



**MEA**

**3.1**

**Ruggedized  
Mobile Modem  
Users Guide**

Documentation Revision 3.1.2



**Copyrights**

The Motorola products described in this document may include copyrighted Motorola computer programs. Laws in the United States and other countries reserve for Motorola certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola computer programs contained in the Motorola products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola. Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppels or otherwise, any license under the copyrights, patents or patent applications of Motorola, except for the normal nonexclusive, royalty-free license to use that arises by operation of law in the sale of a product.

**Disclaimer**

Please note that certain features, facilities and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola contact for further information.

**Trademarks**

Motorola, the Motorola logo, and all other trademarks identified as such herein are trademarks of Motorola, Inc. All other product or service names are the property of their respective owners.

**Copyrights**

© 2006 Motorola, Inc. All rights reserved. No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola, Inc.



## Table of Contents

<b>1</b>	<b>PRODUCT INTRODUCTION .....</b>	<b>1</b>
1.1	Product Contents .....	1
1.2	Product Specifications .....	1
<b>2</b>	<b>DEVICE INSTALLATION .....</b>	<b>3</b>
2.1	Software Requirements .....	3
2.2	Equipment Requirements.....	3
2.3	MAC Address Label Location .....	4
2.3.1	MAC Address Table .....	4
2.4	RMM6300 Assembly Information .....	5
2.5	Installing the RMM6300 Device.....	5
2.5.1	Deployment Considerations .....	5
2.5.1.1	Deployment Tips.....	6
2.6	Testing the Device Installation.....	6
<b>3</b>	<b>DEVICE CONFIGURATION .....</b>	<b>7</b>
3.1	IP Addressing Considerations .....	7
3.2	Accessing the MEA Device Administration Web Pages.....	7
3.2.1	Administrator and Access Account Information.....	7
3.2.1.1	Password Information.....	8
3.2.2	Viewing MEA Device Administration Redirect Page .....	9
3.2.3	Viewing MEA Device Administration Home Page as an Administrator.....	10
3.2.4	Viewing MEA Device Administration Home Page as a Normal User.....	11
3.2.5	RMM Device Administration Configuration Tab .....	12
3.2.5.1	Viewing the RMM Configuration Tab as an Administrator .....	12
3.2.5.2	Viewing the RMM Configuration Tab as a Normal User .....	13

3.2.6	RMM Device Administration Geo Position Tab .....	14
<b>3.3</b>	<b>Device Addressing Schemes .....</b>	<b>15</b>
3.3.1	Network DHCP Scheme .....	16
3.3.2	Statically Provisioned Scheme .....	16
3.3.3	User Supplied Scheme .....	16
<b>3.4</b>	<b>Setting User Supplied IP Addresses .....</b>	<b>17</b>
<b>3.5</b>	<b>External Device Provisioning .....</b>	<b>19</b>
3.5.1	Connecting to the Ethernet Port .....	20
<b>3.6</b>	<b>Working with MeshTray .....</b>	<b>20</b>
3.6.1	MeshTray Status Information .....	21
3.6.2	MeshTray Security Tab .....	22
3.6.3	MeshTray Authentication Activity .....	22
<b>4</b>	<b>DEVICE MAINTENANCE .....</b>	<b>24</b>
<b>4.1</b>	<b>Changing the Web Interface Password .....</b>	<b>24</b>
<b>4.2</b>	<b>Upgrading the Device Firmware .....</b>	<b>25</b>
<b>4.3</b>	<b>Security Provisioning Web Page .....</b>	<b>28</b>
4.3.1	Provision Username Section .....	28
4.3.2	Provision Groupname Section .....	28
<b>4.4</b>	<b>Resetting the RMM via the Device Administration Web Page .....</b>	<b>29</b>
<b>4.5</b>	<b>Restoring Factory Settings – User Supplied Mode Limitations .....</b>	<b>30</b>
4.5.1	Recovering from RMM Reset-to-Default in User-Supplied Mode .....	30
4.5.1.1	Resetting Device Addressing Mode Using Device Manager .....	31
4.5.1.2	Resetting Device Addressing Mode via Configuration Web Page .....	31
4.5.1.3	Resetting User-Supplied Parameters via Configuration Web Page .....	31
<b>4.6</b>	<b>Restoring Factory Settings – Normal Operations .....</b>	<b>32</b>
<b>5</b>	<b>CUSTOMER SERVICE INFORMATION .....</b>	<b>34</b>
<b>5.1</b>	<b>Obtaining Support .....</b>	<b>34</b>

**5.2 System Information..... 34**

**5.3 Return Material Request..... 35**

**5.4 Radio Products and Services Division..... 35**

    5.4.1 Radio Products and Services Division Telephone Numbers..... 35

**5.5 Returning System Components to Motorola..... 35**

**6 WARRANTY INFORMATION..... 36**

**7 END USER LICENSE AGREEMENT..... 39**

**8 FCC REGULATORY INFORMATION..... 44**

    8.1 FCC Information..... 44

    8.2 FCC RF Radiation Exposure Statement..... 44

**9 SAFETY INFORMATION FOR THE MEA PRODUCTS..... 45**

**10 SAFETY CERTIFICATION..... 46**

    10.1 CE Mark Certification..... 46

## List of Figures

Figure 2-1.	RMM External Connection Points .....	5
Figure 3-1.	Enter Network Password Initial Web Page Authentication Dialog.....	8
Figure 3-2.	MEA Device Administration Redirecting Web Page.....	9
Figure 3-3.	MEA Device Administration Home Page (Super User Login).....	10
Figure 3-4.	MEA Device Administration Home Page (Normal User Login).....	11
Figure 3-5.	RMM Device Administration Configuration Page (Super User Login)....	12
Figure 3-6.	RMM Configuration Page (Normal User Account).....	14
Figure 3-7.	Geo Position Tab (Same view for Super User and Normal accounts)....	15
Figure 3-8.	Configuration Change Dialog.....	17
Figure 3-9.	System Update Save Completed Web Page .....	18
Figure 3-10.	External Device Provisioning Table.....	19
Figure 3-11.	MeshTray Status Tab (RMM) .....	21
Figure 3-12.	MeshTray Security Tab (RMM) .....	22
Figure 3-13.	MeshTray Authentication Activity tab (RMM) .....	23
Figure 4-1.	Enter New Password Web Page.....	24
Figure 4-2.	Confirm Changes Window for Enter New Password .....	25
Figure 4-3.	Password Changed Confirmation Web Page.....	25
Figure 4-4.	Update Device Firmware Web Page.....	26
Figure 4-5.	Confirm Upload Window for Firmware Update.....	26
Figure 4-6.	Firmware Upload Progress Web Page.....	27
Figure 4-7.	Security Provisioning Web Page .....	28
Figure 4-8.	Device Reset Prompt Web Page .....	29
Figure 4-9.	Device Reset in Progress Page.....	30
Figure 4-10.	Restore Factory Settings Web Page.....	32
Figure 4-11.	Confirm Changes Window for Restore Factory Settings.....	33
Figure 4-12.	Factory Settings Restored Web Page.....	33

# 1 Product Introduction

Thank you for purchasing the RMM6300 Ruggedized Mobile Modem (RMM). **It is important to note that the RMM6300 device is similar internally to the VMM6300 (Vehicle Mounted Modem), but sports a ruggedized external enclosure. Because of the similarity of these two devices, references to the VMM will be made in the setup configuration procedures throughout this Users Guide. Please note that all the instructions pertaining to the VMM also apply to the RMM.**

The RMM6300 and the VMM6300 are designed to integrate with the Mesh Enabled Architecture (MEA) wireless communication system capable of supporting high data rate mobile communication at variable rates of vehicular speeds. This document provides detailed installation and configuration instructions for the MEA RMM6300 device.

The RMM6300 is a wireless modem that has been designed for permanent in-vehicle mounting. It provides access to the MEA network via an Ethernet connection to mobile data terminals, laptop computers, or any other device that has an Ethernet port. The RMM operates on 5 to 14 VDC and is rugged enough for installation in commercial and public safety vehicles.

The RMM and VMM efficiently combine the functionality of a MEA subscriber device and client modem into a single cost-effective wireless network component. This makes it easy for any Ethernet-ready device to access a MEA mobile broadband network. Computers, IP video cameras, sensors, signs, signals, etc. can all be Mesh Enabled to send and receive data at burst rates of up to 6 Mbps. All standard subscriber device functionality including Multi-Hopping™, non-line-of-sight communications and geo-location services are fully supported.

The MEA Ruggedized Mesh Modem allows connection of multiple IP addressable devices using standard Ethernet connectivity. This allows devices that cannot accept the PCMCIA based WMC6300 product to function transparently on a MEA network without additional drivers.

## 1.1 Product Contents

Each MEA RMM is a full-featured wireless networking device. The following is a list of the items provided with each RMM:

- MEA Ruggedized Mobile Modem (flange mount)
- 15 foot cable assembly
- 1 Mag Mount 0 dBi antenna.
- 1 N-type to SMA adapter

## 1.2 Product Specifications

The following specifications shown in the table below apply to the RMM6300.

**RMM Product Specification Table**

<b>RMM6300 Physical Specifications</b>	
Dimensions	6 1/8" x 6 1/8" x 2"
Weight	1.8 lbs



Packaging	7.374" x 6.250" x 4.090"
Std Mounting	Sheet metal screws, not provided
<b>POWER</b>	
Power Requirement	5-14 VDC
Current Drain	1.5 amps
Power Consumption	Rx 1.0 amp / Tx 1.5 amp
Power Cable	External DC Power Cable
<b>RADIO CHARACTERISTICS</b>	
Output Power:	24 dBm
Receive Sensitivity:	-85 dBm
RF Modulation:	QDMA
Operating Freq (GHz):	2.4000-2.4835
Tot. Spectrum Used	80MHz
Antenna Type (std):	Omni, 0 or 4dBi
Antenna Connector:	N-Type Female
<b>ENVIRONMENTAL</b>	
Temp range	-35 to 60C
Humidity	0 to 100%
Certification	FCC Part 15, UL, CE Mark, CSA
Vibration – MIL Std	vibration - MIL Standard 810F, Method 514.5 Procedure 1, Category 24
Vibration - TIA	vibration - TIA/EIA-603, paragraph 3.3.4
IP ##	IP54
<b>NETWORK</b>	
Management	MeshManager via SNMP
Net Interface	10/100 Mbps Ethernet, RJ45, Sealed Ethernet boot, No cord included
Web Interface	Web (HTTP) based management interface
Serial Interface	One Standard Serial Port
<b>WARRANTY</b>	
Standard	1 yr standard

## 2 Device Installation

### 2.1 Software Requirements

Two types of software interfaces will be required during the installation and setup process of the RMM3600 device: MeshManager and the RMM Device Administration web interface.

MeshManager software needs to be installed and running on a network computer prior to RMM installation and configuration. MeshManager will be used in the RMM setup process to validate the installation of the device. In addition, MeshManager will be used to manage a RMM and other subscriber devices within the MEA network.

The RMM/VMM Device Administration web interface is used to administer and configure the device and can be accessed by connecting a PC to the wired interface. Additional information is provided later in the manual.

Detailed information about MeshManager software and its usage is found in the following publications: *MeshManager User's Guide* and *QuickStart for MeshManager*.

### 2.2 Equipment Requirements

A RMM6300 is utilized similarly to a subscriber device within a MEA network and will be used with the IAP6300 and MWR6300 infrastructure devices.

The following list defines the standard MEA hardware components to install a RMM:

- N-type Antenna Connector
- 0dBi Antenna (supplied)
- 15 foot cable assembly

The Network Operator must supply the following:

- Mounting Location
- Power Source (12V DC) (from vehicle or other DC power supply)
- A Hub or Switch (if more than 1 Ethernet device will be used)
- Hand tools for bracket installation



## 2.3 MAC Address Label Location

The transceiver and SBC (Ethernet) MAC addresses are listed on the label located on the side of the RMM unit. Record these numbers in the MAC Address Table provided in the next section.

### 2.3.1 MAC Address Table

The MAC Address table has been included for recording the Ethernet MAC address and transceiver MAC address for a set of RMM devices as a quick reference. These addresses will be required later in the configuration and management process.

Write the MAC numbers into the MAC Address Table provided below.

MAC Address Table	
MAC Address (00-05-12-0A-xx-yy)	ETH MAC Address (00-05-12-30-xx-yy)

## 2.4 RMM6300 Assembly Information

The RMM6300 Assembly shows the external connection points on a RMM6300 box.

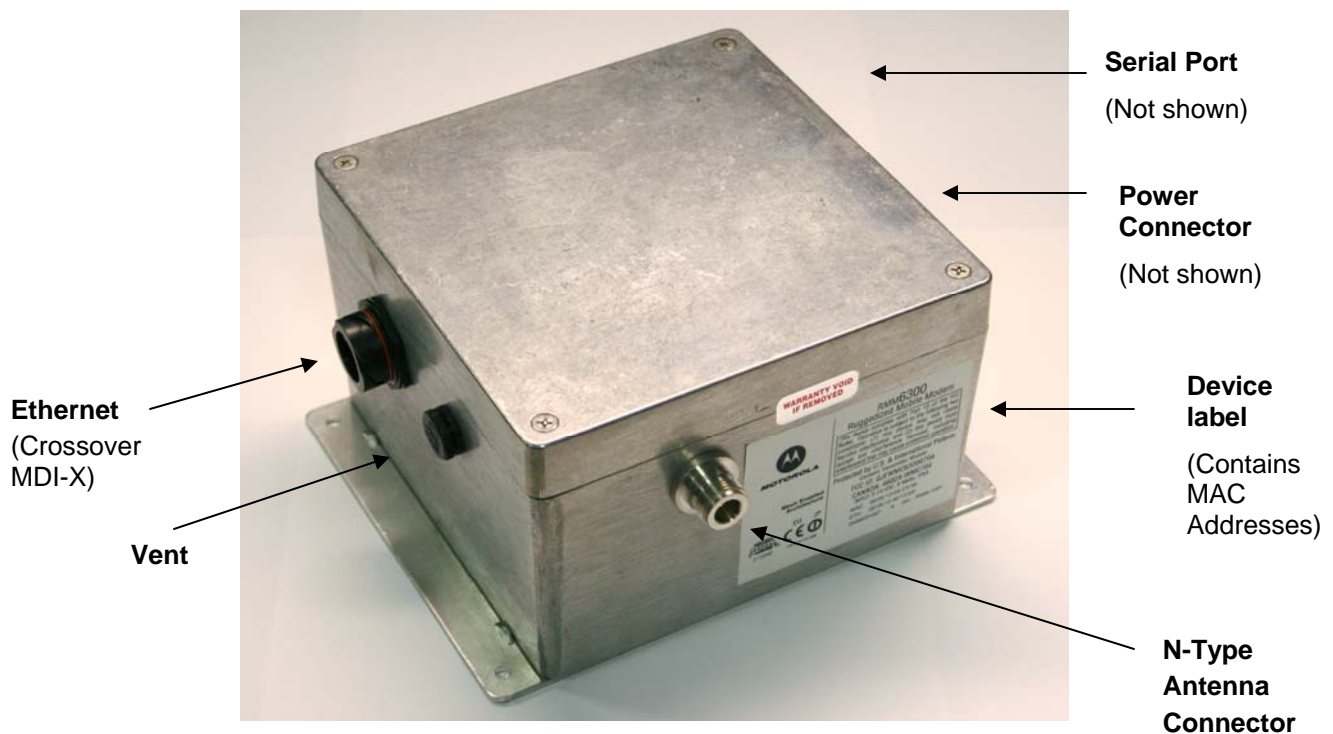


Figure 2-1. RMM External Connection Points

## 2.5 Installing the RMM6300 Device

The following instructions describe the RMM6300 hardware installation procedure:

1. Mount the RMM box in a suitable location to allow for ventilation. Note that the device is not waterproof and should be reasonably protected from moisture and other exposed outdoor environments.
2. Connect the antenna to the N-type connector.
3. Insert the Power Plug into DC Power Connector.
4. Verify that both MAC addresses have been recorded in Section 2.3.1, as this information will be required to configure and test the device.
5. If installing more than one IP device to the RMM6300, a separate hub device can be connected to the RMM ETH port. Up to three IP devices can be provisioned to interface with the RMM.

NOTE: For more information about how to configure additional devices to the RMM, refer to the [External Device Provisioning](#) section of this manual.

### 2.5.1 Deployment Considerations

When deploying the RMM6300 consider the following:

- The antenna should be a minimum of 30 inches from any nearby metal poles to avoid distortion of the RF pattern.



