



**MEA**  
**3.1**  
**Setup and Installation**  
**Guide**

Documentation Revision 3.1.8

## 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

© 2007 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

**OVERVIEW ..... 1**

**Introduction ..... 1**

**Acronyms ..... 2**

        Related Documentation..... 2

**DESCRIPTION OF THE MEA SYSTEM ..... 3**

**Introduction ..... 3**

**Subscriber Devices (SDs) ..... 4**

**Wireless Routers (WRs) ..... 5**

**Intelligent Access Points (IAPs) ..... 6**

**Vehicle Mounted Modem (VMM6300) ..... 6**

**Enhanced Wireless Router (EWR6300)/Portable Wireless Router (PWR6300) ..... 7**

**Mobile internet Switching Controller (MiSC)..... 7**

**Operational View of the MEA System ..... 8**

**Network Architecture ..... 9**

**Addressing Schemes ..... 10**

        Network DHCP Scheme..... 10

        Statically Provisioned Scheme..... 10

        User Supplied Scheme ..... 10

**Quality of Service (QoS) and User Priority Features..... 13**

        Quality of Service ..... 14

        User Priority ..... 14

**SETUP AND INSTALLATION ..... 15**

**Subscriber Device (SD) ..... 15**

        Equipment..... 15

Record MAC Address of the WMC6300 .....	15
Loading and Verifying WMC6300 Software .....	15
Testing .....	18
<b>Intelligent Access Point (IAP).....</b>	<b>18</b>
Equipment.....	18
Record MAC Address of the IAP.....	19
IAP Assembly.....	20
Deployment.....	22
Initial IAP Configuration.....	22
Testing .....	22
<b>Wireless Router (WR).....</b>	<b>23</b>
Equipment.....	23
Record MAC Address of the MWR6300 .....	24
MWR6300 Assembly.....	24
Deployment.....	25
Initial Configuration .....	25
Testing .....	25
<b>Procedures for Grounding Infrastructure Devices.....</b>	<b>26</b>
Antenna Installation.....	26
Device Installation.....	26
Device Removal .....	26
<b>Mobile Internet Switching Controller (MiSC).....</b>	<b>27</b>
MiSC Configuration 1 .....	27
MiSC Configuration 2.....	30
<b>Upgrade MiSC/DHCP Configuration (optional).....</b>	<b>32</b>
Changing the Wireless Subnet.....	32
Onsite Configuration of Routers.....	34

---

**Mesh Enabled Architecture**

**Setup and Installation Guide**

- Network Configuration – Device Manager ..... 35
- Network Configuration – IAP Configuration via Web Interface ..... 35
- Testing ..... 51
- Default Addresses and Logins ..... 52
  
- MAC ADDRESS TABLES..... 54**
  - IAP MAC Addresses ..... 54**
  - WR MAC Addresses ..... 54**
  - WMC MAC Addresses ..... 55**
  
- SITE SELECTION/DEPLOYMENT GUIDELINES ..... 56**
  - General Site Selection Guidelines ..... 56**
  - Antenna Guidelines ..... 56**
  - Lab Checkout ..... 57**
  - General Deployment Guidelines ..... 57**
  
- CUSTOMER SERVICE INFORMATION ..... 58**
  - Obtaining Support ..... 59**
    - System Information ..... 59
  - Return Material Request ..... 59**
    - Radio Products and Services Division ..... 59
    - Returning System Components to Motorola ..... 60
    - Returning FREs..... 60
  
- PRODUCT WARRANTY INFORMATION..... 61**
  
- REGULATORY INFORMATION ..... 64**
  - FCC Information..... 64**
  - FCC RF Energy Exposure Statement..... 64**
  - Regulatory and RF Safety Exposure..... 65**

## List of Figures

<b>Figure 1.</b>	<b>Elements of the MEA System .....</b>	<b>4</b>
<b>Figure 2.</b>	<b>Operational View of the MEA System.....</b>	<b>8</b>
<b>Figure 3.</b>	<b>MEA Network Architecture .....</b>	<b>9</b>
<b>Figure 4.</b>	<b>Control Panel – Network and Dial-up Connections Icon .....</b>	<b>11</b>
<b>Figure 5.</b>	<b>Network and Dial-up Connections Window .....</b>	<b>12</b>
<b>Figure 6.</b>	<b>Local Area Connection Properties Dialog Box.....</b>	<b>12</b>
<b>Figure 7.</b>	<b>Internet Protocol (TCP/IP) Properties Dialog Box .....</b>	<b>13</b>
<b>Figure 8.</b>	<b>WMC6300 Antenna Port and LED Indicators .....</b>	<b>15</b>
<b>Figure 9.</b>	<b>IAP6300 Identification Label.....</b>	<b>19</b>
<b>Figure 10.</b>	<b>IAP6300 Connection Points.....</b>	<b>20</b>
<b>Figure 11.</b>	<b>IAP6300 Bracket .....</b>	<b>20</b>
<b>Figure 12.</b>	<b>Bracket Adjustment Bolts.....</b>	<b>21</b>
<b>Figure 13.</b>	<b>MWR6300 Identification Label.....</b>	<b>24</b>
<b>Figure 14.</b>	<b>MWR6300 External Connection Points.....</b>	<b>24</b>
<b>Figure 15.</b>	<b>MiSC Configuration 1 .....</b>	<b>27</b>
<b>Figure 16.</b>	<b>MiSC Configuration 1 – SMC 6724L2 Switch .....</b>	<b>28</b>
<b>Figure 17.</b>	<b>MiSC Configuration 2.....</b>	<b>30</b>
<b>Figure 18.</b>	<b>MiSC Configuration 2 – Cisco 2950 Switch.....</b>	<b>31</b>
<b>Figure 19.</b>	<b>MEA Subnet Data.....</b>	<b>33</b>
<b>Figure 20.</b>	<b>MEA Device Administration Connection.....</b>	<b>35</b>
<b>Figure 21.</b>	<b>MEA Device Administration Logon Window .....</b>	<b>36</b>
<b>Figure 22.</b>	<b>MEA Device Administration Authentication Window.....</b>	<b>36</b>
<b>Figure 23.</b>	<b>MEA Device Administration Home Tab .....</b>	<b>37</b>
<b>Figure 24.</b>	<b>MEA Device Administration Enter New Password Window .....</b>	<b>38</b>
<b>Figure 25.</b>	<b>MEA Device Administration Confirmation Window .....</b>	<b>38</b>
<b>Figure 26.</b>	<b>MEA Device Administration Password Changed Window .....</b>	<b>39</b>
<b>Figure 27.</b>	<b>MEA Device Administration Logon Window .....</b>	<b>39</b>

**Figure 28. MEA Device Administration Update Device Firmware Window ..... 40**

**Figure 29. MEA Device Administration Choose File Window ..... 41**

**Figure 30. MEA Device Administration Update Device Firmware Window (2)..... 41**

**Figure 31. MEA Device Administration Update Confirmation Window ..... 42**

**Figure 32. MEA Device Administration Update Device Status Window ..... 42**

**Figure 33. MEA Device Administration Restore Factory Defaults Window ..... 43**

**Figure 34. Restore Factory Defaults Confirmation Message ..... 44**

**Figure 35. MEA Device Administration Factory Settings Restored Window ..... 45**

**Figure 36. MEA Device Administration Device Reset Window ..... 46**

**Figure 37. MEA Device Administration Device Reset Window ..... 47**

**Figure 38. MEA Device Administration Device Reset Window (2)..... 48**

**Figure 39. MEA Device Administration System Settings Tab ..... 49**

**Figure 40. System Settings Confirmation Message ..... 50**

**Figure 41. System Settings Saved Message..... 50**

**Figure 42. MEA Device Administration Associations Tab..... 51**

**Figure 43. Antenna Mounting ..... 56**



## Overview

### *Introduction*

The Motorola Enabled Architecture (MEA®) wireless broadband system allows a network operator to deploy a wireless, multi-hopping ad hoc network. This document describes how to setup, configure, and deploy a MEA system to operate in infrastructure mode.

The MEA system is designed for easy installation. The infrastructure components of a MEA system are preinstalled with a default configuration for connection to a wired network. Any configuration items described in this document are for site-specific information.

Motorola recommends that the Network Operator receive setup and deployment training at Motorola' facility prior to deploying the MEA network. Motorola may optionally provide the Network Operator assistance with site surveys and deployment.

**Note:** The MWR6300 Wireless Routers and IAP6300 Intelligent Access Points require professional installation to ensure the installation is performed in accordance with FCC licensing regulations.

## **Acronyms**

HAS	Hardware Authentication Server
IAP	Intelligent Access Point
MEA	Motorola Enabled Architecture
MiSC	Mobile Internet Switching Controller
SD	Subscriber Device
WMC	Wireless Modem Card
WR	Wireless Router
VMM	Vehicle Mounted Modem
EWR	Enhanced Wireless Router

## **Related Documentation**

Location Analyzer Deployment Tool Users Guide

MEA WMC6300 Windows 2000 and XP Users Guide

MeshFlash User's Guide

MeshManager Users Guide

MeshView Users Guide

MEA MiSC Configuration Guide

## Description of the MEA System

### *Introduction*

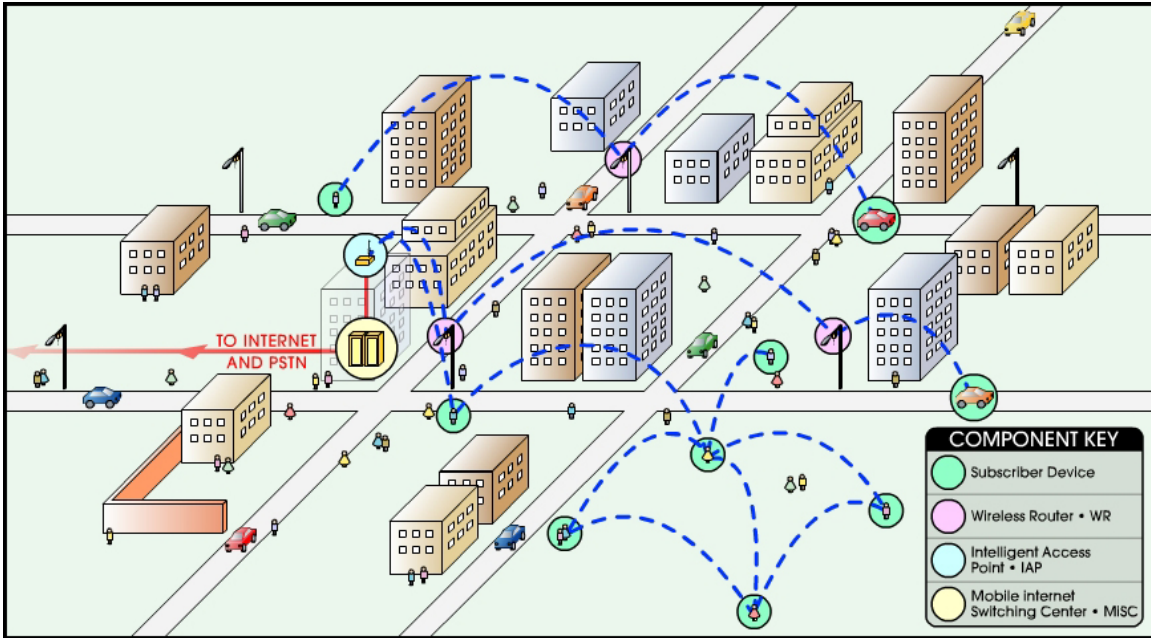
Motorola develops Mobile Broadband communications systems with ad hoc architectures. That is, each node can connect directly, or indirectly (by hopping through other nodes), with any other node in the network. The peer-to-peer nature of the ad hoc architecture combined with data rate control in each subscriber and infrastructure node in the network insures reliable delivery while providing increased network capacity through geographic reuse of the frequency spectrum.

The network is comprised of following distinct elements:

- Mobile internet Switching Controllers (MiSCs)
- Intelligent Access Points (IAPs)
- Wireless Routers (WRs)
- Enhanced Wireless Routers / Portable Wireless Routers (EWRs/PWRs)
- Subscriber Devices (SDs)
- Vehicle Mounted Modems (VMMs)

Additional SD and infrastructure components are described separately.

The overwhelming portion of the value that Motorola provides is in the Wireless Modem Card (WMC6300). The WMC functionality is used in Subscriber Devices as well as in the Wireless Router and Intelligent Access Point (IAP), both of which are types of infrastructure equipment. Motorola provides a Mobile Internet Switching Controller (MiSC) which is assembled from industry standard equipment and conforms to industry standards. Motorola also provides the network applications, which are required for proper operation and value extraction from the MEA mobile Internet system.



**Figure 1. Elements of the MEA System**

All network elements are designed to support mobile applications. Subscriber Devices can be either mobile or fixed, while the remaining components are typically fixed. Wireless Routers and IAPs can be mounted on utility poles, light poles, traffic apparatus, billboards, and buildings. Their fixed positions allow the Subscriber Device to pinpoint its location within one second. WRs and IAPs can also be mobile, attached to emergency vehicles, utility vehicles, or fleet vehicles. It is important to note that the WMC technology within a Subscriber Device is identical to the WMC technology in Wireless Routers and IAPs.

The MEA system was designed to minimize the cost associated with deploying a broadband mobile network with end user data access rates on the order of DSL or Cable Modem. The chosen metric of network efficiency for a data centric network is bits per second per Hertz per square kilometer per dollar (bps/hz/km<sup>2</sup>/\$). This metric balances the user data rates, allocated bandwidth, coverage area, and cost.



### **Subscriber Devices (SDs)**

The Motorola Wireless Modem Card (WMC) is provided as a PCMCIA form factor device. The WMC is used with an off-the-shelf IP-enabled laptop computer or PDA. These two devices together make up a Subscriber Device (SD).

The WMC provides access to the fixed infrastructure network and other networks, such as the Internet, and it can also function as a Wireless Router and repeater for other SDs.

SDs can therefore be a key part of the network infrastructure. Adding subscribers can effectively increase the number of Wireless Routers in the network, which increases the number of alternative paths that subscribers may utilize. This can reduce both the time and cost to deploy network infrastructure, while also increasing the spectral efficiency and therefore the capacity of the network. In addition, because SDs can also operate in an ad hoc peer-to-peer mode, two or more SDs can form a network without the need for any fixed infrastructure.

### ***Wireless Routers (WRs)***

The Wireless Router (WR) is a low-cost small-sized wireless device that is primarily deployed to seed a geographical area, extending the range between IAPs and subscribers, and to simultaneously increase the network's spectral efficiency. Wireless Routers provide a number of functions in the network, such as:

- Range Extension for Subscriber Devices and IAPs
- Automatic Load Balancing
- Route Selection
- Network capacity optimization through small packet consolidation
- Fixed reference for geo-location services



The Wireless Router's small size and light weight allow it to be mounted almost anywhere. No towers are required. WR software can be updated via over-the-air downloads.

## ***Intelligent Access Points (IAPs)***

The Intelligent Access Point (IAP) is a low-cost, small device that acts as the transition point from the wireless network to the wired core network and from there, through media gateways, out to the Internet. Each IAP offers up to 6 Mbps burst data rate to subscribers. IAPs support the 10/100 base-T Ethernet interface. Other interfaces are supported through commercially available media translation devices. If additional network capacity is required, more IAPs can be easily deployed - without the need for extensive RF or site planning. IAPs provide functions such as:



- Local mobility management of SDs
- Fixed reference for geo-location services
- Hopping points for subscriber peer-to-peer networking
- Transition point from the wireless to the wired portions of the network
- Route Selection

The IAP's small size and lightweight allow it to be mounted anywhere power and network connectivity is available. No towers are required. The IAP software can be updated via over-the-wire downloads.

## ***Vehicle Mounted Modem (VMM6300)***



Compact and ruggedly designed, the Motorola Vehicle Mounted Modem (VMM) turns a vehicle into a mobile office. Mobile Data Terminals (MDT), IP video cameras, and other IP ready devices can access a high-speed, mobile broadband network via a standard RJ45 Ethernet Port. This low cost, high performance, wireless modem supports up to 6 Mbps burst data rates at speeds of over 100 mph.

The VMM provides high bandwidth access to mission-critical information on the move. Remote database inquiries, on-scene report submission, multi-megabyte file transfers and live video streams will make field personnel more efficient. The VMM also supports real-time position location without relying on GPS.

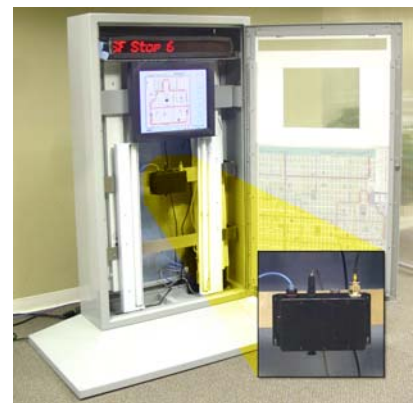
Like all MEA products, the VMM acts as a wireless router/repeater – automatically extending the range, robustness and performance of the wireless network.

## ***Enhanced Wireless Router (EWR6300)/Portable Wireless Router (PWR6300)***

The Enhanced Wireless Router (EWR) is deployed to guarantee wireless coverage in large geographic areas while providing wireless network access to one or more IP devices via its built-in RJ45 Ethernet port. The EWR efficiently combines the functionality of a Motorola Wireless Router and client modem in 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 (as pictured at right), sensors, signs, signals, etc. can all be mesh enabled to send and receive data at burst rates of up to 6 Mbps. All of the standard Wireless Router functionality, including Multi-Hopping®, non-line-of-sight communications and geo-location services, is fully supported.



The PWR6300 Portable Wireless Router (PWR) has the same functionality as the EWR, but in a smaller form factor. It combines the functionality of a Wireless Router and the Wireless Modem Card into a single device. .



