



mēa

**Enhanced Wireless
Router
User's Guide**

Version 3.0

Foreword

This document describes in detail the confidential and proprietary technology of MeshNetworks' MEA™ Architecture. MeshNetworks' products and technology are protected by US and international patent and patent pending technology. This document represents the current MEA design; the contents are subject to change at any time at the discretion of MeshNetworks, Inc.

MEA, MeshTray, and MeshNetworks' logo are trademarks or registered trademarks of MeshNetworks, Inc. All other product names and services identified throughout this publication are trademarks or registered trademarks of their respective companies. No such uses or the use of any trade name is intended to convey endorsement or other affiliation with this publication.

Copyright © 2003-2004 MeshNetworks, Inc. All Rights Reserved

Table of Contents

1 ENHANCED WIRELESS ROUTER..... 1

1.1 Introduction..... 1

1.2 What's in the Box 1

2 INSTALLATION REQUIREMENTS..... 1

2.1 Enhanced Wireless Router (EWR) 2

 2.1.1 Equipment 2

 2.1.2 Record MAC Address of the EWR6300 3

 2.1.3 EWR6300 Assembly..... 4

 2.1.4 Deployment 4

 2.1.5 Deployment Tips..... 5

 2.1.6 Initial Configuration..... 5

 2.1.7 Testing..... 5

3 INSTALLING THE MEA ENHANCED WIRELESS ROUTER 7

3.1 Device Administration: Configuring the EWR Devices..... 7

 3.1.1 Accessing the MEA Device Administration Web Pages 7

 3.1.2 Configuring the Device 11

 3.1.2.1 Device Addressing..... 12

 3.1.2.2 Network DHCP Scheme 12

 3.1.2.3 Statically Provisioned Scheme 13

 3.1.2.4 User Supplied Scheme 13

 3.1.2.5 Setting the User Supplied IP Address 14

 3.1.3 Resetting the EWR 16

 3.1.4 Restoring Factory Settings – User Supplied Mode Limitations 18

 3.1.4.1 EWR Reset-to-Default Recovery In User-Supplied Mode 18

 3.1.4.2 Reset the Device Addressing Mode Using DeviceManager 18

 3.1.4.3 Reset the Device Addressing Mode via the Configuration Web Page..... 18

MeshNetworks

3.1.4.4	Reset the User-Supplied Parameters via the Configuration Web Page	18
3.1.5	Restoring Factory Defaults – Normal Operations	19
3.1.6	Changing the Web Password	21
3.1.7	Upgrading the Device Firmware	23
3.2	External Device Provisioning	25
3.2.1	Connecting to the Ethernet Port	26
3.3	Infrastructure Requirements	26
3.4	EWR6300 Mounting Bracket	27
3.4.1	EWR MAC Addresses	29
4	LICENSE AND WARRANTY INFORMATION	30
4.1	Important Information	30
5	FCC REGULATORY INFORMATION	32
5.1	FCC Information	32
5.2	FCC RF Radiation Exposure Statement	32
6	SAFETY INFORMATION FOR THE MEA PRODUCTS	33
7	SAFETY CERTIFICATION	33
7.1	CE Mark Certification	33

List of Figures

Figure 2-1.	EWR6300 Identification Label	3
Figure 2-2.	EWR6300 External Connection Points	4
Figure 2-3	Typical EWR Deployment	5
Figure 3-1.	Enter Network Password Initial Web Page Authentication Dialog	8
Figure 3-2.	MEA Device Administration Redirecting Web Page.....	9
Figure 3-3.	MEA Device Administration Home Page (Super User Login).....	10
Figure 3-4.	EWR Device Administration Configuration Page (Super User Login).....	11
Figure 3-5.	Configuration Change Verification	14
Figure 3-6.	System Update Save Completed Web Page	15
Figure 3-7.	Device Reset Prompt Web Page	16
Figure 3-8.	Device Reset in Progress Web Page	17
Figure 3-9.	Restore Factory Settings Web Page.....	19
Figure 3-10.	Confirm Changes Window for Restore Factory Settings	20
Figure 3-11.	Factory Settings Restored Web Page.....	20
Figure 3-12.	Enter New Password Web Page.....	21
Figure 3-13.	Confirm Changes Window for Enter New Password	22
Figure 3-14.	Password Changed Confirmation Web Page.....	22
Figure 3-15.	Update Device Firmware Web Page.....	23
Figure 3-16.	Confirm Upload Window for Firmware Update	24
Figure 3-17.	Firmware Upload Progress Web Page.....	24
Figure 3-18.	External Device Provisioning Table.....	25
Figure 3-19.	EWR6300 Mounting Bracket.....	27
Figure 3-20.	C-Clamp Bracket Assembly.....	28
Figure 3-21.	EWR Pivot and Angle Locking Bolts	29

1 Enhanced Wireless Router

1.1 Introduction

Thank you for purchasing the MEA Enhanced Wireless Router (EWR). MEA is a wireless communication system capable of supporting high data rate mobile communication at variable rates of vehicular speeds.

