendix - VE Connections in Central Ethernet Source Topologies for more information.
Reset	N/A in current version

The front panel LEDs are described below.

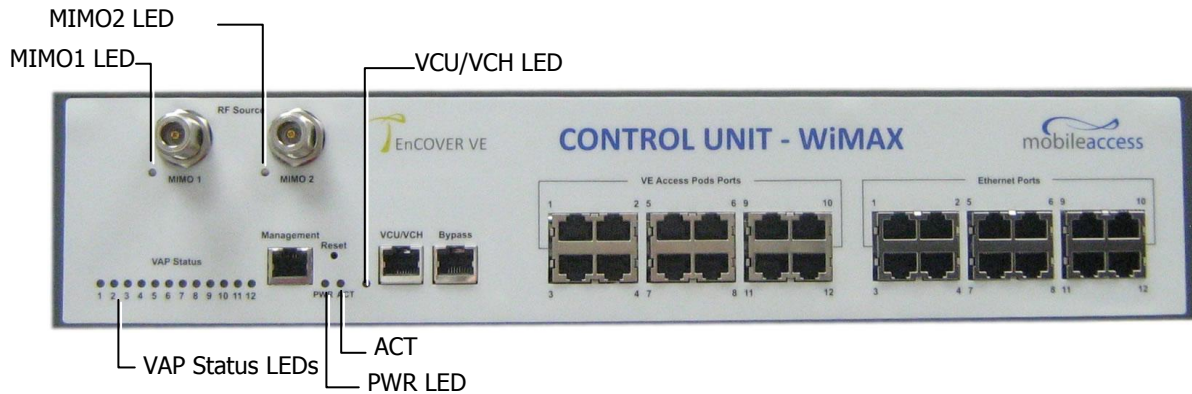


Figure 1-5. VCU Front Panel LEDs

Table 1-2: VCU LEDs Description

LED	Description
PWR	Indicates whether the VCU receives power: Green - Power OK Disabled - No power received by VCU
ACT	VCU activity LED: Solid Green – During initialization Blinking Green – Normal system operation Fast Blinking Green – User activated <i>VCU Identify</i> on this VCU
VAP Status (one LED per port)	Indicates the status of the <i>corresponding</i> unit (VAP or VCU) Blinking Green – Unit is initializing Solid Green – Normal operation of unit Solid Orange – Unit is faulty, or unmanaged. This can be due to mismatch type, VoIP phone, etc. Fast Blinking Green – User invoked "Identify" command on the unit Off – No VAP or VCU connected to this port.
RF (one LED per Channel)	Indicates the status of connected RF capacity source: Green – Master VCU only. Normal RF level Orange – Master VCU only. RF level is either too low, too high, or service has been turned off by the user. Off – VCU is Slave.
VCU/VCH	Indicates the status of the connection to the Master VCU: Off – Master mode (not connected to VCU) Blinking Green – During Attachment process with Master VCU Solid green – Slave (IF-IF) mode and connected to Master

1.2.1.2 VCU Rear Panel

The rear panel includes the power input, the AUX alarms and service connections.



Figure 1-6. VCU Rear Panel

Table 1-3: VCU Rear Panel Description

Connector	Description
Console	RS232 local connection for service personnel (D-Type 9)
Alarms	AUX alarms connections - see section 3.3.
Power Input	Standard 3-pins AC power connector equipped with an ON/OFF switch. 90-264V AC, 47-63 Hz AC; 350W power consumption maximum.

1.2.2 VE Access Pod (VAP)

Each VAP provides the following functions:

- WiMAX Antennas – distributes the WiMAX signals. The antennas are internal, where external antennas can also be connected.
- Connection to Ethernet port – relevant when connected to jacks where an Ethernet connection is already available.

The VAP can be mounted/hung on the wall or placed on a flat surface (such as a desk).

The following figure shows the desktop assembly.



Figure 1-7. VE Access Pod-Front

Table 4: VAP LEDs

LED	Description
Power	Solid Green - Power supplied to VAP Off - No power supplied to VAP
Activity	Off - No power supplied to VAP or Overall Status of VAP is faulty Blinking Blue - Power on, VAP is initializing (connecting to VCU) Solid Blue - Power on, unit operating normally Fast Blinking Blue - User invoked "Identify" command on corresponding VAP

The following figure shows the desktop VAP rear side and the underside view with the CAT-5e/6 patch-cord cable.

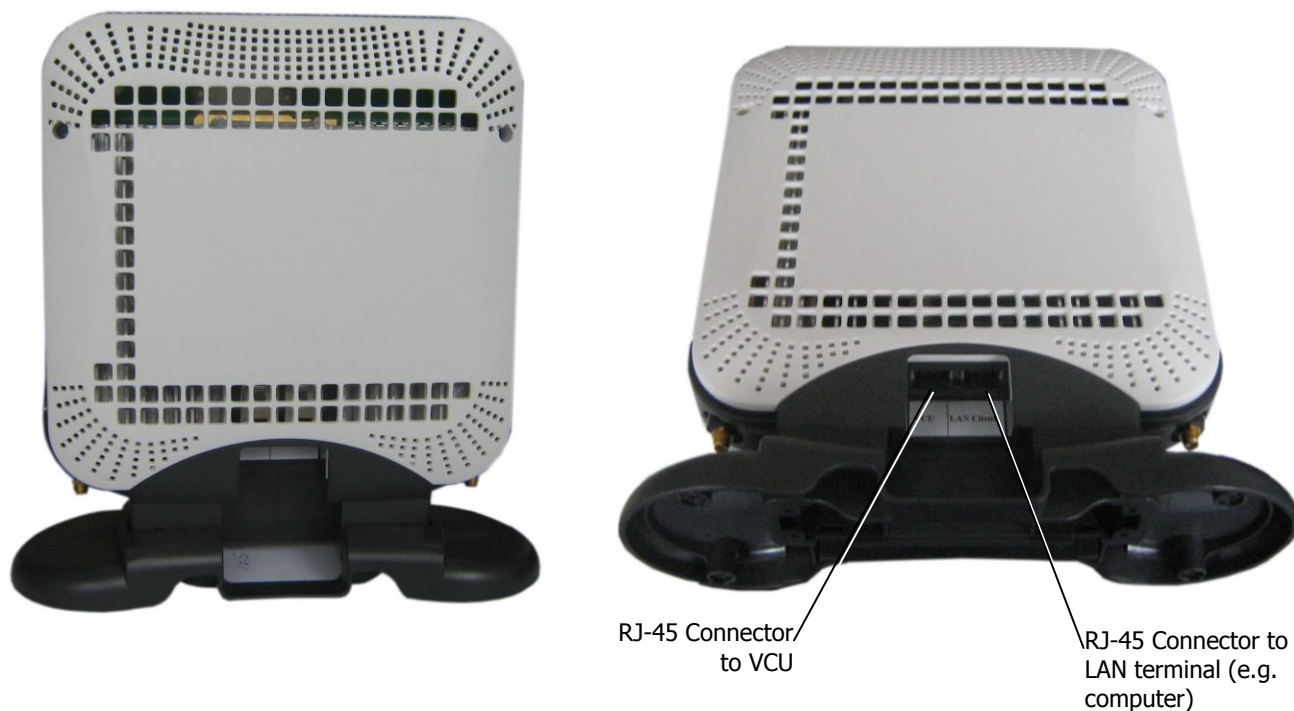


Figure 1-8. VE Access Pod-Rear

1.2.2.1 VAP Antenna Options

Two antenna options are available for VAPs:

- Integral internal antennas
- Connectors that interfaces to external antennas (for special coverage requirements).

By default, the VAP is set to transmit through the integrated internal antennas. To use the external antennas connectors, select the "**External Antenna**" option in **VAP Config-Service RF** tab of the VE Web GUI application (see section 7.3).

1.3 System Monitoring and Management

The MobileAccess**VE** system (Master VCU, Slave VCUs and VAPs) is centrally managed via a single Web connection to the Master VCU.

Note: When locally connecting to a specific Slave VCU, only the VAPs connected to this VCU can be monitored. When connected to the Master VCU, the entire deployment can be monitored.

The basic screen, as illustrated below, is the **Config** tab. It allows the user to view the system topology and setup parameters, the Master and Slave VCUs, and the corresponding Access Pods. The following image shows the VCU Master tabs and the corresponding Alarms pane.

The screenshot shows the MobileAccess VE Web interface. The navigation menu at the top includes Monitor, Config (selected), Events, Set-up, Management, and Help. The main content area is divided into several sections:

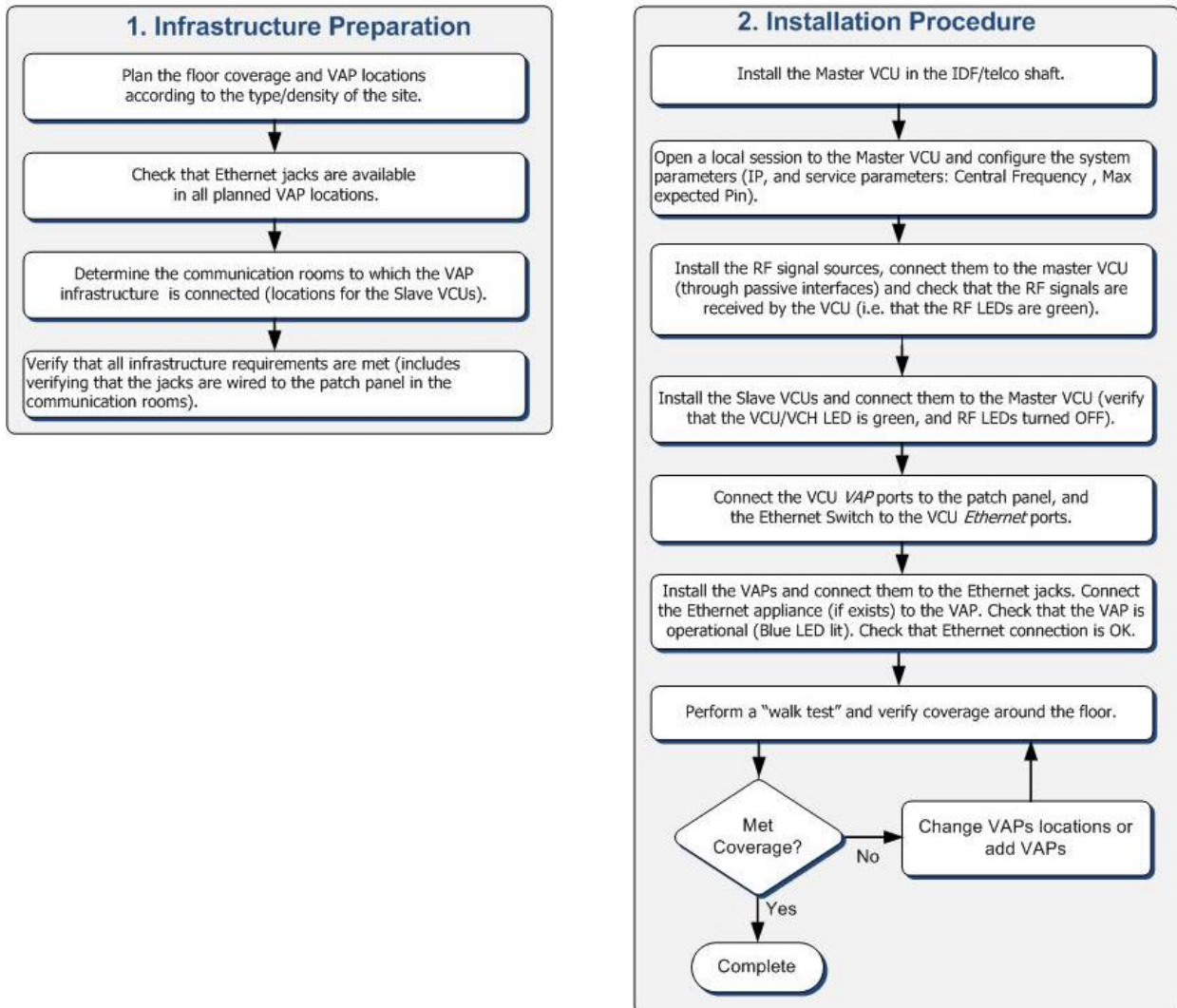
- Left Panel (Tree View):** Lists components under MobileAccess VE WiMAX:
 - (Selected) Master VCU: VCU-M - MasterControl
 - VAPs corresponding to Slave VCU: VAP2 - MeetingRoom, VAP8 - Room-1, VAP9 - Room-2
 - Slave VCU: VCU5 - Floor-2
 - Master VCU RF parameters: VAP5 - ConferenceRoom, VAP11 - Corridor
- Center Panel:** Displays a 3D rendering of a VCU hardware unit.
- Bottom Panel:** Contains three sub-sections:
 - VCU Alarms & Mask:** A list of alarms with checkboxes for masking:
 - VCU Faulty (checked)
 - Over Temperature (checked)
 - Service Off (checked)
 - Channel 1 RF Tx Pwr Low (unchecked)
 - Channel 1 RF Tx Pwr High (checked)
 - Channel 2 RF Tx Pwr Low (unchecked)
 - Channel 2 RF Tx Pwr High (checked)
 - Module Info:** Displays configuration parameters:
 - Type: WiMAX
 - Service Mode: MIMO
 - DL CF: 2520.0 MHz
 - Max Exp Pin: 33 dBm
 - Channel 1 Pin: LOW
 - Channel 2 Pin: LOW
 - Rx System Gain: 0 dB
 - RF Parameters:** (Partially visible, showing similar parameters to Module Info).

1.3.1 Integration with an External Fault Management System

The MobileAccess**VE** system can be seamlessly integrated into any existing Fault Management (FM) system that supports SNMP events. The Master VCU generates SNMP event for each relevant system alarm and forwards this trap to the pre-configured IP address of the external Fault Management system.

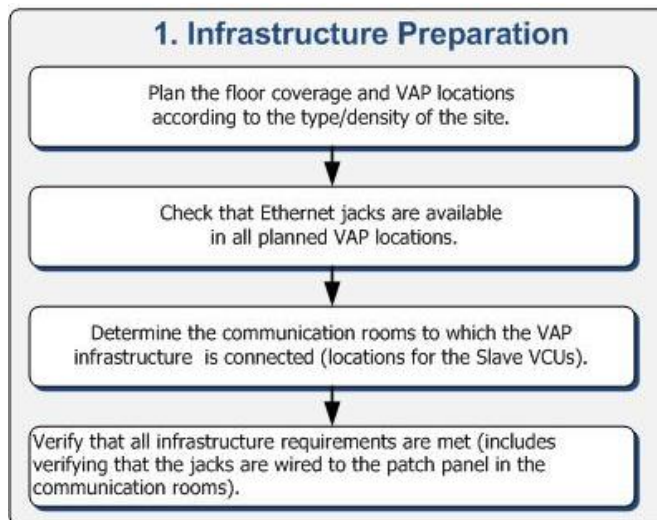
1.4 Overview of the Installation Procedure

The following figure provides an overview of the installation procedure.



2 Infrastructure Requirements and Layout Planning

The following figure shows the flow for the infrastructure preparation.



2.1 Summary of Unit Locations and Connections

- **Service provider's RF equipment** - Macrocell, Microcell, Picocell, Femtocell, BDA, etc. connects to the VCU through a passive interface.
- **VCUs:**
 - **Master VCU** installed at the main IDF/telco cabinet and connected to all VCUs.
 - **Slave VCUs** installed at the IDF/telco cabinet of each covered floor and connected to the Master VCU, the Ethernet switch and the VAPs (through the cabling patch panel).
- **WiMAX service signals from Master VCU to VCUs** – routed through dedicated Ethernet CAT-6 or CAT-7 cabling.
- **WiMAX service signals from VCUs to the VAPs** – routed through existing Ethernet CAT-5e/6 cabling infrastructure.
- **VAP location and mounting** - wall-mounting or desktop-mounting. Connection to existing Ethernet jack (and external antenna if required).
- **VAP power source** - No power connections required. VAPs are power fed from the VCU using PoE (Power over Ethernet) technology.