EWRs/PWRs also provide:

- Range extension between clients and IAPs
- Fixed reference points between clients and IAPs
- Up to three assignable IP addresses



## ***Mobile internet Switching Controller (MiSC)***

The Mobile internet Switching Controller (MiSC) provides connectivity between the IAPs and the wired world, and hosts the network's management and provisioning functions. The MiSC is composed of off-the-shelf hardware components, such as LAN routers and application servers. MiSC software consists of both off-the-shelf and Motorola' proprietary software, MeshManager. The MeshManager software provides functions for the network such as:

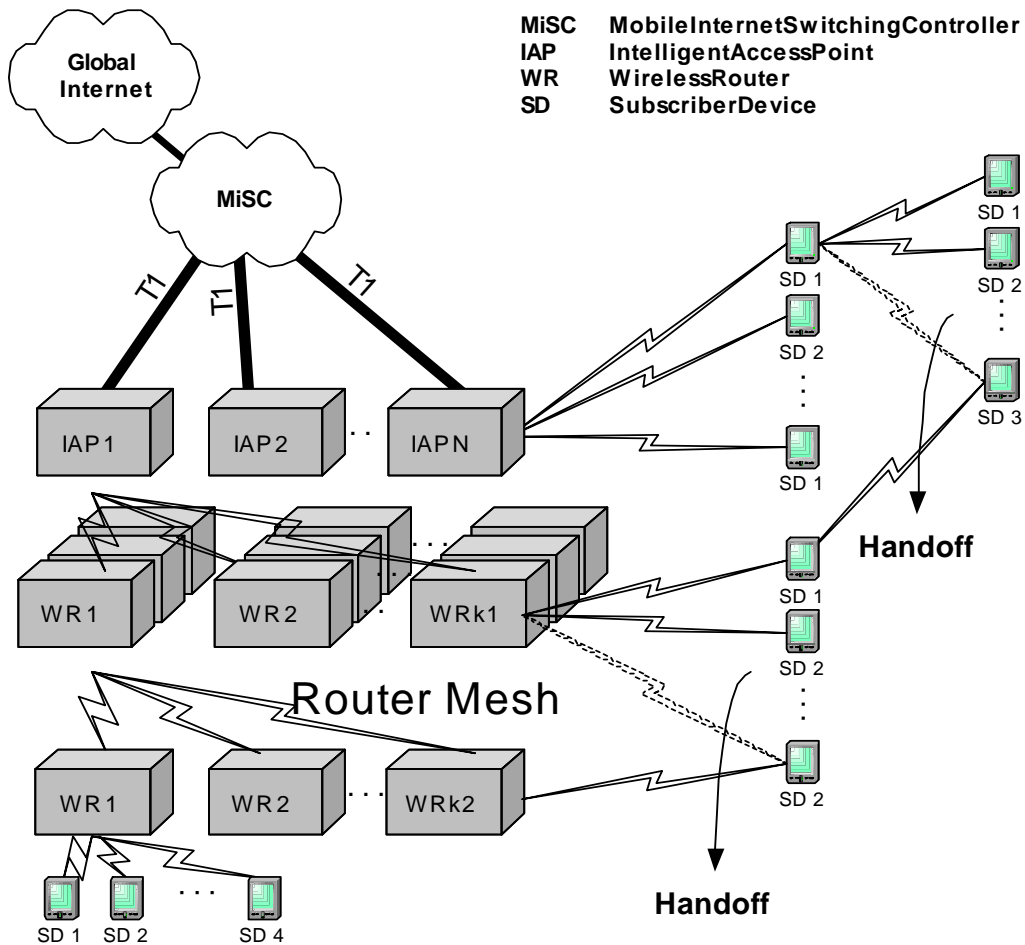
- Subscriber Provisioning, Management, and Authentication
- Configuration and Fault Management
- Network Monitoring and Reporting

## Operational View of the MEA System

Figure 2 shows the different ways a subscriber can reach an IAP. It can connect directly, or hop through any number or combination of WRs and SDs. Additionally, if the subscriber wishes to execute a peer-to-peer application such as a file transfer, the subscriber can communicate directly, or through any combination of SDs, WRs, and IAPs.

The ability to use ad hoc routing to forward traffic improves the scalability of the mobile wireless network. In particular, the ability for the user to accomplish a peer-to-peer application without the use of infrastructure has tremendous advantages.

A significant problem in every mobile wireless network is backhaul. The MEA architecture provides the ability to route traffic from applications through SDs and WRs without ever reaching an IAP or the wired network. This reduces the amount of backhaul required by enabling the SDs to accomplish the backhaul whenever the opportunity arises. In turn, this results in lower deployment costs, reduced backhaul, and lower operating expenditures. The service provider can provide the same level of service with less equipment by empowering the SDs with ad hoc networking capability.



**Figure 2. Operational View of the MEA System**

### ***Network Architecture***

The basic MEA network utilizes two subnets, one for the MEA wireless elements and one for the server elements. For seamless IAP mobility, all of the MEA wireless elements must be in the same subnet. The subnets are connected together by the core router, and the edge router provides Internet connectivity.

Figure 3 shows the logical network layout of a MEA network.

**Figure 3. MEA Network Architecture**



## Addressing Schemes

There are three addressing schemes that allow the IT manager increased flexibility in deployment: Network DHCP, Statically Provisioned, and User Supplied.

### Network DHCP Scheme

*Network DHCP* means that the 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 network device will forward any DHCP requests 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 user must associate and acquire an address from the network before establishing communications. Once a lease has been granted, the address will be valid 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.

This scheme is best for a larger, closely managed network of subscribers who need to communicate inside the network and require brief outside of network coverage.

### Statically Provisioned Scheme

Under the Statically Provisioned scheme addresses are hashed from the MAC address by default. This serves to eliminate the 10.x.x.x limitation on the network range.

When operating under the Statically Provisioned scheme, the network device will accept DHCP requests from the user's host and internally generate responses to grant the host an IP address and assign any other provisioned options.

This scheme requires that the host be configured to request an address from a DHCP server but does *not* require a DHCP server on the core network.

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 granted IP addresses granted by the server and options are configurable per-device using MeshManager. The internally generated DHCP messages will assign the host a static lease to the provisioned address, which 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.

### User Supplied Scheme

Operating under the *User Supplied* scheme, the user's host 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.

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.

### Setting the User Supplied IP Address

To setup the addressing for the User Supplied Scheme, first obtain a valid IP address from your Network Administrator. This is the IP address to be entered in the IP Address box on the Internet Protocol (TCP/IP) Properties dialog General tab.

From the **Start** menu, select **Settings** → **Control Panel**. Double click on the Network and Dial-up Connections icon.



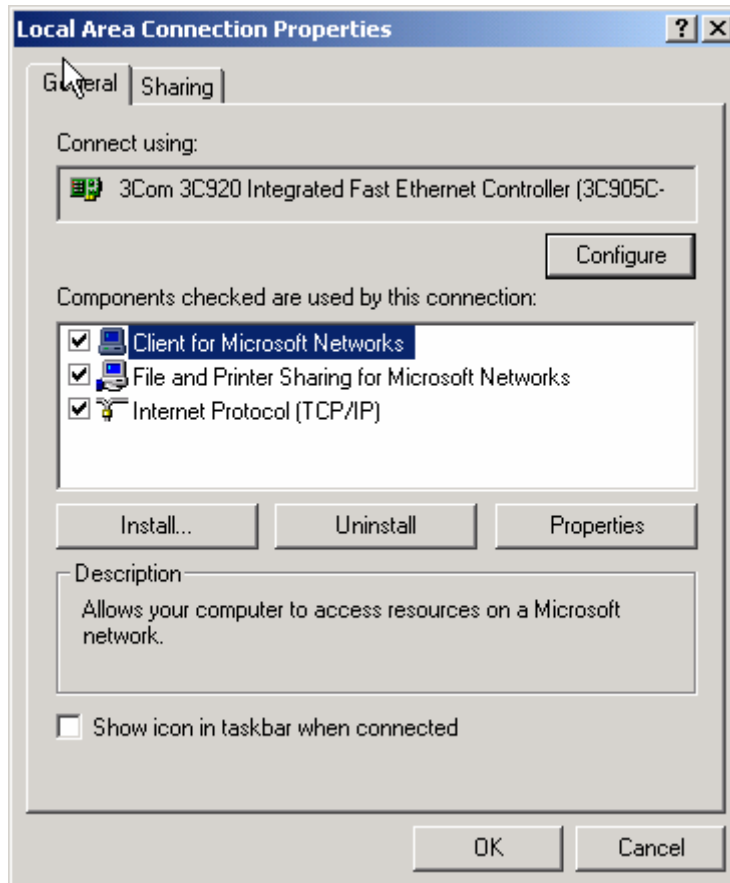
**Figure 4. Control Panel – Network and Dial-up Connections Icon**

The *Network and Dial-up Connections* window will be displayed. Double click on the *Local Area Connection* icon.



**Figure 5. Network and Dial-up Connections Window**

On the *Local Area Connection Properties* dialog, click to select *Internet Protocol (TCP/IP)* then click on the **Properties** button.



**Figure 6. Local Area Connection Properties Dialog Box**

The Internet Protocol (TCP/IP) Properties dialog box will be displayed.

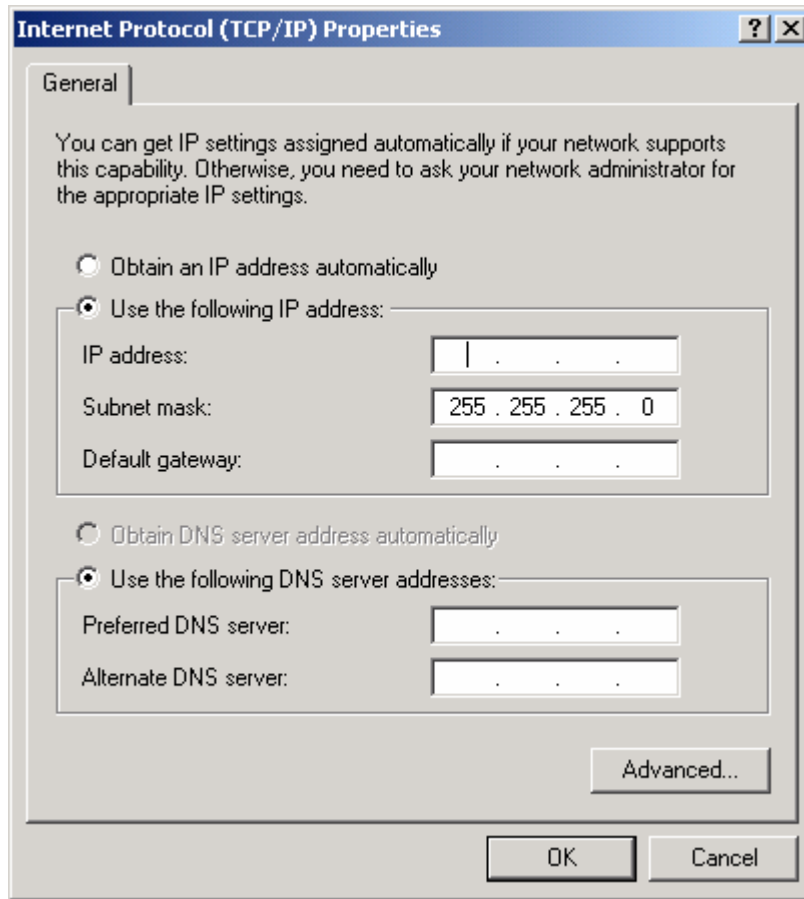


Figure 7. Internet Protocol (TCP/IP) Properties Dialog Box

With the *Use the following IP address:* radio button selected, enter the IP address supplied by the Network Administrator in the *IP Address:* box. Double click in the *Subnet Mask:* box to set the default subnet mask. The *Default gateway:* and the DNS server addresses should have already been set by the Network Administrator. Click on the **OK** button to accept the changes and dismiss the dialog box.

**Quality of Service (QoS) and User Priority Features**

The Motorola MEA system offers lower throughput than typical wired network systems. As a result, it may be necessary to regulate traffic flows over the wireless portion of the network so that interactive data flows and bulk data flows can be provided the proper levels of latency and reliability. The required level of regulation is provided by the *Quality of Service (QoS)* feature of the MEA system.

It may also be necessary to provide certain nodes higher priority access to the wireless network for all of their traffic, such as in emergency or tiered service systems. This functionality is provided by the *User Priority* feature.

Both QoS and User Priority deal with prioritization and shaping of packet traffic, are incorporated into the MEA system design as a single design feature. QoS allows a traffic generator to request special handling for enhanced throughput or reliability versus the standard *best effort* traffic. User Priority allows a user to request that traffic to/from a node be given preferential treatment. The resulting priority order is reflective of queuing order.



## Quality of Service

The primary objective for QoS is to provide the capability of differentiating traffic classes. The QoS provision will be implemented on a per-hop basis without explicit end-to-end QoS management.

Three main QoS functionalities have been implemented:

- 1) Packet classification
- 2) Prioritized channel access
- 3) Priority queue management with rate limiting

## User Priority

The User Priority service can be provisioned per-node for use with tiered service and emergency access systems. This priority feature is unique to the MEA network and only exists between endpoints within the MEA network or between a MEA network node and the ingress/egress node on the MEA network.

Nodes outside of the MEA Core LAN cannot request a particular priority for transmitted or received traffic. Any traffic into the MEA network needing prioritization must be prioritized at the ingress access point or router. Any traffic out of the MEA network will lose its priority assignment at the egress.

MEA wireless traffic will carry priorities attached to each packet. The MeshAPI can be used to tune the default priority of the local node

There is also an optional *Emergency* mode for use by special applications. The priority for use in emergency mode is separately provisioned and must be explicitly enabled per node by the network operator.

## Setup and Installation

### Subscriber Device (SD)

A Subscriber Device consists of both a Wireless Modem Card (WMC6300) and an End User provided host device such as a notebook computer. The WMC6300 is designed for insertion into an industry-standard Type II PCMCIA card slot located in a Host device. The WMC6300 has an antenna port to connect the external antenna and two LED Indicators. The Red LED is the transmit indicator and the Green LED is the receive indicator as shown in Figure 8.

### Equipment

The following list defines the MEA hardware components required to setup the WMC6300:

- WMC6300 Wireless Modem Card
- Antenna with a MMCX connector
- WMC6300 Software and Documentation CD for Windows 2000™ and Windows XP™

Equipment that must be supplied by the End User includes the following:

- Notebook PCs running the Microsoft Windows 2000 (service pack 3) or Windows XP (service pack 1) Operating System

### Record MAC Address of the WMC6300

The transceiver MAC address is recorded on the back of the WMC6300 cards. Record this number in [Section 4 - MAC Address Tables](#), as it will be required later to configure and test the device.

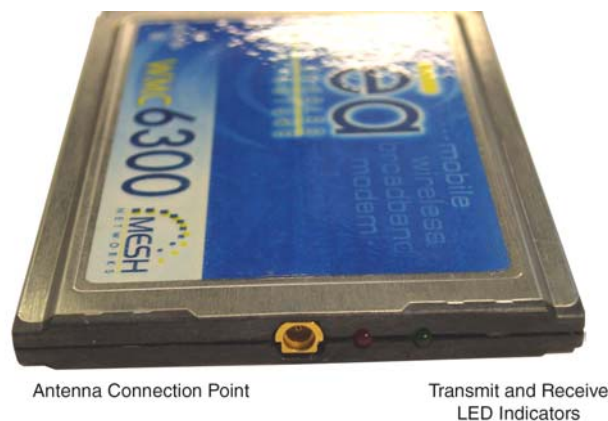


Figure 8. WMC6300 Antenna Port and LED Indicators

### Loading and Verifying WMC6300 Software

The MEA WMC6300 Software and Documentation CD contain the MEA drivers and MeshTray software for use on the End User's equipment. Please review the instructions for each operating system as there is a different sequence of events depending on the operating system. Detailed instructions can be found in the MEA WMC6300 Windows 2000 and XP Users Guide.

In addition, the MEA Administration Software and Documentation CD includes installation software to



load the MeshView Administration Tool. MeshView may be installed as an option on a subscriber device to assist the Network Operator with network deployment. Refer to the MeshView Users Guide for additional information on this application.

### Installing the WMC6300 Software for Windows

The MEA WMC6300 Wireless Modem Card Users Guide for Windows 2000 and XP provides complete step-by-step instructions for use during the installation and configuration of the WMC6300. The following is an abbreviated version of the installation process.

Complete the following procedure to install the WMC6300 software and drivers:

1. Insert the WMC6300 Software and Documentation CD into the computer's CD-ROM drive.
2. If the installation does not auto-start, start the driver installation by clicking on `d:\software\meaclientinstall.exe` (where "d" is the CD-ROM drive)
3. The MEA Setup program will be displayed. Click the **OK** button.
4. Click the **Next** button to continue the software installation process.
5. Follow the on screen prompts to complete the software installation process.
6. Insert the antenna into the WMC6300 card.
7. Insert the WMC6300 card into the computer.
8. Follow the on screen prompts to complete the installation process.

### Installing MeshView

Complete the following procedure to install MeshView:

1. Insert the MEA Administration Software and Documentation CD into the CD-ROM drive.
2. Click the Windows **Start** menu. Click on **Run** and enter `d:\setupmv.exe` in the textbox (Note: **d** is the letter of the CD-ROM drive). Click the **OK** button to continue the installation process.
3. Follow onscreen prompts to complete the installation process.

### DNS Server Configuration

The DNS server IP address is automatically supplied to the Subscriber Device upon successfully connecting to the Network. If there are problems with resolving web URLs, the DNS address can also be manually configured. The Network Operator must supply the DNS IP address for the Internet connection.

#### Instructions to setup a Windows 2000 Host:

1. Start/Settings/Network and Dial-up Connections/Local Area Connection  
(choose the Local Area Connection Corresponding to the Wireless Modem Card)
2. Click on the **Properties** button.
3. Highlight **Internet Protocol (TCP/IP)** in the Components window.
4. Click on the **Properties** button.
5. Click on the **Advanced** button.
6. Click on the **DNS** tab
7. Click on the **DNS Add** button.

8. Enter the *DNS Server IP Address* provided by the network administrator and then click the **Add** button.
9. Click the **OK** button to close the Advanced TCP/IP Settings windows.
10. Click the **OK** button to close the Internet Protocol (TCP/IP) Properties windows.
11. Click the **OK** button to close the Local Area Connection Properties windows.
12. Click the **Close** button to close the Local Area Connection Status window.

This configuration should remain in the Windows 2000 host.

### Instructions to setup a Windows XP host:

1. Click on Start/Control Panel/Network and Dial-up Connections/Local Area Connection
2. Right click on the Local Area Connection Corresponding to the Wireless Modem Card and select **Properties** from the pop up menu.
3. Highlight **Internet Protocol (TCP/IP)** in the Components window.
4. Click on the **Properties** button.
5. Click on the **Advanced** button.
6. Click on the **DNS** tab
7. Click on the DNS **Add** button.
8. Enter the *DNS Server IP Address* provided by the network administrator and then click the **Add** button.
9. Click the **OK** button to close the Advanced TCP/IP Settings windows.
10. Click the **OK** button to close the Internet Protocol (TCP/IP) Properties windows.
11. Click the **OK** button to close the Local Area Connection Properties windows.
12. Click the **Close** button to close the Local Area Connection Status window.
13. This configuration should remain in the Windows XP host.