- The antenna must have a separation distance of at least 2 meters from the body of all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Users and installers must be provided with antenna installation and transmitter operating conditions to satisfy RF exposure compliance.
- Typically, Ruggedized Mobile Modems are distributed within a network and are used as subscriber devices. A rule of thumb is to deploy 2-3 hop networks to optimize range, latency, and throughput to subscriber devices.
- The RMM6300 installation location must provide applicable DC power for the device.
- It is **required** that the RMM chassis be grounded to minimize the possibility of ESD (electrostatic discharge) induced damage.

### **2.5.1.1 Deployment Tips**

Locate the antenna to minimize multipath:

- Minimize interference from nearby transmitters
- Maximize chance of a direct line of sight connection to other devices.
- Mount the supplied antenna vertically

## **2.6 Testing the Device Installation**

**Note:** By default, Subscriber Devices (SDs) and VMMs are not automatically loaded into MeshManager's DeviceManager. This is as designed, due to the possibility of too many SDs and VMM slowing down the application.

Verify the operation of the RMM6300 using the following procedure:

1. Apply power to the RMM6300.
2. Obtain the transceiver MAC address and the ETH address that was recorded earlier in section [2.3.1](#). The address will be in the format 00-05-12-0A-xx-yy for the transceiver and 00-05-12-30-xx-yy for ETH.
3. From the MeshManager software screen, display the devices using the MAC address.  
**Note:** This step assumes that the MeshManager software has been installed and running on a networked computer.
4. To load subscriber devices within the MeshManager software screen, select **File | Load Subscriber Devices**.
5. Double-click on the specific device in MeshManager's *device tree* section to verify a successful loading of the device stats.
6. Select the desired RMM in the *device tree*. **Note:** The RMM device will be shown as a VMM device.
7. Right-click on the device *MAC Address (in the device tree)* and select the **Ping** option. A successful response to the Ping command verifies that the RMM is communicating to the infrastructure devices.

## 3 Device Configuration

### 3.1 IP Addressing Considerations

The RMM/VMM provides network access to one or more IP devices connected to the Ethernet port of the RMM. In order for the RMM to provide service to the IP devices, some configuration must be done prior to connecting the IP devices.

The local default gateway address is used only on the wired interface, and is only visible to the attached IP devices. It is not advertised to the wireless network, and the network cannot access the RMM using this gateway address. The RMM has another IP address for the wireless interface that can be used to access the RMM from the network. Because the gateway address is limited to the local wired interface, the same address could be used for the gateway service in several RMM client devices. The local gateway should be a part of the overall subnet chosen for your MEA network.

Care must be taken to ensure that the selected IP address is on the same subnet and does not conflict with any other devices or the chosen Local Gateway service address on the MEA network.

### 3.2 Accessing the MEA Device Administration Web Pages

To modify the IP configuration for the RMM using the web interface, you must know the IP address assigned to the RMM SBC. The mechanism for assigning the IP address is controlled by the addressing mode of the RMM SBC. Regardless of the mechanism, the assigned IP address can always be displayed using MeshManager.

If the factory setting is used, then the default addressing mode will be *Remote DHCP*, and the RMM SBC IP address will be assigned by the network DHCP server.

If the SBC addressing mode was changed to *Statically Provisioned*, and an IP address was entered, then the entered IP address will be used.

If the SBC addressing mode was changed to *Statically Provisioned*, but no IP address was entered, then the default SBC IP address will be derived from the transceiver MAC address (10.xx.yy.1, where the MAC address is 00:05:12:0A:XX:YY), similar to the default IP addresses described in [External Device Provisioning](#). XX and YY are hex values from the transceiver MAC address, and the lowercase xx and yy are the same values in decimal. For example, a RMM with a transceiver MAC address of 00:05:12:0A:80:20 would have a default SBC IP address of 10.128.32.1.

When the IP address is known, the device web page can be accessed by pointing your web browser to the IP address of the RMM SBC. For example, if the RMM SBC address is 10.128.32.1, then the web page would be found at *http://10.128.32.1/*.

#### 3.2.1 Administrator and Access Account Information

The device has two accounts for the web pages - an **administrative account**, and an **access account**. The administrative account must be used for provisioning the device, and the access account may be used for monitoring the status of the device.

**NOTE:** If you are running a RMM/VMM as a standalone device, the configuration web page can be reached by connecting a PC to the wired interface. The installation procedure described here



requires administrator access. Alternatively, all of the parameters that are provisioned via the web page may be provisioned via MeshManager instead.

### 3.2.1.1 Password Information

#### Administrator Password

The username is *admin* and the default (initial) password is *admin*.

The password for the *admin* account should be changed during installation.

#### Access (User) Password

The username is *monitor* and the default password is *monitor*.

The password for the *Access* account can be changed by the administrator.

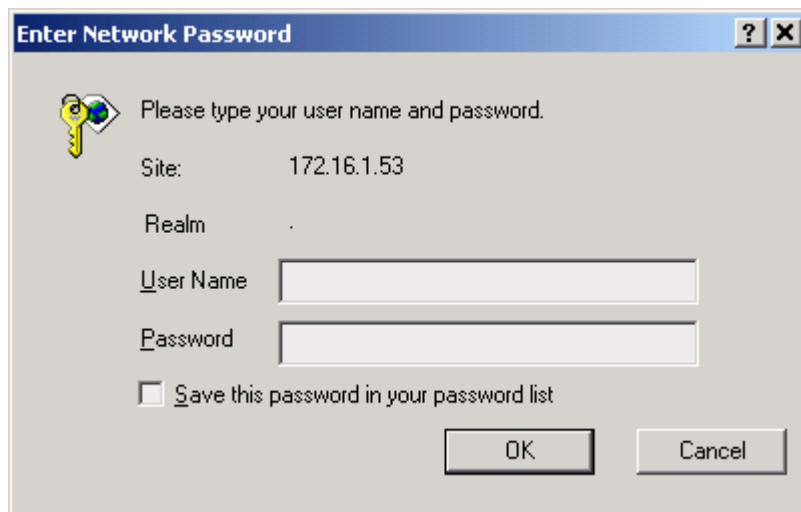
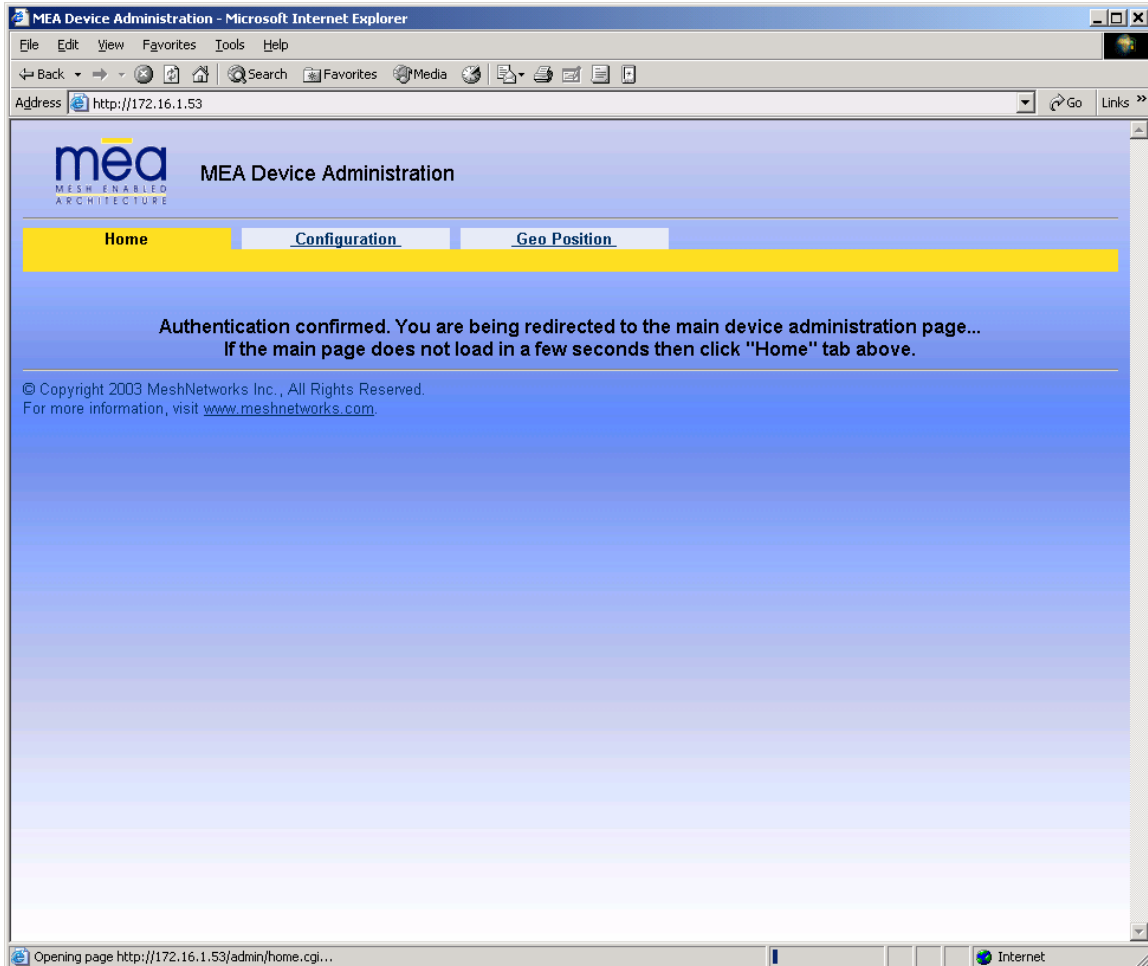


Figure 3-1. Enter Network Password Initial Web Page Authentication Dialog

### 3.2.2 Viewing MEA Device Administration Redirect Page

After the login authentication has been completed, the web browser will display a *redirecting* page, and your browser will automatically transition to the home web page for MEA *Device Administration*.



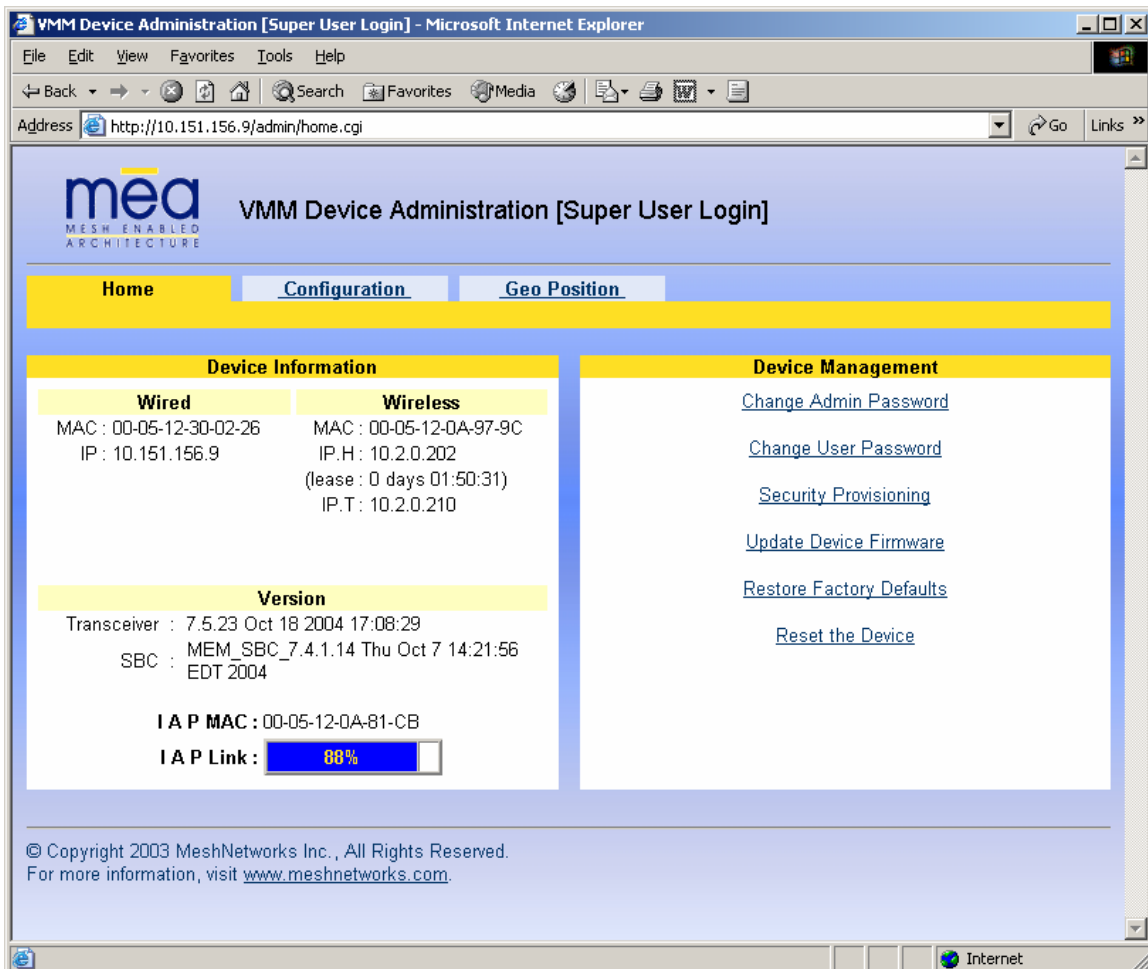
**Figure 3-2. MEA Device Administration Redirecting Web Page**

### 3.2.3 Viewing MEA Device Administration Home Page as an Administrator

The *MEA Device Administration* home page provides you with some basic information about the device, including the IP addresses assigned to the device, the MAC addresses of the device, the firmware revision number, and the reported link quality for the link to the IAP.

Additional web page links are available when logging-in as an Administrator (same as Super User). In the **Device Management** section of the **Home** tab, the Administrator can:

- Change Admin password
- Change User password (Access Account)
- Security Provisioning
- Update Device Firmware
- Restore Factory Defaults
- Reset the Device



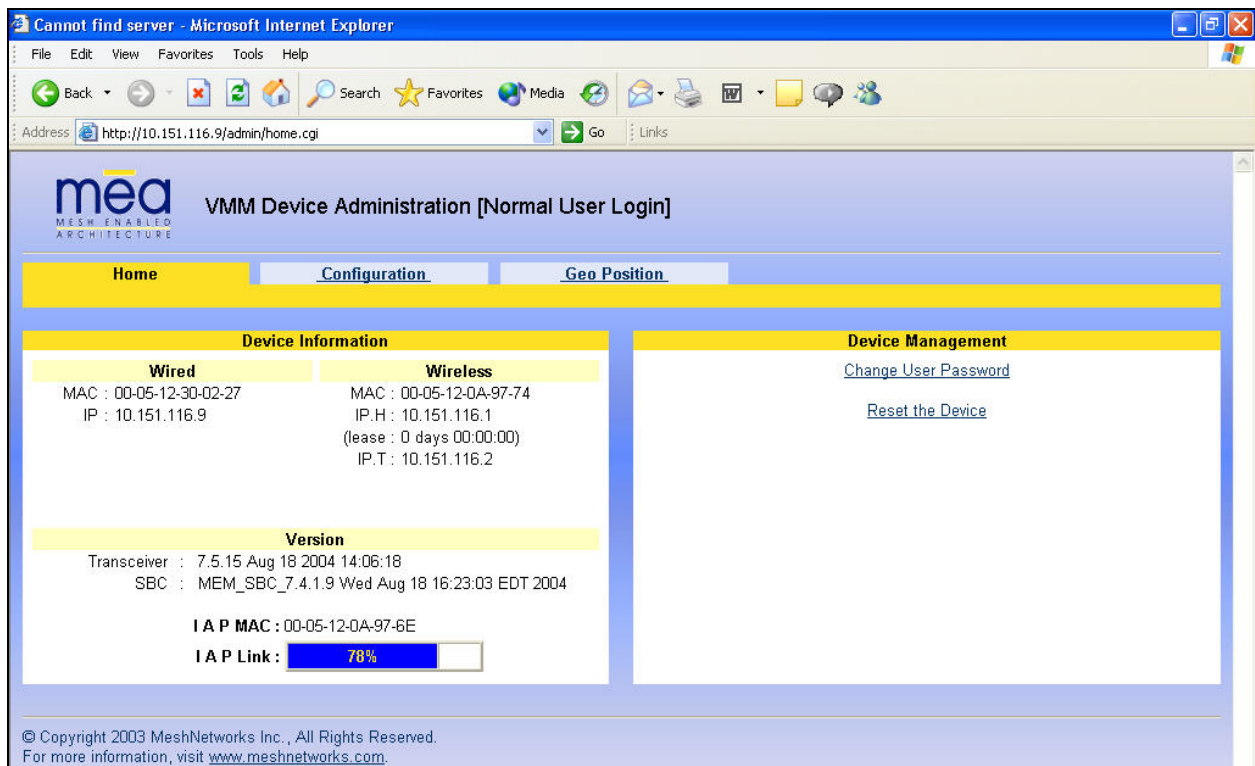
**Figure 3-3. MEA Device Administration Home Page (Super User Login)**

### 3.2.4 Viewing MEA Device Administration Home Page as a Normal User

The *MEA Device Administration* home page provides the Normal User (same as Access Account) with some basic information about the device, including the IP addresses assigned to the device, the MAC addresses of the device, the firmware revision, and the reported link quality for the link to the IAP.