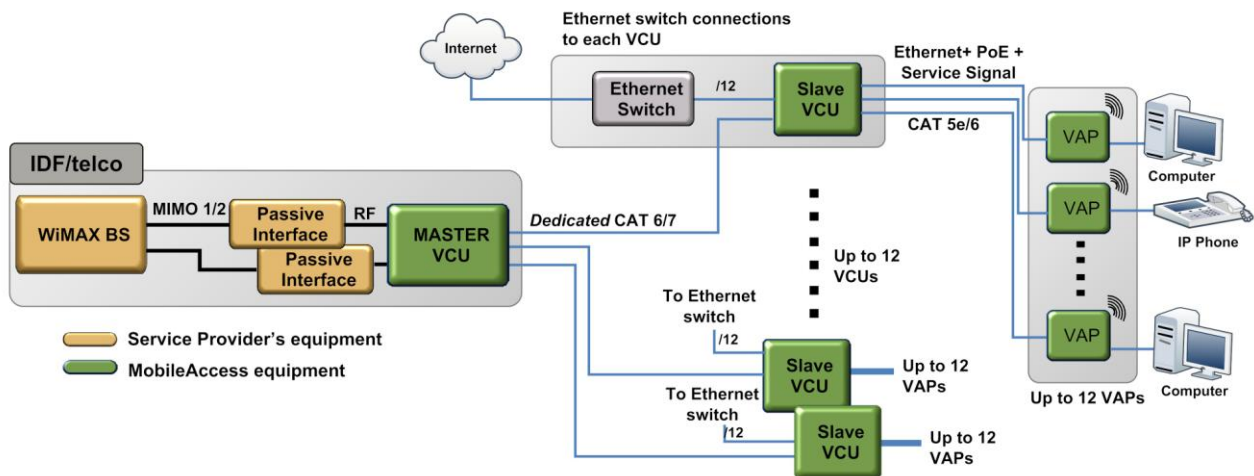


Figure 2-1. WiMAX VE Basic Architecture

2.2 Infrastructure Requirements

Ethernet standards specify that the maximum distance between an Ethernet switch and appliance (computer, WLAN AP etc) shall not exceed 100m (300ft). Therefore, when VE shares the IT LAN, the maximum distance for a given cable run, cannot be longer than 100 meters (300ft) between the Ethernet switch and appliance, including all patch cords (from switch to VCU, from VCU to patch panel, from RJ-45 outlet to VAP, and from VAP to appliance).

Typically the horizontal cabling system will be connected to patch-panels in the communication rooms. The entire cabling system (including the patch panels and patch cords) shall adhere to the CAT-5e (or CAT-6) standard. Specifically all pairs of the CAT-5e cable should be wired in the patch panels (and patch cords).

1. IDF/telco closet space for one VCU (48.3 x 30 x 4.44 cm).

Note: When planning the IDF/telco shaft, take the RF equipment (Picocell/Microcell or BDA) and the VCU in to consideration.

2. 350 Watts of AC power to the VCU IDF/Telco closet.

3. Building infrastructure:

- Category 5e or CAT-6 cabling, Shielded Twisted Pair (STP)
- 24 AWG minimum diameter for CAT-5e cabling
- Dedicated CAT-6/7 STP cable from Master VCU to Slave VCUs with run lengths NOT exceeding 100m (300ft) and not shorter than 10m.

NOTE: in certain deployments the master-slave CAT-6 STP connection may be shared with Ethernet signals - refer to Appendix VE Connections in Central Ethernet Source Topologies for more details

- CAT-5e/6 STP cable from VCU to each VAP with run lengths NOT exceeding 100m (300ft) and not shorter than 10m (33ft). VAPs can be connected over existing CAT-5e/6 cabling infrastructure and existing Ethernet jacks without affecting the LAN.

Note: Verify with the IT department that the existing cables support the VE installation. If available, review the infrastructure documentation to determine cable types and lengths. If the cable information is not available, attempt to visually identify the cable type. Depending on the cable vendor, the cable type may be listed on the cable sheath. It is recommended to use a Fluke cable tester to measure the cable length of the most remote VAPs.

4. Master VCU Cable Connections:

- 2 x N-type female, 50 ohm interfaces to carrier equipment
- Up to 12 x RJ-45 interfaces to Slave VCUs
- 1 x RJ-45 interface to Management
- 1 x D-Type 9 pins RS-232 interface for local craft
- 1 x D-Type 15 pins interface for External Alarms (dry contacts)

5. Slave VCU Cable Connections

- 1 x RJ-45 interface to Master VCU (not used in small single tier deployments)
- 12 x RJ-45 interfaces to VAPs
- 12 x RJ-45 interfaces to Ethernet Switch for LAN service
- (1) RJ-45 connector for switch bypass
- 1 x D-Type 9 pins RS-232 interface for local craft

2.3 Coverage and Installation Planning

Note: The following section provides the information required for planning the VAP installation on a single floor. In a multi-tier installation, this procedure is performed for each individual floor.

The WiMAX coverage area of each VAP is affected by the density and type of environment to be covered. Therefore, it is recommended to determine the location in two phases:

- Plan the *ideal* location of each VAP in order to achieve complete WiMAX coverage of the floor and then
- Select *exact* location according to the location feasibility, where each VAP unit may be mounted on a wall or placed on a desk and an option for an external antenna is available.

The supplied services (WiMAX only or Ethernet and WiMAX) depend on the jack to which the VAP is connected:

- If the jack supports an active Ethernet connection – the VAP will distribute LAN traffic along with the WiMAX service.
- If the jack is not currently active (not connected to an Ethernet switch) - the VAP will distribute only WiMAX.

This section provides information on coverage criteria in various types of environments (Open, Standard, Dense and Combined) and provides rules-of-thumb for various installations of the VAPs.

Note: Section 2.4 provides a detailed example of installation planning in various types of environment. It is recommended to review this example after reading this section.

2.3.1 Types of Environment

This section describes the different types of installation environments and provides guide lines for best coverage of each type of space.

The coverage guidelines in this section are conservative “rule of thumb” estimates of RF coverage per VAP, meant to be used in scenarios in which detailed designs are not performed. When the coverage layout is designed, the coverage per VAP is expected to increase by up to 33%. Coverage estimates in this section assume 25% overlap between the coverage areas of neighboring VAPs to ensure robust, full coverage throughout the enterprise with no “dead zones”.

2.3.1.1 **Open environment**

An environment with minimum of obstacles (such as walls). This type of space can be a large conference or meeting room, cubical areas, lobby or atrium areas.

Table 2-1: Open Environment Installation Distances

Signal Propagation from VAP	64 feet (21 m)
Recommend spacing between VAPs	128 feet (42 m)
Recommended maximum distance of VAPs from outer walls	64 feet (21 m)
Coverage area per VAP	12,750 sqft (1,185 sqm)

2.3.1.2 **Standard Environment**

A traditional office environment with offices, hallways and scattered cubicles.

Table 2-2: Standard Environment Installation Distances

Signal Propagation from VAP	56 feet (19 m)
Recommended Spacing between VAPs	112 feet (38 m)
Recommended Maximum distance of VAPs from outer walls	56 feet (19 m)
Coverage area per VAP	9,900 sqft (920 sqm)

2.3.1.3 **Dense Environment**

A dense environment consists of a relatively large amount of walls, offices, equipment, tall file cabinets, bookshelves and other items that could potentially impact the wireless signal.

Examples for this type of environment are dense offices, hospitals and manufacturing spaces.

Table 2-3: Standard Environment Installation Distances

Signal Propagation from VAP	41 feet (13.5 m)
Recommended Spacing between VAPs	82 feet (27 m)
Recommended Maximum distance of VAPs from outer walls	41 feet (13.5 m)
Coverage area per VAP	5,300 sqft (495 sqm)

2.3.1.4 **Combination of Environments**

In areas with combinations of environments of various densities, place the VAPs on the border between the different types of areas – closer to the denser area.

For example, in a cubical area with the outside wall having offices, simply locate the VAPs a little *closer to the outside offices* to provide coverage through the office walls. (See VAPs 11 and 13 in the floor plan map in section 2.4.3.)

To ensure maximal coverage, VAPs can be re-located or added. If a coverage gap is detected, the VAPs can be re-located until the coverage gaps are filled.

2.4 Planning VAP Layout

This section describes the steps for planning the VAPs along the covered floor. An example of planning map is attached at the end of this section.

Note: It is highly recommended to use a floor plan when planning the VAPs locations.

2.4.1 RF Coverage Factors

It is important to note the type of factors that can severely impact RF coverage which should be avoided:

- **Metallic structures** such as elevators, high file cabinets and some moveable metallic partitions severely degrade RF signal and all efforts should be made to locate VAPs in front of or above metallic objects (desks, filing cabinets) to allow the signal to propagate.
- **Wall materials** such as concrete, tile and cinderblock along with bathroom fixtures typically have fairly high signal attenuation and should be considered as dense spaces.
- **Types of glass** (typically exterior or mirrored) that have metallic coatings on it which can affect RF coverage, however that is typically not encountered inside a building.

2.4.2 Mapping Locations

To map the VAP Locations

1. Map out the available Ethernet jack locations: mark all the CAT-5e/6 drops locations on the floor plan map.

TIP: The size and number of the ceiling tiles can be used to measure distances.

2. Using the floor plan and the VAPs coverage guidelines (as given in 2.4.3), mark the approximate location of each VAP in the facility.
VAPs may be added (or removed) at anytime for optimal coverage.
3. For each jack to be used for connecting a VAP, check if the jack is already connected to the Ethernet switch (via the patch panel). Record the connections for each jack, for reference.
4. Connect the Ethernet cables corresponding to the selected jacks according to section 3.4.1.
5. It is also recommended to check the area in which the VAPs are to be installed and make sure that the installation is feasible.

2.4.3 Connecting Directional Antennas

Each VAP has an integrated internal antenna that provides isotropic radiation as well as two interfaces for external antennas which enable connecting directional antennas to VAPs installed near outer walls in order to prevent interference. It is then required to configure the VAP to operate with the external antennas – see section 7.3.

2.4.4 Installation Plan Example

The Following figure shows a floor plan map with all required marks:

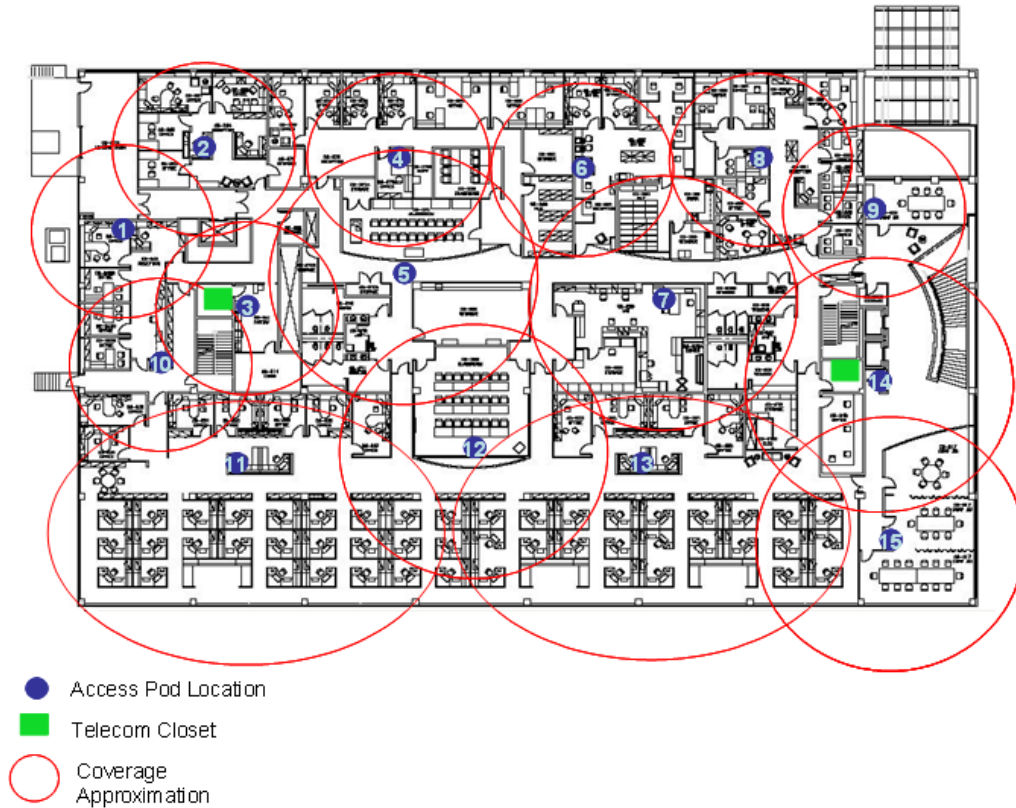


Figure 2-2. Floor Plan Example

Notes:

- The red VAP coverage circles are approximately 41, 56 and 64 foot (13.5, 19 and 21 m) radius for the small, medium and large circles respectively (drew according to the guidelines given in section 2.3.1).
- VAP 3 is surrounded by dense objects, the bathroom and stairwell which would reduce coverage in that area by the other VAPs.
- VAP 5 is an example of a unit that provides good coverage down the hallways.
- VAPs 11 and 13 are placed closer to the offices to cover them well but on the open side will actually cover a much greater area which is why the coverage is larger and shown here more as an oval than a circle.
- The area between VAPs 7 and 14 outside the bathrooms and stairwell on either side of that area. If after the system installed, this area is still a little low on coverage, a VAP can be added, but it may also be covered by VAP 14.

Note: The plan can be modified at any time by moving the units around or by adding units.

The following figure depicts an actual measured quantified coverage of a floor area planned according to the above rules

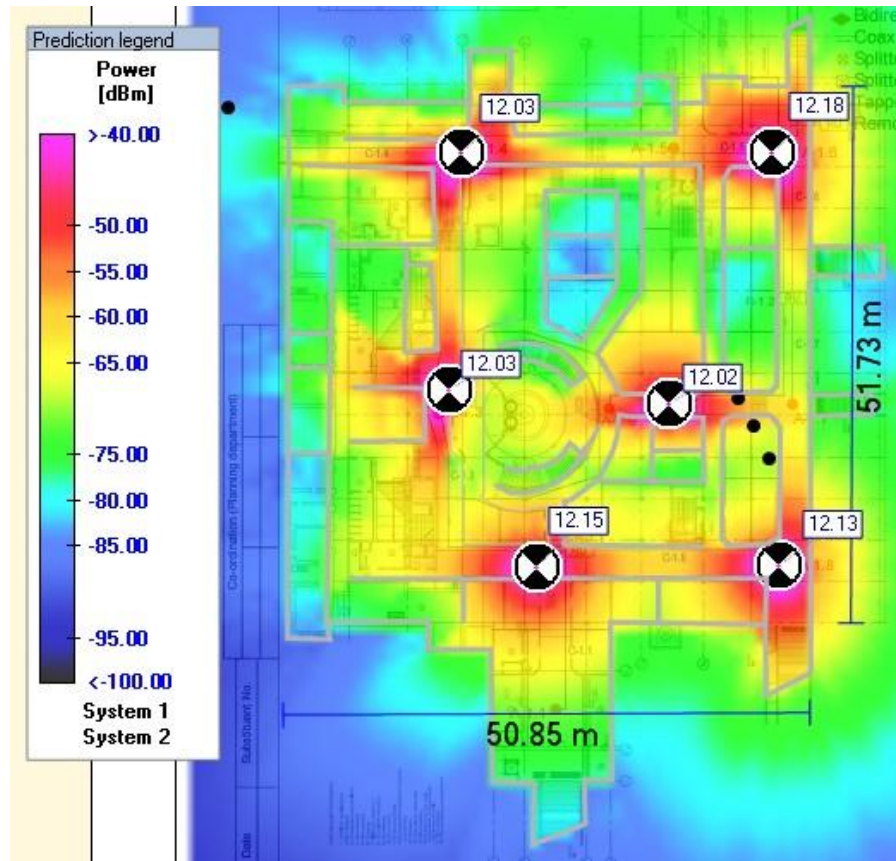
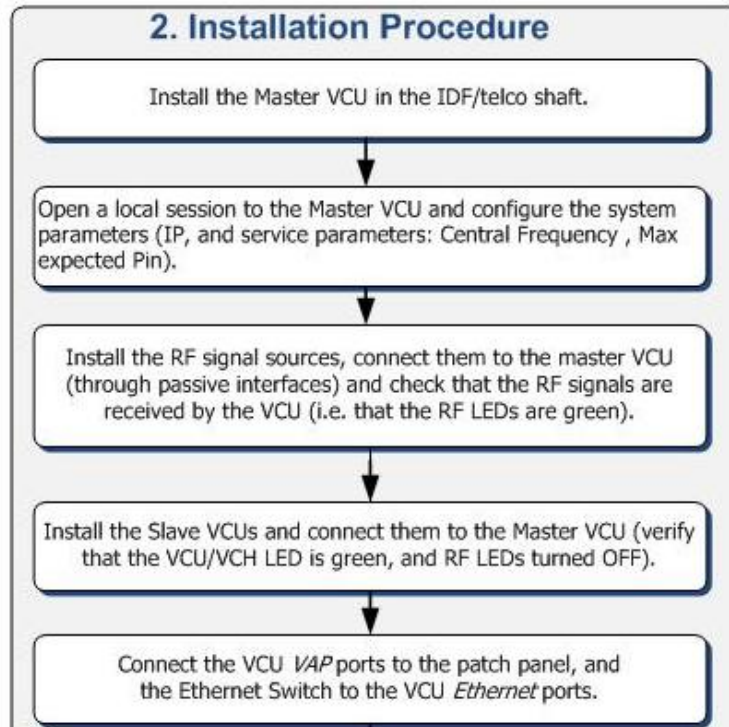


Figure 2-3. Distributed VAPs propagation, 12dBm output power at 1.8GHz.