### Installing the WMC6300 Software for Windows 2000

The MEA WMC6300 Wireless Modem Card User's Guide for Windows 2000 provides complete step-by-step instructions for use during the installation and configuration of the WMC6300. The following is an abbreviated version of the installation process.

**Note:** Please install the MEA Software **before** you insert the WMC6300 card.

Complete the following procedure to install the WMC6300 software and drivers:

1. Insert the WMC6300 Software and Documentation CD into the computer's CD-ROM drive.
2. Start driver install by clicking on d:\software\meaclientinstall.exe (where "d" is the CD-ROM drive)
3. The MEA Setup program will be displayed. Click the **OK** button.
4. Click the **Next** button to continue the software installation process.
5. Follow the onscreen prompts to complete the installation process.
6. Insert the antenna into the WMC6300 card.



7. Insert the WMC6300 card into the PCMCIA slot of the host computer.

If MeshView is desired, insert the MEA Administration Software and Documentation CD, open the Windows **Start** menu, click on **Run**, and then type **d:\software\meamvsetup.exe** (where **d** is the letter of the CD-ROM drive) and click the **OK** button. Follow onscreen prompts to complete the installation process.

## Testing

When the WMC6300 is inserted, you should receive an audible indicator that the device has been recognized. (If there was a problem with the driver installation, Windows will prompt you for a new device installation.)

Using MeshTray, select the **Configuration** tab, and then configure the WMC6300 address scheme to be "Statically Provisioned".

Click on the Windows **Start** button and select **Run** from the popup menu. Enter the command **ipconfig** in the textbox and click on the **OK** button to check your IP address. If an IP address in the range of **10.x.y.1** is displayed, the transceiver is working properly. Using MeshTray, reset the WMC6300 back to addressing scheme used to deploy the network.

## Intelligent Access Point (IAP)

The IAP is an infrastructure device that is positioned at a fixed location such as a building rooftop. The IAP6300 requires professional installation to ensure that the installation is performed in accordance with FCC licensing regulations.

The principle function of the IAP is to provide the Subscriber Devices in the coverage area of the IAP access to wired services. The IAP also provides a fixed location reference for Geo-Location, provides wireless routing for units in the IAPs coverage area, and is the principal network management interface to associated Wireless Routers and Subscriber Devices.

The MEA IAP provides a mounting bracket designed to be attached to a pole. For a MEA deployment, a permanent power source for each IAP must be provided. The standard IAP requires AC power, however there is an optional configuration for DC power. The RJ-45 weatherproof plug can be terminated in the field, allowing custom lengths to be assembled quickly on site.

## Equipment

The following list defines the standard MEA hardware components for the IAP:

- IAP Box with N-type Female Antenna Connector
- 120VAC Power Cable with a NEMA 5-15 plug
- Antenna with N-type Male Antenna Connector
- Weatherproof RJ-45 Connector
- Mounting Bracket

The Network Operator must supply the following:

- Mounting Location
- Power Source (100-240 VAC (0.08A) or 5VDC, depending on IAP model)
- Ethernet connection between the IAP and the MiSC
- Hand tools for bracket installation (7/16 wrench (2), Phillips screwdriver)

Optional Equipment:

- DC powered IAP (IAP6300-DC-IN)
- Power cord to connect to a photoelectric cell

## Record MAC Address of the IAP

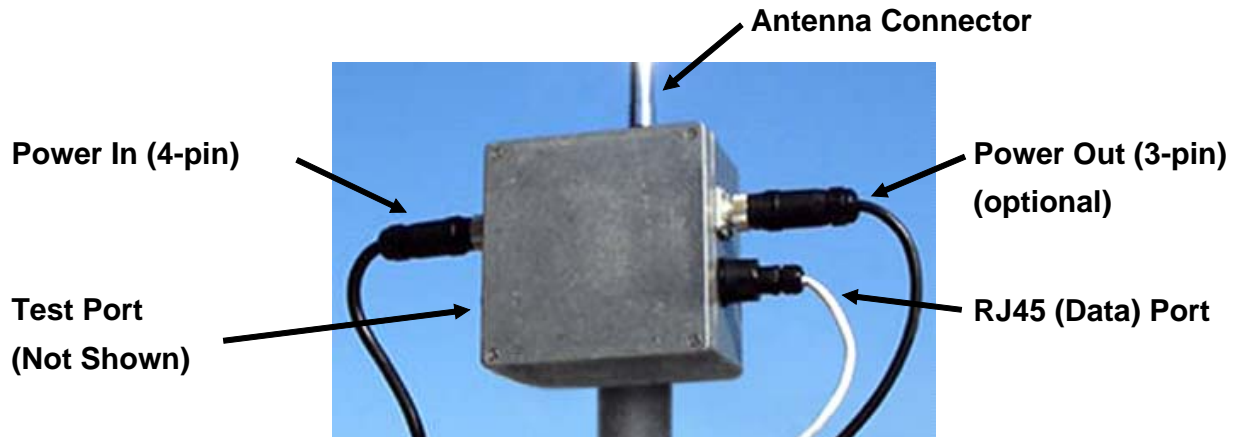
The transceiver MAC address is recorded on a label located on the antenna end of the IAP as shown in Figure 9. Record this number in [Section 4 - MAC Address Tables](#), because it will be required later to configure and test the device. Both SBC ETH and XCVR MAC addresses should be recorded.



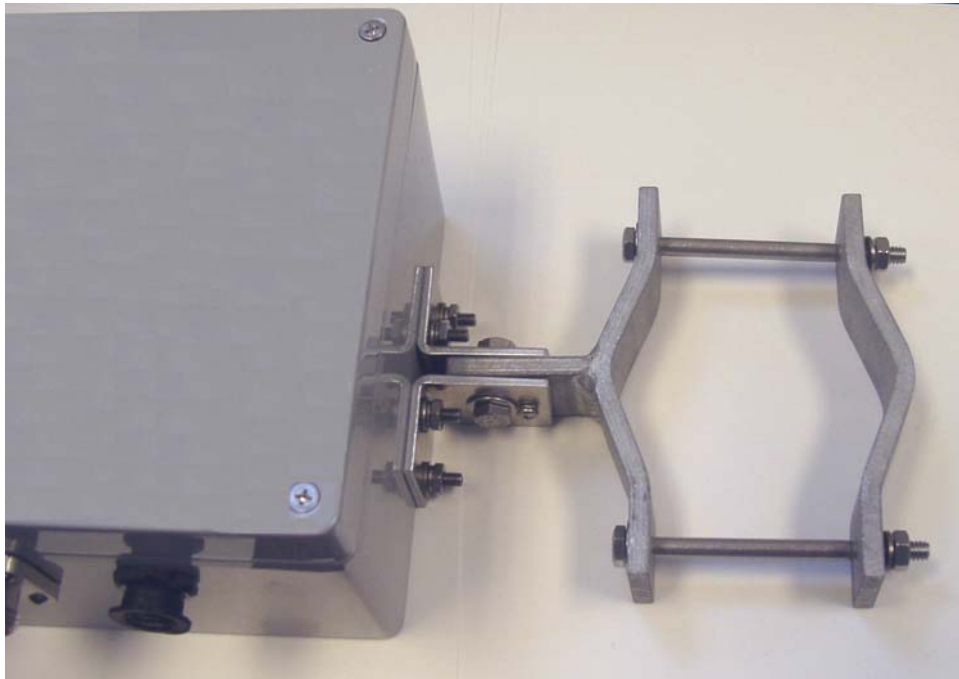
**Figure 9. IAP6300 Identification Label**

## IAP Assembly

Figure 10 shows the external connection points on an IAP6300 box. Figure 11 show the mounting bracket.



**Figure 10. IAP6300 Connection Points**



**Figure 11. IAP6300 Bracket**

## Assemble the IAP using the following procedure:

1. If desired, mount the IAP6300 box using the enclosed bracket. Refer to Figure 11.
2. Place the bracket at the desired position on the pole. The bracket can accommodate pole diameters between 1-3.5 inches.
3. Adjust the position of the box so that the antenna will be in a vertical position. Tighten the pivot and angle locking bolts on the shaft of the bracket as shown in Figure 12
4. Insert the antenna into the N-type Connector on the top of the box, and rotate to close.
5. Insert the IAP Power Plug into the 4-pin connector.

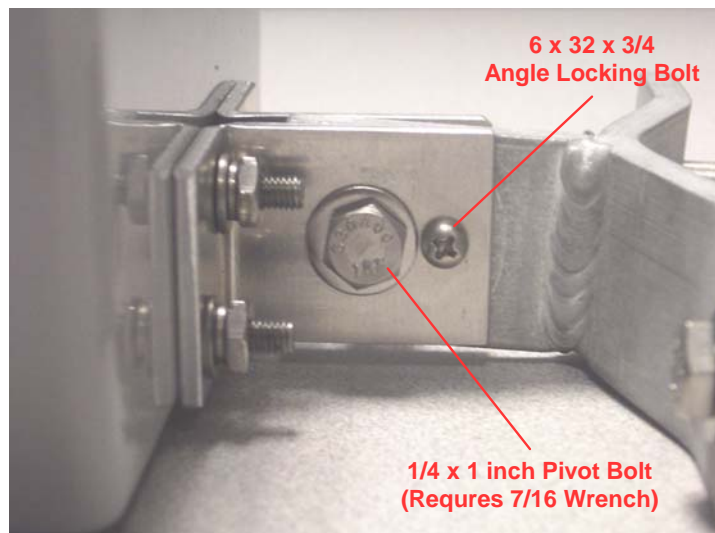


**For outdoor deployments, use only power cables rated for outdoor use.**

**To eliminate risk of electric shock, DO NOT connect/disconnect the end of the cable while the unit is energized.**

**This connection utilizes a keyed connector to ensure a proper connection. DO NOT FORCE.**

6. Install the weatherproof connector on the Ethernet cable as described at: [http://www.siemon.com/installation\\_instructions/pdf/IMAXIndustrialUTPPlug.pdf](http://www.siemon.com/installation_instructions/pdf/IMAXIndustrialUTPPlug.pdf)
7. Insert the Ethernet Cable into the RJ-45 port and tighten the connector to ensure a weatherproof seal.
8. If used, insert the Media Converter Power Cable into the optional 3-pin connector.
9. The Test Port is unused during deployment



**Figure 12. Bracket Adjustment Bolts**

## Deployment

When deploying the IAP consider the following:

- The IAP may be mounted on a pole having a diameter of 1-3.5 inches, utilizing the provided bracket.
- 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.
- When deploying the IAP, the antenna should be a minimum of 30 inches from any nearby metal poles to avoid distortion of the RF pattern.
- The IAP must have an Ethernet connection to the MiSC. If the distance between the IAP and the MiSC is greater than 100 meters, the Network Operator may utilize a T1 with the optional Net-to-Net boxes. The IAP optionally has a 5V, 3-pin, power out connection on the side of the box to power the Net-to-Net boxes. Other media converters may be used at the network operator's discretion.
- The installation location must provide power to the IAP.
- It is *required* that the IAP6300 chassis be grounded to minimize the possibility of ESD (electrostatic discharge) induced damage.
- It is the responsibility of the Network Operator to ensure that the installation complies with any local building codes and permits.

## Initial IAP Configuration

Prior to attempting configuration of the IAP, the IAP must be powered on and have connectivity to the MiSC.

Geo-location is a configuration item that is entered into an infrastructure device via the *Device Manager* tool, located on the MeshManager server (refer to the MeshManager User's Guide). Motorola recommends that a DGPS receiver be used to obtain accurate GPS coordinates, and that the longitude, latitude, and altitude values have a precision of 5 digits following the decimal point.

## Testing

Once there is an Ethernet connection to the MiSC, verify the health of the IAP with the following procedure:

1. Apply power to the IAP.
2. Obtain the transceiver and SBC MAC addresses that were recorded in [Section 4 - MAC Address Tables](#). The address will be in the format 00-05-12-30-xx-yy.
3. From MeshManager, display devices using the MAC address.
4. Select the appropriate IAP in the device tree, and then ping the device (right click and select ping).

A response to the ping commands verifies that both the transceiver and SBC are communicating.

### ***Wireless Router (WR)***

The MWR6300 (Wireless Router) is an infrastructure device positioned in a fixed location, such as on a pole, wall, or rooftop. The MWR6300 requires professional installation to ensure the installation is performed in accordance with FCC licensing regulations.

The Wireless Routers provides range extension, a means to route around obstructions, and a fixed location reference for use in Geo-Location.

The MEA MWR6300s comes with a mounting bracket that can be attached to a pole with a diameter of 1-3.5 inches. For a MEA deployment, a power source for each WR must be provided.

### **Equipment**

The following list defines the standard MEA hardware components needed to setup a WR:

- WR Box with N-type Antenna Connector
- 120VAC Power Cable with a NEMA 5-15 plug
- Antenna with N-type Male Antenna Connector
- Mounting Bracket

The Network Operator must supply the following:

- Mounting Location
- Power Source (100-240 VAC (0.08A) or 5 VDC depending on WR model)
- Hand tools for bracket installation (7/16 wrench (2), Phillips screwdriver)

Optional Equipment:

- DC powered WR (MWR6300-DC-IN)
- Power cord to connect to a photoelectric cell

## Record MAC Address of the MWR6300

The transceiver MAC address is recorded on the label located on the antenna end of the MWR6300 as shown in Figure 13.

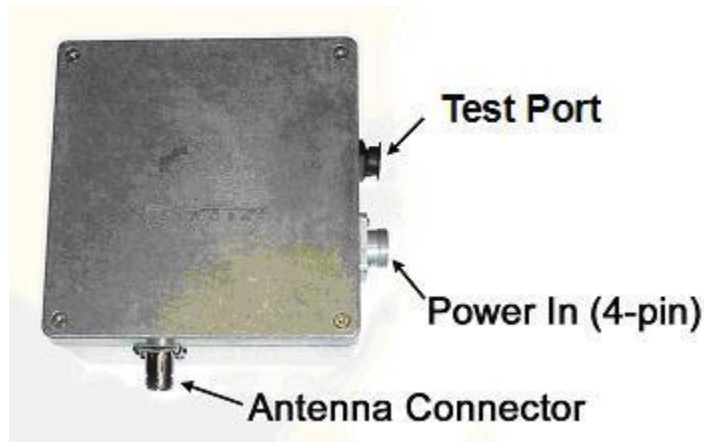
Record this number in [Section 4 - MAC Address Tables](#), because it will be required later to configure and test the device.



**Figure 13. MWR6300 Identification Label**

## MWR6300 Assembly

Figure 14 shows the external; connection points on a MWR6300 box.



**Figure 14. MWR6300 External Connection Points**

### Assemble the WR using the following procedure:

1. If desired, mount the WR box using the enclosed bracket. Refer to the procedure in the IAP assembly section of this document.
2. Insert the Antenna into the N-type Connector on the top of the box, and rotate to close.
3. Insert the Power Plug into the 4-pin Connector.



**For outdoor deployments, use only power cables rated for outdoor use.**

**To eliminate risk of electric shock, DO NOT connect/disconnect the end of the cable while the unit is energized.**

**This connection utilizes a keyed connector to ensure a proper connection. DO NOT FORCE.**

4. Verify the MAC address has been recorded in [Section 4 - MAC Address Tables](#), as it will be required to configure and test the device.
5. The Test Port is unused during deployment.

## Deployment

When deploying the MWR6300 consider the following:

- The MWR6300 can be mounted on a pole by using the provided bracket.
- When deploying the MWR6300, 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.
- A rule of thumb is to deploy 3-4 hop networks to optimize range, latency, and throughput. Typically, wireless routers are distributed within a network to extend range and guarantee coverage.
- The MWR6300 installation location must provide applicable AC or DC power for the device.
- It is **required** that the MWR6300 chassis be grounded to minimize the possibility of ESD (electrostatic discharge) induced damage.
- It is the responsibility of the Network Operator to ensure that the installation complies with any local building codes and permits.

## Initial Configuration

The configuration process for Geo-Location is the same as the IAP.

## Testing

Verify the operation of the MWR6300 using the following procedure:

1. Apply power to the MWR6300.
2. Obtain the transceiver MAC address that was recorded in [Section 4 - MAC Address Tables](#). The address will be in the format 00-05-12-0A-xx-yy.
3. From MeshManager, display devices using the MAC address.
4. Select the appropriate WR in the device tree, and then ping the device (right click and select ping).

A response to the ping command verifies that the transceiver is communicating.

---

## **Procedures for Grounding Infrastructure Devices**

The following section defines the procedures necessary to reduce the risk of damage to a me a infrastructure device (IAP/MWR/EWR) during the field installation or replacement process. These procedures are necessary, due to the use of sensitive electronic components and the presence of static electricity, especially in dry, high-static environments.

When installing or removing a me a device (IAP/MWR/EWR) from a permanently installed configuration (e.g. attachment to a tower or light pole), it is necessary to mitigate the risk of damage due to static electricity. Static electricity can be significant, especially in the presence of strong magnetic fields (near power lines) or in dry climates. To reduce the risk of ESD damage, the following procedures should be followed:

### **Antenna Installation**

1. The antenna should be installed or removed from an IAP/MWR/EWR away from power lines (>25') while minimizing the presence of static.
2. When changing the antenna, the box should be grounded or in contact with an ESD safe work surface. Before installing the antenna, residual static should be removed from the antenna by grounding both the antenna radiating element (N connector center pin) center pin and the antenna base (N connector outer shield). Grounding of these elements can be accomplished by touching these elements to the mounting bracket on the grounded box.
3. A suitable ESD work surface can be set up in the field by electrically connecting the work surface to an earth grounded metal object such as a metal light pole, earth grounded rod or a heavy metal chain (>10') lying on the earth's surface.

### **Device Installation**

1. The IAP/MWR/EWR and antenna should always be installed as a single unit.
2. The installer should employ the use of an ESD wrist strap during installation and removal. The wrist strap should be connected to the metal object on which the IAP/MWR/EWR will be attached.
3. A connection between the IAP/MWR/EWR and the metal object on which it will be mounted should be made *first* through an ESD wrist strap or equivalent connection. This will significantly reduce the static discharge rate from the IAP/MWR/EWR to ground and eliminate the build up of static during installation.
4. After the IAP/MWR/EWR is permanently affixed to the mounting structure the ESD strap connecting the IAP/MWR/EWR to the mounting structure may be removed.