In the **Device Management** section of the **Home** tab, the Access Account User can:

- Change User password
- Reset the Device



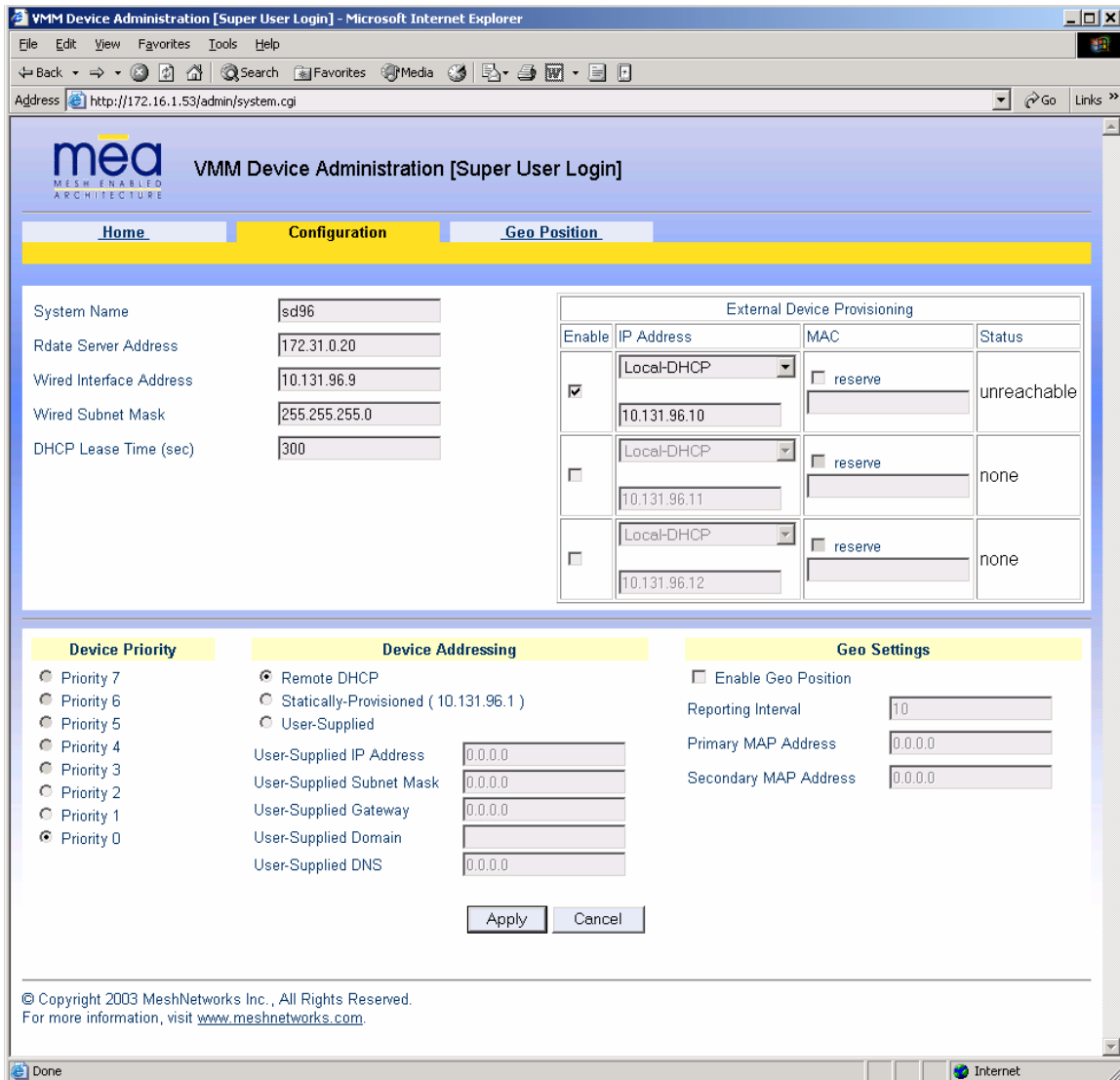
**Figure 3-4. MEA Device Administration Home Page (Normal User Login)**

### 3.2.5 RMM Device Administration Configuration Tab

Once you have accessed the MEA Device Administration home page, click on the *Configuration* tab to display the IP address configuration.

#### 3.2.5.1 Viewing the RMM Configuration Tab as an Administrator

The *RMM Device Administration Configuration* page when viewed as an Administrator (same as Super User Login) allows for changes to the configuration of the *RMM6300*.



**Figure 3-5. RMM Device Administration Configuration Page (Super User Login)**

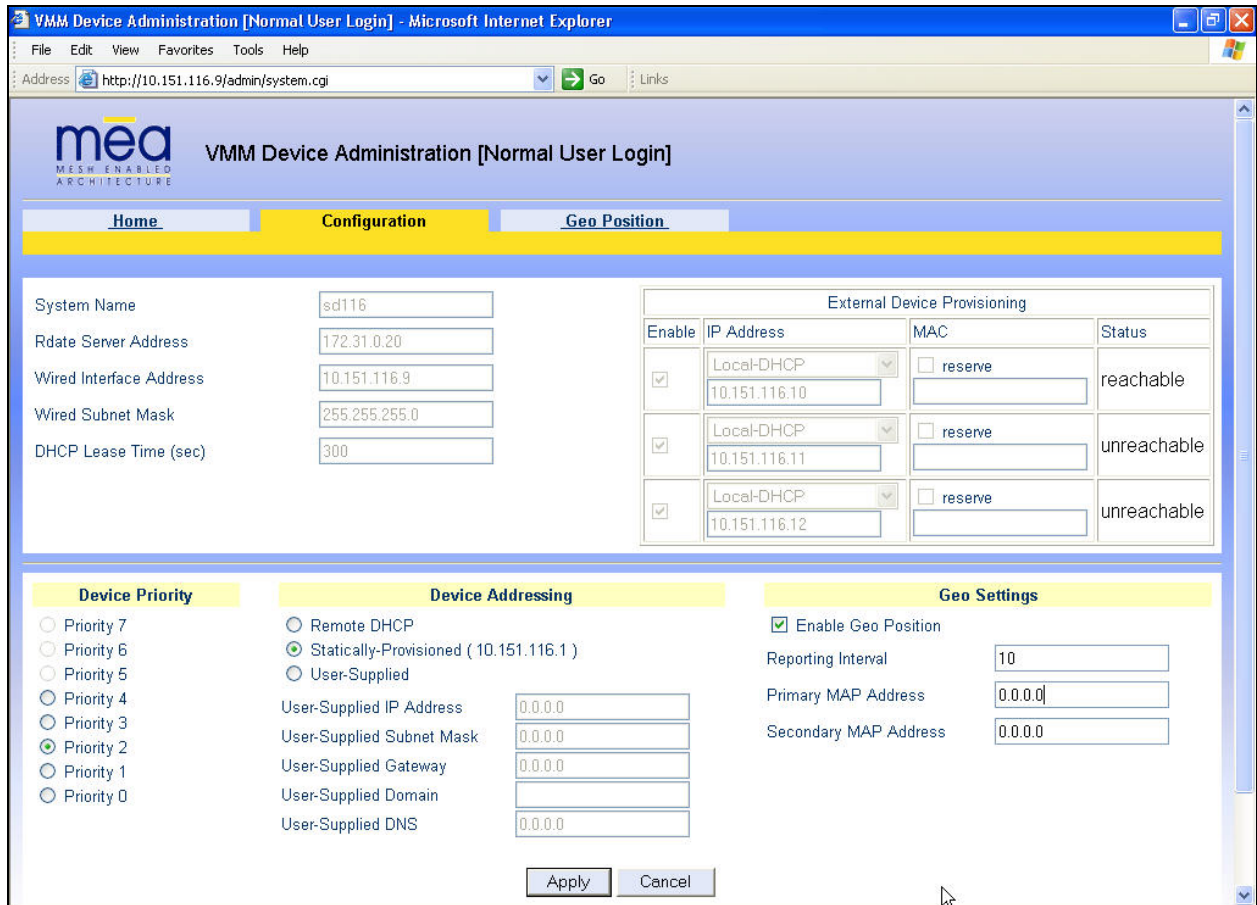
The fields displayed in the *Configuration* tab are described in the following table.

<b>RMM Device Administration Page Fields (Administrator / Super User Login)</b>		
<b>Field Name</b>	<b>Field Description</b>	<b>Field Default Value</b>
<b>System Name</b>	This is the name of the device as shown by MeshManager	Assigned by Network Administrator
<b>RDATE Server IP Address</b>	The IP address of the RDATE server. This is usually the MiSC when operating in infrastructure mode. The RDATE server provides the current date to the RMM. The RMM can operate without an RDATE server.	172.31.0.20
<b>Wired Interface Address</b>	The RMM will tell the attached Ethernet devices to use this address for the default gateway, and the RMM will use the address when accessing the local Ethernet segment.	MAC-derived
<b>Wired Interface Subnet Mask</b>	This is the subnet mask for the local Ethernet segment.	255.255.255.0
<b>DHCP Lease Time</b>	This is the duration (in seconds) of the DHCP leases that the RMM offers to the attached Ethernet devices.	300
<b>Device Priority</b>	The Device Priority provisioning area allows the operator to set the priority assigned to wireless messages transmitted by this device. A priority of 7 is the highest priority setting.	Levels 0-7 are available, based on your configuration as set by the Network Administrator
<b>Geo Settings</b>	The <i>Geo Settings</i> area allows the operator to enable and disable the Geo Reporting feature (if provisioned), as well as control the frequency of reports and provision the destination server to which those Geo reports will be sent. Requires entry of the primary Map server's IP address. The secondary Map address is optional.	Reporting Interval is set to 10 seconds.

The *External Device Provisioning* frame of this web page is described in [Section 3.5](#).

### **3.2.5.2 Viewing the RMM Configuration Tab as a Normal User**

A similar screen will be displayed for the Access account (the web page will indicate *Normal User Login*). Normal users can change only those settings for which they have system privileges.



VMM Device Administration [Normal User Login] - Microsoft Internet Explorer

Address: http://10.151.116.9/admin/system.cgi

mea MESH-ENABLED ARCHITECTURE

VMM Device Administration [Normal User Login]

Home Configuration **Geo Position**

System Name: sd116

Rdate Server Address: 172.31.0.20

Wired Interface Address: 10.151.116.9

Wired Subnet Mask: 255.255.255.0

DHCP Lease Time (sec): 300

External Device Provisioning			
Enable	IP Address	MAC	Status
<input checked="" type="checkbox"/>	Local-DHCP 10.151.116.10	<input type="checkbox"/> reserve	reachable
<input checked="" type="checkbox"/>	Local-DHCP 10.151.116.11	<input type="checkbox"/> reserve	unreachable
<input checked="" type="checkbox"/>	Local-DHCP 10.151.116.12	<input type="checkbox"/> reserve	unreachable

**Device Priority**

Priority 7  
 Priority 6  
 Priority 5  
 Priority 4  
 Priority 3  
 Priority 2  
 Priority 1  
 Priority 0

**Device Addressing**

Remote DHCP  
 Statically-Provisioned ( 10.151.116.1 )  
 User-Supplied

User-Supplied IP Address: 0.0.0.0  
 User-Supplied Subnet Mask: 0.0.0.0  
 User-Supplied Gateway: 0.0.0.0  
 User-Supplied Domain:   
 User-Supplied DNS: 0.0.0.0

**Geo Settings**

Enable Geo Position  
 Reporting Interval: 10  
 Primary MAP Address: 0.0.0.0  
 Secondary MAP Address: 0.0.0.0

Apply Cancel

**Figure 3-6. RMM Configuration Page (Normal User Account)**

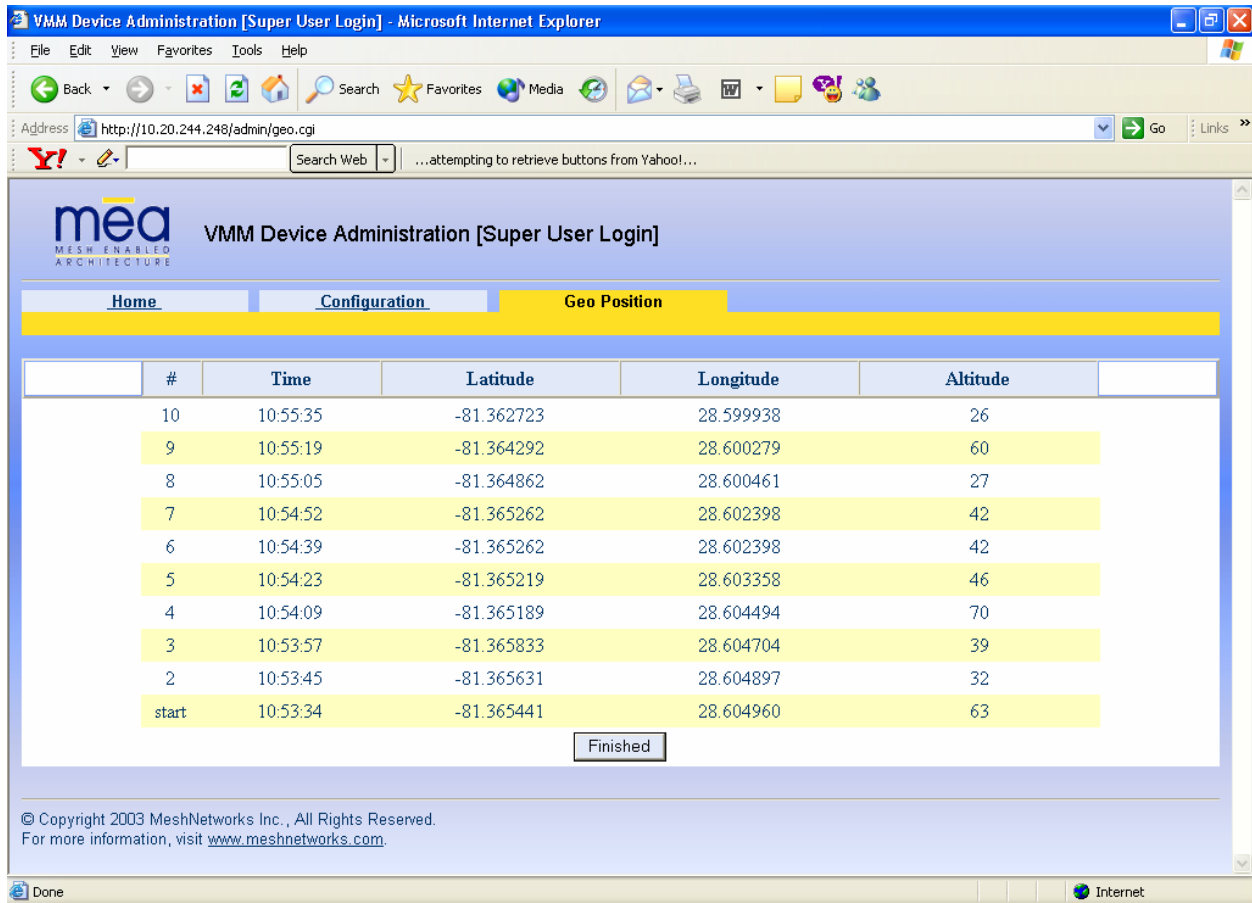
### 3.2.6 RMM Device Administration Geo Position Tab

The geo position feature has to be provisioned on the destination or map server by the Network Administrator.

Before any data can be viewed on the *Geo Position* tab:

1. The **Enable Geo Position** check box has to be checked on the *Configuration* tab, in the **Geo Settings** section of the screen.
2. The map server's IP address needs to be provided in the **Primary Map Address** field in the **Geo Settings** section. The **Secondary Map Address** is optional.