The Enhanced Wireless Router (EWR™) is designed to be deployed outdoors for wireless coverage in large geographic areas to wireless network access to one or more IP devices via its built-in RJ45 Ethernet port. The EWR efficiently combines the functionality of a Meshnetworks Wireless Router and client modem in to a single cost-effective wireless network component. This makes it easy for any Ethernet ready device to access a Mesh Enabled Architecture (MEA™) mobile broadband network. IP-enabled computers, video cameras, sensors, signs, signals, etc. can all be Mesh-Enabled to send and receive data at burst rates of up to 6 Mbps. All standard Wireless Router functionality including Multi-Hopping™, near line of sight communications and geo-location services are fully supported.

The MEA Enhanced Wireless Router is configured for the connection of multiple IP addressable devices using standard Ethernet connectivity. This allows devices that cannot accept the PCMCIA based WMC3600 product to function transparently on a MEA network without drivers.

This document provides detailed installation and configuration instructions for installing the MEA EWR.

1.2 What's in the Box

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

- MEA Enhanced Wireless Router
- High Gain Antenna
- Power Cord

2 Installation Requirements

NOTE: All Intelligent Access Points (IAPs) on the MEA network require a software upgrade to support EWR Devices.

The EWR will require the following in a typical installation:

- Power Cord
- 110/220 volts AC Power along with appropriate power connection cable
- A Hub or Switch (Use of a X-Over cable is not recommended at this time)
- Antenna and RF cabling appropriate for use in the 2.4 GHz band

2.1 Enhanced Wireless Router (EWR)

The MEA Enhanced Wireless Router 6300 (EWR6300) is an infrastructure device positioned in a fixed location, such as on a pole, wall, or rooftop. The EWR6300 requires professional installation to ensure the installation is performed in accordance with FCC licensing regulations.

The EWR6300 provides range extension, a means to route around obstructions, a fixed location reference for use in Geo-Location, and the capability of enabling IP devices.

The EWR6300 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 EWR must be provided.

2.1.1 Equipment

The following list defines the standard MEA hardware components needed to set up a EWR:

- EWR Box with N-type Antenna Connector
- 120V A/C 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 (120V A/C or 5 V D/C depending on EWR configuration)
- Hand tools for bracket installation (7/16" wrench (2), Phillips screwdriver)

Optional Equipment:

- DC powered EWR (EWR6300-DC-IN)
- Power cord to connect to a photoelectric cell

Optional FCC Approved Antennas:

Manufacturer	Part Number	Gain	Usage
Maxrad	MFB24008	8 dBi	Infrastructure
Maxrad	MFB24004	4 dBi	Infrastructure
Hyperlink	HG2409U	8 dBi	Infrastructure

2.1.2 Record MAC Address of the EWR6300

The transceiver Media Access Control (MAC) address is recorded on the label located on the antenna end of the EWR6300 and the Ethernet MAC address is recorded on the label located on the antenna end of the EWR6300 as show in [Figure 2-1](#).

Record the MAC Address and ETH MAC Address in the tables in [Section 3.4.1](#), because it will be required later to configure and test the device.



Figure 2-1. EWR6300 Identification Label

2.1.3 EWR6300 Assembly

[Figure 2-2](#) shows the external connection points on a EWR6300 box.

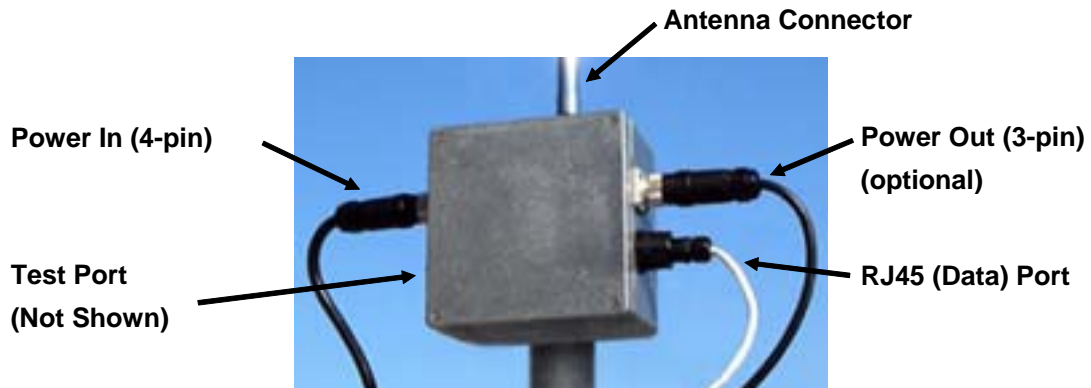


Figure 2-2. EWR6300 External Connection Points

Assemble the EWR using the following procedure:

1. If desired, mount the EWR box using the enclosed bracket. Refer to the [EWR6300 Mounting Bracket](#) section.
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.
4. Verify the MAC address and Ethernet (ETH) address has been recorded in [Section 3.4.1](#). Both addresses will be required to configure and test the device.
5. The Test Port is unused during deployment.