### **Device Removal**

1. The IAP/MWR/EWR and antenna should always be removed as a single unit.
2. The installer should employ the use of an ESD wrist strap during installation and removal. The wrist strap should be connected to the metal object on which the IAP/MWR/EWR will be removed.
3. A connection between the IAP/MWR/EWR and the metal object on which it will be removed should be made *first* through an ESD wrist strap or equivalent connection. This will significantly reduce the static discharge rate from the IAP/MWR/EWR to ground in the event that the IAP/MWR/EWR comes in contact after it is initially removed from the mounting structure.

- 4. After the IAP/MWR/EWR is removed from the mounting structure, the ESD strap connecting the IAP/MWR/EWR to the mounting structure may be removed.

**Note:**

This procedure assumes that metal mounting structures have a suitable earth ground that is as short as possible. The earth ground is required for UL compliance as a safety ground and eliminates the potentially harmful build-up of static within the device.

**Mobile Internet Switching Controller (MiSC)**

The MiSC provides routing, switching, and management functions for the wireless network, and the connection to the wired world. There are currently two physical configurations of the MiSC staged by Motorola: MiSC Configuration 1 and MiSC Configuration 2.

**MiSC Configuration 1**

An example of MiSC Configuration 1 is shown in [Figure 15](#).

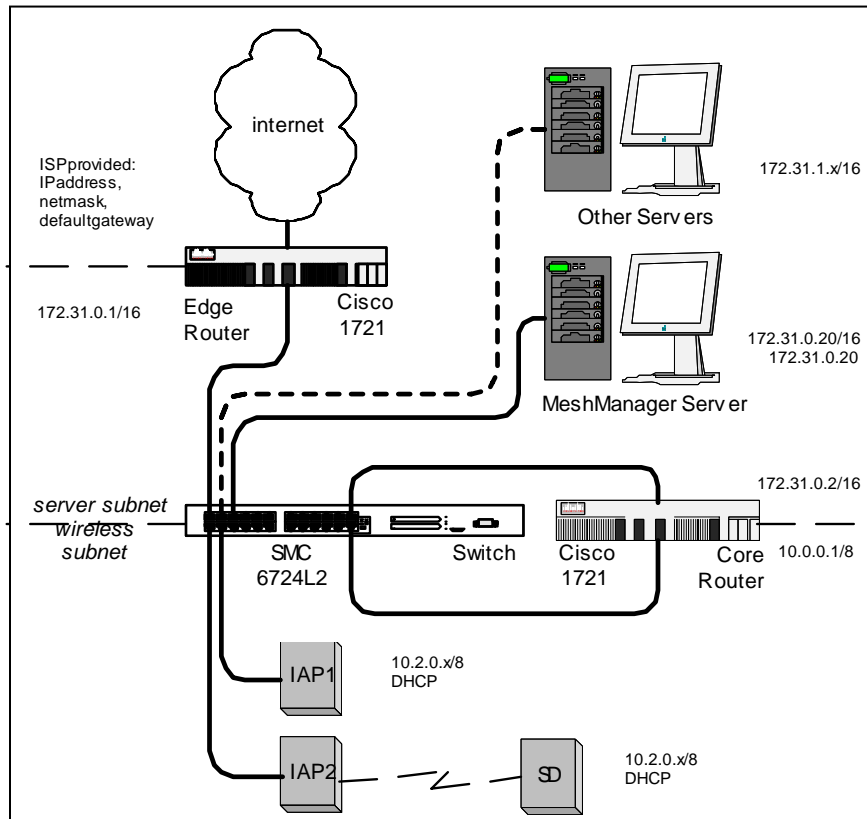


Figure 15. MiSC Configuration 1

This configuration includes an SMC 6724L2 Switch and Cisco 1721 Routers.

**MiSC Configuration 1 IP Network Configuration**

Two MiSC subnetworks are configured, one for the MEA wireless equipment, and the other for the server equipment. The wireless subnet is 10.0.0.0/8, and the server subnet is 172.31.0.0/16.

## MiSC Configuration 1 Routers

Two Cisco 1721 series Modular Access Routers are provided. They are designated the Core Router and the Edge Router. One Ethernet interface is standard, and a WIC-1ENET interface card is installed to provide a second Ethernet interface.

The Core Router utilizes the two Ethernet interfaces to connect the wireless and server subnets together. The 10 Mbps interface is 172.31.0.2/16 on the server subnet, and the 100 Mbps interface is 10.0.0.1/8 on the wireless subnet. The default route for the Core Router is to the Edge Router. The Core Router is configured with a "helper address" to forward DHCP broadcast requests from the 100 Mbps interface to the Sun Sever.

The Edge Router connects the server subnet with external networks for internetwork connectivity. The 100 Mbps Ethernet interface connects to the server subnet, and the 10 Mbps Ethernet interface is provided for connecting to an existing LAN. The 10 Mbps interface is field replaceable with a variety of external interfaces, such as T1, ADSL, or ISDN, see the Cisco 1721 series Modular Access Router documentation for a complete list of available interfaces.

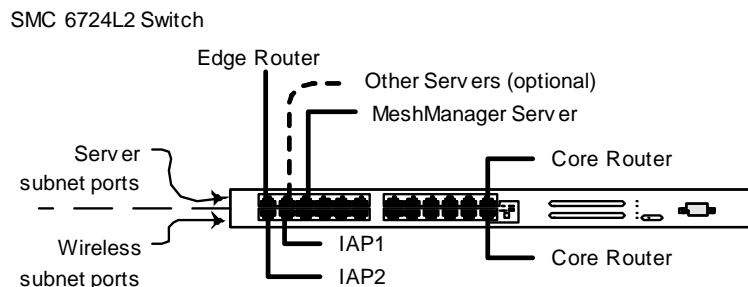
The 100 Mbps Ethernet interface is 172.31.0.1/16 on the server subnet (inside), and the 10 Mbps Ethernet interface must be configured based on the network being connected to (outside). The default route for the Edge Router is to the outside interface. The Edge Router NATs inside to outside, and routes all wireless subnet traffic (10.0.0.0/8) to the Core Router.

Sample router configuration files are provided in the *Appendix* section of the *MiSC Configuration Guide*.

## MiSC Configuration 1 Switch

Both of the MiSC subnets require an Ethernet switch or hub. A single SMC 6724L2 24-port Ethernet Switch is provided and is configured to provide two logical switches.

The 24 Ethernet ports are separated into two 12-port VLANs. The upper row of ports (1-12) is for the server subnet, and the lower row (13-24) is for the wireless subnet. This provides the equivalent of two switches, with independent broadcast domains for each of the subnets.



**Figure 16. MiSC Configuration 1 – SMC 6724L2 Switch**

## MiSC Configuration 1 Assembly

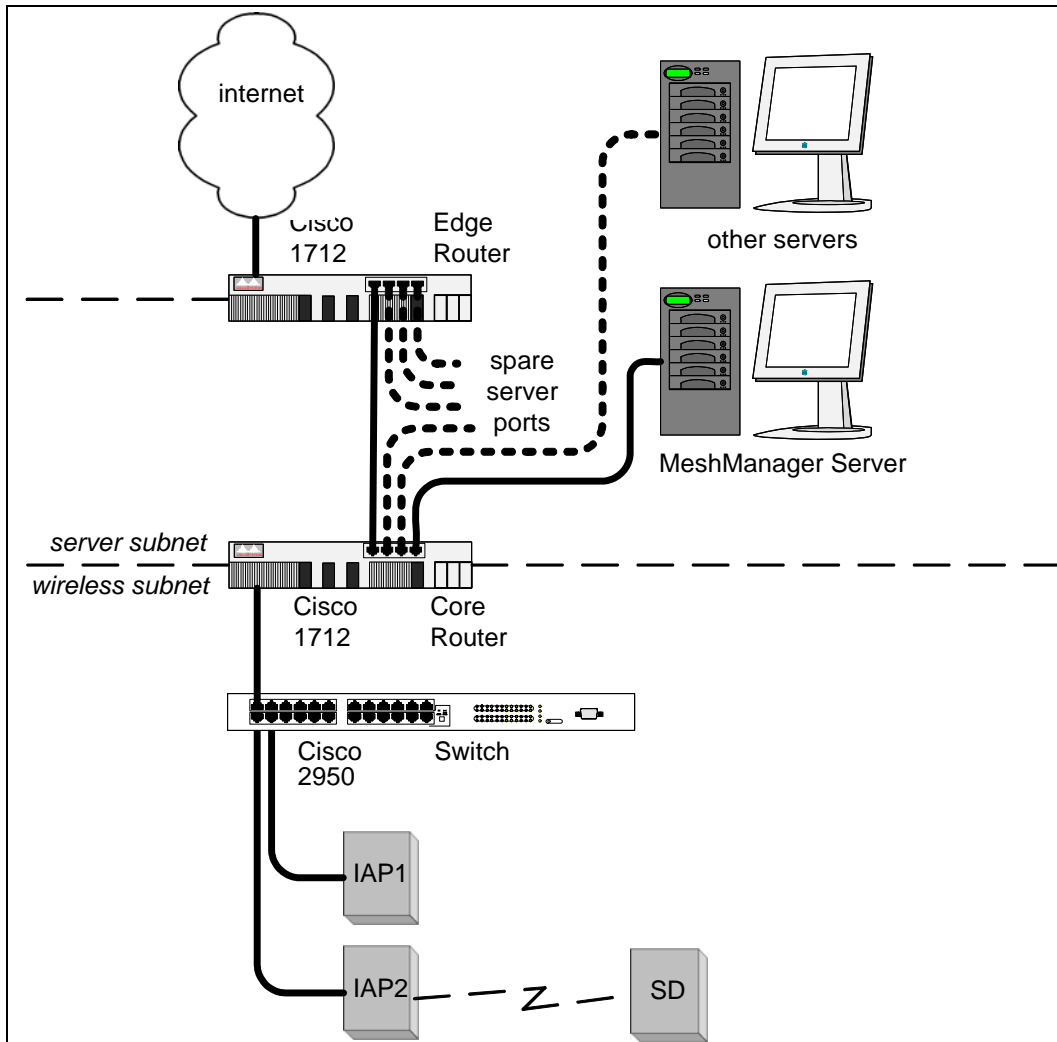
The MiSC hardware consists of commercial off-the-shelf components. The components are pre-configured with a basic configuration that requires minimal site-specific changes.

1. The SMC switch arrives configured as two virtual LANs. The upper row of Ethernet ports is for the server subnet; the lower row of ports is for the wireless subnet.

2. Unpack the SMC switch and mount as desired (either in a rack or on a table top). Connect the switch to a power source.
3. Unpack the Cisco router labeled *EdgeRTR* and connect to a power source. Plug interface labeled *10BT Ethernet* into the Internet or the Network Operator's private network. (The network operator supplies this cable; it will be an Ethernet cable for connecting to a hub or switch, or an Ethernet crossover cable if connecting to another router.) Plug interface labeled *10/100 Ethernet* into the SMC switch on port 1.
4. Unpack the Cisco router labeled *CoreRTR* and connect to a power source. Plug interface labeled *10BT Ethernet* into the SMC switch on port 12. Plug the interface labeled *10/100 Ethernet* into the SMC switch on port 24.
5. Unpack the Sun Blade/MeshManager server and monitor and connect to a power source. Plug the network interface into any of the ports 2-11 on the SMC Switch.
6. Connect Network Operator supplied computer running Windows 2000. Plug the network interface into any of the ports 2-11 on the SMC Switch.
7. Connect the IAPs to any of the ports 13-23 on the SMC switch.

## MiSC Configuration 2

An example of MiSC Configuration 2 is shown in [Figure 17](#).



**Figure 17. MiSC Configuration 2**

### MiSC Configuration 2 IP Network Configuration

Two MiSC subnetworks are configured, one for the MEA wireless equipment, and the other for the server equipment. The wireless subnet is 10.0.0.0/8, and the server subnet is 172.31.0.0/16.

### MiSC Configuration 2 Routers

Two Cisco 1712 series Modular Access Routers are provided. They are designated the Core Router and the Edge Router. Each router has a single Ethernet port, as well as a built-in 4-port switch.

The Core Router connects the wireless and server subnets together. The router appears on the server subnet as 172.31.0.2, and as 10.0.0.1 on the wireless subnet. The default route for the Core Router is to the Edge Router. The Core Router is configured with a "helper address" to forward DHCP broadcast requests from the 100 Mbps interface to the Sun Server.

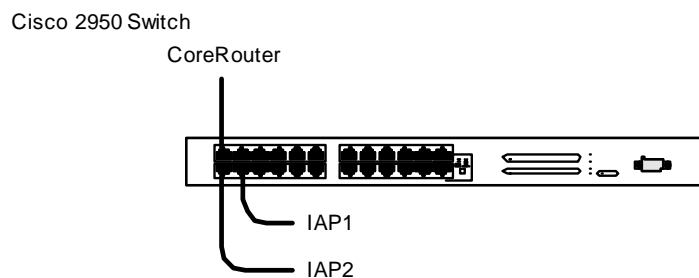
The Edge Router connects the server subnet with external networks for internet connectivity. The single 100 Mbps Ethernet interface (FastEthernet 0) connects to an existing LAN, and the edge router appears on the server subnet as 172.31.0.1. The single 100 Mbps interface is field replaceable with a variety of external interfaces, such as T1, ADSL, or ISDN, see the Cisco 1712 series Modular Access Router documentation for a complete list of available interfaces.

The default route for the Edge Router is to the outside interface. The Edge Router NATs inside to outside, and routes all wireless subnet traffic to the Core Router.

Sample router configuration files are provided in the *Appendix* section of the *MiSC Configuration Guide*.

### MiSC Configuration 2 Switch

The wireless subnet requires an Ethernet switch or hub. A single Cisco 2950 24-port Ethernet switch is provided. One port connects to the Core Router, leaving 23 ports available for connecting to IAPs on the wireless network.



**Figure 18. MiSC Configuration 2 – Cisco 2950 Switch**

### MiSC Configuration 2 Assembly

The MiSC hardware consists of commercial off-the-shelf components. The components are pre-configured with a basic configuration that requires minimal site-specific changes.

1. Unlike previous revisions of MiSC hardware, the switch is NOT configured with any virtual LANs (VLANs). Server hardware and IAPs may be connected to any port on the Cisco switch and/or the switch ports on the back of each router.
2. Unpack the Cisco switch and mount as desired (either in a rack or on a table top). Connect the switch to a power source.
3. Unpack the Cisco router labeled *EdgeRTR* and connect to a power source. Plug interface labeled *10/100 Ethernet* into the Internet or the Network Operator's private network.
4. Unpack the Cisco router labeled *CoreRTR* and connect to a power source. Plug interface labeled *10/100 Ethernet* into the switch on any port.
5. Connect a cable between the switch ports labeled 4x on the *EdgeRTR* and *CoreRTR* routers.
6. Unpack the MeshManager server and monitor and connect to a power source. Plug the network interface into the 1x switch port on either router.
7. Optionally, plug the Network Operator supplied computer into any of the switch ports on either router.
8. Connect the IAPs to any of the ports on the switch.

## ***Upgrade MiSC/DHCP Configuration (optional)***

MEA Release 2 or later continues to use the 10.x.x.x addressing scheme as a default. However, it can be changed to a site-specific address. The following procedure describes the changes necessary to accomplish this.

The following items must be configured to change the MEA wireless subnet.

Edge router

IP route to the wireless subnet via the core router (default 10.0.0.1)

NAT access list for wireless subnet

Core router

IP address of the wireless network interface (default 10.0.0.1)

Sun server

DHCP dhcpd.conf, for the new pool of addresses, new default router, new broadcast address

DNS named.conf and zones file, for the new subnet range

The MiSC switch does not require any changes, since the partitioning of the switch does not involve IP addresses.

When the MEA upgrade of the IAPs is complete, the MEA devices should all be handled automatically by the DHCP changes. These should refresh automatically when the DHCP lease time expires (600 seconds) and they refresh their DHCP lease. This can be hurried by simply resetting the devices once the other changes have been completed.

## **Changing the Wireless Subnet**

The IP address of the default gateway used by any MEA device must not be within the either of the wireless subnets configured in all IAPs. Otherwise, SD hosts will be unable to resolve the IP address of the default gateway. There are two wireless subnets configured for IAPs in MeshManager on the IAP device configuration window, the local wireless subnet, fields Local Wireless Subnet and Local Wireless Subnet CIDR (defaults are 10.2.0.0 and 16), and the global wireless subnet, fields Global Wireless Subnet and Global Wireless Subnet CIDR (defaults are 172.16.1.50 and 24).

If wired devices will be connected to the MEA subnet, all IAPs must be configured with the address range of the wired devices if MEA devices need to communicate with them. Otherwise, SD hosts will be unable to resolve IP addresses of wired devices within the same subnet. The wired device address range is configured for IAPs in MeshManager on the IAP device configuration window, fields Global Wireless Subnet and Global Wireless Subnet CIDR (defaults are 172.16.1.50 and 24).

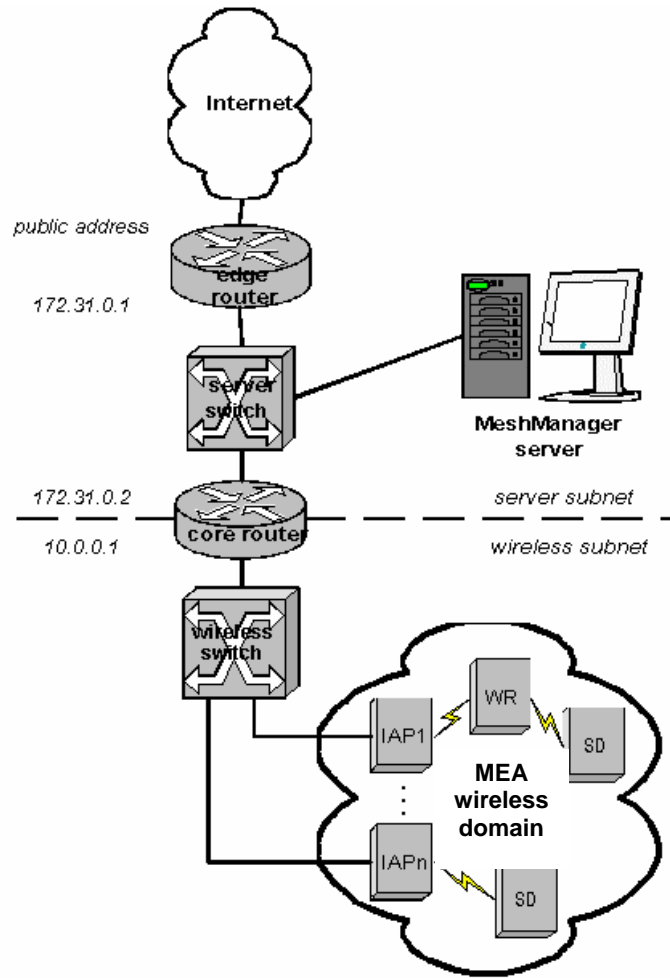


Figure 19. MEA Subnet Data



**Network Configuration – Device Manager**

*Device Manager* is a utility located on the MeshManager server. It is used to configure and monitor the deployed network. Refer to the MeshManager User’s Guide for detailed instructions on how to use the Device Manager.