For additional information about the Geo Location feature, refer to the *MeshPositioning Application Users Guide*.



**Figure 3-7. Geo Position Tab (Same view for Super User and Normal accounts)**

The *Geo Position* tab displays readings of the RMM device when the feature is enabled. The information contained on this screen will look the same to the Administrator and to the Access User role.

### 3.3 Device Addressing Schemes

The concept of unified modes of operation centers on the current state of network communication: Associated State and Unassociated State. In the associated state, the device is using infrastructure equipment to communicate. In the unassociated state, the device operates in peer-to-peer mode. There are three addressing schemes which allow the IT manager increased flexibility in deployment: Network DHCP, Statically Provisioned, and User Supplied.

All of these schemes may be assigned per device, either by the user or by the network manager. The network manager can also limit the user-selectable schemes or force a specific scheme. Devices in each of these schemes can interoperate and communicate with each other, so long as the assigned addresses do not conflict and are mutually routable.

### 3.3.1 Network DHCP Scheme

*Network DHCP* means that the RMM device can be configured to request an address from a DHCP server and requires the inclusion of a DHCP server in the core network configuration to answer these requests. With Network DHCP selected, the RMM will send DHCP requests for its own address to the core network once it becomes associated and establishes communications with the infrastructure. Operation under the Network DHCP scheme allows users to temporarily wander outside of the network infrastructure without losing connectivity.

The server may be configured by the operator to hand out temporary or static leases. The RMM must associate and acquire an address from the network before establishing communications. Once a lease has been granted, the address will be valid out of network coverage for the remainder of the lease or, if a static lease was granted, until the next power cycle. If the lease expires or the user cycles power while outside of network coverage, the user will again lose the ability to communicate with the wireless network.

This scheme is best for a larger, closely managed network of subscribers who don't need to communicate or communicate only briefly outside of network coverage.

### 3.3.2 Statically Provisioned Scheme

Under the Statically Provisioned scheme, the RMM device will use provisioned DHCP-like information to establish an IP address for use in the wireless network. A DHCP server is not required on the core network because the addresses are derived from the MAC address by default. It should be noted that a DHCP server can still exist on the network to hand out addresses to other nodes using the Network DHCP Scheme as long as the server's address range does not conflict with addresses assigned to devices using the Statically Provisioned or User Supplied Schemes.

The IP addresses and options used are configurable per-device using MeshManager. The provisioned address may be freely used to communicate while associated or unassociated.

The operator must ensure that the provisioned addresses are routable and do not conflict with any other addresses in use. The operator is free to provision any option ordinarily provisioned by a DHCP server (subnet mask, DNS, etc.) through programming of the appropriate fields in each device using MeshManager.

This scheme is ideal for a managed network of users who regularly need to communicate inside and outside of network coverage or for a network lacking a DHCP server.

### 3.3.3 User Supplied Scheme

Operating under the *User Supplied* scheme, the RMM device is configured to use a *fixed* IP address and subnet mask. The user is responsible for configuring options that would otherwise be configured by a DHCP server.

It is also up to the user to ensure that the assigned address is routable on the core network (if core network access is needed) and that it does not conflict with other addresses in use. This is analogous to and carries the same caveats as plugging an Ethernet card into a LAN and manually assigning an address to the card.

The user is free to communicate while associated or unassociated. This scheme is ideal for small, unmanaged networks lacking a DHCP server.

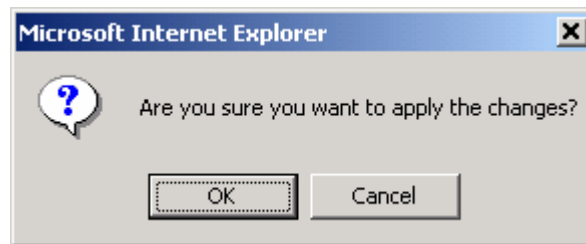
### 3.4 Setting User Supplied IP Addresses

In order to set the user-supplied IP address for the RMM, the User-Supplied radio button must be selected. At that point, the user may enter an IP address and subnet mask consistent with the existing network. The user should also enter the IP address of the default gateway and DNS server, as well as enter the domain name.

Note that this configures the *user-supplied address* for the RMM device. To configure addresses for Ethernet clients, refer to the description in the *External Device Provisioning* section of this guide.

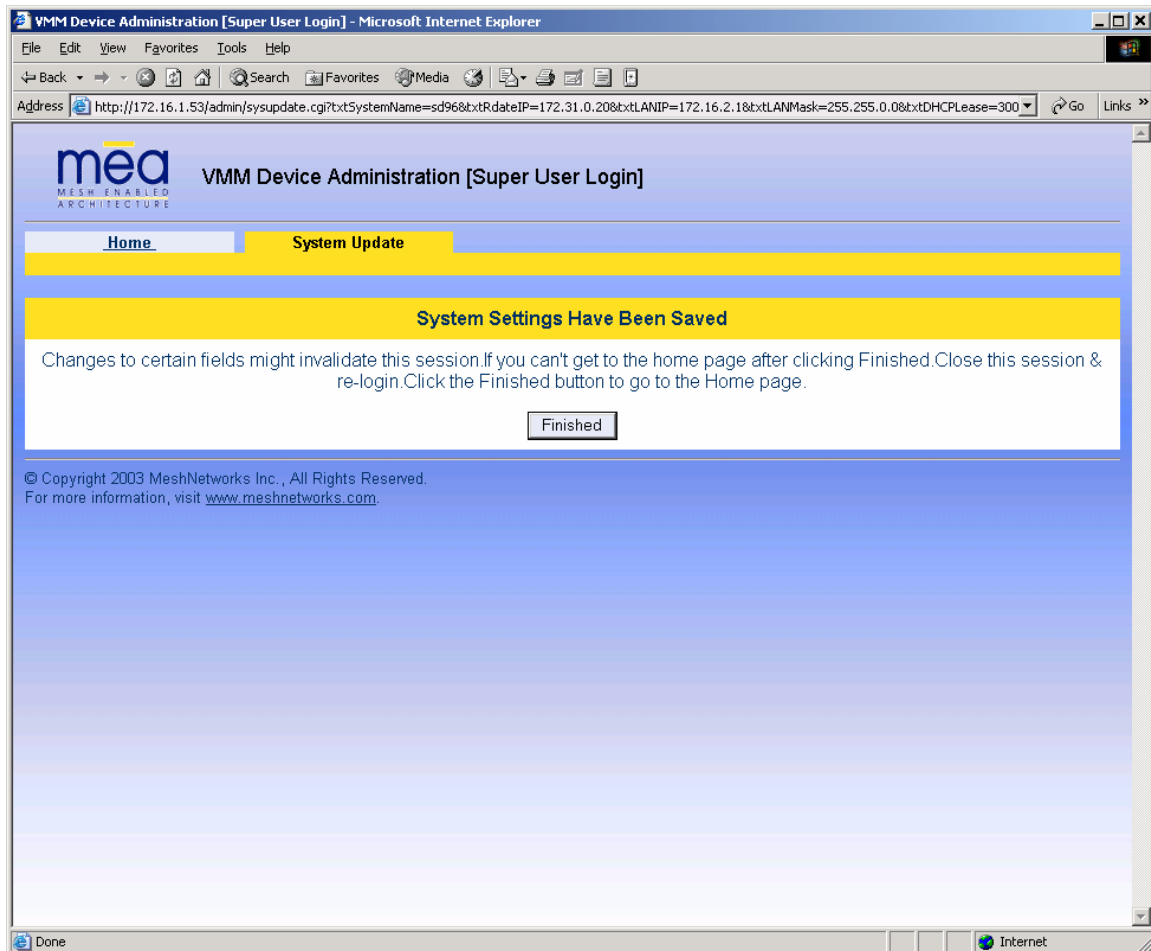
A similar screen will be displayed for the access account (the web page will indicate *Normal User Login*). Normal users can change only those settings for which they have system privileges.

When the desired configuration has been completed, click on the **Apply** button on the *Device Addressing* panel on the Device Administration Configuration Page. You will be prompted to verify that the changes to the configuration are correct before the changes are actually applied.



**Figure 3-8. Configuration Change Dialog**

When you click on the **OK** button, the configuration will be saved in flash. The *System Settings Have Been Saved* message, on the *System Update Save Completed* page, will then confirm that the changes have been saved.



**Figure 3-9. System Update Save Completed Web Page**

After the settings have been saved, click the **Finished** button. Your web browser should return to the *MEA Device Administration* home page. A reboot of the device is not required for the changes to take effect.

### 3.5 External Device Provisioning

The *External Device Provisioning* section of the *RMM Device Administration* page is used to configure addresses for the attached nodes on the local Ethernet segment. Up to three addresses are provisioned.

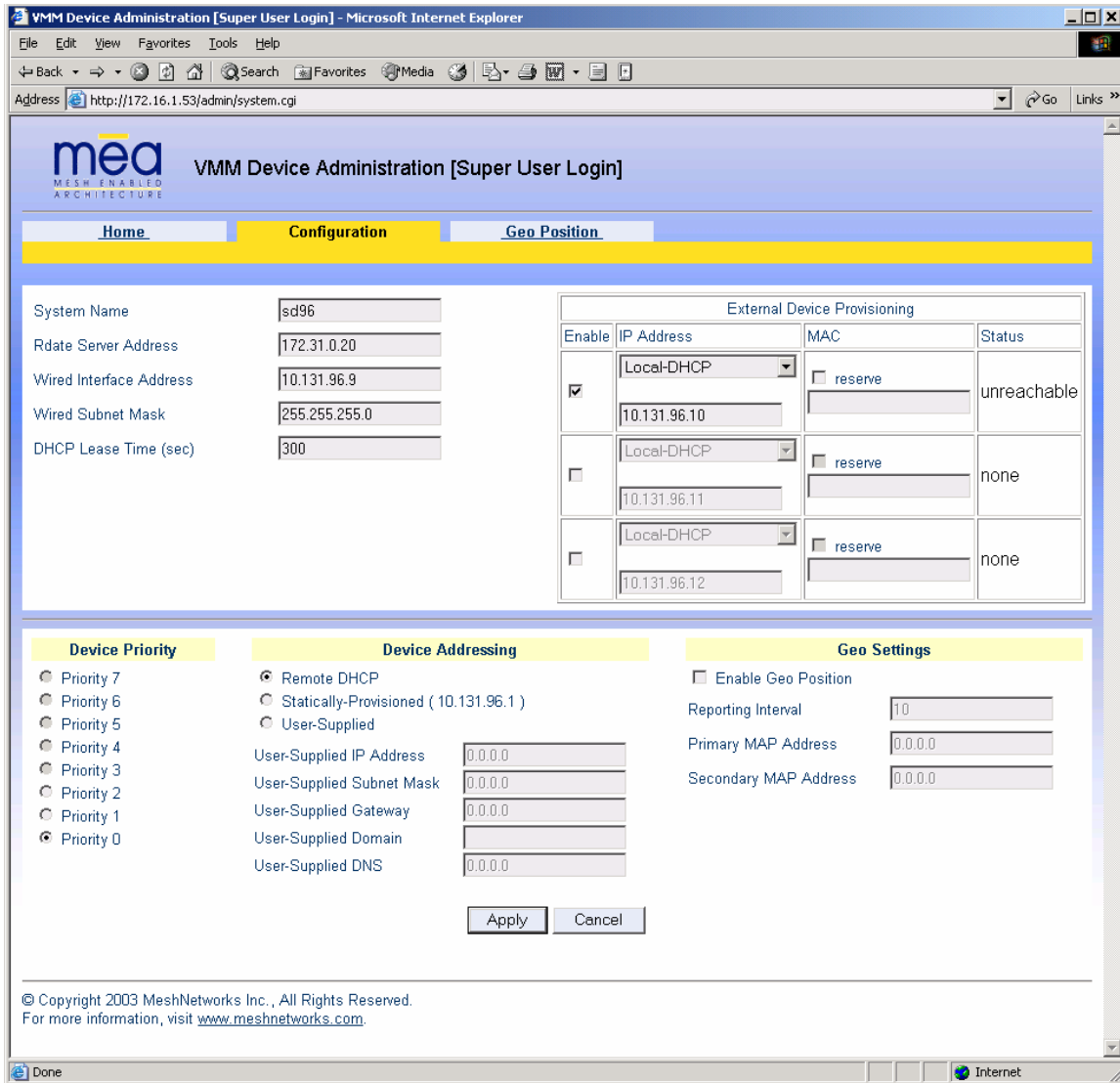


Figure 3-10. External Device Provisioning Table

The *Enable* checkbox indicates this row contains a valid address. Any address can be disabled by clearing the checkbox. The pull-down menu options indicate whether this address will be offered via the local DHCP service (“Local-DHCP”) or “Statically-Provisioned”.

The *Statically-Provisioned* setting is used to support devices that do not use DHCP to acquire an address.

The MAC address field is used for *Local-DHCP* addresses, so that the IP address can be reserved for a specific device. The *reserved* checkbox must be marked for this kind of IP address reservation. The *Status* field indicates whether the provisioned IP address was



detected (via a ping) when the web page was brought up.

The IP addresses default to values based on the transceiver MAC address of the device. The derivation is described below. By default, only the first IP address is enabled (for *local-DHCP*), and no addresses are reserved for specific MAC addresses. Make sure to check the checkbox for the client IP addresses you have entered. Client 2 and Client 3 are not enabled by default.

The RMM has two interfaces and must use two IP addresses. The wireless network must use the IP address on the wireless interface because that is the address for which the IAP will proxy and advertise. The same address will be accessed by the Device Manager when using MeshManager.

The *wired interface address* will be used by the RMM as the gateway address for the local Ethernet segment. The *wired subnet mask* is configurable so that the user may select a more restrictive subnet on the local Ethernet segment than what is normally provided to the wireless subscribers.

The MAC-derived default values are a means to ensure that these devices are likely to work out-of-the-box. The IP addresses are derived as follows:

Transceiver MAC address: 00:05:12:0A:XX:YY

Derived MAC addresses:

Local gateway:	10.xx.yy.9
Client1:	10.xx.yy.10
Client2:	10.xx.yy.11
Client3:	10.xx.yy.12

Where XX and YY are hex values (from the transceiver MAC address), and the lowercase xx and yy are the same values in decimal. For example, a RMM with a transceiver MAC address of 00:05:12:0A:80:20 would have a default local gateway address of 10.128.32.9.

### 3.5.1 Connecting to the Ethernet Port

If only one device is to be connected to the RMM, you can connect directly to the device using an Ethernet cable.

If you are going to connect more than one device to the RMM, you will need to connect a hub to the RMM, and connect the other devices to the hub.

## 3.6 Working with MeshTray

MeshTray™ is a status and configuration application that reports vital and statistical information about the RMM. The application must be run on a client attached to the Ethernet port.

To start the MeshTray application, *double-click* on the MeshTray icon, or from the **Start** menu select **Programs → mea → MeshTray.exe**.

For detailed information about using the MeshTray application, refer to the MeshTray section of the MEA WMC6300 Windows Users Guide documentation.

### 3.6.1 MeshTray Status Information

When the utility is launched, the MeshTray *Status* tab displays useful system information such as a *Description* of the device, the *MAC* and *IP* address of the device, and the *Type* of device (i.e., Ruggedized Mobile Modem, Subscriber Device, etc.). The *Firmware Version* and *Firmware Build Date* displayed here can be used to verify that the correct firmware revision is currently loaded on the device, particularly after a firmware upgrade. The associated *IAP MAC* address and the *IAP Link Quality* are also displayed.

**Note:** Viewing the *Configuration* tab in MeshTray from a laptop that is connected directly to a RMMs Ethernet port, will show the “Addressing Scheme” section as grayed-out, or not available.