3 VCU Unit Installation and Configuration

This section describes the installation and configuration procedures of the VE Control Unit (VCU). These should be performed only after planning the floor coverage and installation locations as described in section 2.3.





The following figure summarizes the main steps of the installation procedure:



3.1 Installation Kit Contents

The MobileAccess**VE** Single Tier Solution VCU kit includes:

Table 3-1: VCU Kit

Description	UNIT
WiMAX VE Control Unit (VCU) Kit (including brackets for securing the VCU to 19" rack)	
Power cord	
VE SW CD	
Local configuration cable (crossed RJ-45 cable)	

3.2 Installing Master VCU

The VE control unit can be installed as a Master VCU and control up to 12 Slave VCUs. The Master VCU is installed in the main IDF/telco closet. This section describes the Master VCU installation procedure.

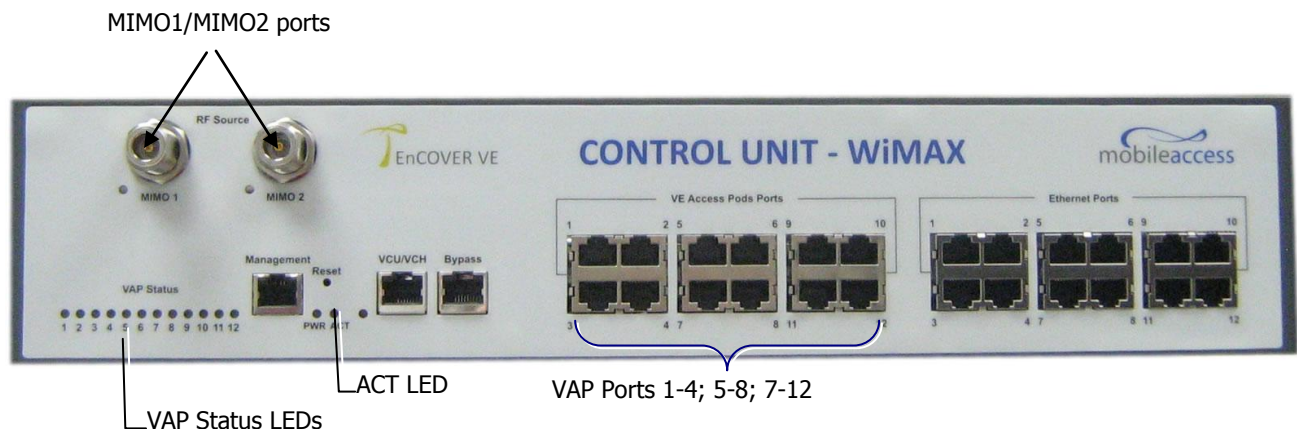
1. Install the **Master VCU** in the main IDF/Telco closet. The Master VCU can be installed in the rack (placed on a shelf or secured using supplied bracket) in the IDF closet along with the provider's signal sources.
2. Apply power to the Master VCU and verify that the **PWR** LED is lit. Also verify that the unit **ACT** LED completes initialization (blinking light) and shows a solid green light.
3. Connect (or request the service provider's service personnel to connect) the provider's **signal source** (Macrocell, Microcell, Picocell or BDA) through passive interface to the **Master VCU front panel RF ports** (MIMO1 and MIMO2).

Note: In SISO service mode, only the **MIMO 1** RF port is relevant.

Power on the signal sources.

Note: The RF Source LED (see following figure) of the connected port on the Master VCU should be lit GREEN, indicating that the Master VCU senses the RF signal from the source at the expected level (according to Max Expected Pin). In case the LED remains RED after connecting the capacity source, verify that Max Expected Pin is configured properly and that the service is enabled.

4. Connect the **Master VCU VAP ports** to the **Slave VCUs VCU/VCH** ports via the patch-panel that feeds the dedicated CAT-6 or 7 cabling system.



NOTE: After the Slave VCUs are connected, verify that that the Master VCU **VAP Status** LEDs, corresponding to the connected Slave VCUs, complete initialization (blinking light) and show a solid green light.

3.3 Auxiliary Alarm Output Connections

The auxiliary connections are performed through the Master VCU rear panel **Alarms** port. See following figure.



The controller can provide Major and Minor output alarms. These alarms can be connected directly to the auxiliary input of the Base Station, or to any other dry-contact application.

A Major alarm is generated when there is an alarm condition in one (or more) VCU's while a Minor alarm is generated when there is an alarm condition in one (or more) of the VAPs.

Note: If only one alarm is required (Minor or Major) an external connection of a wire jumper between pins 8 and 13 is necessary (normally closed).

Connect the relevant alarms according to the connector pinout below.

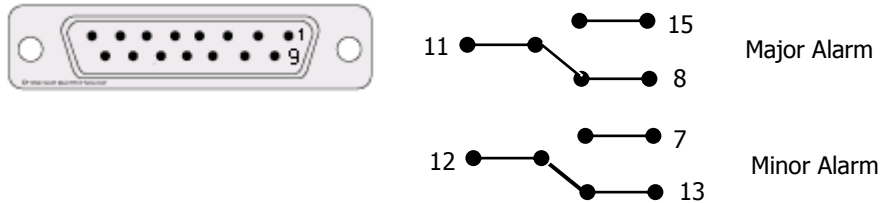


Table 2. Alarms Connector – used pins

8 – Major Error signal (normally closed)	7 – Minor Error signal (normally open)
11 – Major COM	12 – Minor COM
15 –Major Error signal (normally open)	13 – Minor Error signal (normally closed)

3.4 Installing Slave VCU

1. Install the Slave VE Control Unit (VCU) in the IDF/Telco closet corresponding to the floor to be covered. The Slave VCU can be installed in the rack using the supplied bracket in the IDF closet.

Apply power to the Slave VCUs and verify that the VCU **PWR** LED is lit and that the unit **ACT** LED completes initialization (solid light) and shows a blinking green light. See Figure 3-1.

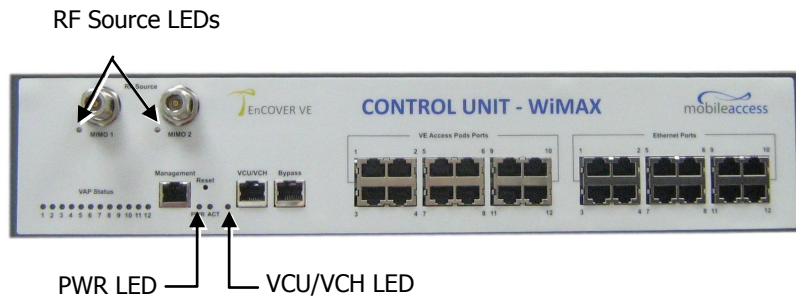


Figure 3-1. VCU PWR, RF and VCU/VCH LEDs

2. Connect the Slave VCU front panel **VCU/VCH** port to the Master VCU **VAP** port via the patch panel using dedicated CAT6 cables and verify that the VCU/VCH LED completes initialization (blinking light) and shows a solid green light. The RF LEDs (of both MIMOs) should turn OFF.

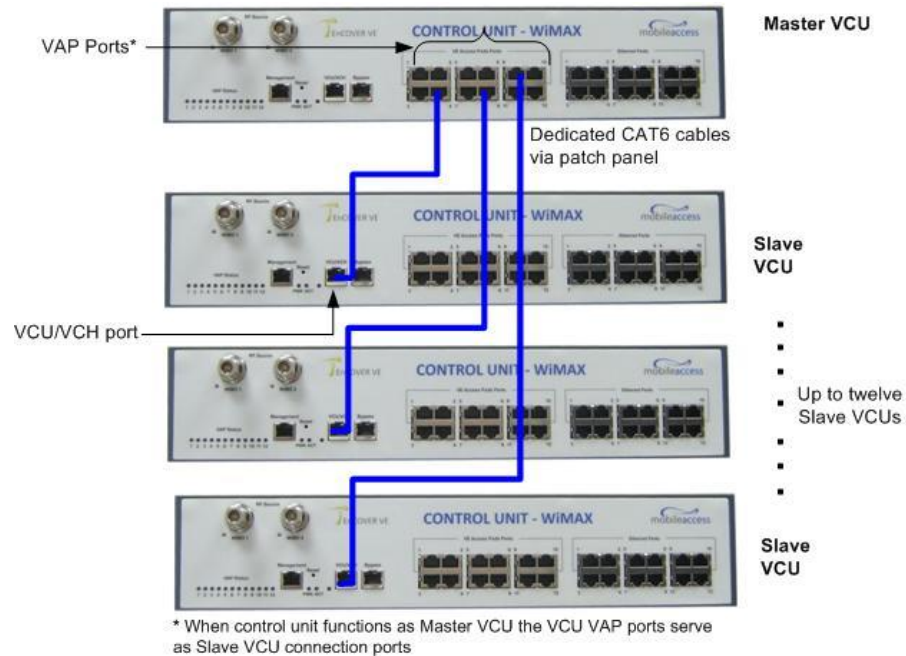
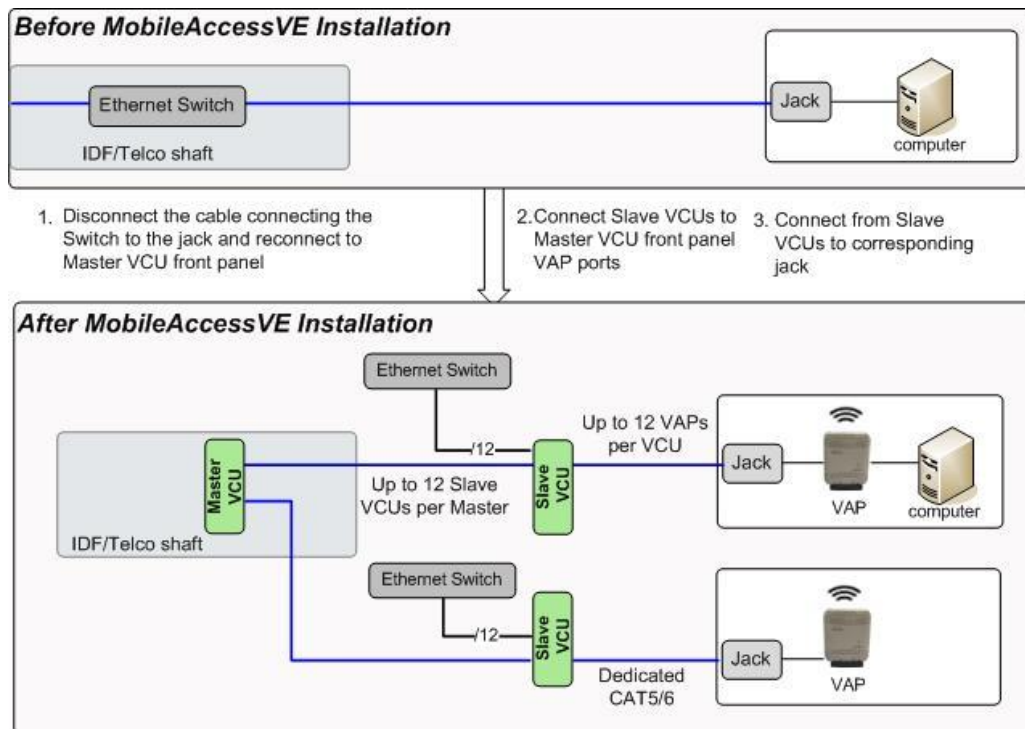


Figure 3-2. Master and Slave VCU Connections

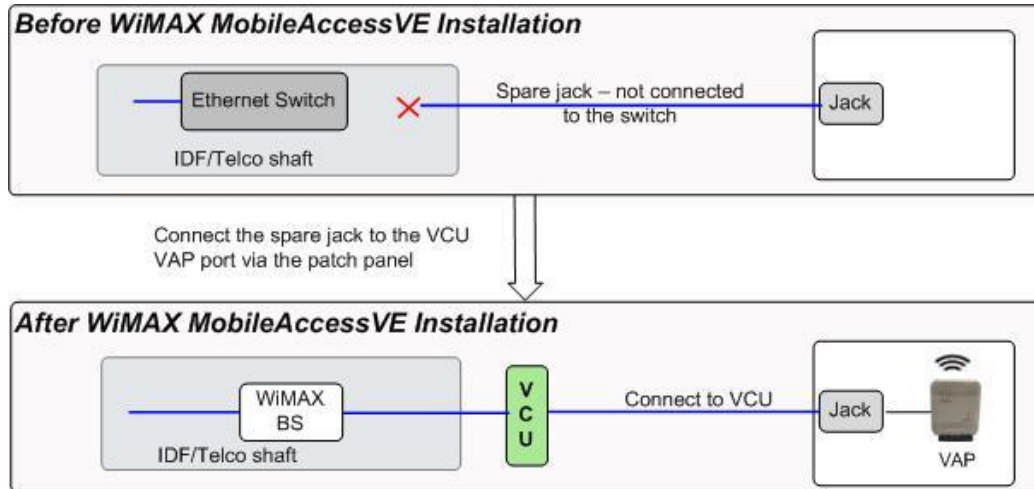
3. Connect the Slave VCU **VAP** ports to the patch-panel that feeds the existing structured CAT-5e/6 cabling system.
4. According to VAPs layout plan (as explained in section 2.4.2) connect the Ethernet switch cables (see section 3.4 for more detailed explanation):
 - If the jack to be used is already in use (connected to Ethernet switch) – disconnect it from the Ethernet switch and re-connect it to the corresponding **Ethernet** port in the Slave VCU front panel.
 - Jacks not in use will be connected only to the Slave VCU.

3.4.1 Connecting VAP Ethernet Cables

For VAPs installed on currently ACTIVE Ethernet ports - shift the relevant Ethernet LAN connections as follows.



For VAPs installed on currently INACTIVE Ethernet ports – connect as follows.



NOTE: After the Slave VCUs are installed, and connected to the right ports in the patch panels, you can proceed with VAP installation as described in chapter 4 . However it is recommended to first complete the VCU provisioning (see section 3.5) so that when installing the VAPs they will instantly provide the wireless service (and the installer will be able to check the coverage).

3.4.2 Operation with LAN utilizing Power over Ethernet (PoE)

Power over Ethernet (PoE) is a technology that enables passing electrical power over the Ethernet cabling. Power can either come from a PoE-enabled Ethernet device (e.g. switch) or from a "mid-span" device built for "injecting" power into the Ethernet cabling.

PoE can operate over two different pairs in a CAT-5e/6 cable - these two methods are referred to as 'alternative a' and 'alternative b'. All PoE compatible appliances such as WLAN APs and IP Phones support both alternatives and automatically detect and use the power on the appropriate pairs (alternative a or b).

MobileAccessVE supports sharing LAN infrastructure that use either 802.3af PoE or 802.3at PoE. Both alternative a or b are seamlessly supported through the VE system.

3.5 Provisioning the Master VCU

This section describes how to set the basic parameters required for operation and remote management of the Master VCU using the Web GUI. The configuration dialogs are fully described in Chapter 5 .

The Master or Slave mode is automatically detected according to the VCU's physical connection. If a connection to another VCU is detected the VCU will be identified as a Slave; otherwise it will assume the role of a Master.

Notes:

The initial configuration of the Master VCU is performed via local connection (using a cross-cable and connecting to VCU's default IP address). After performing the initial configuration and assigning the Master VCU an IP, the system can be connected, monitored and configured via a remote management connection.

The configuration and management of all of the system units (VCUs and VAPs) is performed via the Master VCU unit (local or remote connection).