MEA systems are delivered with the initial configuration of IAPs, WRs, and SDs in the MeshManager system. This allows for easy testing of the system as units are tested on site.

**Enable SNMP Trap Forwarding**

It is possible to configure all SNMP traps that are received by the device Manager to be forwarded to an external IP address/port. Enabling this functionality does not impact Device Manager functionality. Rather, it provides additional functionality which allows integration with external alarm management systems. Use the following procedure to enable and configure SNMP trap forwarding functionality.

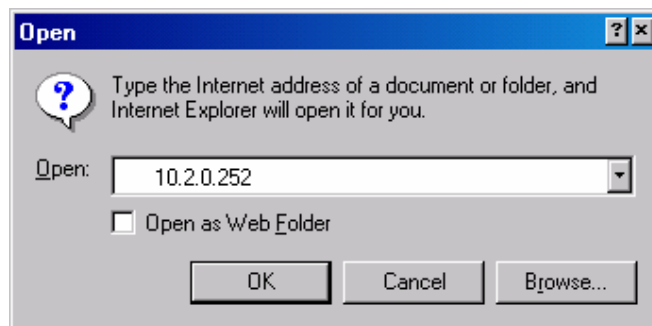
1. Locate the *ep.conf* file. For MeshManager installations on the MiSC the file will be located in *opt/MiSM/EventProcessor/ep.conf*. For MeshManager EZ installations, the file will be located in *C:\Program Files\MeshManager\EventProcessor\ep.conf*.
2. Edit the *ep.conf* file to make the following changes:
  - a. *trapforward=false* to *trapforward=true*
  - b. *trapforwardlist=* to *trapforwardlist=<IP Address>:<Port Number>* or *trapforwardlist=<IP Address>*

where *<IP Address>* and *<Port Number>* indicate the IP address and Port number to be used for SNMP Trap Forwarding. If the *<Port Number>* is not specified when changing the *ep.conf* file, the default Port Number of 162 will be used.

Restart MeshManager Services to complete the SNMP Trap Forwarding enable process.

**Network Configuration – IAP Configuration via Web Interface**

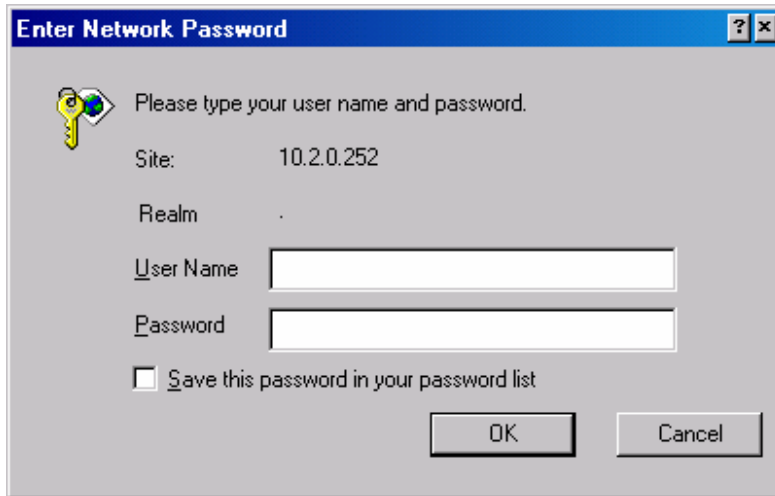
A second method of performing various network configuration functions for an IAP may be accomplished using a standard web browser. Connect a host PC to the switch in the MiSC. Using a standard Internet Browser such as Microsoft’s Internet Explorer or Netscape, enter the IP Address corresponding to the IAP’s SBC MAC to be configured as shown in **Figure 20**. It is recommended that you install and configure the IAPs one at a time.



**Figure 20. MEA Device Administration Connection**

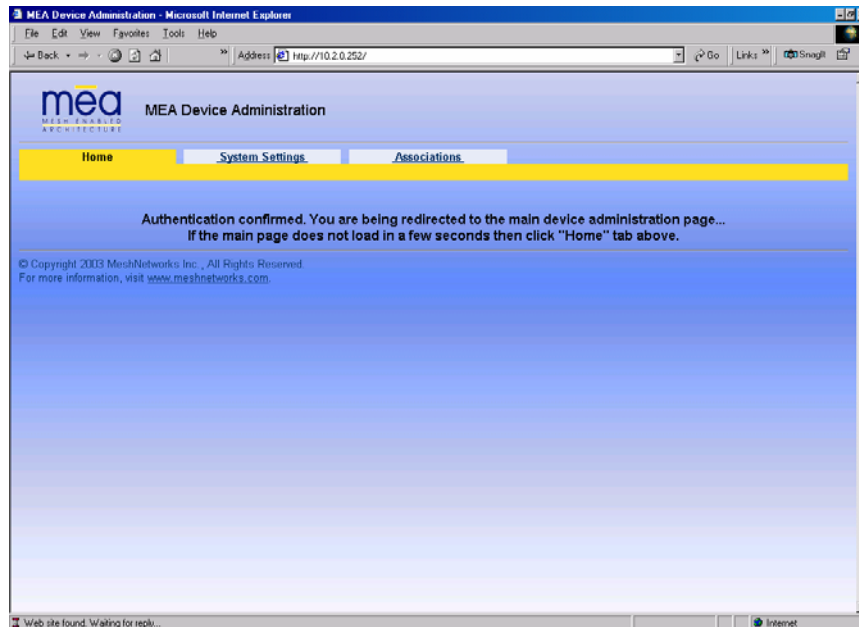
A Log On window for the Administration Utility will be displayed in the browser, as shown in **Figure 21**. Before the Administration Utility is displayed, the user must complete the simple logon procedure

before proceeding. The default login is **admin** and the password is **admin**. The password can be changed, as described further in this document.



**Figure 21. MEA Device Administration Logon Window**

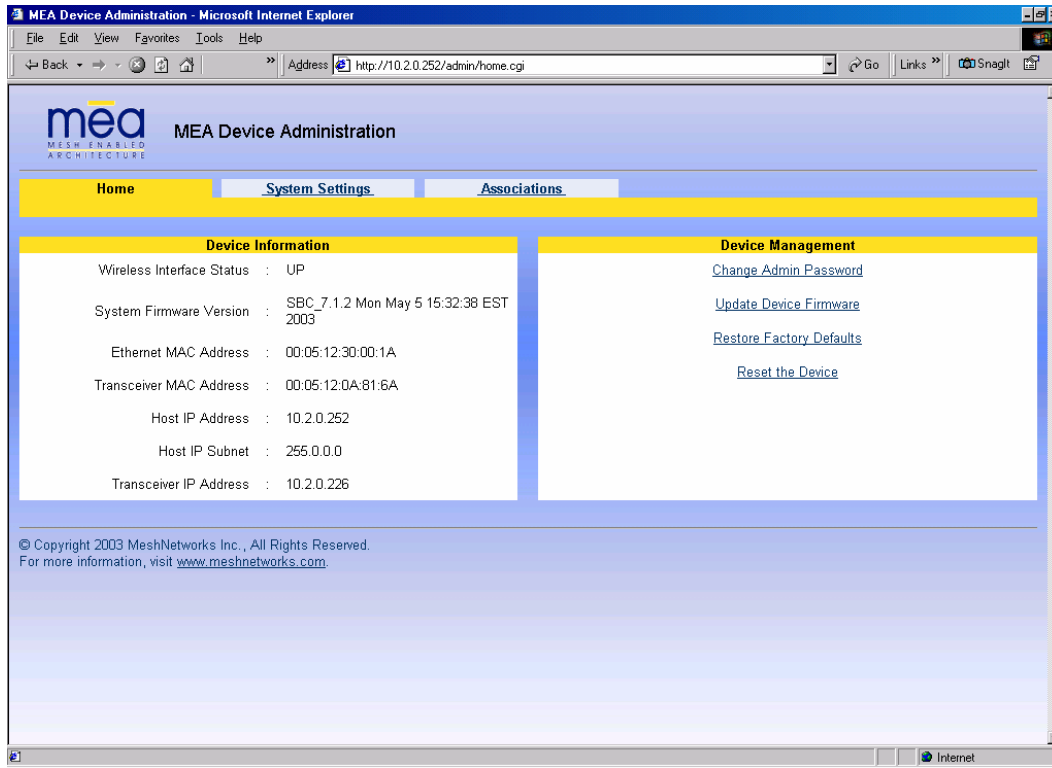
When the User Name and Password has been verified, the Administration window will be displayed as shown in **Figure 22**.



**Figure 22. MEA Device Administration Authentication Window**

At the completion of the logon, the Home Tab screen will be displayed as shown in Figure 23.

## Home Tab



**Figure 23. MEA Device Administration Home Tab**

The Device Information window provides data on:

- Wireless Interface Status (interface between the Host and the transceiver)
- System Firmware Version (software running on the Host in the IAP)
- Ethernet MAC Address (MAC address of the Host)
- Wireless MAC Address (MAC address of the transceiver)
- Host IP Address (the DHCP provided address for the Host)
- Transceiver IP Address (the DHCP provided address for the transceiver)

Also located on the Home Tab are Device Management options for

- Change Administration Password
- Update Device Firmware
- Restore Factory Defaults
- Reset the Device

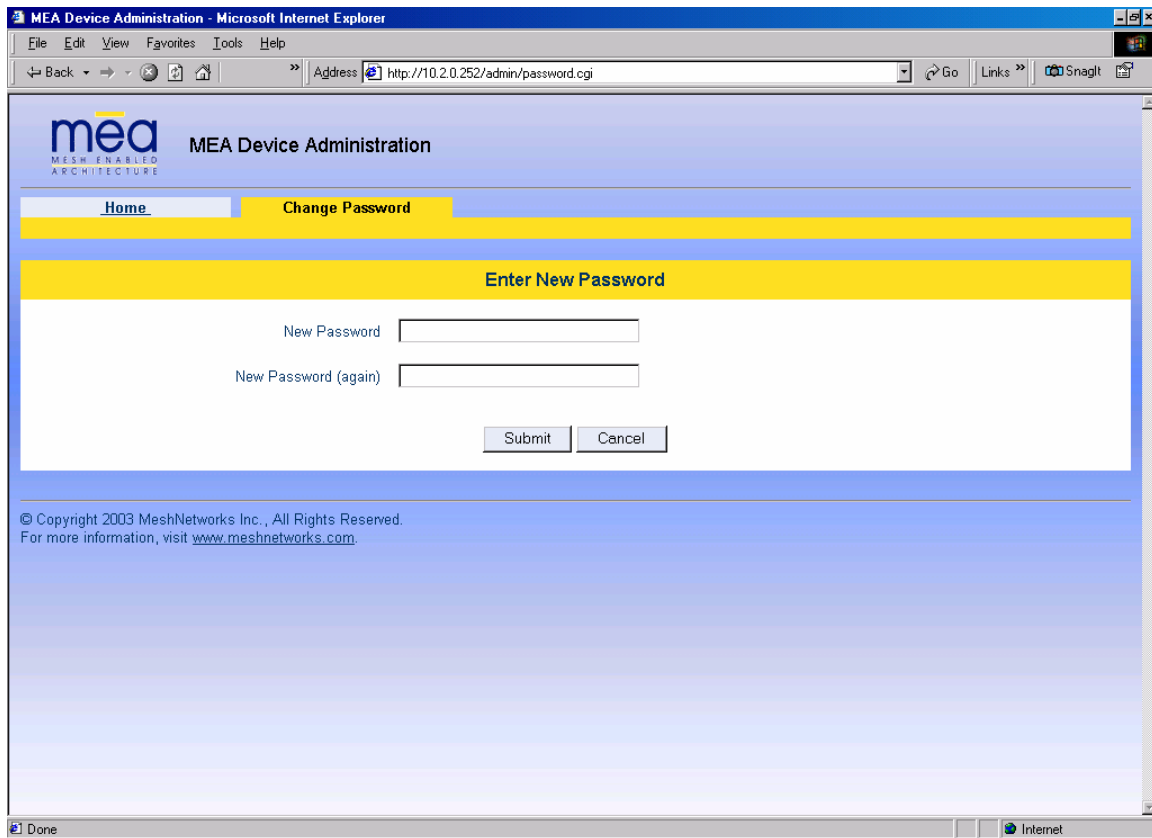
The Device Management options are detailed below.

## Home Tab – Change Admin Password

From the Home tab, the user can select the **Change Admin Password** to change the administrator password of the device.

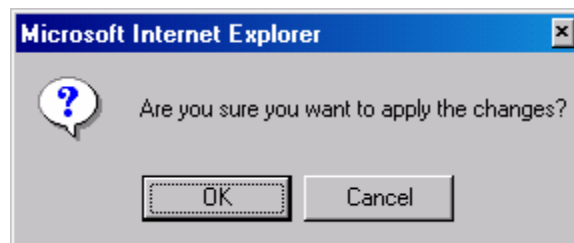
**WARNING** – If the password is lost, the password can only be reset at the factory. Do not forget to record the information in an appropriate location for future use.

1. To change the password, select **Change Admin Password**.
2. *Enter the new password* will be displayed on the Change Password window as shown in Figure 24. Enter the new password in the **New Password** textbox.
3. Enter the new password again in the **New Password (again)** textbox.



**Figure 24. MEA Device Administration Enter New Password Window**

4. Click on the **Submit** button. A confirmation window will appear as shown in Figure 25. Click on the **OK** button to continue.



**Figure 25. MEA Device Administration Confirmation Window**

- 5. The browser will display a message that confirms the password change as shown in Figure 26. Click on the **Finished** button to continue.

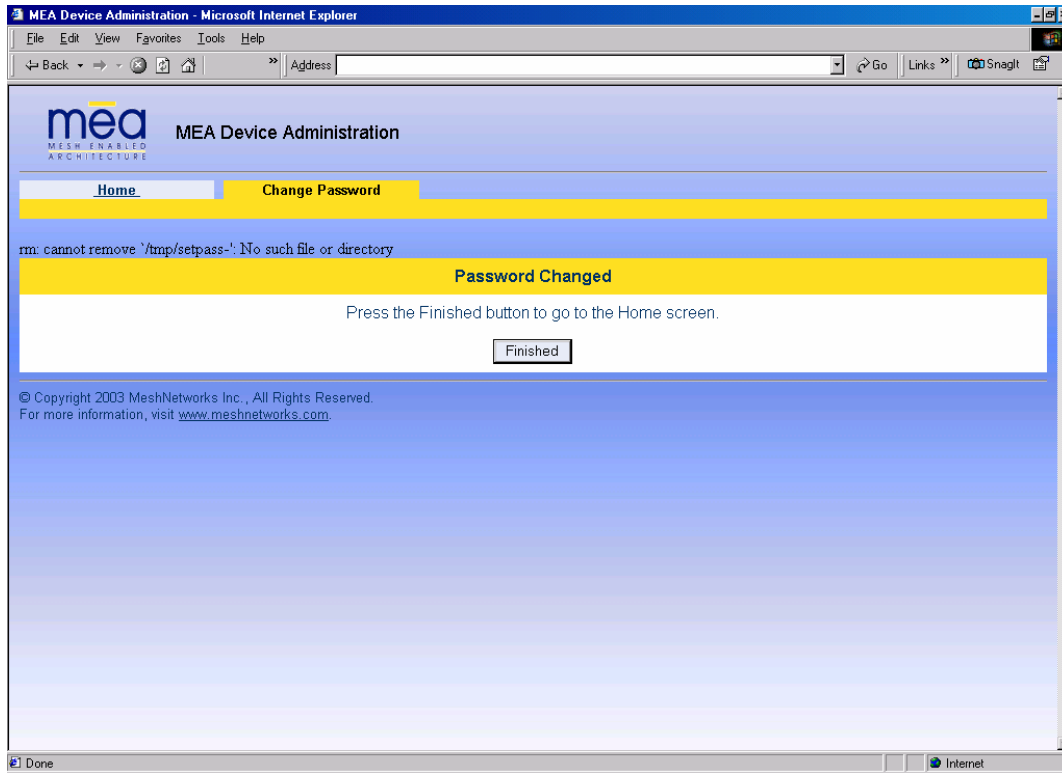


Figure 26. MEA Device Administration Password Changed Window

- 6. A Logon window will now prompt for the new password.