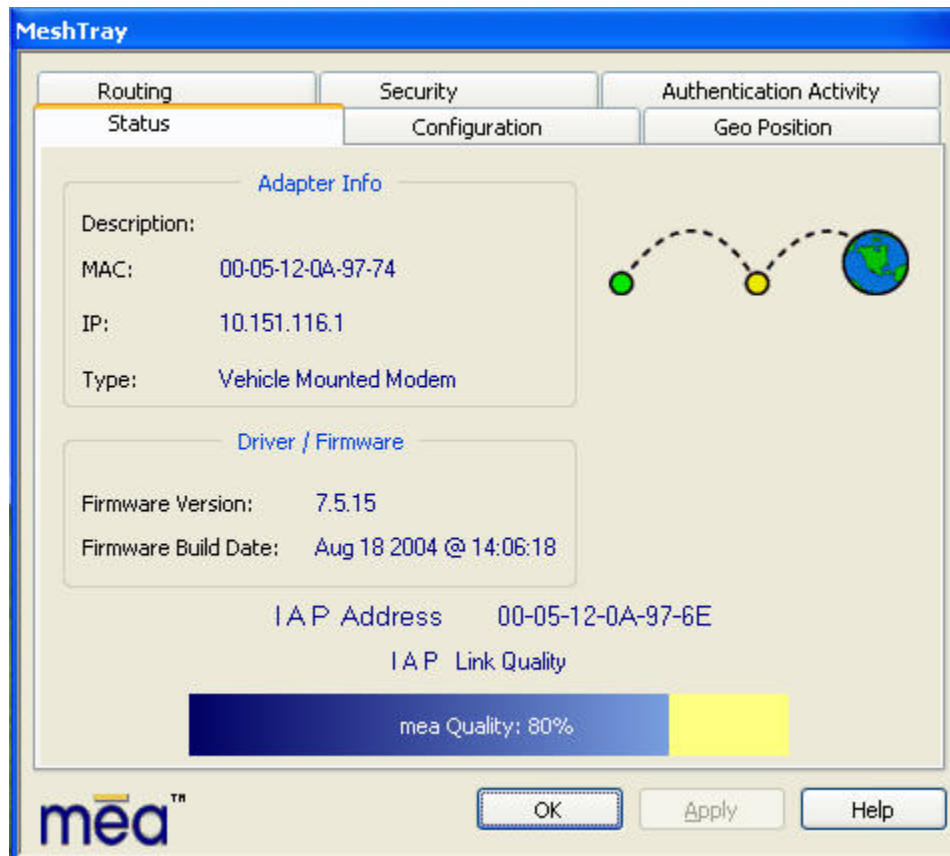
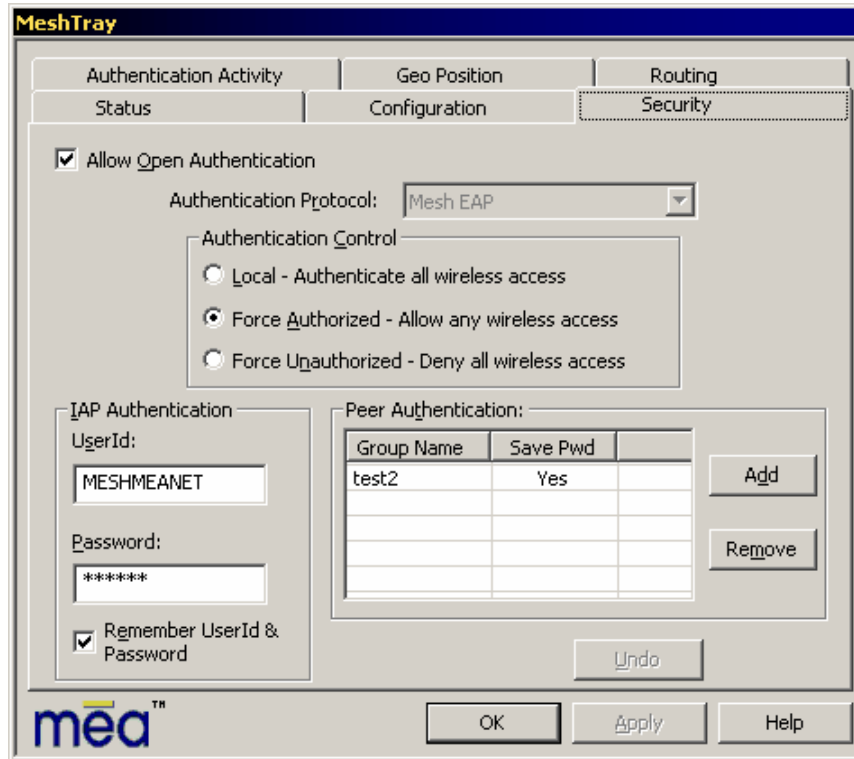


Figure 3-11. MeshTray Status Tab (RMM)

### 3.6.2 MeshTray Security Tab

The MeshTray Security tab allows for setting Open Authentication with Authentication Control and provides IAP Authentication information, as well as Peer Authentication configuration.

The *Peer Authentication* section allows for adding and removing *Group Names* and each of their passwords. There is a maximum of eight group names.



**Figure 3-12. MeshTray Security Tab (RMM)**

### 3.6.3 MeshTray Authentication Activity

The Authentication Activity tab displays any activity occurring between the RMM and the IAP and between the RMM and another Subscriber device (Peer-to Peer). The *Clear* button can be used to delete activities.

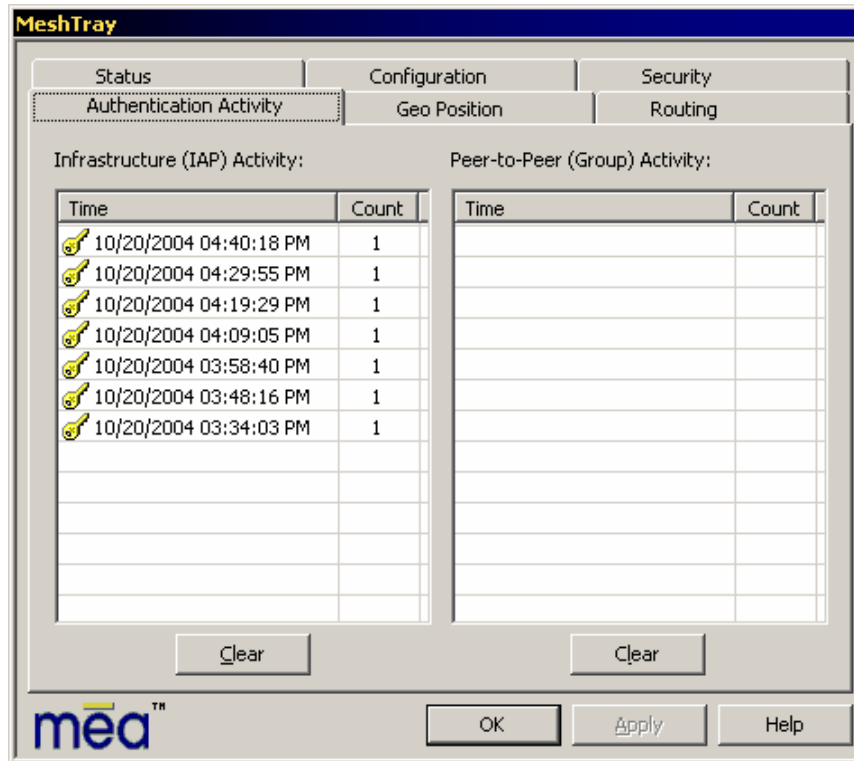
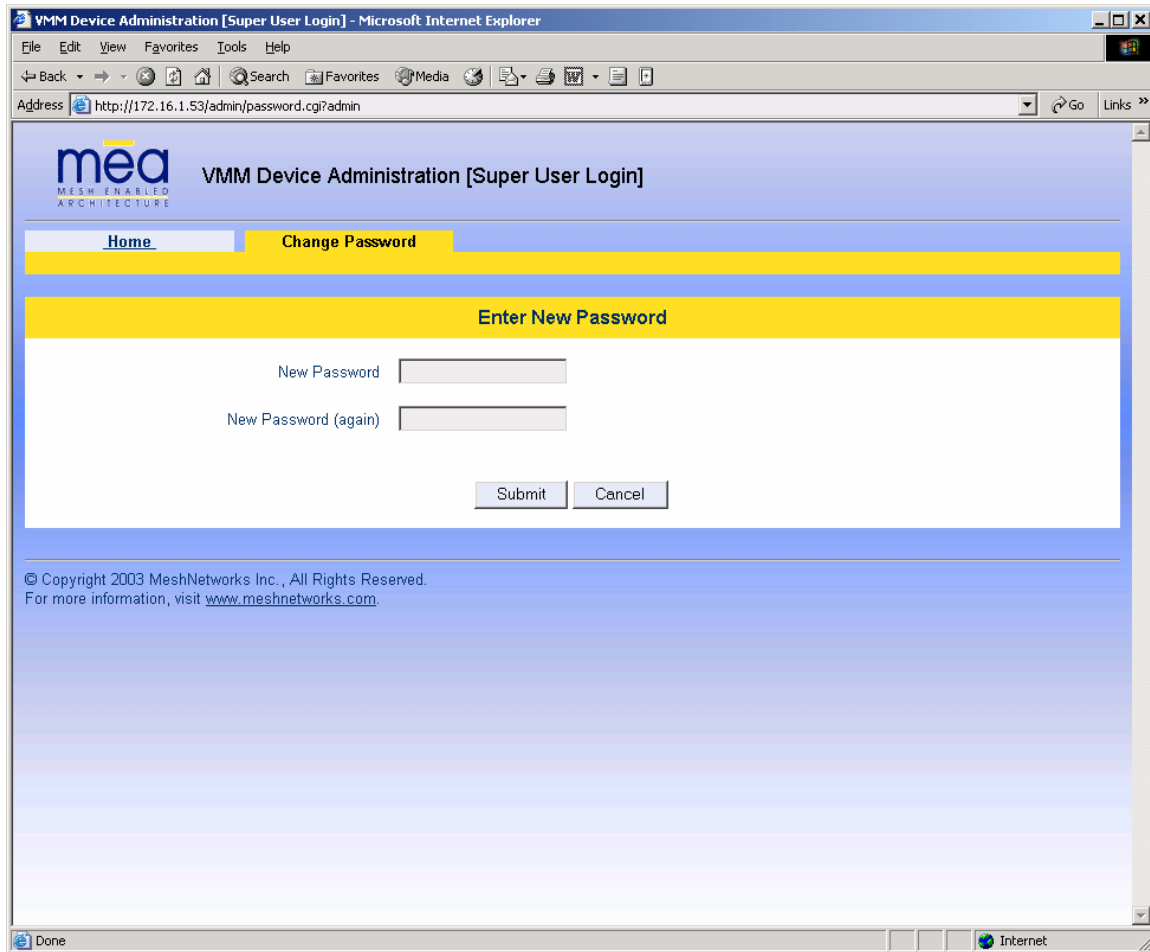


Figure 3-13. MeshTray Authentication Activity tab (RMM)

## 4 Device Maintenance

### 4.1 Changing the Web Interface Password

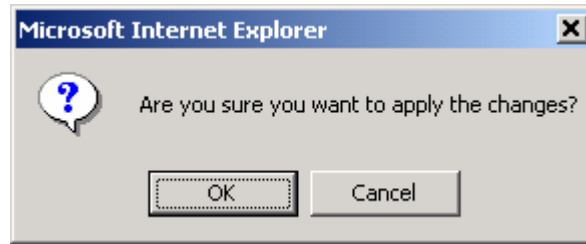
When the *Change Admin Password* function is selected from the *RMM Device Administration* Home Page by the administrator, or the *Change User Password* function is selected, the device will present the following web page:



The screenshot shows a Microsoft Internet Explorer browser window titled "VMM Device Administration [Super User Login]". The address bar displays "http://172.16.1.53/admin/password.cgi?admin". The page content includes the "mea" logo (Mesh Enabled Architecture) and the title "VMM Device Administration [Super User Login]". A navigation bar has "Home" and "Change Password" tabs, with "Change Password" being the active tab. Below this is a yellow header section titled "Enter New Password". The form contains two input fields: "New Password" and "New Password (again)". At the bottom of the form are "Submit" and "Cancel" buttons. A copyright notice at the bottom of the page reads: "© Copyright 2003 MeshNetworks Inc., All Rights Reserved. For more information, visit [www.meshnetworks.com](http://www.meshnetworks.com)."

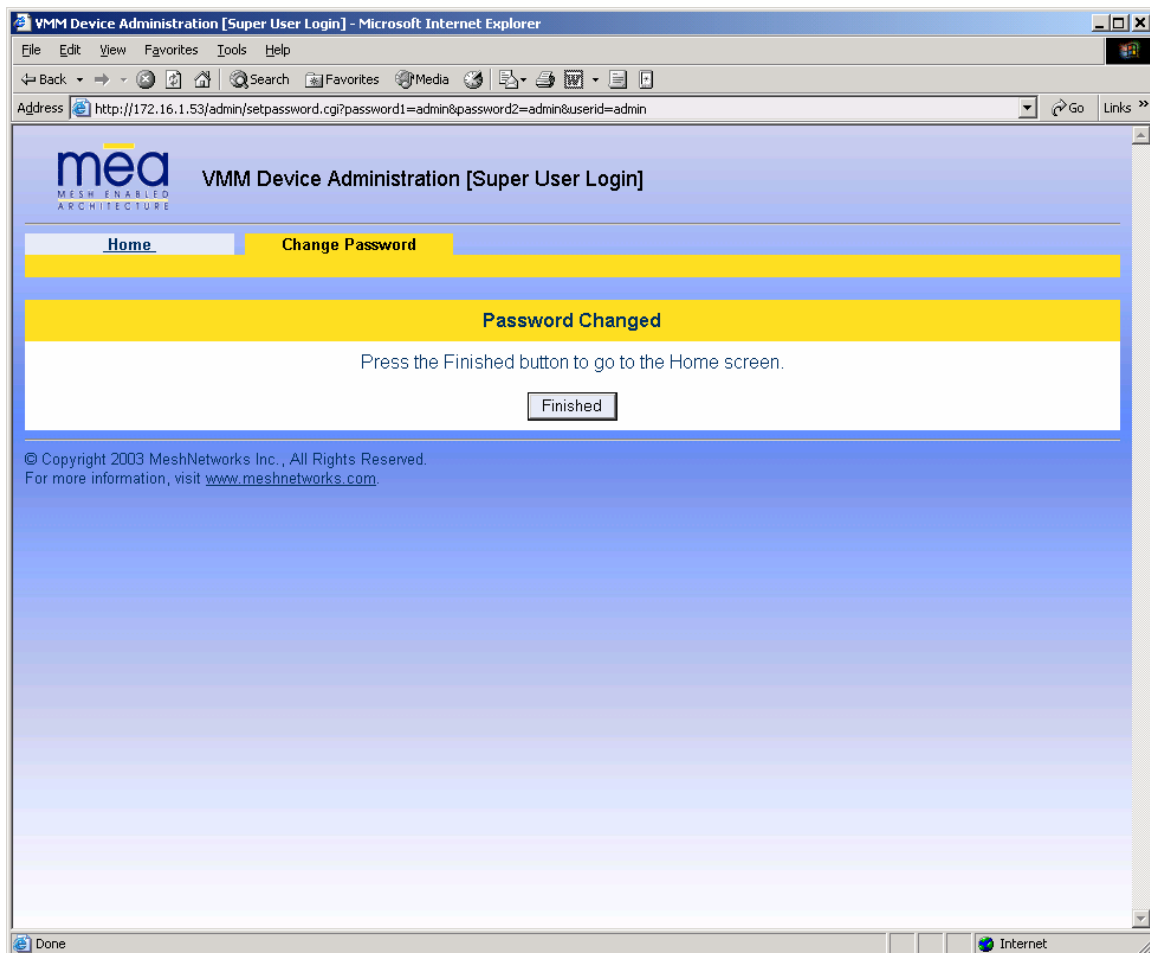
**Figure 4-1. Enter New Password Web Page**

The operator is expected to enter a new password for the web account and click on the “submit” button. Once the password entry is complete, the device will prompt the operator for confirmation of the change.



**Figure 4-2. Confirm Changes Window for Enter New Password**

When the operator confirms the change, the new password will be stored in flash, and the device will present a status screen indicating that the change was successful.