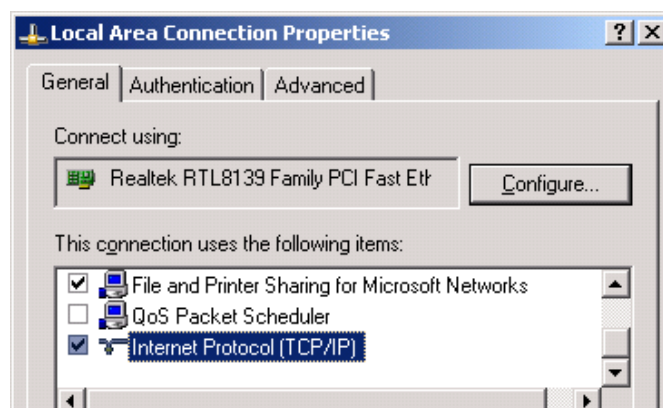
3.5.1 Configuring the Computer IP Parameters

Configure the computer local LAN connection to operate in the same subnet as the default VCU IP address. Note that the procedure may vary slightly depending on the operating system installed on your computer. The following procedure is for Windows XP.

To configure the computer's IP parameters:

1. Click the **Start** menu and choose **Control Panel**.
2. In the **Control Panel**, click **Network and Internet Connections**.
3. Click **Network Connections** and then double-click **Local Area Connection**.

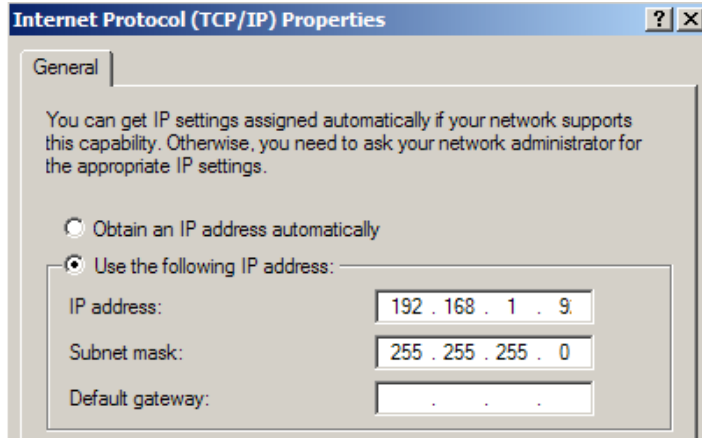
The Local Area Connections Properties dialog appears with the General tab displayed by default.



4. In the Items list, select "Internet Protocol (TCP*IP)" and click the Properties button.
5. The "Internet Protocol (TCP/IP) Properties" dialog appears.

NOTE: The Master VCU is supplied with the default IP address 192.168.1.1.

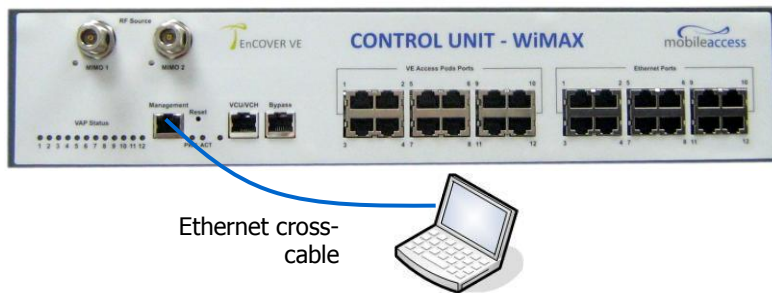
- In order to communicate with the unit, it is necessary to assign your computer a *Static IP* address in the same subnet: 192.168.1.2 to 192.168.1.250.
(i.e. 192.168.1.9 as shown in the example).
- Define the subnet mask as shown: 255.255.255.0



6. Click **OK**.
7. The computer communication parameters are now defined and you can open a session to the Master VCU and provision the unit.

3.5.2 Login

1. Perform a local connection to the Master VCU unit by connecting the Master VCU front panel **Management** port and a laptop computer.



- Open a web browser and type the Master VCU IP address in the address bar (default: 192.168.1.1).



The Login window appears.



- Type the **User Name "engineer"** and enter the **Password "eng"**.

The MobileAccessVE Web GUI appears.

 A screenshot of the MobileAccessVE Web GUI. The interface is blue-themed. At the top is a "Main menu bar" with icons for Monitor, Config, Events, Set-up, Management, and Help, along with a "Log Out" button. On the left is a "Network Topology tree" listing various VCU and VAP components. The main content area shows a 3D rendering of a VCU unit. Below the rendering are two panels: "VCU Alarms & Mask" with a list of status indicators and checkboxes, and "Module Info" with fields for Name, Serial Number, Product Revision, SW Active Version, and SW Inactive Version, along with "Restart VCU" and "Identify" buttons.

Main menu bar

Network Topology tree

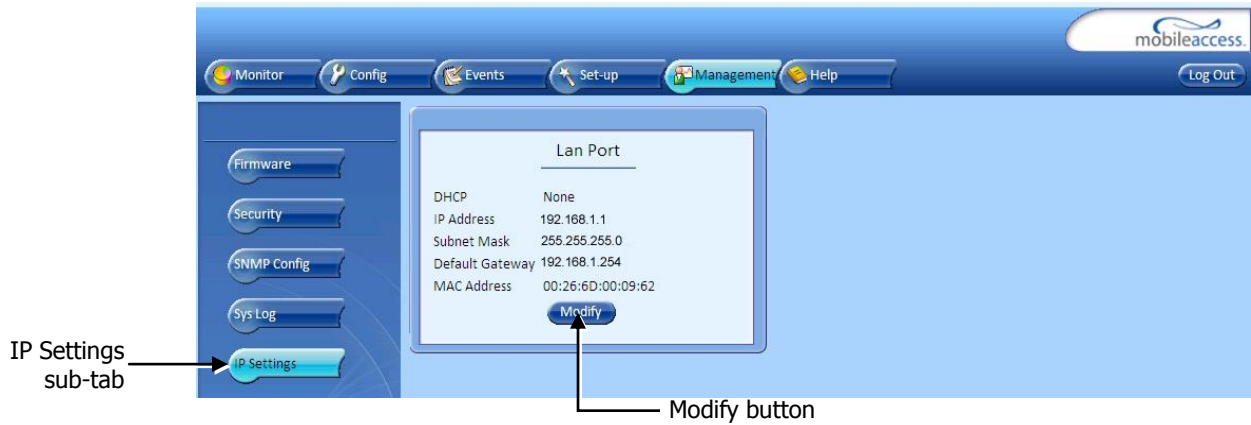
Sub-tabs that correspond to each main tab

VCU Alarms & Mask	
<input checked="" type="checkbox"/>	VCU Faulty
<input checked="" type="checkbox"/>	Over Temperature
<input checked="" type="checkbox"/>	Service Off
<input type="checkbox"/>	Channel 1 RF Tx Pwr Low
<input checked="" type="checkbox"/>	Channel 1 RF Tx Pwr High
<input type="checkbox"/>	Channel 2 RF Tx Pwr Low
<input checked="" type="checkbox"/>	Channel 2 RF Tx Pwr High
Overall Status <input checked="" type="checkbox"/>	

Module Info		RF Parameters	
Name	MasterControl	Date:	17/Feb/10
Serial Number	FFFFFFFF	Time:	10:30:28
Product Revision	N/A	<input type="button" value="Modify"/>	
SW Active Version	0.7		
SW Inactive Version	N/A		
Restart VCU	<input type="button" value="Restart"/>		
Identify	OFF		

3.5.3 IP Settings

1. In the invoked application window, choose the **Management** tab in the main menu bar and click the **IP Settings** tab on the side bar.



Note: See section 5.3.2 for a description of the Management tab.

2. Click the **Modify** button to define the STATIC **IP Address** according to existing LAN.

Note: After the initial IP configuration, the Master VCU can be accessed remotely via Ethernet.



- Set the Static IP address parameter (DHCP is not currently available)
Default definitions:
The Default IP Address : 192.168.1.1
The Default Subnet Mask: 255.255.255.0
The Default Gateway: 192.168.1.254
 - Click **OK**.
3. Log out and then log in again with the new IP settings.

3.5.4 Assigning Identifying Information

1. Select the **Config** tab in the main menu bar.

Note: See section 5.3 for a complete description of the **Config** tab.

2. The Master VCU appears in the Network Topology Tree as **VCU-M**. Select the Master VCU by clicking on it.

The screenshot shows the MobileAccess VE WIMAX configuration interface. The 'Config' tab is selected in the main menu bar. The Network Topology Tree on the left shows 'VCU-M - MasterControl' selected. The main area displays a 3D model of the VCU unit. The 'Module Info' sub-tab is active, showing a list of status indicators (VCU Faulty, Over Temperature, Service Off, etc.) and a 'Module Info' panel with fields for Name (MasterControl), Serial Number (FFFFFFFF), Product Revision (N/A), SW Active Version (0.7), and SW Inactive Version (N/A). A 'Modify' button is visible next to the Name field.

3. Before configuring the Master VCU it is recommended to give the unit an indicative name. To assign the Master VCU an indicative name:

- Select the **Module Info Tab** and click the **Name Modify** button.

The close-up screenshot shows the 'Module Info' panel. The 'Name' field is set to 'MasterControl' and has a 'Modify' button next to it. The 'Date' is 17/Feb/10 and the 'Time' is 10:30:28. A 'Click Modify' label points to the 'Modify' button next to the Name field.

- Type the unit name (up to 17 alpha-numeric characters) in the **Controller Name** dialog and click **OK**.



3.5.5 Setting RF Parameters

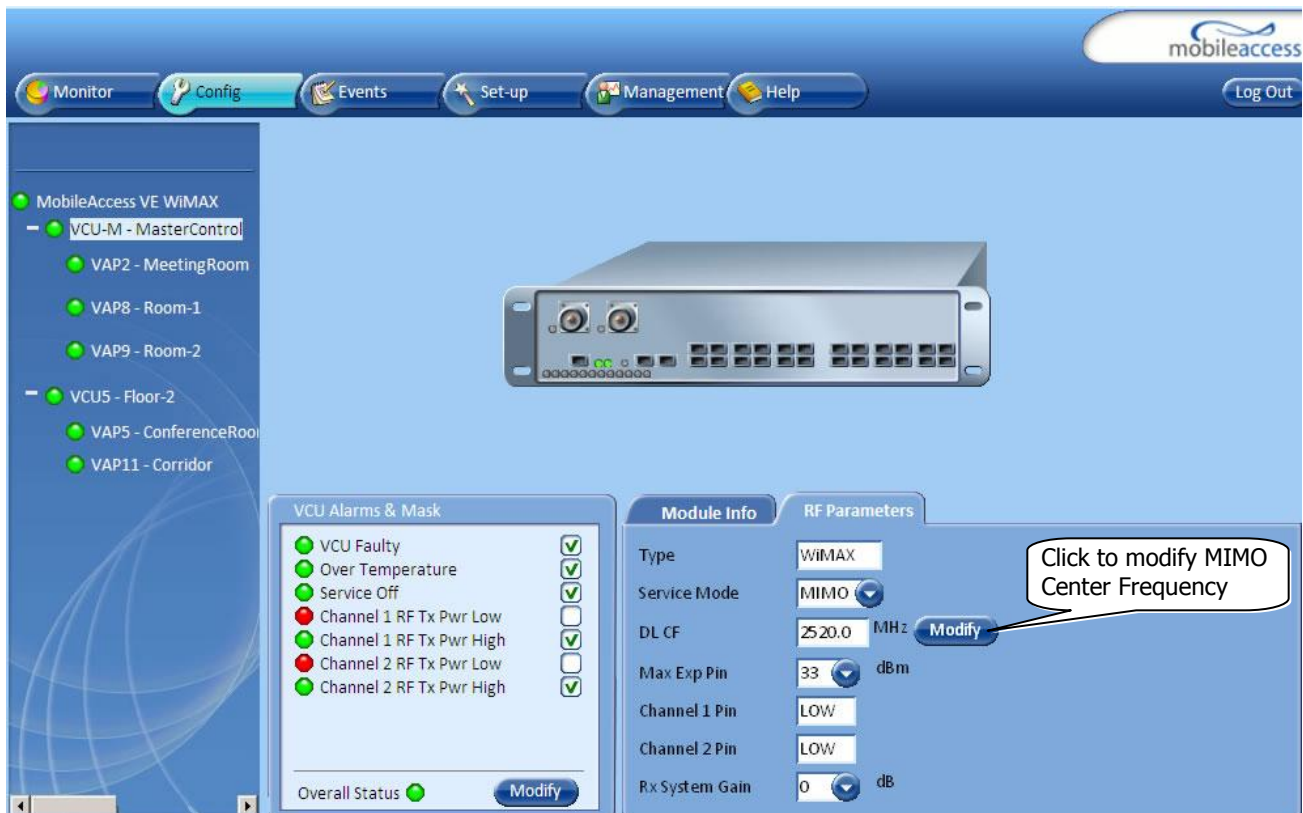
In a Master-Slave mode (multi-tier architecture) the RF parameters are only configured for the Master VCU unit.

Set the RF parameters according to the BS transmission configuration (MIMO or SISO). Each type of configuration is defined through a dedicated tab.

This section describes the MIMO and the SISO configuration procedures.

To configure the MIMO RF parameters:

1. Select the Master VCU in the topology tree and then select the **RF Parameters** tab. Verify that the **Service Mode** parameter is defined as **MIMO**.



- Click the **DL CF Modify** button. Enter the Base Station central frequency and click **OK**.

Note: The MIMO DL CF parameter defines the same DL central frequency for Channel 1 and Channel 2.

- Define Max expected power of BS (0-33dBm).
- Define Rx System Gain (-15 to 5dB)

Notes:

Max expected Pin and DL CF parameters can be obtained from your service provider.

The remaining parameters are predefined to their default values. (Service Bandwidth is set to 10MHz per channel).

Any updates of the service definition (DL CF or Service Mode) are sent to all connected VAPs.

To configure the SISO RF parameters:

Note: The RF tab is displayed for MIMO by default.

- Select the Master VCU in the topology tree and select the **SISO** option in the **Service Mode** drop-down list. The RF parameters tab will display the SISO RF parameters.

Service Mode
drop-down list

- Click the **DL CF Modify** button and enter the Base Station central frequency. Click **OK**.

3. Define Max expected power of BS (0-33dBm).
4. Define Rx System Gain (-15 to 5dB)

Notes:

Max expected Pin and SISO DL CF parameters can be obtained from your service provider.

The remaining parameters are predefined to their default values. (Service Bandwidth is set to 10MHz).

Any updates of the service definition (DL CF or Service Mode) are sent to all connected VAPs.

3.5.6 Verifying System Operation

To verify proper operation of the system, refer to the **VCU Alarms and Mask** sub-tab (in the Config tab). The following figure illustrates the MIMO alarms.

Note: SISO alarms are similar, however only **Channel 1** alarms appear.

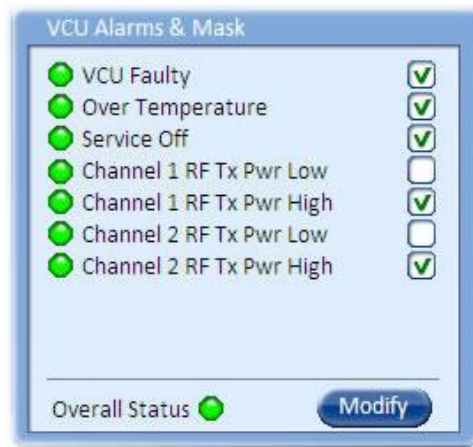


Figure 3-3. VCU MIMO Alarms

1. Verify that all the alarms are GREEN.

Note: In the SISO Alarms dialog (Figure 4-3) only **Channel 1** alarms appear.

2. Mask irrelevant alarm conditions to avoid affecting the overall status of the unit.

Refer to the alarm descriptions in the table following the figure below.

Note: When SISO service is used only the Channel 1 alarms are relevant.

Alarm	Description
VCU Faulty	RED - VCU fault. Remove and re-apply power to VCU. If problem persists, replace VCU.
Over Temperature	Temperature of unit exceeds normal range.
Service Off	User has disabled the service.
Channel 1 RF Tx Pwr Low	RED - DL RF Power is lower by 15dBm (or more) from the Max Expected Pin, or lower than -3dBm.
Channel 1 RF Tx Pwr High	RED - the input power exceeds the maximum expected Pin by more than 3 dB.
Channel 2 RF Tx Pwr Low	RED - DL RF Power is lower by 15dB (or more) from the Max Expected Pin, or lower than -3dBm.
Channel 2 RF Tx Pwr High	RED - the input power exceeds the maximum expected Pin by more than 3 dB.
Overall Status	Indicates Fault (RED) level or GREEN if there are no faults.