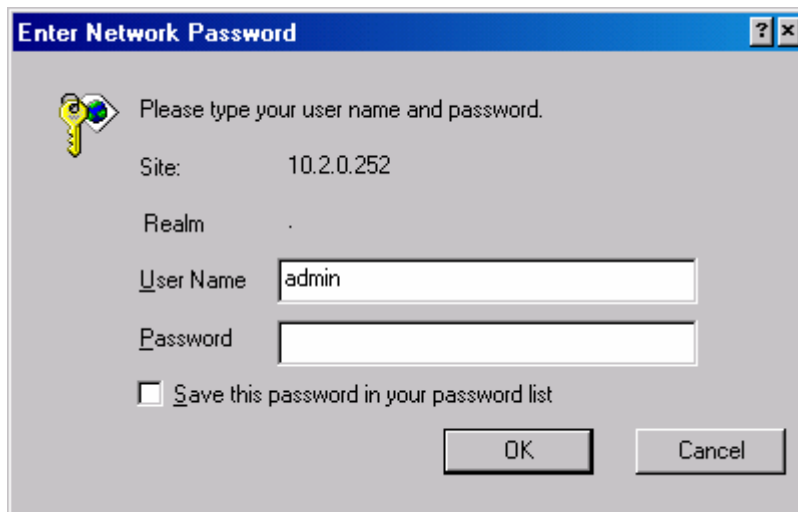
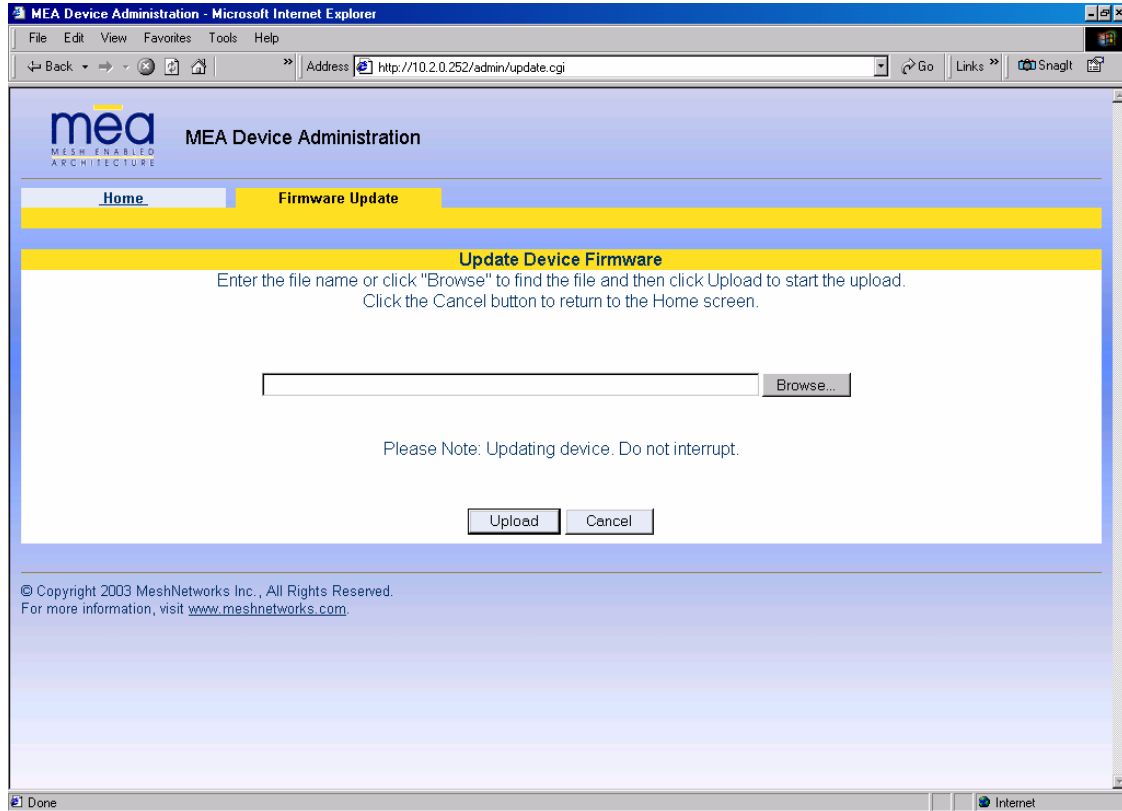


Figure 27. MEA Device Administration Logon Window

## Home Tab – Update Device Firmware

From the Home Tab, select **Update Device Firmware** to load a new version of the firmware into the IAP.

A New Device Firmware window will be displayed as shown in Figure 28



**Figure 28. MEA Device Administration Update Device Firmware Window**

1. Specify the path and file name of the firmware *bin* file to be uploaded to the device. Or click on the **Browse** button to navigate to the correct location of the firmware *bin* file. If the **Browse** button is selected, the **Choose file** window is displayed as shown in *Figure 29*. Locate and select the desired firmware *bin* file to be uploaded to the device. Then click on the **OK** button.

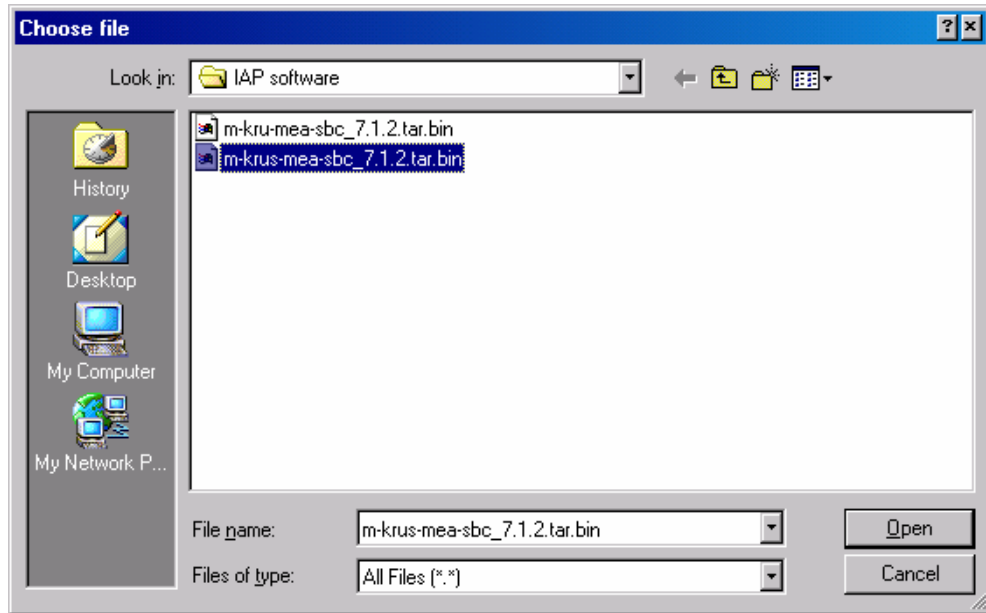


Figure 29. MEA Device Administration Choose File Window

The path and file name of the firmware *bin* file will be displayed in the Update Device Firmware window as shown in Figure 30. Click on the **Upload** button to continue the process or select **Cancel** to terminate the Firmware Update procedure

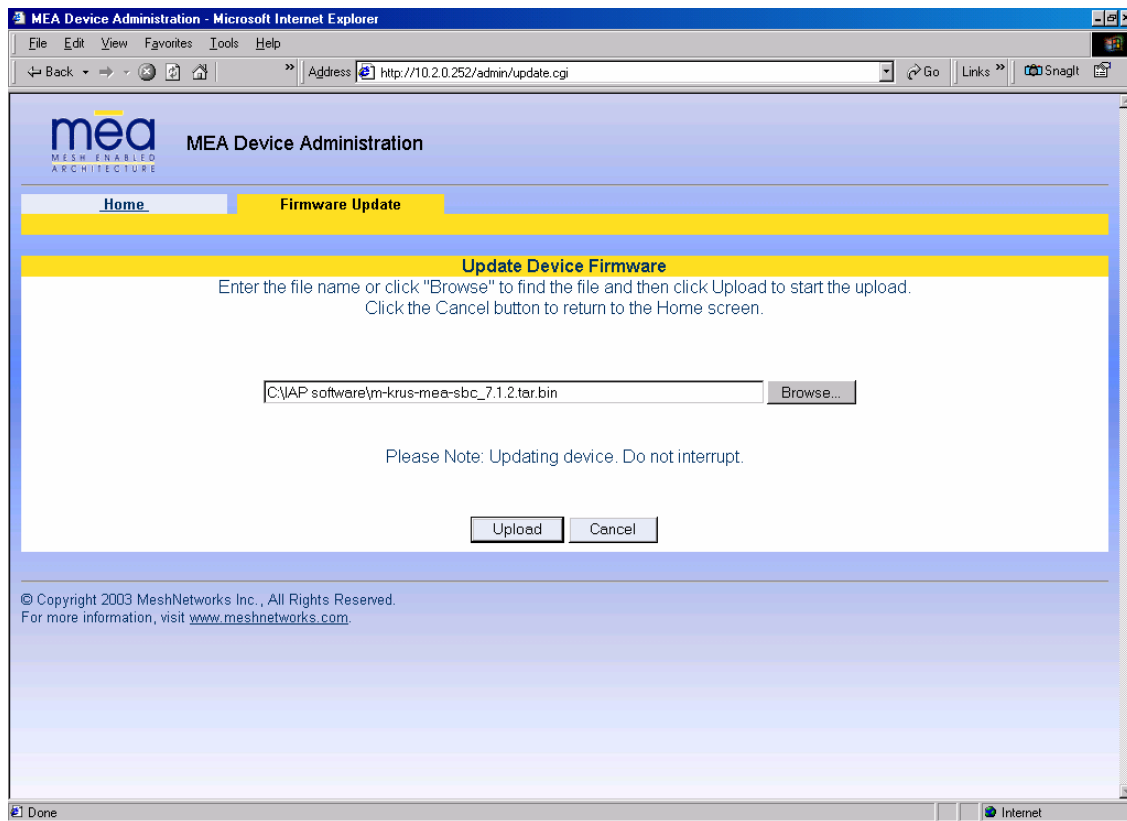
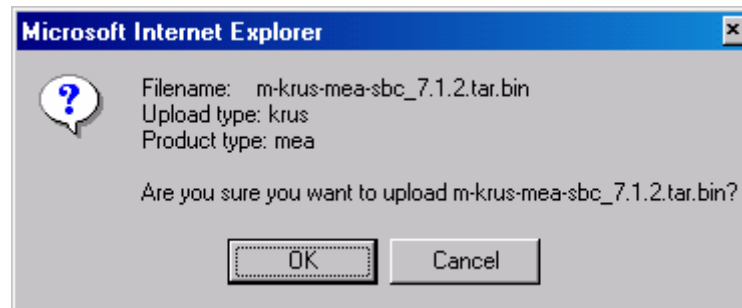


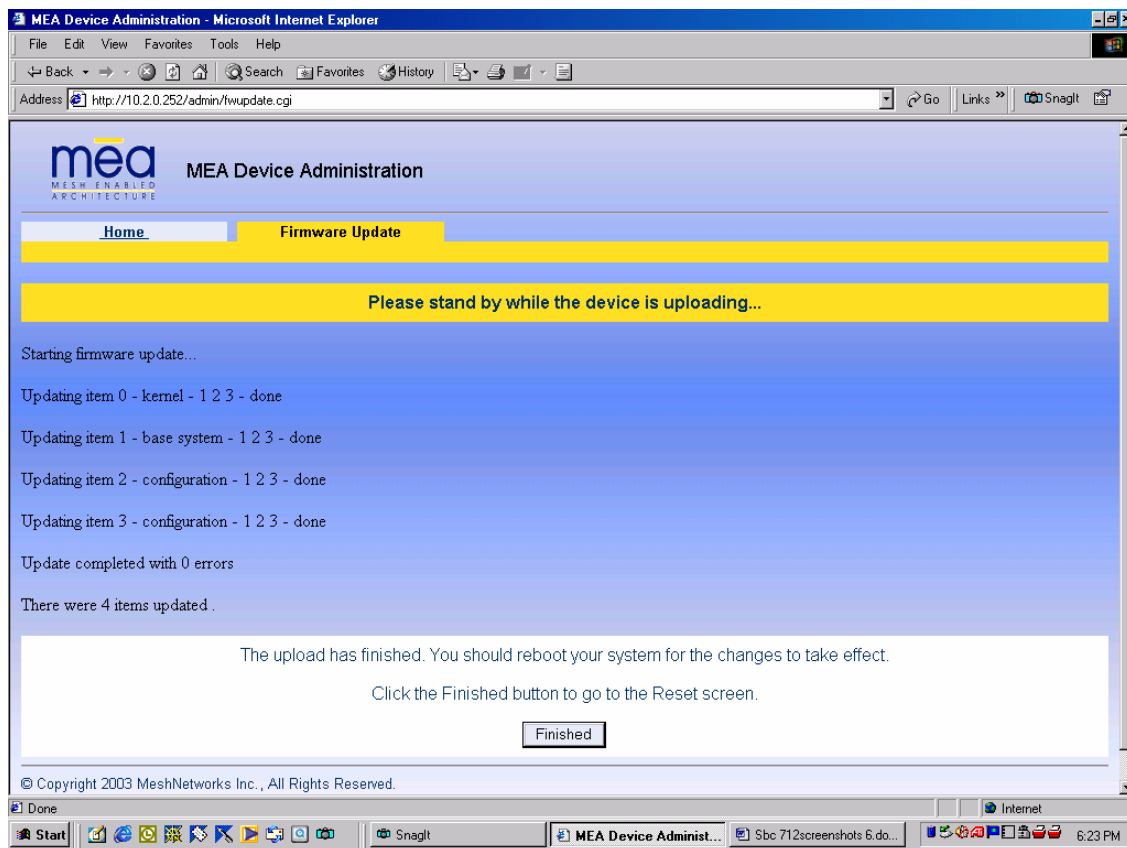
Figure 30. MEA Device Administration Update Device Firmware Window (2)

2. If the **Upload** button is selected, an upload confirmation message is displayed as shown in *Figure 31* to confirm that you want to continue the Firmware Update procedure. Click on the **OK** button to continue or select **Cancel** to terminate the Firmware Update procedure.



**Figure 31. MEA Device Administration Update Confirmation Window**

3. If the **OK** button is selected, the new Firmware is loaded into the device. The Firmware Update window will then be displayed to indicate that the selected file was successfully uploaded and to recommend that you reboot the device.
4. As the Firmware is being uploaded, a status page is displayed as shown in *Figure 32*.



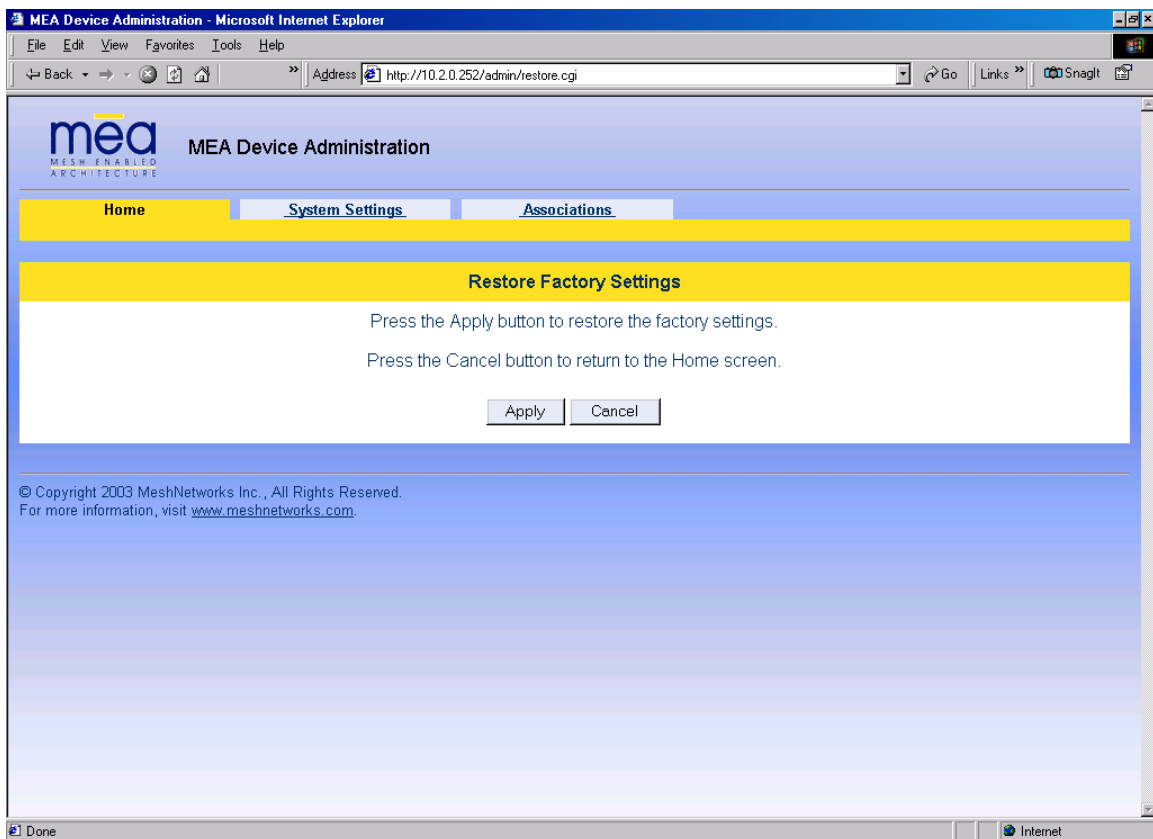
**Figure 32. MEA Device Administration Update Device Status Window**

- At the completion of the update, the IAP’s SBC must be reset for the update to take effect. Select the **Finished** button to navigate to the Reset Device window, and then click on the **Reset** button as described in the procedure located on page 47. The device will reset and return to the **Home** tab.

**Note:** Do not close the browser until the process is complete.

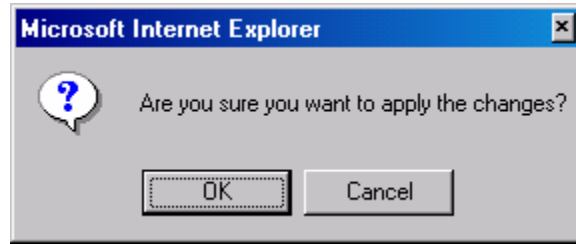
### Home Tab – Restore Factory Defaults

From the Home Tab, the user can select **Restore Factory Defaults** to restore the configuration settings to Factory Default settings. By selecting the **Restore Factory Defaults** button, the IAP setting will be returned to the default configuration. The user will receive a caution message before proceeding with the restore process as shown in *Figure 33*.