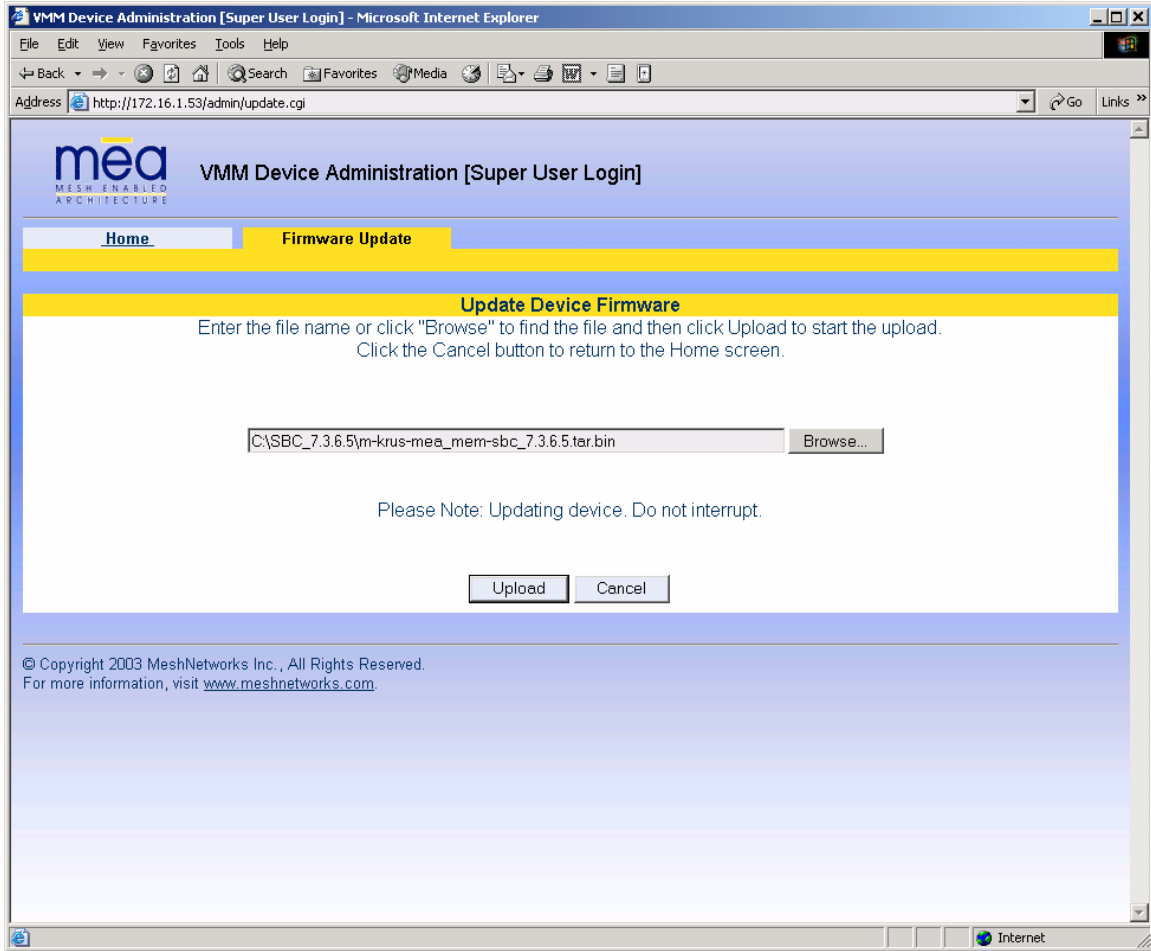


**Figure 4-3. Password Changed Confirmation Web Page**

## 4.2 Upgrading the Device Firmware

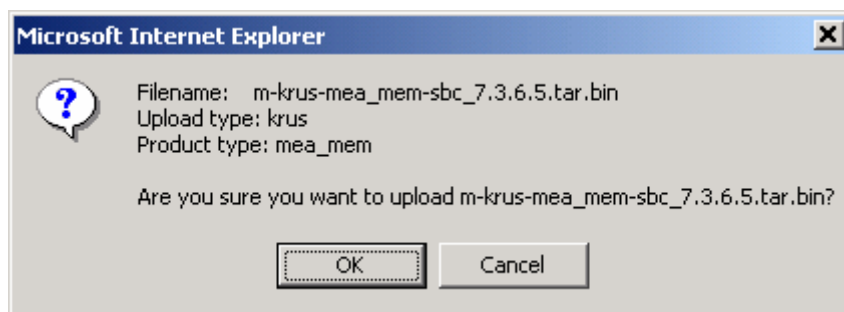
The web interface for the device also provides the ability to upgrade the firmware on-site. To use this feature, you must have an upgrade file from a released upgrade package.

When the *Upgrade Device Firmware* function is selected from the *MEA Device Administration Home Page*, the device will present the following web page:



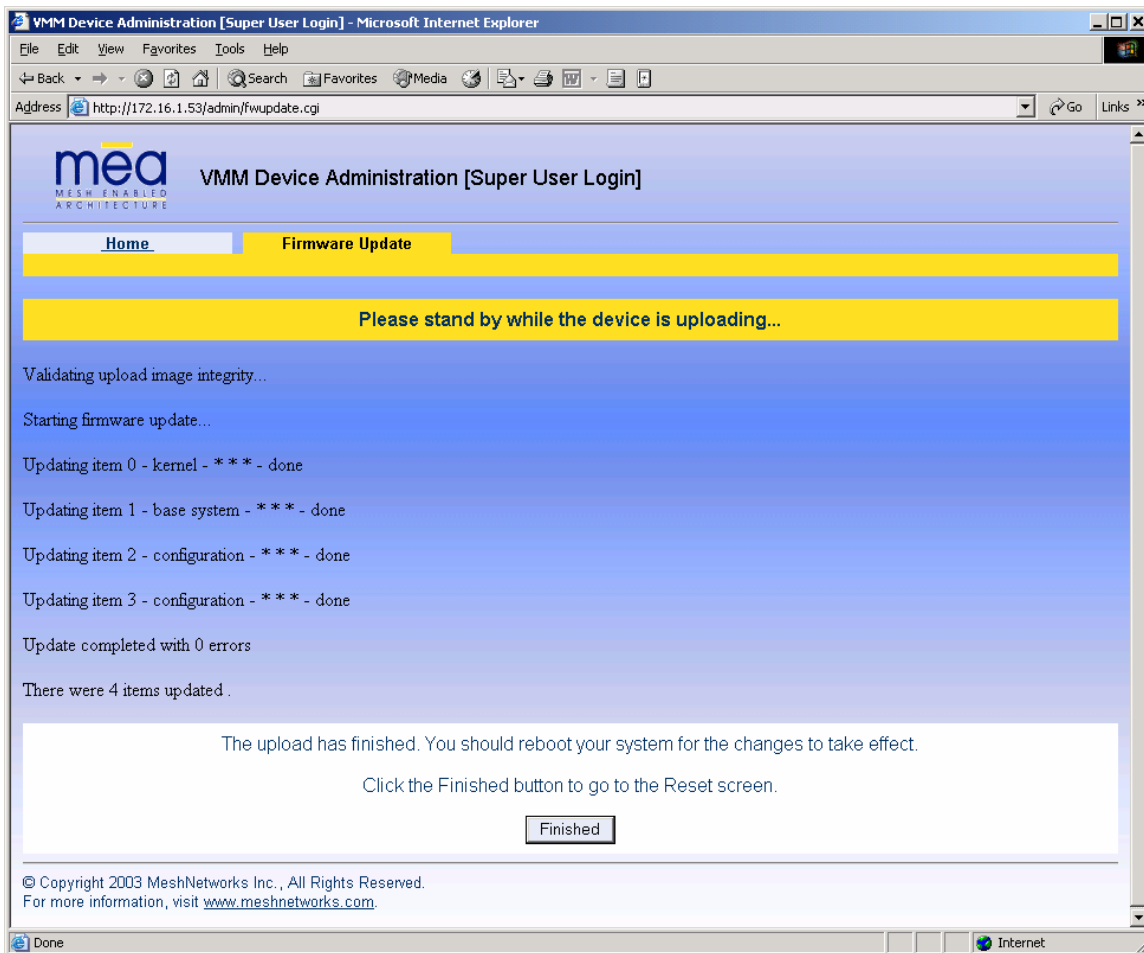
**Figure 4-4. Update Device Firmware Web Page**

This page allows entry of the name (and path) of the upgrade file. Once the correct filename has been entered, the device will prompt for confirmation:



**Figure 4-5. Confirm Upload Window for Firmware Update**

Once the filename has been confirmed, the web browser will transmit the file to the device, and the device will present an upgrade progress screen. This page will indicate the current stage in the upgrade process.

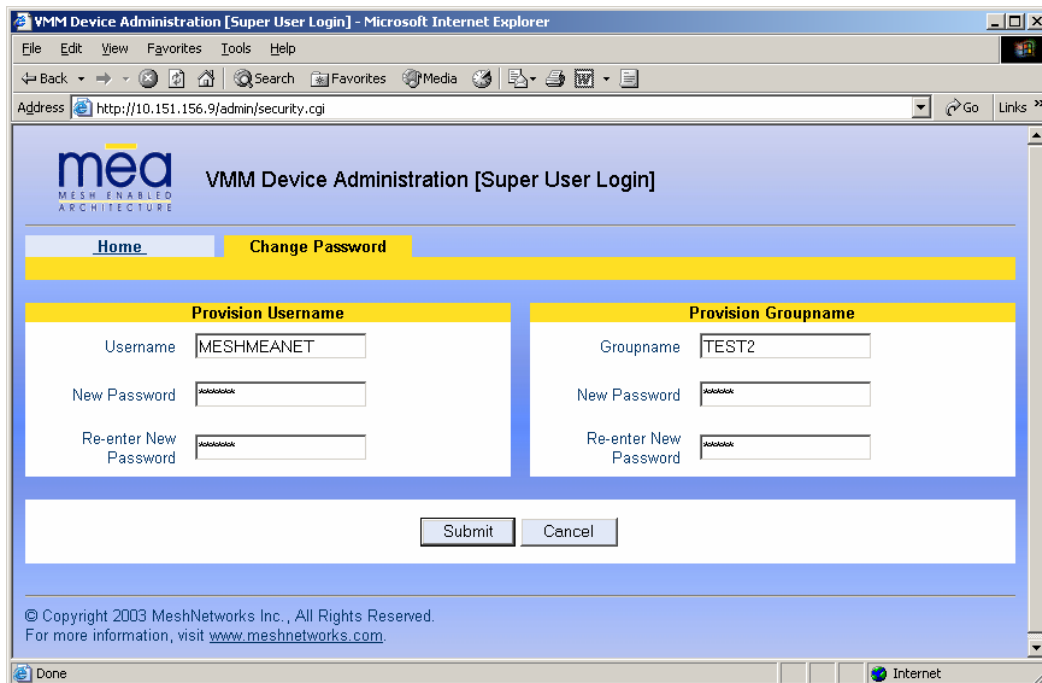


**Figure 4-6. Firmware Upload Progress Web Page**

Once the upgrade is completed, the device must be reset. The *Finished* button will transition the web browser to the reset screen. See the [Resetting the RMM via the Device Administration Web Page](#) section in this manual for additional information.

### 4.3 Security Provisioning Web Page

When the *Security Provisioning* option is selected from the *RMM Device Administration Home Page* by the administrator, the device will present the following web page:



**Figure 4-7. Security Provisioning Web Page**

The Security Provisioning web page contains two main sections: *Provision Username* and *Provision Groupname*. Each item in both sections can be changed as needed.

#### 4.3.1 Provision Username Section

**Username** – the *username* provided in this field is used to communicate to the IAP and can be changed from this screen. If a new username is entered, the previous username is not retained.

**Password and Re-enter new password** – These two fields can be used to change the password for an existing username, or to provide a password for a new username.

#### 4.3.2 Provision Groupname Section

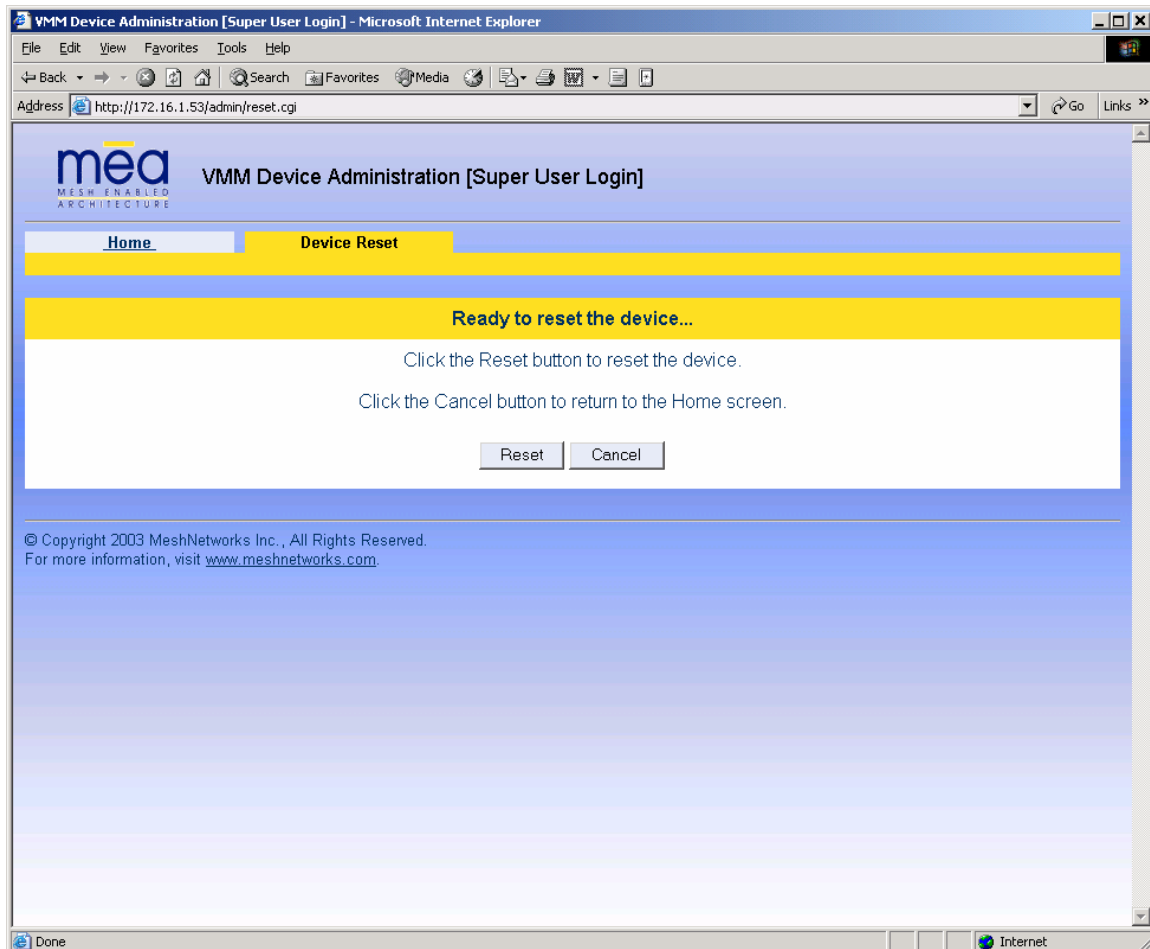
**Groupname** – the *groupname* provided in this field is used for peer-to-peer communication and can be changed from this screen. If a new groupname is entered, the previous groupname is not retained.

**Password and Re-enter new password** – These two fields can be used to change the password for an existing Groupname, or to provide a password for a new Groupname.

#### 4.4 Resetting the RMM via the Device Administration Web Page

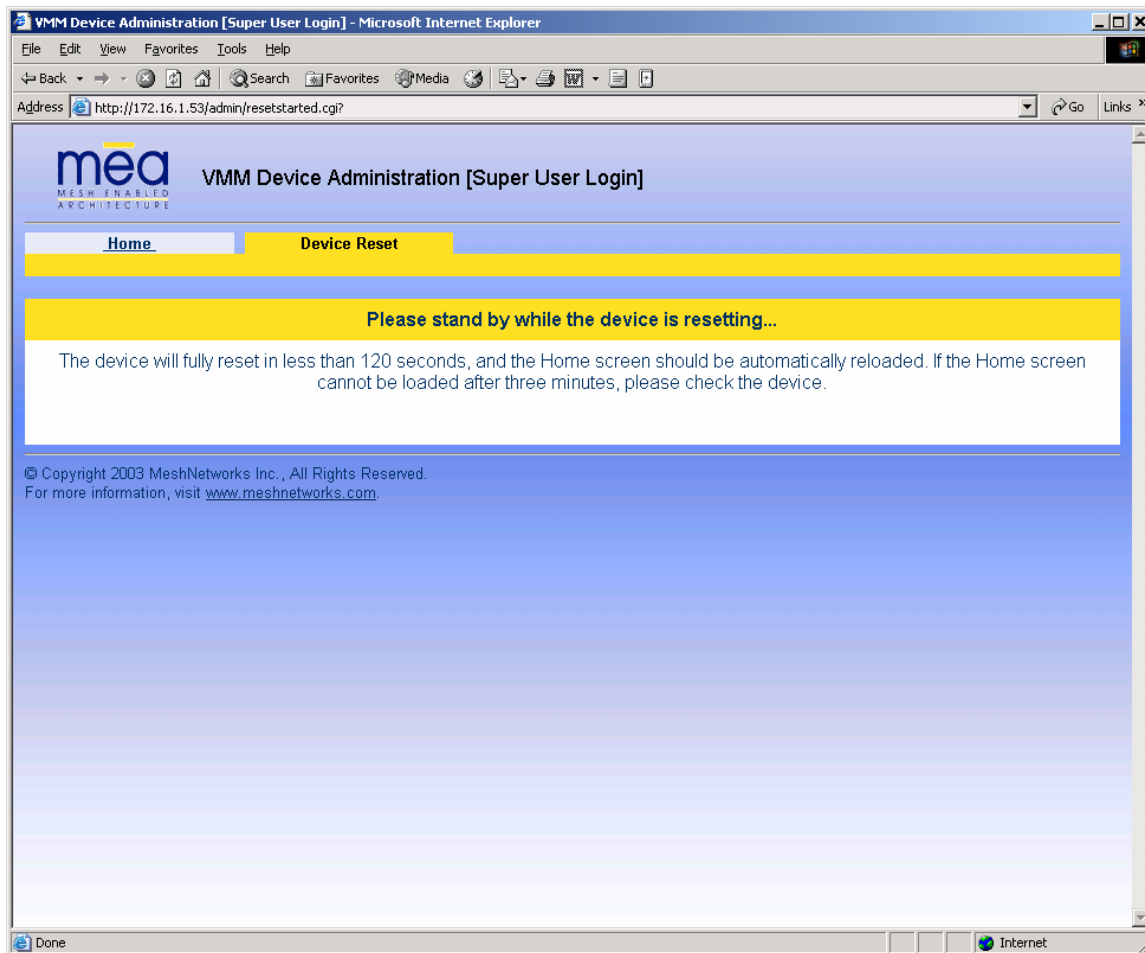
Although you should not have to reset the RMM device, the device can be commanded to reset via the web pages. In order to reset the device, return to the MEA Device Administration home page, and click on the *Reset the Device* link in the Device Management panel.