Note: To briefly check the VCU status, click on the VCU name in the Topology Tree. The VCU icon will appear, showing the LEDs status.

The screenshot displays the MobileAccess VE WiMAX management interface. On the left, a 'Topology Tree' lists various VCU units, with 'VCU-M - MasterControl' selected. An arrow points to this entry with the text 'Click VCU Master'. The main area shows a 3D model of the VCU hardware. Below the model, there are two panels: 'VCU Alarms & Mask' and 'Module Info / RF Parameters'. The 'VCU Alarms & Mask' panel shows a list of alarms with checkboxes for enabling or disabling them. The 'Module Info / RF Parameters' panel displays details for the 'MasterControl' unit, including its name, serial number, product revision, software versions, and a 'Restart VCU' button. The overall status is shown as green.

Example of Alarm Mask (Disabling)

NOTE: Tx signal refers to the DL signal from the BS side towards the remote units (VAPs).

In the example below "Channel 2 RF Tx Pwr High" alarm is masked (disabled) – this is the alarm for the DL signal (from the BS side).

The left dialog shows the alarm response when MIMO2 Tx RF Pwr High alarm is enabled and a fault corresponding to that alarm is detected. (MIMO2 Tx RF Power exceeds the defined range). The Overall Status will be RED indicating a fault.

The right dialog shows the alarm response when MIMO2 Tx RF Pwr High alarm is disabled (MASKED). The MIMO2 Tx RF Pwr High LED be RED; but, the Overall Status will be GREEN – showing NO Fault.

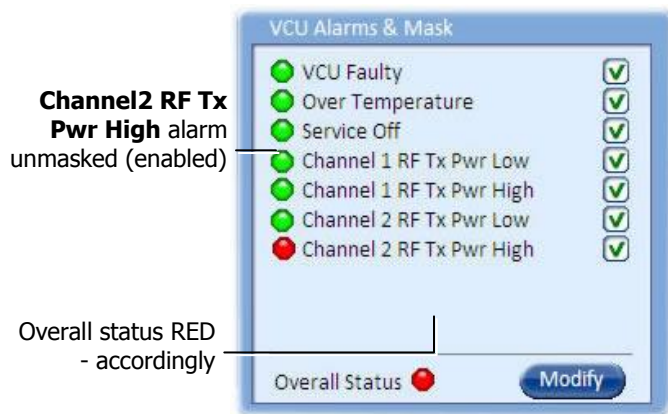


Figure 3-4. Enabled alarm showing fault

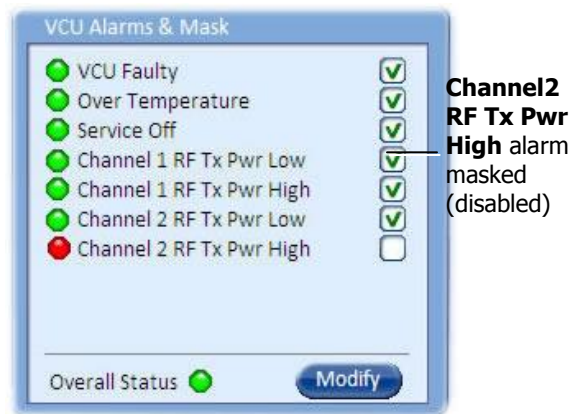


Figure 3-5. Disabled alarm showing fault

3.6 Assigning the Slave VCU an Identifiable Name

The Slave VCU RF parameters are automatically configured according to the Master VCU definitions; there is no need to configure the RF parameters individually for each connected Slave VCU. It is recommended to assign each Slave VCU an indicative name.

The Slave VCU options are accessed performed through a remote connection to the Master VCU, via the web management.

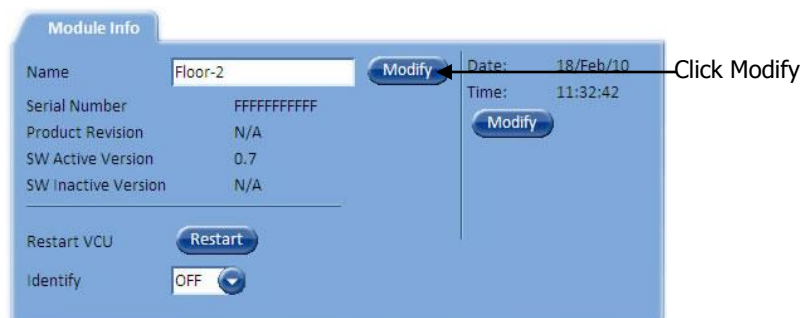
To assign a name to a Slave VCU:

1. Connect to the Master VCU unit (either locally as explained in section 3.5.1 or remotely) and select the Slave VCU to be provisioned from the Network Topology Tree.



Each VCU has a default name of the form "VCUPx-name", where:

- **Px** - Master VCU port number to which the Slave VCU is connected
 - **Name** - user-defined name
2. To assign the Slave VCU an indicative name:
 - Select the **Module Info Tab**
 - Click the **Name Modify** button



- Type the unit name (up to 17 alpha-numeric characters) and click **OK**.

4 VAP Installation and Provisioning

This section provides a description of the VE Access Pods (VAPs) installation and verification of normal VAP operation. The VAPs are designed for plug-and-play installation.

The only required configuration is for VAPs to which external antennas are connected since by default, VAPs are provided to operate with their internal antennas.

4.1 VAP Installation






The VAPs installation procedure consists of connecting each VAP to the Ethernet jack in the appropriate location to provide optimal coverage (see sections 2.3 and 4.1.2).

4.1.1 VAP Kit Contents

The WiMAX VE Access Pod (VAP) kit includes:

Note: VAPs are provided with two mounting options: desk-mount and wall-mount

Table 3: VAP Kit

Kit Items	UNIT
VE Access Pod (VAPs)	
Wall-mount adaptor (with double sided sticky tape located on rear for fast installation)	 <p style="text-align: center;">Front Rear – showing tape</p>
Desk-mount adaptor	
8 screws: <ul style="list-style-type: none"> ○ 4 short screws – for securing adaptor to pod ○ 4 longer screws – for securing wall-mount adaptor to the wall (“anti-theft” installation) 	 <p style="text-align: center;">Long screws Short screws</p>
RJ-45 jumper cable	

4.1.2 VAP Locations and Mounting

It is recommended to place the VAPs on top of desks, cube walls, filing cabinets or higher on walls so as to maximize the provided coverage per VAP.

Note: Mounting a VAP beneath a desk or other low location (e.g office corner) decreases the effective coverage of the VAP and therefore a higher number of VAPs would be required to cover the same area.

When installing the VAPs, consider the following:

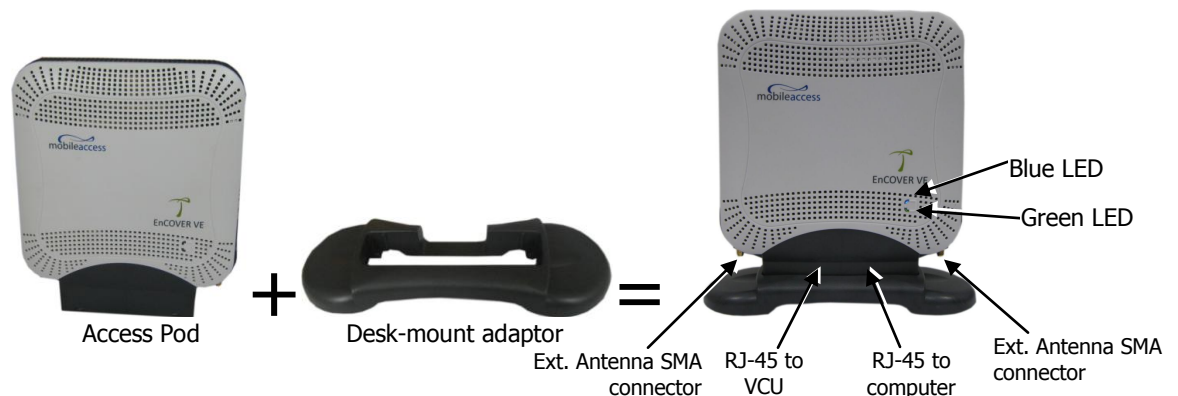
- Placing the units (whenever possible), in an open area
- Availability of CAT-5e/6 infrastructure
- The VAPs plug into standard (RJ-45) Ethernet connection jacks.
- If the jack to be used is already connected to Ethernet switch. For more information see 2.4.2 and 3.4.
- Aesthetics of the VAP location

4.1.2.1 Desk Mount

- Place the VAP on the Desk-mount
- Secure the Desk-mount adaptor to the VE Access Pod using the four supplied short screws.
- Connect the RJ-45 jumper cable (CAT-5e/6) to the VAP's RJ-45 connector to be connected to the VCU (the adaptor, screws and cable are included in the VAP kit).
- Place the VAP on a flat surface according to the planned location
 Plug the other side of the cable into standard (RJ-45) Ethernet connection jack of the cable which is routed to the VCU.
- When using an external antenna, connect the **Ext. Antenna** SMA connector(s) to the external antenna(s). This option must be SW configured via the web GUI (internal antenna is enabled by default).

Note: The maximum external antenna gain should not exceed 10 dBi.

- Verify that the VAP receives power and connects to the VCU via the LEDs on the unit (both the GREEN LED and the BLUE LED should be lit).



4.1.2.2 Wall Mount

Assemble the VAP to the wall-mount (the adaptor with sticky tape and wall mount screws and cable are included in the VAP kit as described in Table 3: VAP Kit)

- Attach the VAP to the wall according to the planned location using supplied screws (for “anti-theft” installation) or the double sided sticky tape for the wall-mount adaptor located on the rear (for “plug-and-play” installation)
- Plug the other side of the cable into the adjacent standard (RJ-45) Ethernet connection jack.
- When using an external antenna, connect the Ext. Antenna SMA connector(s) to the external antenna(s). **This option must be SW configured via the web GUI** (internal antenna is enabled by default).

Note: The maximum external antenna gain should not exceed 10 dBi.

- Verify that the VAP receives power and connects to the VCU via the LEDs on the unit (both the GREEN LED and the BLUE LED should be lit).



4.2 Verifying VAP Coverage Area

Verify coverage in the areas, adding and moving VAPs for optimal coverage according to the principles described in 2.3.

4.3 Provisioning the VAPs

Note: This section provides only the information required for provisioning the VAPs. For a full description of the VAP configuration options, refer to Chapter 7

The VAPs are auto-discovered by the VCU and can be monitored via a remote or a local connection to the system Master VCU.

You may (optional) assign each VAP an identifiable name corresponding to its physical location. The only *required* configuration is for VAPs to which external antennas are connected.

4.3.1 Verifying Normal VAP Operation

Use the MIMO/SISO RF and Module Info sub-tabs to review the VAP information and status.

1. If a session is not already open to the MobileAccess**VE** Web GUI application, open a session to the Master VCU according to section 3.5.1.
2. Select a VAP from the Network Topology Tree.

Each VAP has a default name showing the number of the Slave VCU port to which the VAP is connected.

3. To verify normal operation of the VAP:
 - In the Network Topology Tree, under the Control Unit, verify that a GREEN LED is displayed (either RED or GREEN) for each connected VAP.



- If the VAP LED is **RED**, select the VAP from the network topology tree then select the **Config** tab. Refer to the **Alarms** tab work area. Use the displayed alarms to identify the problems.



Note 1: VAP alarm mask is saved in the VCU, associated with the port to which the VAP is connected. In case you replace the VAP, the newly installed VAP will automatically be set with same alarm mask.

Note 2: For more information on the VAP Alarms, refer to section 0.

4.3.2 Naming the VAP

To assign the VAP an identifiable name:

- Open the Config **Module info** tab.

The screenshot displays the MobileAccess VE WIMAX configuration interface. The top navigation bar includes 'Monitor', 'Config', 'Events', 'Set-up', 'Management', and 'Help'. The left sidebar shows a tree view of the network structure, with 'VAP5 - ConferenceRoom' selected. The main area features a central image of a white VAP device. Below the image, there are two panels: 'VAP alarms & Mask' and 'Module Info'. The 'VAP alarms & Mask' panel shows three alarm types: 'DL Adjustment' (checked), 'Over Temperature' (checked), and 'VAP Faulty' (unchecked). The 'Module Info' panel shows the 'Name' field set to 'ConferenceRoom' with a 'Modify' button. Other fields include 'Serial Number' (00941068000), 'Product Revision' (0.0), 'SW Active Version' (0.6), and 'SW Inactive Version' (0.0). There is a 'Restart VAP' button and an 'Identify' dropdown menu set to 'OFF'.

- Click the **Modify** button.
- Type the unit name (up to 17 alpha-numeric characters) and click **OK**.

4.3.3 Configuring VAP for External Antenna

By default, the VAPs are set to operate using the internal antennas.

Use the procedure described in this section to configure all VAPs to which external antennas are connected.

To configure for operation with external antennas

- Select the relevant VAP from the Topology Tree.
- Select the **RF Parameters** sub-tab.
- Set the Channel 1/2 antennas as **External**.

The screenshot displays the MobileAccess VE WiMAX configuration interface. The top navigation bar includes 'Monitor', 'Config', 'Events', 'Set-up', 'Management', and 'Help'. The left sidebar shows a topology tree with the following structure:

- MobileAccess VE WiMAX
 - VCU-M - MasterControl
 - VAP2 - MeetingRoom
 - VAP8 - Room-1
 - VAP9 - Room-2
 - VCU5 - Floor-2
 - VAP5 - ConferenceRoom
 - VAP11 - Corridor

The main area shows a central image of a VAP device. Below it, the 'RF Parameters' tab is active, displaying the following configuration:

Module Info	RF Parameters
Type	WiMAX
Channel 1 Antenna	Internal
Channel 2 Antenna	Internal
Tx Pout Level	Normal
Channel 1 Tx Pout	LOW dBm
Channel 2 Tx Pout	LOW dBm

Below the RF Parameters tab, the 'VAP alarms & Mask' section is visible, showing the following status:

Alarm	Mask
DL Adjustment	<input checked="" type="checkbox"/>
Over Temperature	<input checked="" type="checkbox"/>
VAP Faulty	<input type="checkbox"/>

The overall status is 'Overall Status' with a green indicator and a 'Modify' button.

5 Navigating the Web Access Application

The MobileAccess**VE** Web management application is accessed through any standard web browser connected to the Master VCU via a network within the same subnet as the Master VCU or a different subnet which is routable.

5.1 Opening a Session and Authentication Levels

After the initial configuration (as explained in 3.5.1) the MobileAccess**VE** system can be accessed via the network.

To access the system:

1. Open a web browser and type in the address bar the Master VCU's IP address as you set it in the Master VCU configuration operation (see section 3.5.1).



2. The Login pane appears.



Enter your User Name and type in your password. The following authentication levels are available:

Level	Default Password	Access
operator	oper	This user has Read-Only access.
engineer	eng	This user has access to basic configuration options.
admin	ma98	This user has Field Engineer permissions in addition to access to changing passwords.

5.2 About the MobileAccessVE Web Access Window

The MobileAccessVE Web window includes six main tabs that provide access to the applications' main options, where the Config tab is displayed by default.

Note: The Monitor, Events, Setup and Help tab are future options.

The appearance of the screens varies according to the tab displayed. The Main Menu Bar tabs are:

- Config(uration) – Displayed by default upon login. Provides the selected units' configuration parameters and alarms
- Management - Provides upgrade, IP configuration and security options

Both of these tabs are described in detail in the following sections.