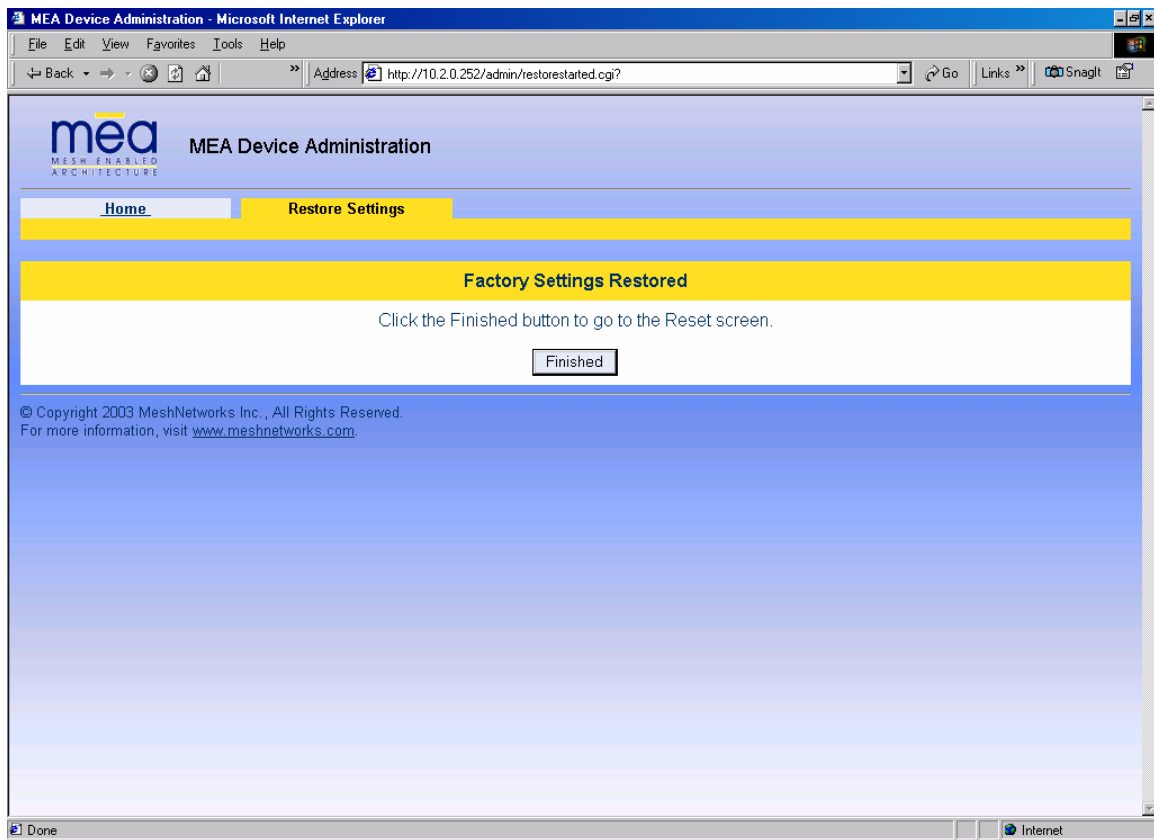
**Figure 33. MEA Device Administration Restore Factory Defaults Window**

- Click on the **Apply** button to continue the restore process or select the **Cancel** button to terminate the process without changing the device settings.
- If the **Apply** button is selected, a confirmation message is displayed as shown in *Figure 34* to confirm that you want to continue the Restore Factory Settings procedure.

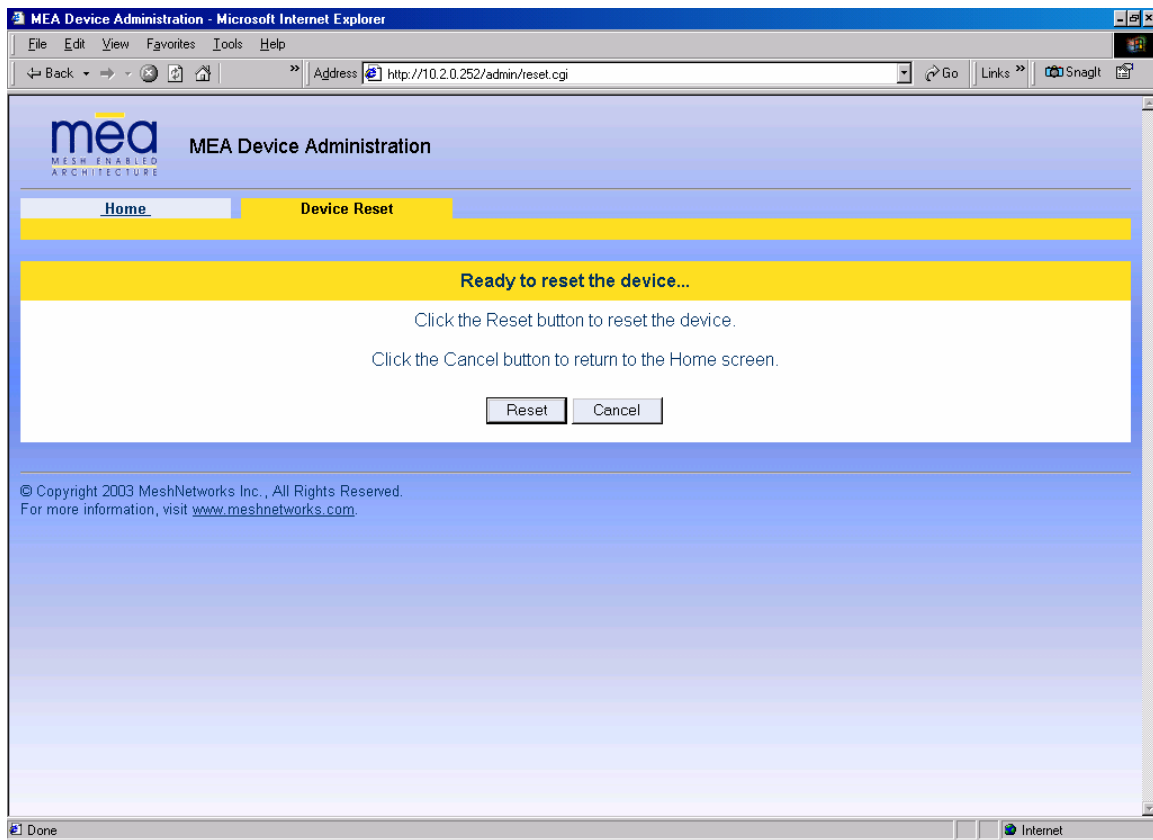


**Figure 34. Restore Factory Defaults Confirmation Message**

8. Click on the **OK** button to continue or select **Cancel** to terminate the procedure.



**Figure 35. MEA Device Administration Factory Settings Restored Window**



**Figure 36 MEA Device Administration Device Reset Window**

If the OK button is selected, the configuration settings will be restored and the device will reset automatically. Upon completion of the process, the browser will return automatically to the **Home** tab.

### **Home Tab – Reset Device**

From the Home tab, the user can select the **Reset the Device** option to reset the device and reinitialize the IAP. The configuration settings are preserved during the initialization process. The user will receive a caution message before proceeding with the reset.

1. Select the **Reset the Device** button to initiate the reset process on the IAP.
2. The Reset the Device window is displayed as shown in *Figure 37*. Select the **Reset** button to continue the process.

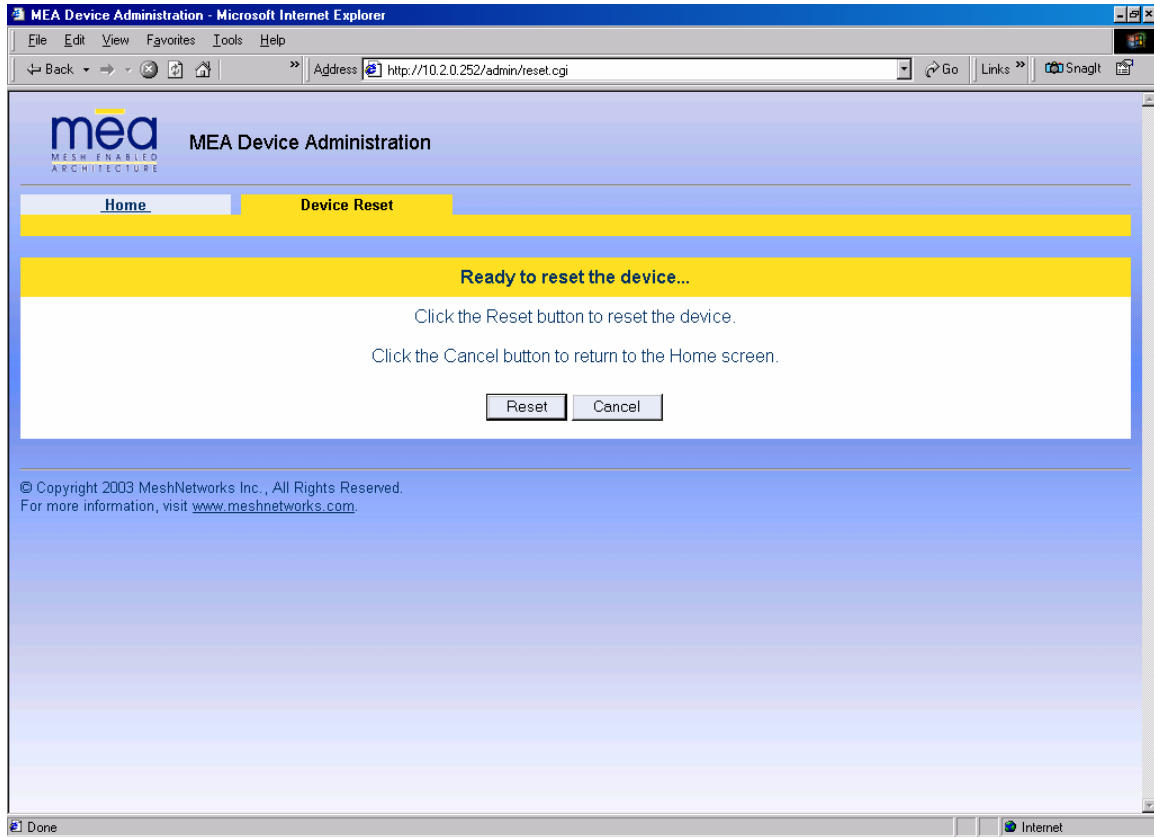
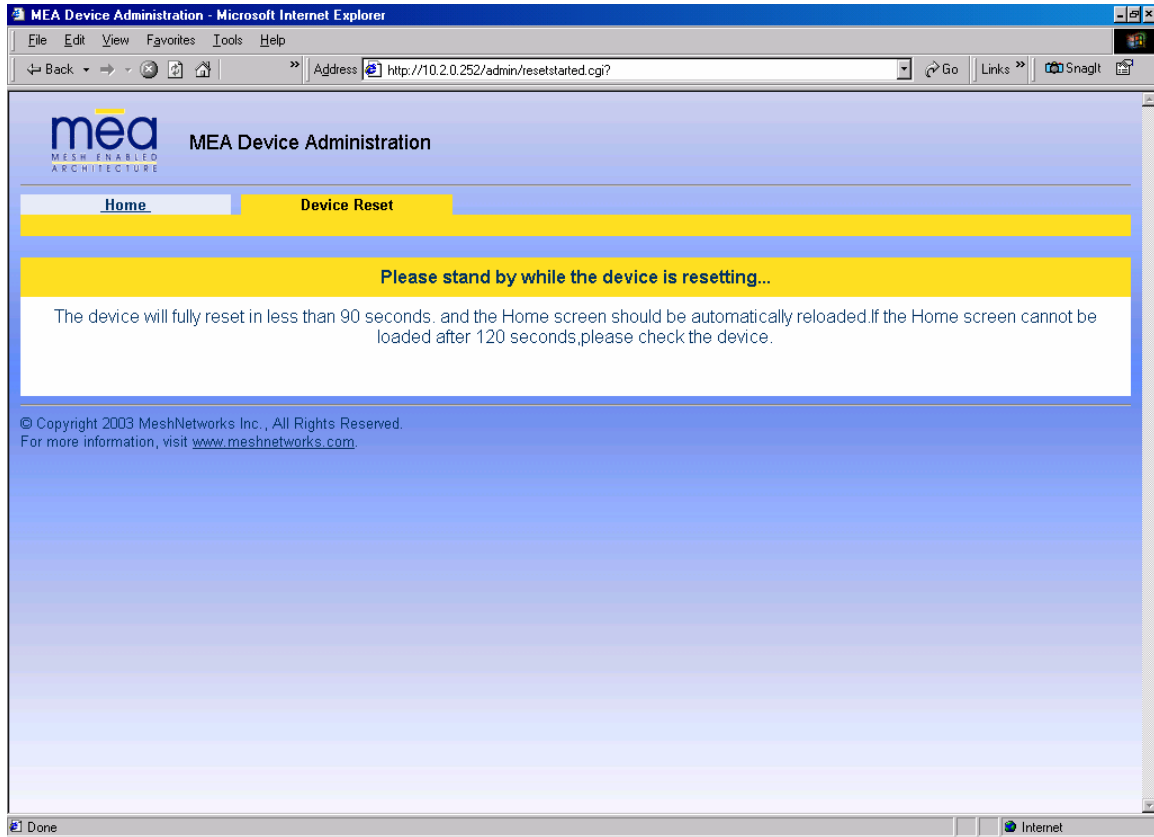


Figure 37. MEA Device Administration Device Reset Window

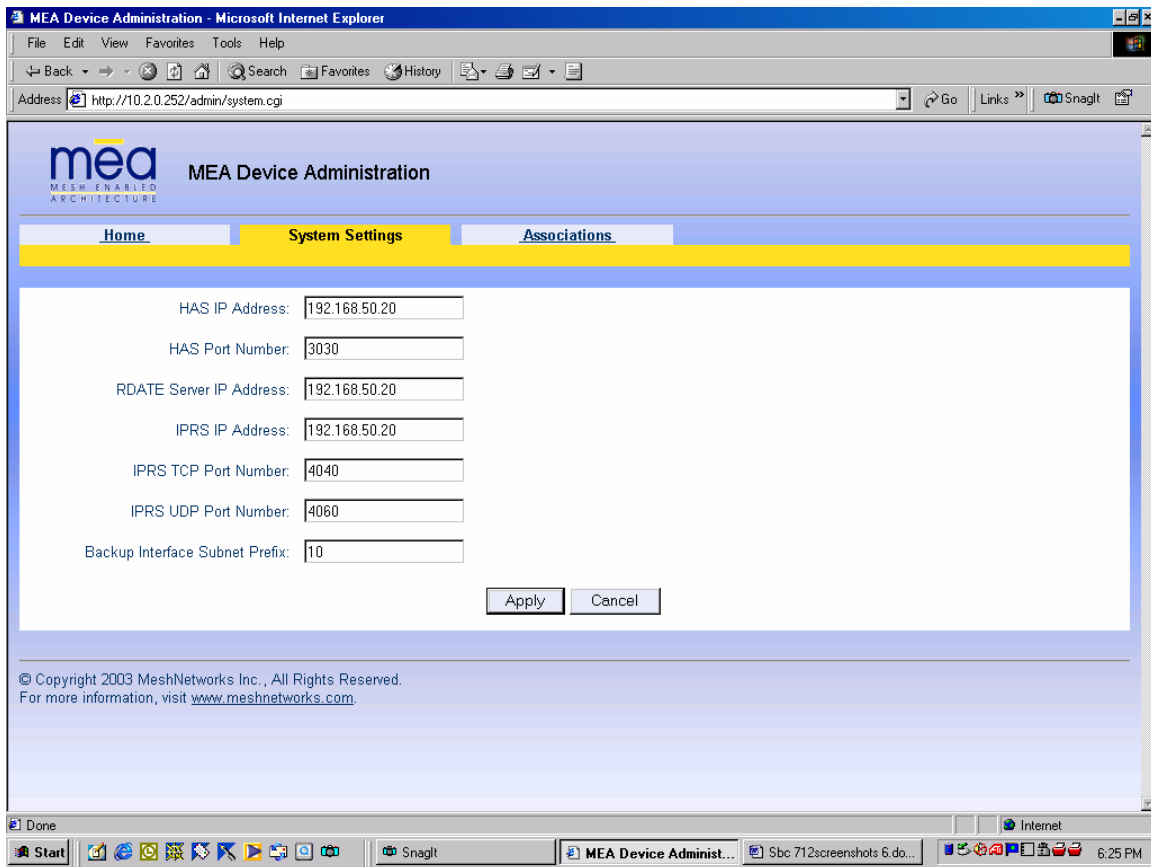
3. The Reset the Device window displays a message that describes the process and the time to completion as shown in *Figure 38*. The browser window will return to the **Home** tab at the completion of the reset.



**Figure 38. MEA Device Administration Device Reset Window (2)**

## System Settings Tab

The System Settings Tab is shown in *Figure 39*.



**Figure 39. MEA Device Administration System Settings Tab**

The System Settings tab allows the network operator to change the following values:

HAS IP Address – (Hardware Authentication Server) Network host from which authentication is requested.

HAS Port Number – Port number on the Network host from which authorization is requested (a value of zero causes the IAP to not request authentication).

RDATE Server IP Address – Network host from which time and date information is retrieved.

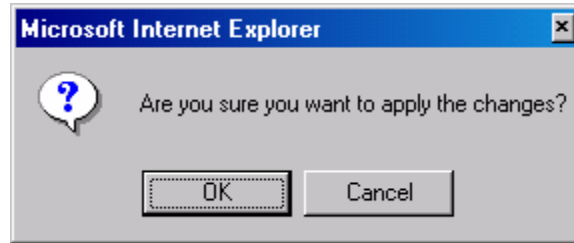
IPRS IP Address - (Internet Protocol Resolution Server) Network host that the IAP relays IP/MAC address information to

IPRS TCP Port - Port number on the Network host which the IAP relays IP/MAC address information

IPRS UDP Port - Port number on the Network host that the IAP responds to when asked for unknown address information

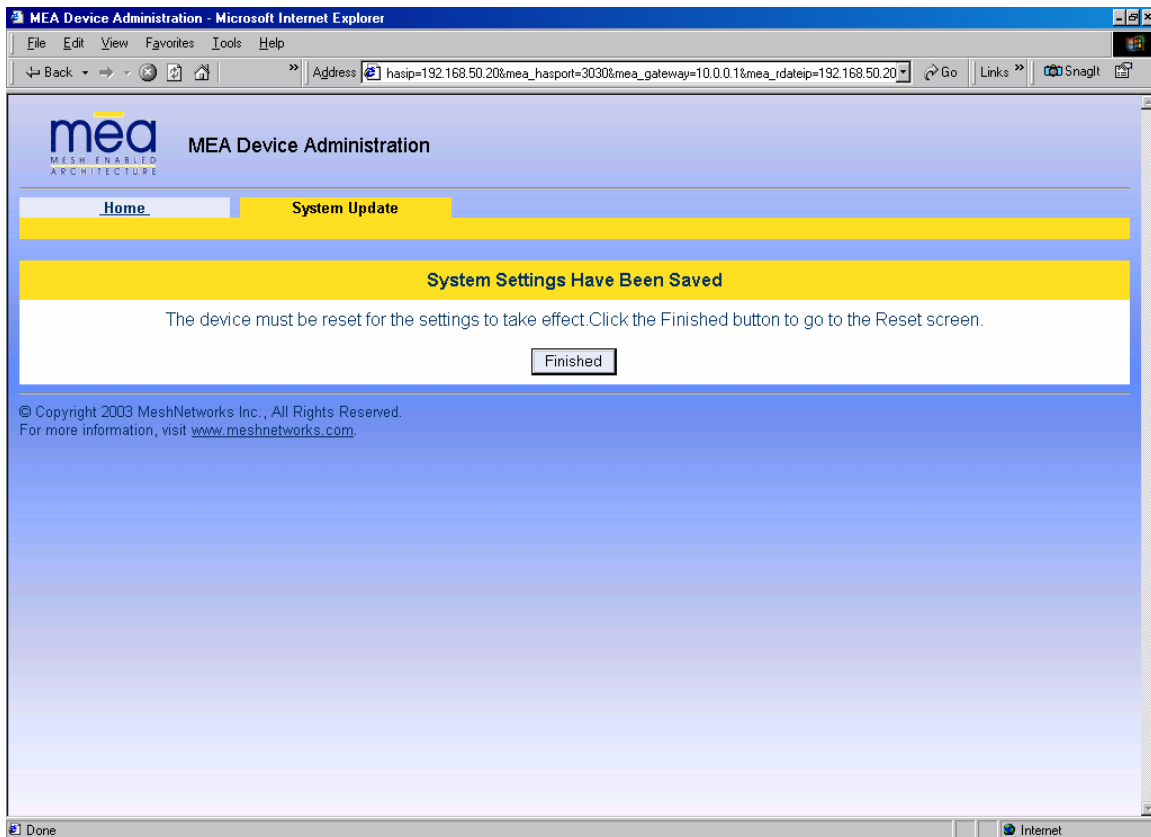
Backup Interface Subnet Prefix – Allows an alternate subnet prefix to be used for the IAPs in the event that the 10.x.x.x subnet is already in use.