The web page displayed will allow you to reset the device.



**Figure 4-8. Device Reset Prompt Web Page**

Once you have commanded the device to reset, the following screen will be displayed. Your browser will delay for a short time, then transition to the home page once more.



**Figure 4-9. Device Reset in Progress Page**

**NOTE:** After the completion of the reset, you may experience a significant delay when bringing up another web page. Be patient.

## **4.5 Restoring Factory Settings – User Supplied Mode Limitations**

**NOTE:** In Release 3.1, there is a known issue that arises if the selected device addressing mode is *User-Supplied* when the user restores the factory default settings for the RMM.

### **4.5.1 Recovering from RMM Reset-to-Default in User-Supplied Mode**

After restoring factory defaults, the RMMs addressing scheme is automatically set to *Network DHCP*. This causes the network connection between the attached Ethernet devices and the core network to become disabled.

There are three available options to recover from this situation and restore the connection to the core network.

#### **4.5.1.1 Resetting Device Addressing Mode Using Device Manager**

Device Manager will be able to manage some but not all of the device parameters at this time. The network operator may change the selected device addressing mode via Device Manager to either User-Supplied or Statically-Provisioned.

#### **4.5.1.2 Resetting Device Addressing Mode via Configuration Web Page**

Because the factory default settings were restored, the RMM will offer one IP address via DHCP. This address will be in the form 10.xx.yy.10, where xx and yy are based on the transceiver MAC address as described in section 3.2 of this manual. The RMM will be accessible via the 10.xx.yy.9 address. Once an Ethernet device has been attached to the RMM, the configuration web page may be accessed at the 10.xx.yy.9 address and the device addressing mode may be changed to either *Remote-DHCP* or *Statically-Provisioned*.

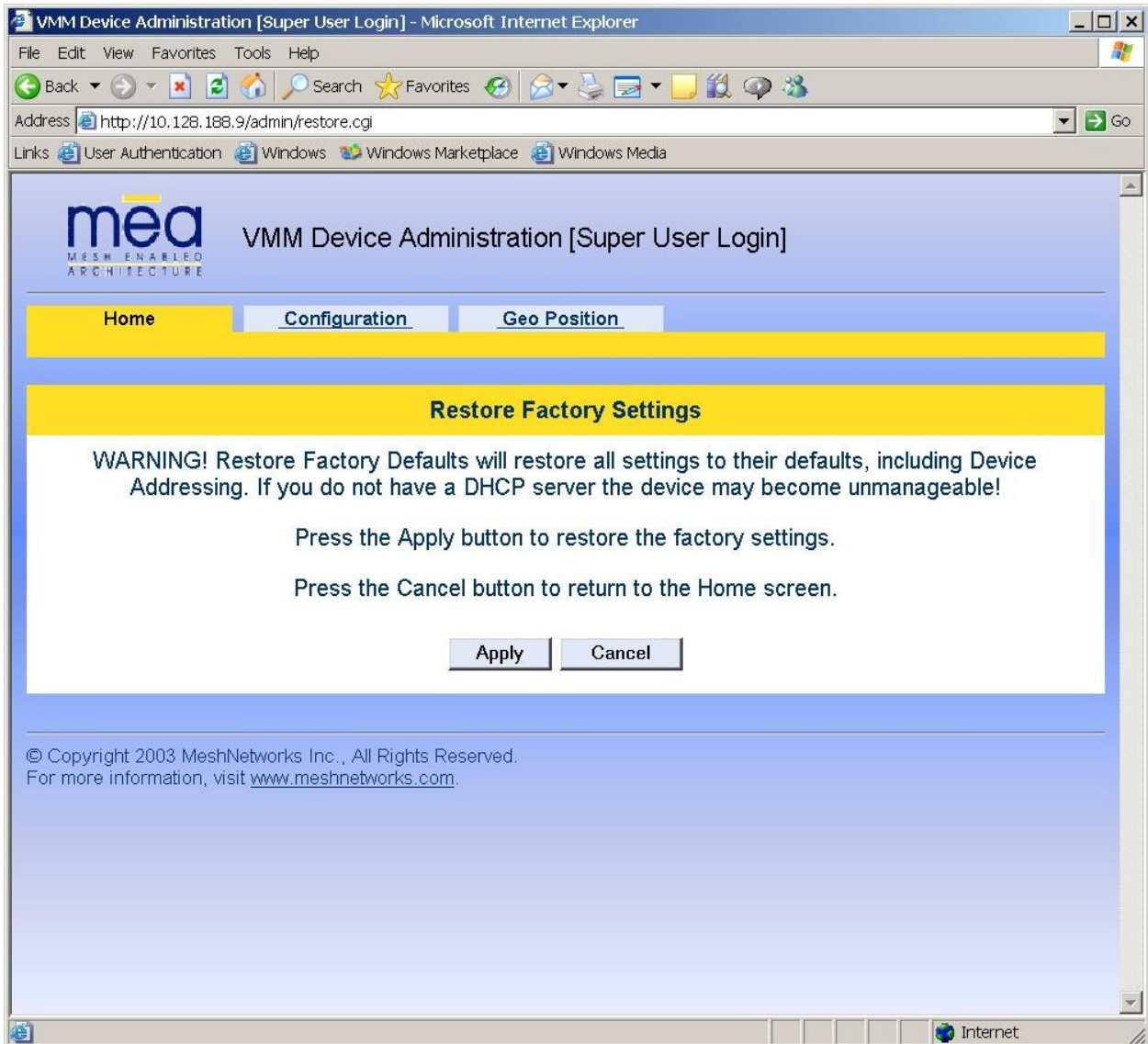
Be aware that the access password for the web page will have also been reset.

#### **4.5.1.3 Resetting User-Supplied Parameters via Configuration Web Page**

If the allowed device addressing modes were restricted to *User-Supplied*, the user may still connect to the RMM (as described above) and access the configuration web page. The User-Supplied parameters may then be set to usable values.

## 4.6 Restoring Factory Settings – Normal Operations

When the *Restore Factory Defaults* function is selected from the *RMM Device Administration* Home Page, the device will present the following web page.



**Figure 4-10. Restore Factory Settings Web Page**

The *Restore Factory Defaults* function allows the operator to return the device to factory defaults. This change will include the web password for the administrator and access accounts. This will also return the local IP addresses to the default MAC-derived values.

The confirmation window will be displayed. Click on the **OK** button to confirm the action.

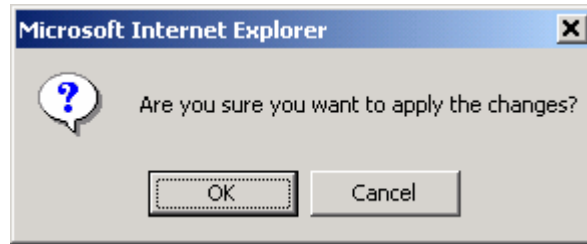


Figure 4-11. Confirm Changes Window for Restore Factory Settings

The *Factory Settings Restored* page will be displayed.

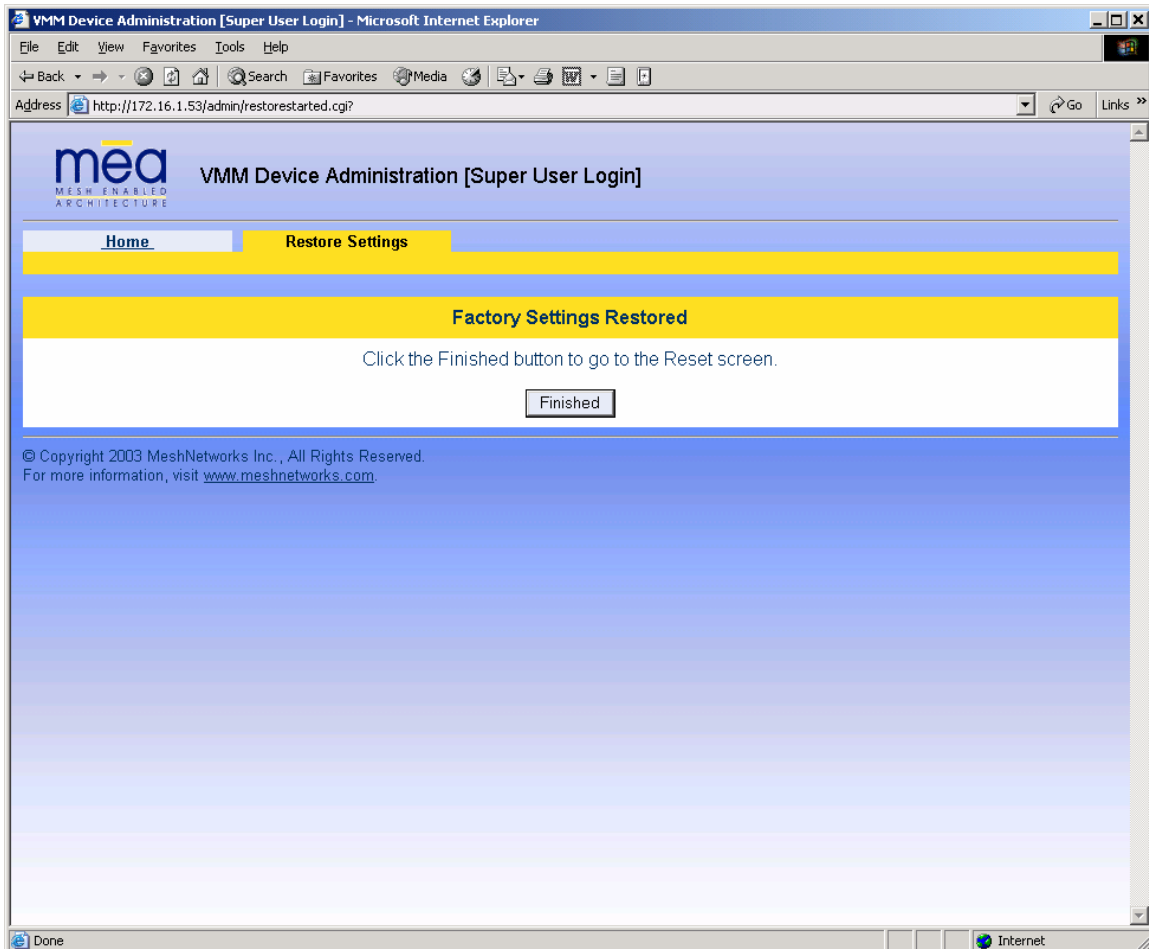


Figure 4-12. Factory Settings Restored Web Page

Click on the **Finished** button to complete the reset procedure.



## 5 Customer Service Information

If you have read this document and made every effort to resolve installation or operation issues yourself and still require help, please contact Motorola System Support Center (SSC) using the following contact information:

### Hours of Operation

7 days a week, 24 hours

**Technical Support:** 800-221-7144 (USA)

### 5.1 Obtaining Support

Motorola provides technical support services for your system and recommends that you coordinate warranty and repair activities through the Motorola System Support Center (SSC). When you consult the Motorola SSC, you increase the likelihood that problems are rectified in a timely fashion and that warranty requirements are satisfied. Check your contract for specific warranty and service information.

### 5.2 System Information

To be provided with the best possible opportunity for support, collect the following system information and have it available when obtaining support.

- Location of the system
- Date the system was put into service
- Software or firmware version information for components of your system
- Serial number(s) of the device(s) or component(s) requiring support
- A written description of the symptom or observation of the problem:
  - When did it first appear?
  - Can it be reproduced?
  - What is the step-by-step procedure to cause it?
- Do other circumstances contribute to the problem? For example, changes in weather or other conditions?
- Maintenance action preceding problem:
  - Upgrade of software or equipment
  - Change in the hardware or software configuration
  - Software reload - from backup or from CD-ROM (note the version and date)

### **5.3 Return Material Request**

After collecting system information, contact the Motorola System Support Center for assistance or to obtain a Return Material Authorization (RMA) number for faulty Field Replaceable Entities (FREs):

North America: 800-221-7144

### **5.4 Radio Products and Services Division**

The Radio Products and Services Division is your source for manuals and replacement parts.

#### **5.4.1 Radio Products and Services Division Telephone Numbers**

The telephone numbers for ordering are: (800)-422-4210 (US and Canada orders)

The Fax numbers are: (800)-622-6210 (US and Canada orders)

The number for help identifying an item or part number is (800)-422-4210; select choice “3” from the menu

### **5.5 Returning System Components to Motorola**

Motorola's service philosophy is based on field replaceable entities (FREs). FREs are system components identified by Motorola to be returned to Motorola for repair.

When you return an assembly for service, follow these best practices:

- Place any assembly containing CMOS devices in a static-proof bag or container for shipment.
- Obtain a return authorization (RA) number from the Motorola System Support Center.
- Include the warranty, model, kit numbers, and serial numbers on the job ticket, as necessary.
- If the warranty is out of date, you must have a purchase order.
- Print the return address clearly, in block letters.
- Provide a phone number where your repair technician can be reached.
- Include the contact person's name for return.
- Pack this assembly tightly and securely, preferably in its original shipping container.



## 6 Warranty Information

This warranty applies within the fifty (50) United States, the District of Columbia and Canada.

### LIMITED WARRANTY MOTOROLA COMMUNICATION PRODUCTS

If the affected product is being purchased pursuant to a written Communications System Agreement signed by Motorola, the warranty contained in that written agreement will apply. Otherwise, the following warranty applies.

#### I. WHAT THIS WARRANTY COVERS AND FOR HOW LONG:

Motorola Inc. or, if applicable, Motorola Canada Limited ("Motorola") warrants the Motorola manufactured Broadband Data communications product, against material defects in material and workmanship under normal use and service for a period of One (1) Year from the date of shipment.

Motorola, at its option, will at no charge either repair the Product (with new or reconditioned parts), replace it with the same or equivalent Product (using new or reconditioned Product), or refund the purchase price of the Product during the warranty period provided purchaser notifies Motorola according to the terms of this warranty. Repaired or replaced Product is warranted for the balance of the original applicable warranty period. All replaced parts of the Product shall become the property of Motorola.

This express limited warranty is extended by Motorola to the original end user purchaser purchasing the Product for purposes of leasing or for commercial, industrial, or governmental use only, and is not assignable or transferable to any other party. This is the complete warranty for the Product manufactured by Motorola. Motorola assumes no obligations or liability for additions or modifications to this warranty unless made in writing and signed by an officer of Motorola. Unless made in a separate written agreement between Motorola and the original end user purchaser, Motorola does not warrant the installation, maintenance or service of the Product.

Motorola cannot be responsible in any way for any ancillary equipment not furnished by Motorola which is attached to or used in connection with the Product, or for operation of the Product with any ancillary equipment, and all such equipment is expressly excluded from this warranty. Because each system which may use the Product is unique, Motorola disclaims liability for range, coverage, or operation of the system as a whole under this warranty.