Menu bar

Sub-tabs corresponding to menu bar options

5.3 Configuration Tab

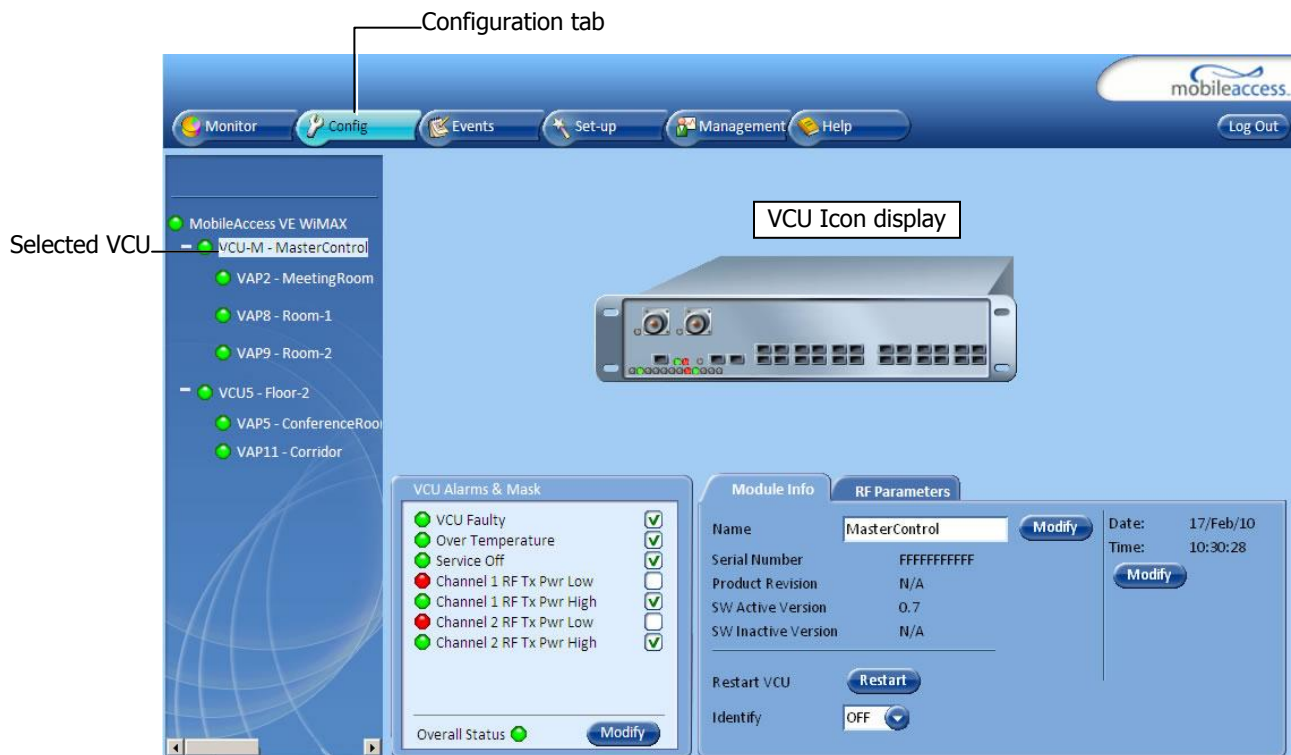
The **Configuration** tab provides the general information and service RF parameters for configuration of the units appearing in the Network Topology tree. VCU Configuration Options

To access a VCU Configuration tab

Select a Master VCU/Slave VCU from the network topology tree on the left hand side of the window a click the **Configuration** tab from the menu-bar. The information and parameters displayed in the Configuration sub-tabs vary depending on whether a VCU or VAP is selected in the topology tree.

The Configuration tab is divided in to three main areas:

- Network Topology Tree – Displays the system units (Master VCU, Slave VCUs and VAPs) and their status
- Display area – Displays the icon of the unit (Master VCU/Slave VCU or VAP) selected in the Topology Tree; the display includes the LED statuses. When selecting an element
- Work area – Displays the Module Info, alarms and RF tabs corresponding to the unit selected in the topology tree (Master VCU, Slave VCU or VAP)

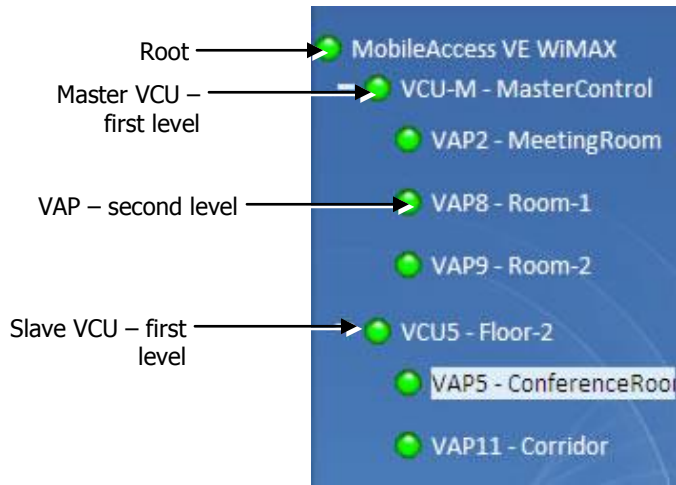


5.3.1 Network Topology Tree

The Configuration Network Topology Tree appears on the left hand side when the **Config** tab is selected and displays the Master VCU, Slave VCUs and VAPs in two levels:

- First level – VCU
- Second level – Up to 12 VAPs

Note: The root is MobileAccess VE.



Each unit is assigned a **Type Px-name**:

- Type – VCU-M, VCU or VAP (for Master VCU, Slave VCU or VE Access Pod)
- Px - VCU port number
- Name – user defined

Each unit is displayed with a colored bullet that indicates its' status:

Color	Indicates
Green	OK
Red	Alarm Condition

The root (the entire MobileAccess**VE** site) is also associated with a colored bullet that indicates the overall status of the deployment:

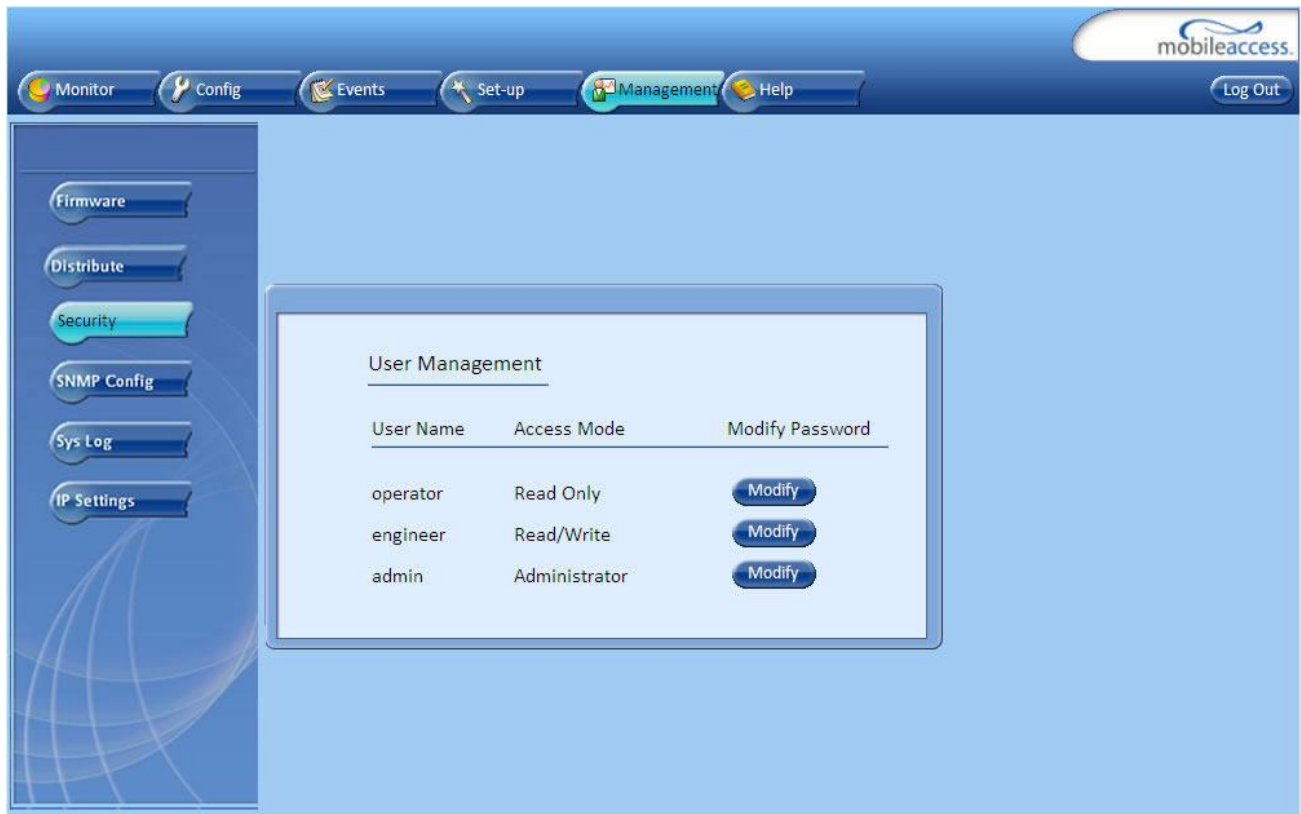
Color	Indicates
Green	OK
Red	Alarm Condition in one or more VCUs or VAPs

5.3.2 Management Tab

The Management tab provides the user administrative management options and includes the sub-menu tabs:

- Firmware – Used for upgrading/downgrading SW to VCU's
- Distribute – Used for distributing the upgrade/downgrade SW files to the VAPs
- Security – Used for changing user passwords
- SNMP Config – Used for defining the SNMP communities and trap destinations
- IP Settings – Used for viewing and modifying the network parameters
- Sys(tem) Log – N/A

The following figure shows the Management screen with the menu options on left (Security dialog is displayed here).



6 VCU Monitoring and Configuration

6.1 Viewing VCU General Information

The VCUs general information (such as unit name and SW versions) can be viewed in the Config **Module Info** sub-tab.

The tab includes two additional options:

- Identify button - Enabling this option enables finding the physical location of the selected element (see 9.1). When this option is set to ON, the LEDs on the corresponding VCU flickers.
- Reset button - SW reset of the unit

To view VCU general information

Click the Config tab from the main menu and select the VCU from the network topology tree. The **Module Info** sub-tab is displayed by default.

The screenshot displays the MobileAccess VE WIMAX configuration interface. The top navigation bar includes Monitor, Config (selected), Events, Set-up, Management, and Help. A Log Out button is also present. The left sidebar shows a network topology tree with the following structure:

- MobileAccess VE WIMAX
 - VCU-M - MasterControl
 - VAP2 - MeetingRoom
 - VAP8 - Room-1
 - VAP9 - Room-2
 - VCU5 - Floor-2
 - VAP5 - ConferenceRoom
 - VAP11 - Corridor

The main content area shows a 3D rendering of a VCU unit. Below the rendering, there are two panels:

VCU Alarms & Mask

<input checked="" type="checkbox"/>	VCU Faulty	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Over Temperature	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Service Off	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Channel 1 RF Tx Pwr Low	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Channel 1 RF Tx Pwr High	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Channel 2 RF Tx Pwr Low	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Channel 2 RF Tx Pwr High	<input checked="" type="checkbox"/>

Overall Status: [Modify](#)

Module Info (selected) | RF Parameters

Name	MasterControl	Modify	Date:	17/Feb/10
Serial Number	FFFFFFFF		Time:	10:30:28
Product Revision	N/A			Modify
SW Active Version	0.7			
SW Inactive Version	N/A			

Restart VCU: [Restart](#)

Identify: [OFF](#)

The following information is displayed:

Field	Description
Name	User defined name for system element (up to 17 characters)
Serial Number	Factory set ID number
Product Revision	Revision number of VCU/VAP
SW Active Version	Version of the SW currently being used to manage and monitor the system
SW Inactive Version	Version of other system SW version not in use

6.2 Viewing VCU Alarms

The alarms displayed in the Alarms tab correspond to the VCU (Master/Slave) selected in the topology tree. When a VCU element is selected in the topology tree, the Alarm tab displays the main alarms in the unit.

To view VCU Alarms

In the Topology Tree, click the **Control Unit (VCU)**, click the **Config(uration)** tab in the menu bar located at the top of the window and refer to the **VCU Alarms and Mask** sub tab.

Config tab

VCU Alarms and Mask

Alarm	Status	Mask
VCU Faulty	Green	<input checked="" type="checkbox"/>
Over Temperature	Green	<input checked="" type="checkbox"/>
Service Off	Green	<input checked="" type="checkbox"/>
Channel 1 RF Tx Pwr Low	Red	<input checked="" type="checkbox"/>
Channel 1 RF Tx Pwr High	Green	<input checked="" type="checkbox"/>
Channel 2 RF Tx Pwr Low	Red	<input type="checkbox"/>
Channel 2 RF Tx Pwr High	Green	<input checked="" type="checkbox"/>

Overall Status: ● **Modify**

Module Info

Name	MasterControl	Modify	Date:	17/Feb/10
Serial Number	FFFFFFFF		Time:	10:30:28
Product Revision	N/A		Modify	
SW Active Version	0.7			
SW Inactive Version	N/A			

Restart VCU: **Restart**

Identify: OFF **▼**

If one or more alarms occur, the corresponding Status indicator is illuminated in RED. If the VCU is OK and no fault occurs, the **Overall Status** indicator will show GREEN.

The following table provides a description of the alarms displayed in the **VCU Alarms and Mask** sub-tab.

Alarm	Description
Channel 1/2 DL RF Pwr Low	DL RF Power is lower by 15dBm (or more) from the Max Expected Pin, or is lower than -3dBm. Note: Channel 2 alarm is not displayed when SISO service is used.
Channel 1/2 DL RF Pwr High	Input power exceeds the maximum expected Pin by more than 3 dB. Note: Channel 2 alarm is not displayed when SISO service is used.
Service Off	User has disabled the service
Over temperature	Temperature of unit exceeds normal range
Adjust	Cable (between VCU to VAP, or between Master to Slave),is too long (over 100m/300ft)
CU faulty	Hardware fault detected in VCU
Overall status	Indicates Fault (RED) level if there are (unmasked) faults, or GREEN if there are no faults

6.3 Master VCU RF Parameters

Note: The RF parameters are not displayed for control units functioning as Slave VCUs.

To access the RF Parameters tab

Click the **Config** tab from the main menu bar and then select the Master control unit from the network topology and click the **RF Parameters** tab. The parameters displayed in RF Parameters tabs correspond to the selected element. The displayed parameters are similar for MIMO and SISO service modes, however in SISO mode only the *Channel 1 Pin* parameter is displayed.

The screenshot shows the MobileAccess VE WIMAX management interface. The top navigation bar includes 'Monitor', 'Config', 'Events', 'Set-up', 'Management', and 'Help'. The 'Config' tab is selected. On the left, a tree view shows the network topology with 'VCU-M - MasterControl' selected. The main area displays a hardware image of a VCU. Below the image, there are two panels: 'VCU Alarms & Mask' and 'Module Info / RF Parameters'. The 'RF Parameters' panel shows the following settings:

- Type: WIMAX
- Service Mode: MIMO
- DL CF: 2520.0 MHz
- Max Exp Pin: 33 dBm
- Channel 1 Pin: LOW
- Channel 2 Pin: LOW
- Rx System Gain: 0 dB

The following table provides a description of the RF parameters displayed in the MIMO RF tab.

Parameter	Description
Type	Set (read only) according to unit type (WiMAX)
Service Mode	Provides the service options: MIMO/SISO. The selected option determines the displayed RF parameters.
DL CF*	Center frequency (from BS). User defined according to WiMAX range. The CF is the same for both UL and DL signals.
Max Exp Pin*	Maximum expected input power from the BS. Used for adjustment procedure. Range: 0-33 dBm. User defined.
Channel1/ Channel 2 Pin	Actual measured Pin (read only). In SISO mode only Channel 1 Pin is relevant.
Rx System Gain	Used for adjusting the UL system gain. Range: -15 dB to +5 dB

* Required parameters to be provisioned by the user.

7 VAP Monitoring and Configuration

7.1 Viewing VAP General Information

The VAPs general information (such as unit name and SW versions) can be viewed in the Config **Module Info** sub-tab.

The tab includes two additional options:

- Identify button - Enabling this option enables finding the physical location of the selected element. When this option is set to ON, the LEDs on the corresponding VAP flickers.
- Reset button - SW reset of the unit

To view VAP general information

Click the Config tab from the main menu and select the VAP from the network topology tree. The **Module Info** sub-tab is displayed by default.

The screenshot shows the MobileAccessVE WiMAX Instant Coverage Solution User Manual interface. The top navigation bar includes 'Monitor', 'Config', 'Events', 'Set-up', 'Management', 'Help', and 'Log Out'. The left sidebar shows a network topology tree with 'MobileAccess VE WiMAX' expanded to 'VCU-M - MasterControl', which includes 'VAP2 - MeetingRoom', 'VAP8 - Room-1', 'VAP9 - Room-2', 'VCU5 - Floor-2', 'VAP5 - ConferenceRoom', and 'VAP11 - Corridor'. The 'Selected VAP' is 'VAP5 - ConferenceRoom'. The 'Module Info' sub-tab is active, displaying the following information:

Field	Description
Name	ConferenceRoom
Serial Number	00941068000
Product Revision	0.0
SW Active Version	0.6
SW Inactive Version	0.0

Below the table, there are buttons for 'Restart VAP' and 'Identify' (set to OFF). There is also a 'VAP alarms' section with checkboxes for 'DL Adjustment' (checked), 'Over Temperature' (checked), and 'VAP Faulty' (unchecked). An 'Overall Status' indicator shows a green dot and a 'Modify' button.