Click the **Apply** button to save the changes, or click the **Cancel** button to delete any changes. If the **Apply** button is selected, a confirmation window will appear as in *Figure 40*. Click on the **OK** button to continue or select **Cancel** to terminate the procedure.



**Figure 40. System Settings Confirmation Message**

If the Apply button is selected, the new values will be saved and *Figure 41* will be displayed. The changes will not take effect until the device is reset. Select the **Finished** button to navigate to the Device Reset option.



**Figure 41. System Settings Saved Message**

## Associations Tab

The Associations Tab is an information only window as is shown in

Figure 42.

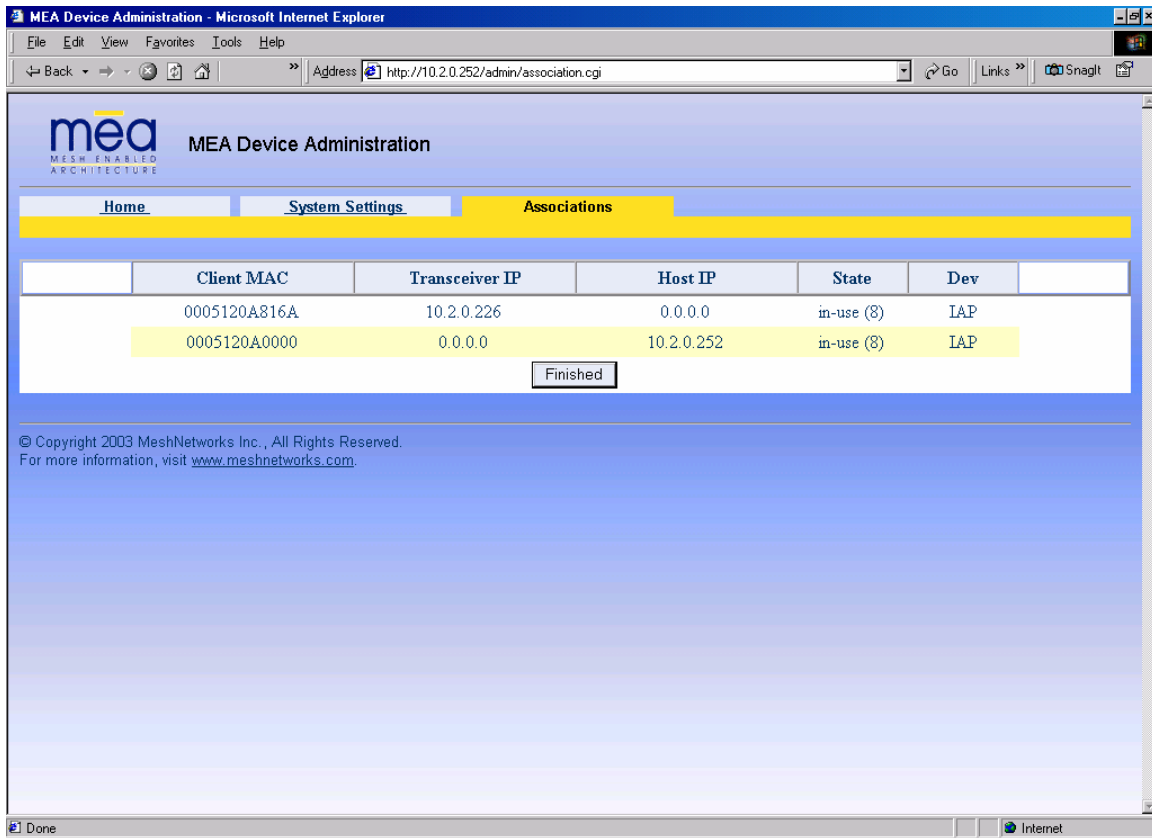


Figure 42. MEA Device Administration Associations Tab

This window displays all devices currently associated with an IAP. There will always be at least 2 entries: one for the IAP’s SBC and one for the IAP’s transceiver. For every wireless router and subscriber device currently associated with the IAP, there will be an additional entry in the table.

## Testing

### Basic MiSC Tests

To verify the basic connectivity of the MiSC, conduct the following from a computer connected to the server subnet of the MiSC:

- Ping an IAP
- Ping the Core Router
- Ping the Edge Router

### Wireless System Tests

There are two basic tests to verify correct operation the system. The first test is to perform ping tests to each device and the second test is to verify access the Internet.



## Ping Test

From Device Manager, complete the following to verify correct operation of the system:

1. Ping the SBC of the deployed IAPs
  - From the Device Manager drop down menu, select Preferences/Use SBC Address
  - For each IAP in the device tree, right click and select **Ping Device**
2. Ping the transceiver of the deployed IAPs
  - From the Device Manager drop down menu, select Preferences/Use Transceiver Address
  - For each IAP in the device tree, right click and select **Ping Device**
3. Ping the transceiver of the deployed WRs
  - From the Device Manager drop down menu, select Preferences/Use Transceiver Address
  - For each WR in the device tree, right click and select **Ping Device**
4. Ping the transceiver of each Subscriber Devices
  - From the Device Manager drop down menu, select Preferences/Use Transceiver Address
  - For each SD in the device tree, right click and select **Ping Device**

## Internet Test

If the MEA system has been configured to access the Internet, complete one of the two following tests to verify correct network setup:

1. From a provisioned SD, start the web browser and enter a URL such as <http://www.Motorola.com>.
2. From a SD, open a DOS/cmd window and ping an URL, e.g., **ping www.motorola.com**.

## Default Addresses and Logins

The following are the default values for the system components. These may be updated during installation.

Device	Description	Default
Core Router	login password	<b>g0ld10</b>
Core Router	enable password	<b>g0ld11</b>
Core Router	IP address on Sever	<b>172.31.0.2</b>
Core Router	Wireless subnet IP address for Core Router	<b>10.0.0.1</b>
Edge Router	login password	<b>g0ld10</b>
Edge Router	enable password	<b>g0ld11</b>
Edge Router	IP address on Server	<b>172.31.0.1</b>
Sun Blade	root password	<b>g0ld11</b>
Sun Blade	node name	<b>MeshManager</b>

<b>Device</b>	<b>Description</b>	<b>Default</b>
Sun Blade	IP address for next-level hierarchical DNS server	<b>(none)</b>
Sun Blade	IP address if Mesh VPN support is provided	<b>172.31.0.20</b>
Sun Blade	Secondary IP address for IAP rdate server	<b>192.168.50.20</b>
Sun Blade	Secondary IP address for IAP HAS server	<b>192.168.50.20</b>
Sun Blade	HAS port address	<b>3030</b>
Sun Blade	Secondary IP address for IAP syslog server	<b>172.18.0.50</b>
Sun Blade	Server subnet DHCP range	<b>172.31.1.1 to 172.31.1.254</b>
Sun Blade	Wireless subnet DHCP range	<b>10.2.0.1 to 10.2.0.254</b>
IAP	Default Gateway	<b>10.0.0.1</b>
IAP	IP address for rdate server	<b>192.168.50.20</b>
IAP	IP address for HAS server	<b>192.168.50.20</b>
IAP	IP address for syslog server	<b>172.18.0.50</b>
Subscriber Device	Default Gateway	<b>10.0.0.1</b>
Subscriber Device	DNS Server	<b>172.31.0.20</b>

## MAC Address Tables

This table has been included for recording the Ethernet MAC address and transceiver MAC address for a set of EWR devices as a quick reference. These addresses will be required for configuration and management of these devices.

### *IAP MAC Addresses*

<b>IAP MAC Address 00-05-12-0A-xx-yy</b>	<b>IAP ETH MAC Address 00-05-12-30-xx-yy</b>

### *WR MAC Addresses*

<b>WR MAC Address 00-05-12-0A-xx-yy</b>



## Site Selection/Deployment Guidelines

### General Site Selection Guidelines

The IAP location(s) should be selected first since they have the additional requirement of routing information back to the MiSC. This may be done via an Ethernet cable if the IAP and MiSC are located within 100 meters (the max length permitted for standard Ethernet) of each other. If the distance is greater than 100 meters, a mechanism for extending the Ethernet connection will be required, e.g., using fiber or T1.

Once the IAPs have been placed, then the location of the WRs can be determined. Optimally, the devices should be distributed such that a SD has no more than 3 hops to an IAP.

Power must be available for both IAPs and WRs. Both IAPs and WRs come standard with AC power; DC power is available as an option.

Lastly, any local building/structure codes must be adhered to, as well as proper permits for placing devices on structures that are not owned by the Network Operator (e.g., light poles).

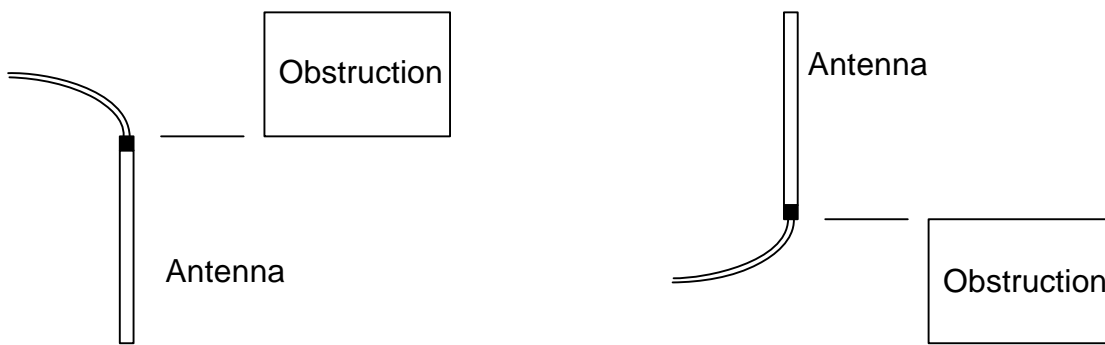
Motorola has developed the *Location Analyzer* tool to assist in the placement of infrastructure. This tool runs on a Windows 2000 SD. The tool collects and analyzes data, ultimately resulting in a deployment quality indication. Refer to the Location Analyzer documentation for information on configuring and using this tool.

### Antenna Guidelines

The location of fixed infrastructure antennas must address proper antenna orientation, selection of elevation pattern for the specific locale, the avoidance of pattern distortion, and the impact of obstructions and non-line-of-sight paths.

**Polarization** - Most of the antennas used in deployment will be vertically polarized. To maximize line-of-sight signal reception, both the transmitting and receiving antennas should be vertically oriented to avoid signal loss due to polarization mismatch. This applies to mobile and stationary antennas. For example, placing a magnetically mounted vehicle antenna on a curved portion of the vehicle roof so that its axis is not vertical risks a measure of signal loss at range, dependent upon the specific elevation pattern details, as discussed above.

**Local obstructions** - Antennas should be mounted either above or below the plane of obstructions as shown in *Figure 43*.



**Figure 43. Antenna Mounting**

Low gain rubber duck antennas that are mounted directly to Mesh transceivers are designed for transmitting and receiving vertically polarized radiation. Hence, care must be taken to insure close-to-vertical orientation of these antennas to avoid substantial signal loss due to polarization mismatch. Additionally, attenuation sustained by use of these antennas inside vehicles can be as high as 10 dB. Typically, losses are in the 4 to 7 dB range if the antenna is above the metal can of the vehicle so that radiation and reception occur at window level.

### **Lab Checkout**

Prior to deploying any equipment in the field, it is recommended to test the equipment in a lab environment to ensure the equipment is functioning.

#### Step 1 - Verify MiSC

First set up the MiSC as discussed in the [Procedures for Grounding Infrastructure Devices](#) section of this document. Attach a Windows computer to the switch. Verify that the following can be pinged: edge router, core router, MeshManager. Refer to the Default Addresses and Logins section for the addresses.

#### Step 2 – Verify IAPs.

Using an Ethernet cable, attach the IAPs, one at a time, to the switch. Using either the MAC or ETH address on the IAP box for reference, use MeshManager to verify that the IAP can be reached, and that it is obtaining an address from the DHCP server. Next, start an SD in infrastructure mode, and ensure that it also receives an IP address from the DHCP server. This verifies that both the SBC and the transceiver in the IAP are functioning.

#### Step 3 – Verify WRs

Connect an IAP as described in Step 2. Power up the WRs one at a time. Using the MAC address on the WR box for reference, verify that the MeshManager console can reach each WR, and that an appropriate IP address is displayed.

#### Step 4 – Verify PCMCIA cards

Connect an IAP as described in Step 2, Load a host computer with the WMC6300 drivers as described in Loading and Verifying WMC6300 Software. Insert a WMC6300 card into the host device. Start MeshTray. Verify that the status tab displays a valid IP address. Eject the WMC6300 card utilizing the *Unplug or Eject Hardware* icon. Insert another WMC6300 card and repeat the MeshTray test.

### **General Deployment Guidelines**

It is recommended that field deployment follow the same steps as described in the *Lab Checkout Procedures*. IAPs should be deployed first and verified as functional. Next the WRs should be deployed in a *near to far* pattern; in other words, WRs that are 1 hop from an IAP should be deployed first, followed by WRs that are 2 hops from an IAP, etc. This allows the functionality of each WR to be determined at the time of installation, thus eliminating any extra truck rolls to trouble-shoot a WR.



## 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 your regional Motorola support representatives

### USA

Motorola System Support Center (SSC) using the following contact information:

**Phone:** 800-221-7144

**Hours of Operation:** 7 days a week, 24 hours

### Europe

**Phone:** +44 (0)1793 564680

**Email:** [essc@motorola.com](mailto:essc@motorola.com)

**Hours of Operation:** Mon-Fri 09:00 - 17:00 GMT

Calls are logged 24 x 7, cases will be worked Mon-Fri 09:00 - 17:00 GMT

### Asia and Pacific Region

Remote Technical Help Desk (Channel Partners)

**Phone:** +63 28 92 79 93

**Email:** [wi4Tech@motorola.com](mailto:wi4Tech@motorola.com)

**Hours of Operation:** Mon - Fri 8 am - 6 pm

Sat 8 am - 12 noon

## ***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.

## **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)

## ***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

## **Radio Products and Services Division**

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



## 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

## 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.

## Returning FREs

Return faulty FREs 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 the assembly tightly and securely, preferably in its original shipping container

## Product 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.



## Regulatory Information

### ***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 IAP6300 (Intelligent Access Point) is an infrastructure device that is positioned at a fixed location such as a building rooftop. The IAP6300 requires professional installation to ensure that the installation is performed in accordance with FCC licensing regulations.

The MWR6300 (Wireless Router) is an infrastructure device positioned in a fixed location, such as on a pole, wall, or rooftop. The MWR6300 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.

### ***FCC RF Energy Exposure Statement***

1. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Although this device complies with the FCC RF Exposure limits in multiple configurations of the antenna, we suggest that the antenna be positioned away from the body when transmitting in order to minimize the level of RF Exposure.

### ***Regulatory and RF Safety Exposure***

Your Motorola Wireless Network Devices are designed and tested to comply with a number of national and international standards and guidelines (listed below) regarding human exposure to RF electromagnetic energy.

#### **This product complies with the following RF energy exposure standards and guidelines:**

- United States Federal Communications Commission, Code of Federal Regulations; 47CFR part 2 sub-part J
- American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers (IEEE) C95. 1-2005
- Institute of Electrical and Electronic Engineers (IEEE) C95.1-1999 Edition
- International Commission on Non-Ionizing Radiation Protection (ICNIRP) 1998
- Ministry of Health (Canada) Safety Code 6. Limits of Human Exposure to
- Radiofrequency Electromagnetic Fields in the Frequency Range from 3 kHz to 300 GHz, 1999
- Australian Communications Authority Radiocommunications (Electromagnetic Radiation – Human Exposure) Standard, 2003
- ANATEL ANNEX to Resolution No. 303 of July 2, 2002 "Regulation of limitation of exposure to electrical, magnetic and electromagnetic fields in the radio frequency range between 9 KHz and 300 GHz" and "Attachment to resolution # 303 from July 2, 2002"

#### **RF Exposure Compliance and Guidelines Operating Instructions**

To ensure compliance with the general population uncontrolled environment RF exposure limits in these standards, the antenna should be kept at a minimum separation distance of 20cm from all persons when used in a personal or laptop computer.

#### **ATTENTION**

**To ensure compliance with FCC requirements, use only Motorola approved, supplied antennas. Use of non-Motorola approved antennas may result in non-compliance with FCC regulations.**

**NOTE: The manufacturer is not responsible for any unauthorized modifications to this equipment. Unauthorized modifications could void user's authority to operate device.**