#### II. GENERAL PROVISIONS:

This warranty sets forth the full extent of Motorola's responsibilities regarding the Product. Repair, replacement or refund of the purchase price, at Motorola's option, is the exclusive remedy. THIS WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. MOTOROLA DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MOTOROLA BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS OR SAVINGS OR OTHER INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PRODUCT, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW.

#### III. HOW TO GET WARRANTY SERVICE:

Purchaser must notify Motorola's representative or call Motorola's Customer Response Center at 1-800-247-2346 within the applicable warranty period for information regarding warranty service.

#### IV. WHAT THIS WARRANTY DOES NOT COVER:

- A) Defects or damage resulting from use of the Product in other than its normal and customary manner.
- B) Defects or damage from misuse, accident, water, or neglect.
- C) Defects or damage from improper testing, operation, maintenance, installation, alteration, modification, or adjustment.
- D) Breakage or damage to antennas unless caused directly by defects in material workmanship.
- E) A Product subjected to unauthorized Product modifications, disassemblies or repairs (including, without limitation, the addition to the Product of non-Motorola supplied equipment) which adversely affect performance of the Product or interfere with Motorola's normal warranty inspection and testing of the Product to verify any warranty claim.
- F) Product which has had the serial number removed or made illegible.
- G) Batteries (they carry their own separate limited warranty).
- H) Freight costs to the repair depot.
- I) A Product which, due to illegal or unauthorized alteration of the software/firmware in the Product, does not function in accordance with Motorola's published specifications or with the FCC type acceptance labeling in effect for the Product at the time the Product was initially distributed from Motorola.
- J) Scratches or other cosmetic damage to Product surfaces that does not affect the operation of the Product.
- K) That the software in the Product will meet the purchaser's requirements or that the operation of the software will be uninterrupted or error-free.
- L) Normal and customary wear and tear.
- M) Non-Motorola manufactured equipment unless bearing a Motorola Part Number in the form of an alpha numeric number (i.e., TDE6030B).
- N) Lift trucks for installation, removal, replacement or repair of the Motorola supplied products from light, power, telephone poles etc.
- O) Dispatch to remote site locations
- P) Loading of software upgrades or fixes into the devices.

#### V. GOVERNING LAW

In the case of a Product sold in the United States and Canada, this Warranty is governed by the laws of the State of Illinois and the Province of Ontario, respectively.

#### VI. PATENT AND SOFTWARE PROVISIONS:

Motorola will defend, at its own expense, any suit brought against the end user purchaser to the extent that it is based on a claim that the Product or its parts infringe a United States patent, and Motorola will pay those costs and damages finally awarded against the end user purchaser in any such suit which are attributable to any such claim, but such defense and payments are conditioned on the following:

- A) that Motorola will be notified promptly in writing by such purchaser of any notice of such claim;
- B) that Motorola will have sole control of the defense of such suit and all negotiations for its settlement or compromise; and
- C) should the Product or its parts become, or in Motorola's opinion be likely to become, the subject of a claim of infringement of a United States patent, that such purchaser will permit Motorola, at its option and expense, either to procure for such purchaser the right to continue using the Product or its parts or to replace or modify the same so that it becomes non-infringing or to grant such purchaser a credit for the Product or its parts as depreciated and accept its return. The depreciation will be an equal amount per year over the lifetime of the Product or its parts as established by Motorola.

Motorola will have no liability with respect to any claim of patent infringement which is based upon the combination of the Product or its parts furnished hereunder with software, apparatus or devices not furnished by Motorola, nor will Motorola have any liability for the use of ancillary



equipment or software not furnished by Motorola which is attached to or used in connection with the Product. The foregoing states the entire liability of Motorola with respect to infringement of patents by the Product or any its parts thereof.

Laws in the United States and other countries preserve for Motorola certain exclusive rights for copyrighted Motorola software such as the exclusive rights to reproduce in copies and distribute copies of such Motorola software. Motorola software may be used in only the Product in which the software was originally embodied and such software in such Product may not be replaced, copied, distributed, modified in any way, or used to produce any derivative thereof. No other use including, without limitation, alteration, modification, reproduction, distribution, or reverse engineering of such Motorola software or exercise of rights in such Motorola software is permitted. No license is granted by implication, estoppel or otherwise under Motorola patent rights or copyrights.

## 7 End User License Agreement

For your convenience, the End User License Agreement (EULA) provided below is the exact copy of the same EULA that is made available in the installation portion of the respective Motorola software application described in this documentation.

**MOTOROLA, INC.**  
**END USER LICENSE AGREEMENT**

**Motorola is willing to license its Mesh Networking Software Solutions (defined as “Products” below) and the accompanying documentation to you only on the condition that you accept all the terms in this License Agreement (“Agreement”).**

**IMPORTANT: READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING PRODUCTS.**

BY CLICKING ON THE “ACCEPT” BUTTON BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, MOTOROLA IS NOT WILLING TO LICENSE THE PRODUCTS TO YOU. YOU SHOULD CLICK ON THE “DO NOT ACCEPT” BUTTON TO DISCONTINUE THE SOFTWARE INSTALLATION PROCESS. IF YOU DO NOT AGREE TO THESE TERMS, YOU MAY, WITHIN FIFTEEN (15) DAYS, RETURN THIS ENTIRE PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE ENTIRE PRODUCT IF YOU HAVE NOT PHYSICALLY RECEIVED A PRODUCT FOR A FULL REFUND.

1. **DEFINITIONS.** In this Agreement, the word “Software” refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word “Documentation” refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word “Product(s)” refers to the specific combination of Software and Documentation that you have licensed and which has been provided to you under the terms of this Agreement.
2. **GRANT OF LICENSE.** Motorola, Inc. (“Motorola”) grants you (“Licensee” or “you”) a personal, nonexclusive, nontransferable license to use the Products subject to the Conditions Of Use set forth in Section 3 below and the terms and conditions of this Agreement. Any terms or conditions appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.
3. **CONDITIONS OF USE.** Any use of the Products outside of the conditions set forth herein is strictly prohibited and will be deemed a breach of this Agreement.



3.1 Only your employees or agents may use the Products. You shall take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.

3.2 You shall use the Products (i) only for your internal business purposes; (ii) only as described in the Products; and (iii) in strict accordance with this Agreement.

3.3 Licensee may install and use the Products on a single client workstation, provided that the use is in conformance with the terms set forth in this Agreement. The Products may not be transferred to another party without the express written consent of Motorola, regardless of whether or not such transfer is accomplished by physical or electronic means.

3.4 Portions of the Products are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Products like any other copyrighted material (e.g., a book or musical recording) except that you may either: (a) make one (1) copy of the transportable part of the Products (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (b) copy the transportable part of the Products to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out one (1) copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Motorola copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement and in the United States is punishable in federal court by fine and imprisonment.

3.5 You shall not export, re-export, resell, ship or divert or cause to be exported, re-exported, resold, shipped or diverted, directly or indirectly, the Products under this Agreement.

4. **TITLE; RESTRICTIONS.** If you transfer possession of any copy of the Products to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Products and any copies made by you remain with Motorola and its licensors. You shall not, and shall not permit others to: (1) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (2) copy the look-and-feel or functionality of the Software or Documentation; (3) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (4) rent or transfer all or some of the Software or Documentation to any other party without Motorola's prior written consent; or (5) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Products be equipped with such a protection device. If the Products contain Software or Documentation that is provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you shall only use the medium which best meets your specific needs, and shall not loan, rent, lease, or transfer the other media contained in the package without Motorola's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this Agreement, will result in automatic termination of this license.

5. **CONFIDENTIALITY.** You acknowledge that all Products contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Products will result in irreparable harm to Motorola for which monetary damages would be inadequate and for which Motorola will be entitled to immediate injunctive relief. Accordingly, you will limit access to the Products to those of your employees and agents who need to use the Products for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Products, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care.

Notwithstanding anything to the contrary herein, you shall have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Motorola prior to such disclosure and provide Motorola with a reasonable opportunity to respond.

6. **RIGHT TO USE MOTOROLA'S NAME.** Except as required in Section 3.4 above, you shall not, during the term of this Agreement or thereafter, use any trademark, of Motorola, or any word or symbol likely to be confused with any Motorola trademark, either alone or in any combination with another word or words.

7. **PAYMENT.** The rights granted hereunder are contingent upon payment for the Products. All payments shall be due net thirty (30) days from date of the invoice.

8. **UPGRADES AND UPDATES.** If the Products are licensed to you as an upgrade or update to a product previously licensed to you, you must destroy the Products previously licensed to you, including any copies, within thirty (30) days of your receipt of the update or upgrade.

9. **MAINTENANCE.** Motorola shall not be responsible for maintenance or field service of the Software under this Agreement.

10. **LIMITED WARRANTY.** All diskettes or CD-ROMS on which the Products are furnished ("Media") are warranted to be free from manufacturing and material defects for ninety (90) days after the shipment date of the Products to you. Media that become defective during such period shall be repaired or, at Motorola's option, replaced. This limited warranty is contingent upon proper use of the Media and does not cover Products which have been tampered with, modified, or subjected to unusual physical or electrical stress. Tampering with or removal of any factory seal or label on any Media voids this warranty and releases Motorola from any and all liability.

11. **DISCLAIMER.** EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTIES, MOTOROLA MAKES, AND YOU RECEIVE, NO OTHER WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. MOTOROLA SPECIFICALLY DISCLAIMS ANY OTHER WARRANTY



INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE PRODUCTS ARE PROVIDED "AS IS." MOTOROLA DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. MOTOROLA MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

12. **REMEDIES.** The entire liability of Motorola, and your exclusive remedy under the warranty provided herein will be, at Motorola's option, to repair or replace any Media found to be defective within the warranty period, or to refund the purchase price and terminate this Agreement. To seek such a remedy, you must return the entire Product to Motorola, with a copy of the original purchase receipt within the warranty period.

13. **LIMITATION OF LIABILITY.** THE TOTAL LIABILITY OF MOTOROLA UNDER THIS AGREEMENT FOR DAMAGES SHALL NOT EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE PRODUCTS LICENSED UNDER THIS AGREEMENT. IN NO EVENT WILL MOTOROLA BE LIABLE IN ANY WAY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING WITHOUT LIMITATION, LOST BUSINESS PROFITS, OR LIABILITY OR INJURY TO THIRD PERSONS, WHETHER FORESEEABLE OR NOT, REGARDLESS OF WHETHER MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some jurisdictions do not permit limitations of liability for incidental or consequential damages, so the above exclusions may not apply to you.

14. **U.S. GOVERNMENT.** If you are acquiring the Products on behalf of any unit or agency of the U.S. Government, the following shall apply. Use, duplication or disclosure of the Products is subject to the restrictions set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement shall each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR or DFARS, as applicable to the particular procuring agency and procurement transaction."

15. **TERM OF LICENSE.** Your right to use the Products will begin when you click the "ACCEPT" button below, which constitutes acceptance of the terms and conditions herein, and will continue in perpetuity unless terminated as follows. Your right to use the Products will terminate immediately without notice upon a breach of this Agreement by you. Otherwise, this Agreement may be terminated by either party upon thirty (30) days prior written notice. Within thirty (30) days after termination of this Agreement, you will certify to Motorola in writing that

through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Motorola, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Products, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

16. **GOVERNING LAW.** This Agreement shall be governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

17. **ASSIGNMENT.** This Agreement may not be assigned or otherwise transferred by you.

18. **SURVIVAL OF PROVISIONS.** The parties agree that where the context of any provision indicates an intent that it shall survive the term of this Agreement, then it shall survive.

19. **ENTIRE AGREEMENT.** This Agreement contains the parties' entire agreement regarding your use of the Products and may be amended only in writing signed by both parties, except that Motorola may modify this Agreement as necessary to comply with applicable laws and regulations including FCC regulations.

20. **THIRD PARTY SOFTWARE.** The Software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software **UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.**

**IF THE FOREGOING TERMS AND CONDITIONS ARE ACCEPTABLE TO YOU, PLEASE INDICATE YOUR AGREEMENT AND ACCEPTANCE BY CLICKING BELOW ON THE BUTTON LABELED "ACCEPT".**

**IF THE FOREGOING TERMS AND CONDITIONS ARE NOT ACCEPTABLE TO YOU, PLEASE CLICK ON THE "DO NOT ACCEPT" BUTTON BELOW.**

MOTOROLA and the Stylized M logo are registered in the US Patent & Trademark Office.



## 8 FCC Regulatory Information

### 8.1 FCC Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

The RMM6300 requires professional installation to ensure the installation is performed in accordance with FCC licensing regulations.

Federal Communications Commission (FCC) Statement:

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**Any changes or modifications not expressly approved by Motorola could void the user's authority to operate the equipment.**

### 8.2 FCC RF Radiation Exposure Statement

**CAUTION:** This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 2 meters between the antenna and your body.

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

## 9 Safety Information for the MEA Products

The Federal Communications Commission (FCC) with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. Motorola MEA products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio according to the instructions found in this manual and the hardware and software guides on the MEA CD will result in user exposure that is substantially below the FCC recommended limits.

- Do not touch or move the antenna(s) while the unit is transmitting or receiving.
- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate a portable transmitter near unshielded blasting caps or in an explosive environment unless it is a type especially qualified for such use (Intrinsically Safe).
- Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio may be damaged.
- Antenna use:
  - In order to comply with FCC RF exposure limits, dipole antennas should be located at a minimum distance of 2 meters or more from the body of all persons.

## 10 Safety Certification



Conforms to UL STD ANSI/UL 60950 3<sup>rd</sup> Edition

Certified to CAN/CSA C22.2 NO. 60950-00

Equipment shall be suitable for use in Air pressure: 86kPa to106kPa.

### 10.1 CE Mark Certification

The CE mark is the official marking required by the European Community for all Electric and Electronic equipment that will be sold, or put into service for the first time, anywhere in the European community. It proves to the buyer or user that this product fulfills all essential safety and environmental requirements as they are defined in the European Directives.

Motorola Products are covered under the following product certification Europe:

**ETSI EN 300 328 V 141 (2003-04)**

**ETSI EN 301 489-1 (2002-08) and 301 489-17**

**EN 55022:1998 and EN 55024:1998**

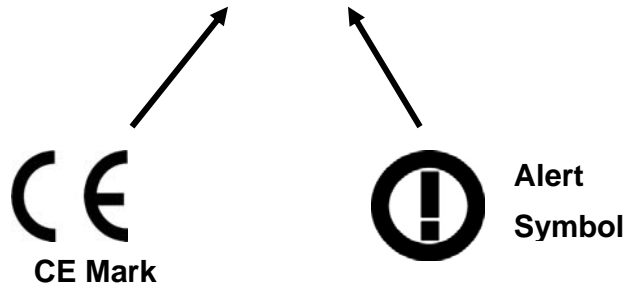
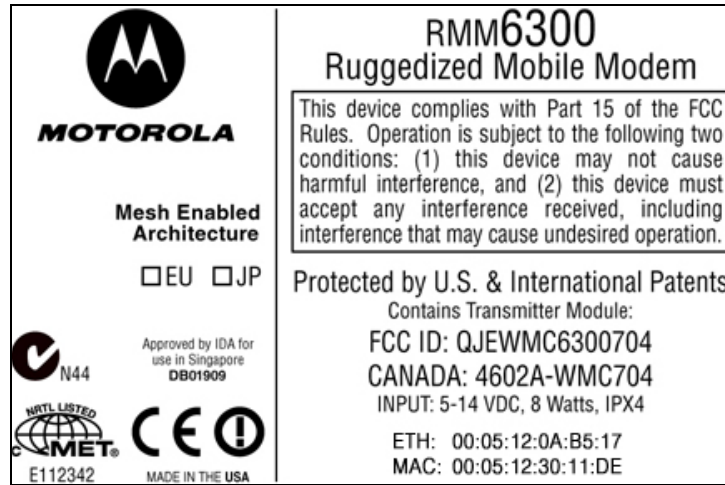
**CENELEC EN 50360 and EN50371 – Specific Absorption Test - SAR**

The following countries are covered under the CE Mark:

Austria, Belgium, Denmark, Finland, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, UK

CE Marking on the product will gain you access to the European Economic Area (EEA). Some countries may require a declaration of conformity, check with your Motorola sales team for details.

An example of the CE Marking on a product label:



The alert symbol indicates that Motorola products are **not** certified to operate in France. Outdoor use in France is restricted to 10mW EIRP for band 2454 – 2483.5 MHz.