The following information is displayed:

Field	Description
Name	User defined name for system element (up to 17 characters)
Serial Number	Factory set ID number
Product Revision	Revision number of VCU/VAP
SW Active Version	Version of the SW currently being used to manage and monitor the system
SW Inactive Version	Version of other system SW version not in use

Note: VAP name is saved in the VCU associated to the port to which the VAP is connected, such that in case you replace a VAP, the new one will be associated with the same name.

7.2 Viewing VAP Alarms

When a VAP element is selected in the topology tree, the Alarm tab displays the main alarms in the unit.

To access VAP Alarms Tab

In the Topology Tree, click the **VAP**, click the **Config(uration)** tab in the menu bar located at the top of the window and click the **VAP Alarms** sub tab.

The screenshot displays the MobileAccess VE WIMAX management interface. At the top, there is a menu bar with tabs: Monitor, Config, Events, Set-up, Management, and Help. The 'Config' tab is selected. On the left, a topology tree shows a hierarchy: MobileAccess VE WIMAX > VCU-M - MasterControl > VAP2 - MeetingRoom > VAP8 - Room-1 > VAP9 - Room-2 > VCU5 - Floor-2 > VAP5 - ConferenceRoom > VAP11 - Corridor. The 'VAP5 - ConferenceRoom' is selected. The main area shows a 3D model of a VAP unit. Below the model, there are two panels: 'VAP alarms & Mask' and 'Module Info'. The 'VAP alarms & Mask' panel has three items: 'DL Adjustment' (checked), 'Over Temperature' (checked), and 'VAP Faulty' (unchecked). Below these is an 'Overall Status' indicator showing a green dot and a 'Modify' button. The 'Module Info' panel shows fields for Name (ConferenceRoom), Serial Number (00941068000), Product Revision (0.0), SW Active Version (0.6), and SW Inactive Version (0.0). It also has a 'Restart VAP' button and an 'Identify' dropdown menu set to 'OFF'.

If one or more alarms occur, the corresponding Status indicator is illuminated in RED. If the VAP is OK and no fault occurs, the **Overall Status** indicator will show GREEN.

Alarm	Description
Adjustment	RED - Cable (between VCU to VAP) is too long (over 100m/300ft)
VAP Faulty	RED - A fault has been detected in the VAP
Overall temperature	RED - Temperature of unit exceeds normal range
Overall status	Indicates Fault (RED) level or GREEN if there are no faults

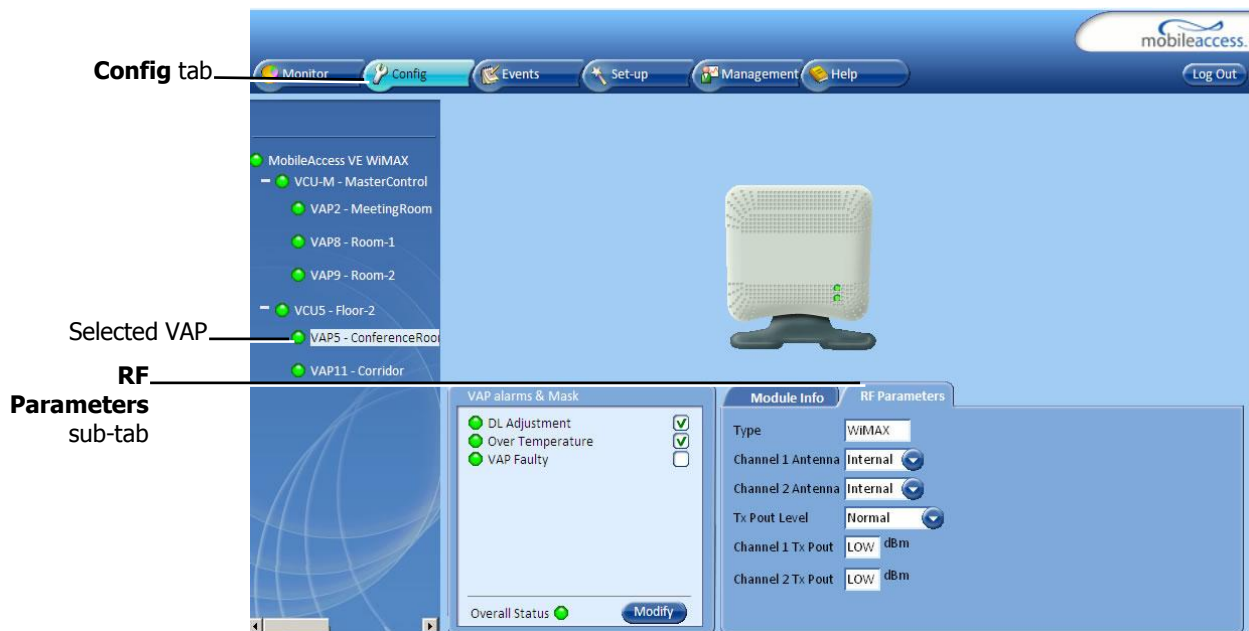
Note: Adjustment alarm is raised when VAP is connected over a cable exceeding system cable length limitation. In such case the system continues to provide the wireless services but you should check the coverage of the VAP (as output power may be degraded due to excess cable loss) and check the Ethernet connection (as Ethernet standard maximum cable length is probably exceeded).

7.3 VAP RF Parameters

The VAP **RF Parameters** sub-tab provides the configurable RF parameters corresponding to the VAP element selected in the network topology tree. The displayed RF parameters are similar for both MIMO and SISO service modes (in SISO service mode only **Channel 1** parameters are displayed).

To view the VAP RF Parameters

Click the **Config** tab from the main menu bar and then select the VAP from the network topology and click the *RF Parameters* sub-tab. The parameters displayed in RF tab correspond to the selected element.



The following table provides a description of the displayed VAP RF parameters (in SISO service mode, only **Channel 1** parameters are displayed).

Parameter	Description
Type	Set according to unit type (WiMAX)
Channel 1/ Channel 2 Antenna	Select External only if an external antenna is connected to this VAP. Otherwise, the option should be set to Internal (default).
Tx Pout Level	Level of from BS side. Normal = output power will be at required (normal) level Low = output power will be attenuated by 5 dB less than the required level. This option can be used for smaller coverage areas that do not require the full power of the VAP for coverage.
Channel 1/ Channel 2 Tx Pout	Measured output power.

Note: VAP RF settings (Service Mode, DL Pout Level, Antenna) are saved in the VCU associated to the port to which the VAP is connected, such that in case you replace a VAP all parameters are automatically set to the new VAP.

8 Administrative Operations

This chapter describes the following Administrative operations:

- Changing password
- IP configuration parameters
- SNMP Configuration parameters
- Unit software upgrade and software management procedures

8.1 Changing Password

The Management - Security tab provides password change options.

To set the application password or change an existing password

1. Select the **Security** option of the Management tab at the top of the window.



2. Click the **Modify** (Password) button of the User Name whose password is to be modified.
3. Enter the **New Password** and re-enter in the **Confirm New Password** field.
4. Click **OK**.

Note: Only when connected as an administrator you can change the passwords.

8.2 IP settings

The IP Settings tab is used for viewing and modifying the network parameters. The default parameter settings are as follows:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.254

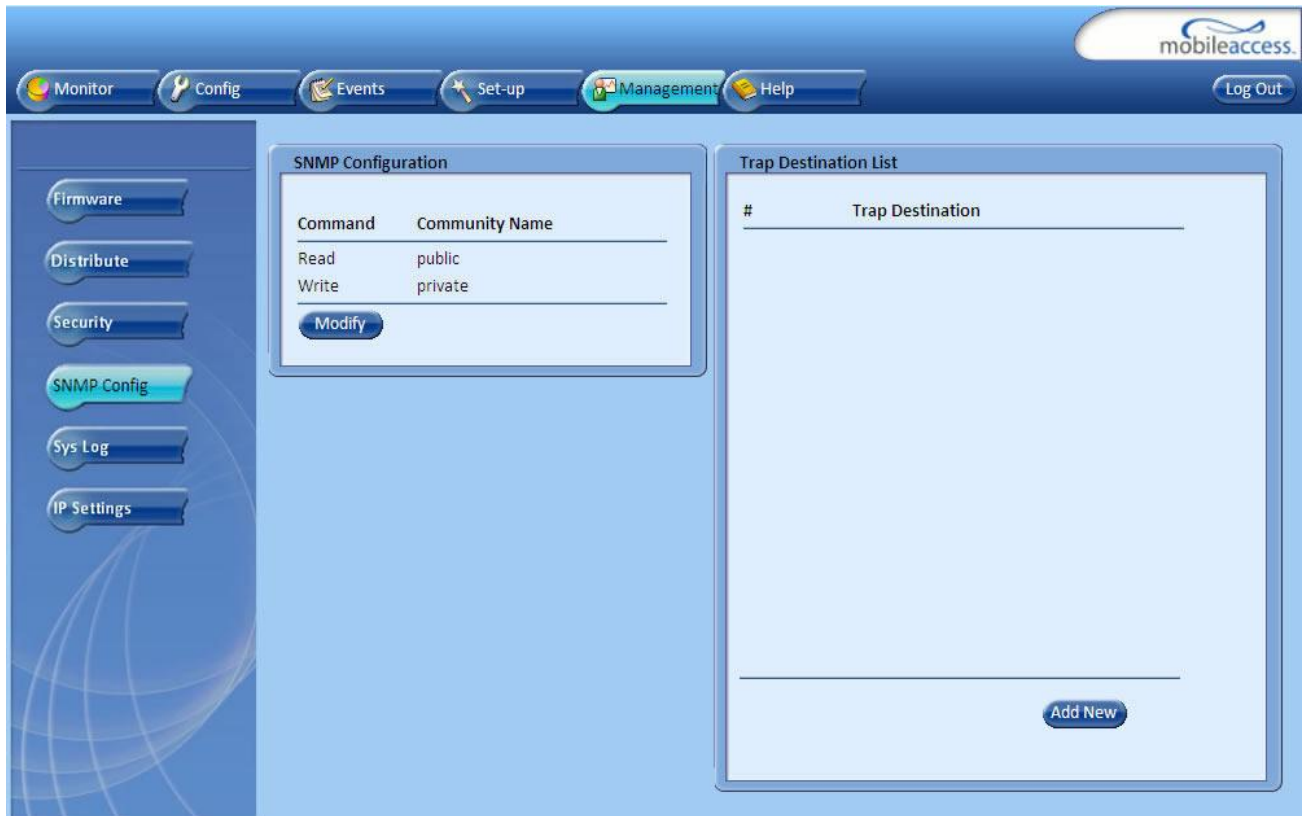


Click **Modify** button to change settings

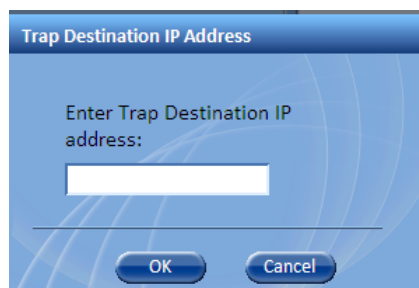
8.3 SNMP Configuration Parameters

The SNMP Config tab is used for defining the SNMP communities that the devices and management station belongs to and to where the traps are sent. The SNMP default communities are:

- Read=public
- Write=private



- The Community Names can be modified by clicking the **Modify** button in the SNMP Configuration display area.
- Additional Trap Destinations can be added by clicking the **Add New** button in the Trap Destination List display area:



8.4 Upgrading (or Downgrading) VCU and VAP Software

NOTE: Before you start, verify that the VCU and VAPs upgrade file(s) are located in an accessible location (i.e. on your computer).

The software for each VCU and its hosted VAPs can be upgraded through access to the VCU.

Note: In installations with Slave VCUs, a session shall be opened to the IP address of the Slave VCU in order to upgrade the SW of the Slave VCU and associated VAPs.

Two types of files are stored on the VCU and on individual VAPs: Active software on which the unit operates, and Standby software. The Active and Standby software can be swapped on each individual unit.

In addition, the VCU holds two software images for VAPs – to be used in download process to VAPs.

The upgrade procedure consists of the following main phases:

1. Uploading the new VCU and VAP software to the host VCU.
2. Setting the new software as the Active software.
3. Activating the new VCU software on the VCU.
4. Downloading the new software to selected VAPs and activating it as the Active software on those VAPs.

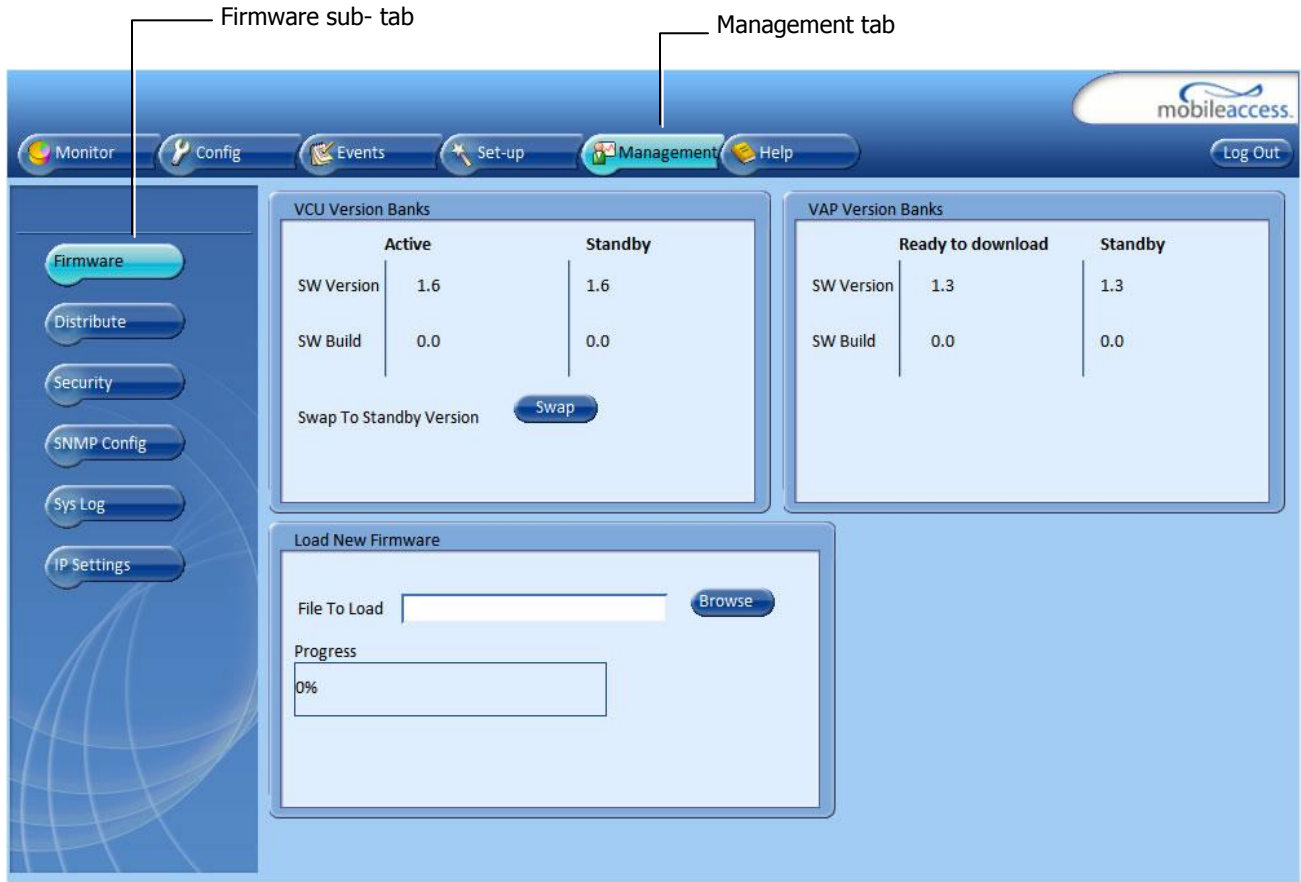
The procedure is performed via two screens:

- Firmware screen – used to manage the software files stored on the VCU.
- Distribute screen – used to download the VAP software version to selected VAPs.

8.4.1 Upgrading the VCU SW

To Upgrade the VCU SW Version:

1. Upload the VCU upgrade files from your storage location (i.e. computer) to the VCU as follows:
 - Click the **Management** menu tab and then click the **Firmware** sub-menu option (left side).



- In the **Load New Firmware** display area, click the **Browse** button.
 - Select the file to be loaded (from your computer location). The Download button appears and the progress bar will show the download status.
 - After download is complete the downloaded SW version will appear in the Standby Bank column of the VCU display area.
2. Define the downloaded version as the Active version (to be used for upgrade) as follows:
 - (In the VCU display area), click **Swap**. The downloaded version appears in the Active Bank column and the Controller is automatically restarted.
 - The VCU Upgrade procedure is complete.

8.4.2 Upgrading the VAP SW

To Upgrade the VAPs SW Version:

1. Upload the VAP upgrade files from your storage location (i.e. computer) to the VCU as follows:
 - Click the **Management** menu tab and then click the **Firmware** sub-menu option (left side).
 - In the **Load New Firmware** display area, click the **Browse** button.
 - Browse for the file to be loaded (from your computer location). The Download button appears and the progress bar will show the download status.

The screenshot shows the MobileAccessVE Web GUI. The navigation menu at the top includes Monitor, Config, Events, Set-up, Management (selected), and Help. The left sidebar contains buttons for Firmware, Distribute, Security, SNMP Config, Sys Log, and IP Settings. The main content area is divided into three sections:

- VCU Version Banks:** A table with columns 'Active' and 'Standby'. The 'Active' column shows SW Version 1.6 and SW Build 0.0. The 'Standby' column shows SW Version 1.6 and SW Build 0.0. A 'Swap' button is located below the table.
- VAP Version Banks:** A table with columns 'Ready to download' and 'Standby'. The 'Ready to download' column shows SW Version 1.3 and SW Build 0.0. The 'Standby' column shows SW Version 1.3 and SW Build 0.0.
- Load New Firmware:** A section with a 'File To Load' input field, a 'Browse' button, and a 'Progress' bar showing 0%.

A red box highlights the 'Load New Firmware' display area, with a red arrow pointing to it from the text 'Load New Firmware display area' on the left.

- After the download is complete, the downloaded SW version will appear in the Standby Bank column of the VAP display area.

Notes:

1. Locate the Firmware files on your local hard-drive prior to the download process.
2. During the download process DO NOT disconnect the Web GUI connection to the VCU.

2. To distribute the new software to selected VAPs:
 - Click the **Distribute** sub-menu option (left side).



3. Download the new version to the selected VAPs (where the downloaded version is stored as Inactive in the VAPs until a Swap procedure is performed):
 - In the **VAP Distribute Table** display area, checkmark the VAPs to be upgraded. (The Active and Inactive SW versions for each VAP are listed in the relevant columns).
 - Click the **Distribute** button to download the new software to the selected VAPs. The software is stored as the Inactive version in the VAPs.
 - Set the new software as the Active version in the selected VAPs by clicking the Swap button.
 - The VAP upgrade procedure is complete.

Notes:

1. As during the distribution process service may be interrupted, it is advised to perform the SW download and distribution in a maintenance window schedule to off-peak hours (e.g. during the night).
2. During the distribution process DO NOT perform configuration changes, DO NOT connect or disconnect VAPs and do not disconnect the web GUI.
3. After the distribution process is complete and after swapping between VAP SW images, the VCU will restart automatically. After restart, the VAP firmware distribution table will be empty and it will be re-populated within several seconds as the VCU re-discovers connected VAPs.

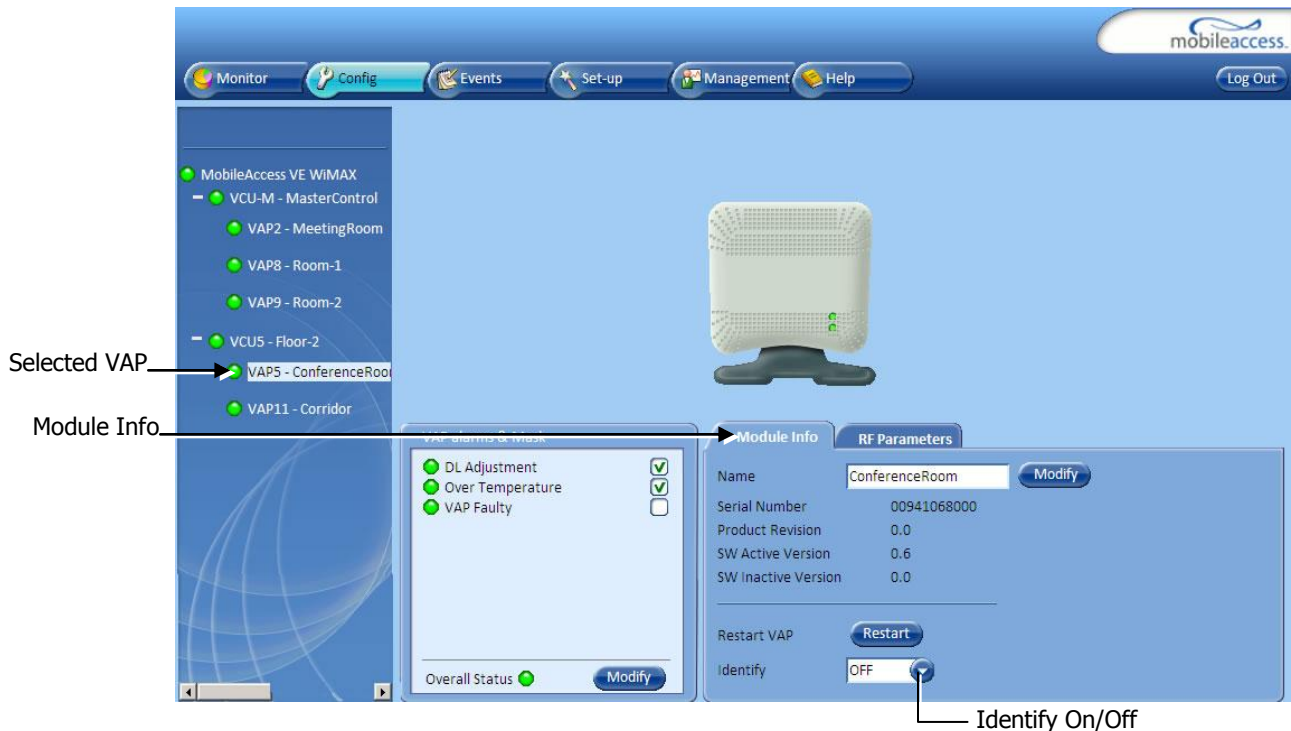
9 Troubleshooting

9.1 Finding a Specific VAP in the Building

It is recommended to assign each VAP an identifiable name corresponding to its physical location as explained in section 4.3.2. If a name was not configured, or for some other reason a specific VAP cannot be physically located, identify the VAP according to the instructions in the following example.

To locate a VAP

1. Click the **Config** tab from the main menu bar and select the VAP to be located from the topology tree.



2. Click the **Module Info** sub-tab.
3. Set **Identify** to **ON**.

The Activity LED (Blue) on the corresponding Access Pod will start blinking fast. (You will need to physically locate the VAP to see the blinking LED).



4. Locate the Access Pod.
5. Once found – it is advisable to assign it an identifiable name via the VAP **Module Info** sub-tab as described in section 4.3.2 (e.g. floor 3, room 2) and set the **Identify** field to **Off** again.

9.2 Wireless Service is Not Available

1. Verify that the Master VCU is connected to the BS, powered up and configured.
2. Verify that the Max Expected Power setting is correct by either:
 - A) Viewing the actual VCU Power Measurement (**Channel 1/Channel 2 Pin**) in the VCU **RF Parameters** sub-tab (see below).



- B) or by measuring the actual BS output using a Spectrum Analyzer.
3. Verify correct settings of center frequency and system gain (see **DL CF** and **Rx System Gain** parameters in RF Parameters sub-tab – see example displayed above).
4. Verify that the RF cables are properly connected to the VCU.
5. View the VCU **Alarms** (above image) and verify that the VCU is working properly.

9.3 Ethernet service is degraded

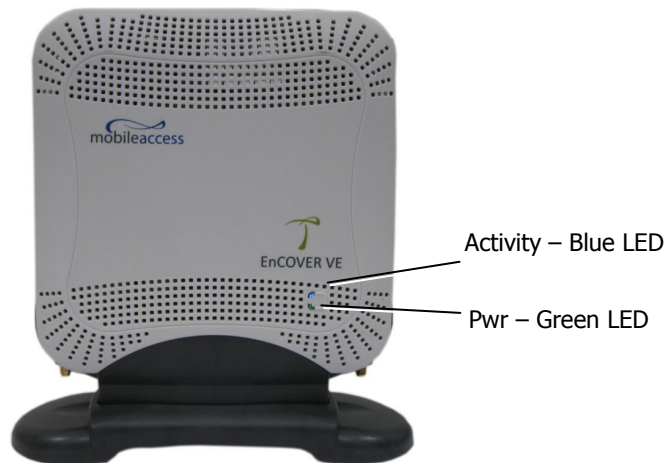
Ethernet standards specify that 100m (300ft) is the maximum distance between an Ethernet switch and appliance (computer, WLAN AP etc). This is relevant when MobileAccess**VE** shares the IT LAN. The distance includes all patch cords (from switch to VCU, from VCU to patch panel, from RJ-45 outlet to VAP, and from VAP to appliance).

1. Review the IT documentation (may be available from your IT department) to determine cable types and lengths.
2. Check the lengths of the patch cords being used and verify the end-to-end distance does not exceed 100m (300ft).
3. A Fluke cable tester can be used to measure cable length.

9.4 No Service from Connected Access Pod

This requires physically accessing the Access Pod to check the LEDs, and accessing the Access Pod through the Web GUI to verify the Access Pod configuration.

1. Physically view the Access Pod and confirm that both LEDs on the Access Pod are lit:
 - Power LED (Green) is OFF – either no connectivity to the VCU or the VAP is faulty. Try replacing the VAP. Try connecting the VAP directly to the VCU – if the Power LED is lit check the cable and the patch cords.
 - Activity LED is constantly blinking – the Access Pod cannot initialize due to exceeded cable length. Try using the closest free RJ-45 jack fed with a different cable.



2. Check other Access Pods connected to the same VCU.
3. Verify that the VAP configuration as follows:
 - Connect to the VCU using the MobileAccess**VE** Web GUI application (see 5.1).
 - In the VCU **Config** tab, click the **RF Parameters** sub-tab and verify that the **Service Mode** parameter is set (MIMO/SISO).



- Select the VAP from the topology tree and click the **RF Parameters** sub-tab.



- Confirm that the VCU port is functioning (VAP status LED - top LED in VAP icon associated with this Pod is green).

Note: The *Activity* LED on the actual VAP is BLUE.

- In case external antennas are connected – verify the VAP was configured to use the *external* antennas (see **Channel 1/ Channel 2 Antenna** parameter in RF Parameters sub-tab, shown in previous figure).

9.5 VCU Cannot be monitored via SNMP

VE traps are not received by the external Fault Monitoring system.

1. Verify that the VCU is powered ON.
2. Verify that the SNMP traps destination address is configured correctly.
3. Verify the IP connectivity to the Fault Monitoring server using "ping."
4. Verify that SNMP port is not blocked or fire-walled in the IP network.
5. Initiate an Alarm and confirm the trap is received by external Fault Monitoring server. For example:
 - Access the VAP RF Parameters sub-tab (see section 7.3).

The screenshot displays the MobileAccess VE WIMAX management interface. The top navigation bar includes 'Monitor', 'Config', 'Events', 'Set-up', 'Management', and 'Help'. The left sidebar shows a tree view of the network hierarchy: MobileAccess VE WIMAX, VCU-M - MasterControl, VAP2 - MeetingRoom, VAP8 - Room-1, VAP9 - Room-2, VCU5 - Floor-2, VAP5 - ConferenceRoom, and VAP11 - Corridor. The main area features a central image of a white VCU device. Below it, there are two panels: 'VAP alarms & Mask' and 'Module Info / RF Parameters'. The 'VAP alarms & Mask' panel lists three alarms: 'DL Adjustment' (green), 'Over Temperature' (green), and 'VAP Faulty' (red). The 'VAP Faulty' alarm is unmasked, indicated by a green checkmark in the 'Mask' column. The 'Module Info / RF Parameters' panel shows settings for a WIMAX module, including antenna type (Internal), Tx Pout Level (Normal), and Channel 1/2 Tx Pout (LOW dBm). A red arrow points from the 'VAP Faulty' alarm to the text 'Unmasked VAP Faulty alarm' on the right side of the image.

- Verify that the alarm is unmasked (for example, **VAP faulty** alarm).
- Disconnect the selected VAP.
- Confirm the trap is received by external Fault Monitoring server.

Appendices

Traps

This section lists the MobileAccess**VE** WiMAX Controller and Access Pod traps

MobileAccess**VE** Control Unit Traps

No	Trap Name	Trap Description
1	vcuChannel_1_DLPowerLow	Input RF power (from BS) is lower by 15dBm (or more) from the Max Expected Pin, or is lower than -3dBm (or no signal).
2	vcuChannel_1_DLPowerHigh	Input power exceeds the maximum expected Pin by more than 3dBm.
3	vcuChannel_1_ServiceOff	Service is off
4	vcuChannel_2_DLPowerLow	Input RF power (from BS) is lower by 15dBm (or more) from the Max Expected Pin, or is lower than -3dBm (or no signal).
5	vcuChannel_2_DLPowerHigh	Input power exceeds the maximum expected Pin by more than 3dBm.
6	vcuChannel_2_ServiceOff	Service is off
7	vcuFaulty	VCU HW is faulty
8	vcuOverTemperature	Temperature is above threshold
9	vcuAdjustment	When adjustment (for Slave VCU) has failed (cable too long)
10	vcuMismatchType	VCU service is different than VAP services

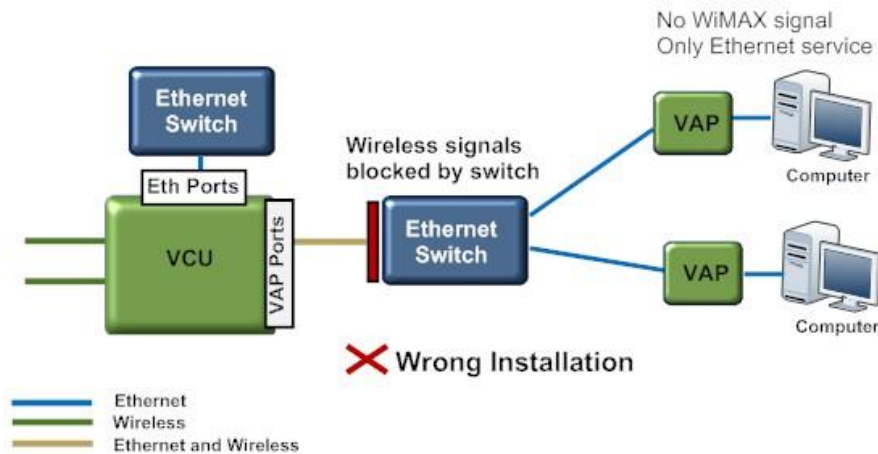
MobileAccess**VE** Access Pod Traps

No	Trap Name	Trap Description
1	vapAdjustment	When adjustment (for VAP) has failed (cable too long)
2	vapFaulty	when VAP HW is faulty
3	vapOverTemperature	when temperature is above threshold

VE Connections in Central Ethernet Source Topologies

This section describes the VE site installation for sites whose Ethernet services are provided from a single Ethernet source in the communication room and distributed throughout the site by daisy-chaining Ethernet switches from the central source.

In VE installation, any switch located in the path between the VCU and the VAPs will block the wireless signals:



The Bypass option allows bypassing the switch by enabling the transport of Ethernet signals over the cable connecting the Master VCU to the slave VCU. (In a typical VE the cable between the Master and Slave VCUs is a dedicated CAT-6/7 cable used only for VE).

The Ethernet signals are combined with the wireless signals at the master VCU, separated at the slave VCU and connected via the Bypass port to the switch.

The wireless signals are then re-combined by the slave VCU with the Ethernet signals (from the Ethernet Switch Ports) and transported to the VAPs and connected PCs.