2.1.4 Deployment

The EWR6300 can be mounted on a pole by using the bracket provided.

NOTE: When deploying the EWR6300, the antenna should be a minimum of 30 inches from any nearby metal poles to avoid distortion of the RF pattern.

The antenna must have a separation distance of at least 2 meters from the body of all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Users and installers must be provided with antenna installation and transmitter operating conditions to satisfy RF exposure compliance.

Typically, enhanced wireless routers are distributed within a network to extend the range, guarantee coverage, and *mesh enable* an Ethernet Internet Protocol (IP) device. A rule of thumb is to deploy 2-3 hop networks to optimize range, latency, and throughput.

The EWR6300 installation location must provide applicable AC or DC power for the device.

It is the responsibility of the Network Operator to ensure that the installation complies with any local building codes and permits.



Figure 2-3 Typical EWR Deployment

2.1.5 Deployment Tips

Locate the antenna to minimize multipath:

- Minimize interference from nearby transmitters
- Maximize chance of a direct line of sight connection to other devices
- The antenna supplied is designed to be mounted vertically

The devices are designed to be vertically mounted with the antenna port at the top or the bottom. The antenna is specified around deployment heights of 3-30 meters. Remotely locating the antenna will degrade the performance through cable loss, though this may be mitigated by better antenna positioning.

2.1.6 Initial Configuration

The configuration process for Geo-Location is the same as the setup for the IAP as described in the **mea Setup and Deployment User's Guide for Infrastructure Mode** User's Guide.

2.1.7 Testing

Verify the operation of the EWR6300 using the following procedure:

1. Apply power to the EWR6300.
2. Obtain the transceiver MAC address and ETH address that was recorded in [Section 3.4.1](#). The address will be in the form of 00-05-12-0A-xx-yy.
3. From the MeshManager user interface, display devices using the MAC address.
4. Select the appropriate EWR in the device tree, right click and select *ping* to test communications with the device.

MeshNetworks

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

NOTE: If you are running an EWR as a standalone device, the configuration web page can be reached by connecting a PC to the wired interface.

3 Installing the MEA Enhanced Wireless Router

3.1 *Device Administration: Configuring the EWR Devices*

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

The EWR serves as a default gateway for the attached IP devices. Because some devices expect the default gateway to reside on the local subnet, the address that the EWR uses for gateway service (on the wired interface) must be configurable. Some consideration should be used in selecting a gateway address for the EWR.

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

When selecting IP addresses for the EWR, care must be taken to ensure that the selected IP addresses do not conflict with any other devices on the mea network.

3.1.1 Accessing the MEA Device Administration Web Pages

To modify the IP configuration for the EWR using the web interface, you must know the IP address assigned to the wireless interface of the EWR. The IP address can be determined from MeshManager, or from the DHCP server (once the device is configured for DHCP). The default IP address for the EWR wireless interface is derived from the transceiver MAC address (10.xx.yy.1, where the MAC address is 00:05:12:0A:XX:YY), similar to the default IP addresses described in [Section 3.2](#).

Once the IP address is known, you can access the web page of the device. Point your web browser to the IP address of the EWR. In the examples following, the EWR address is 172.16.1.53, and the web page would be found at <http://172.16.1.53/>.

MeshNetworks

Once the web browser is directed to the web page of the EWR, you will be prompted for a username and password. A dialog box similar to the following should show up if you are using Internet Explorer:

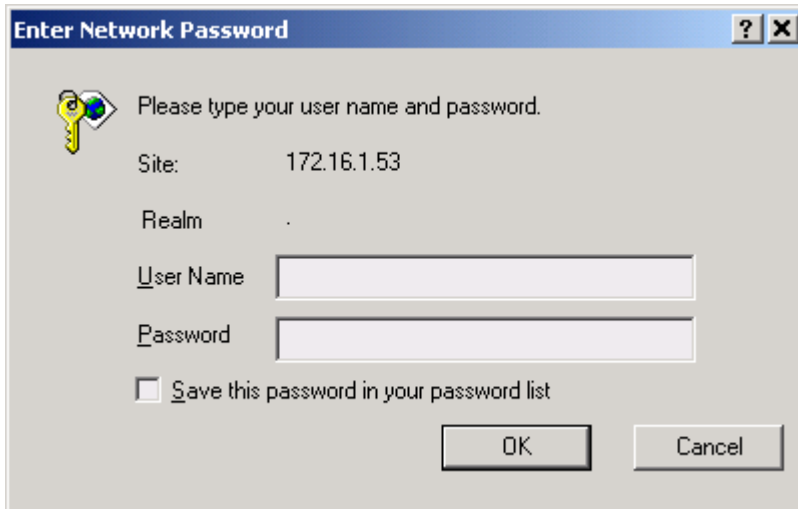


Figure 3-1. Enter Network Password Initial Web Page Authentication Dialog

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

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

The device has two accounts for the web pages - an administrative account (username:*admin*, default password:*admin*), and an access account (username: *monitor*, default password: *monitor*). The administrative account must be used for provisioning the device, and the access account may be used for monitoring the status of the device.

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

The administrator has the ability to change the password for the access account.

NOTE: If you are running an EWR as a standalone device, the configuration web page can be reached by connecting a PC to the wired interface.

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

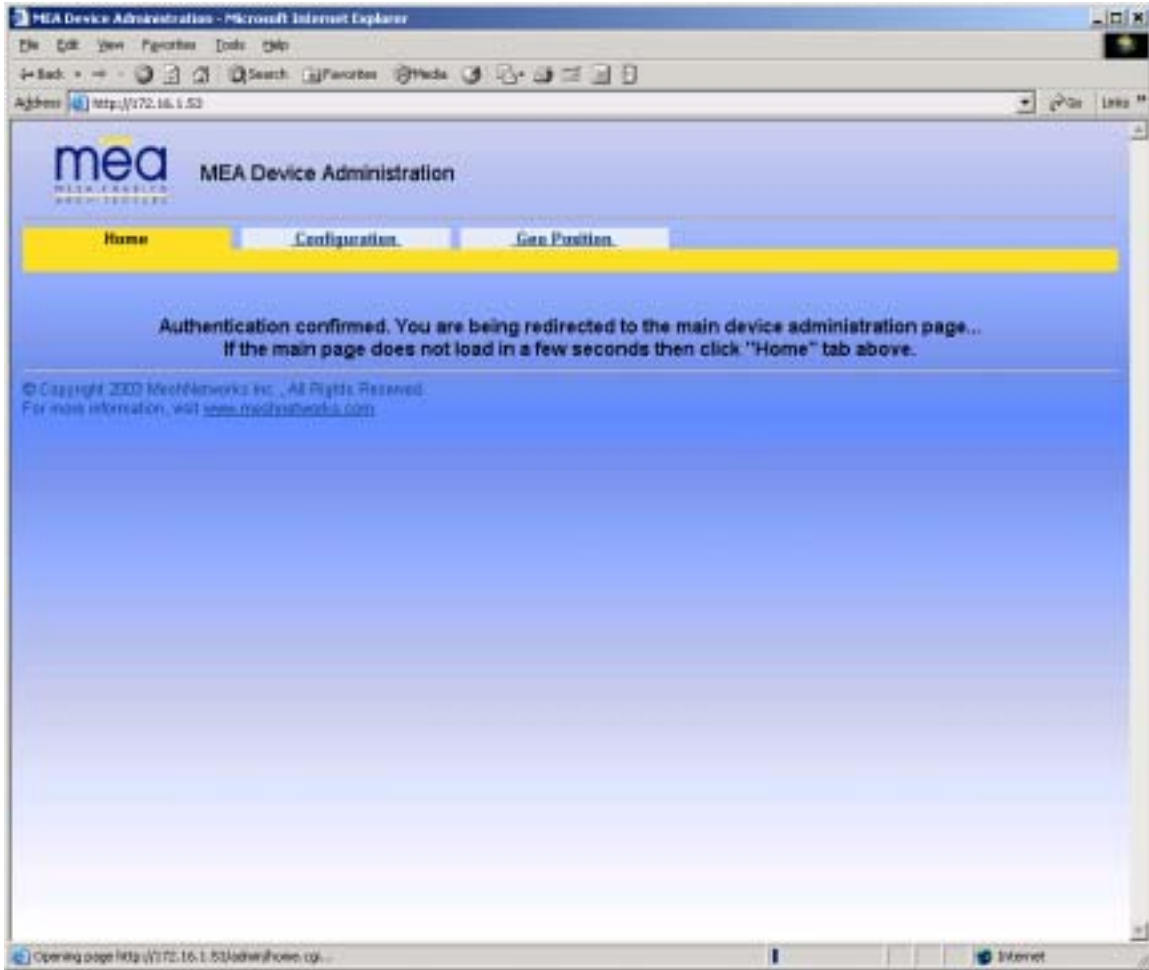


Figure 3-2. MEA Device Administration Redirecting Web Page

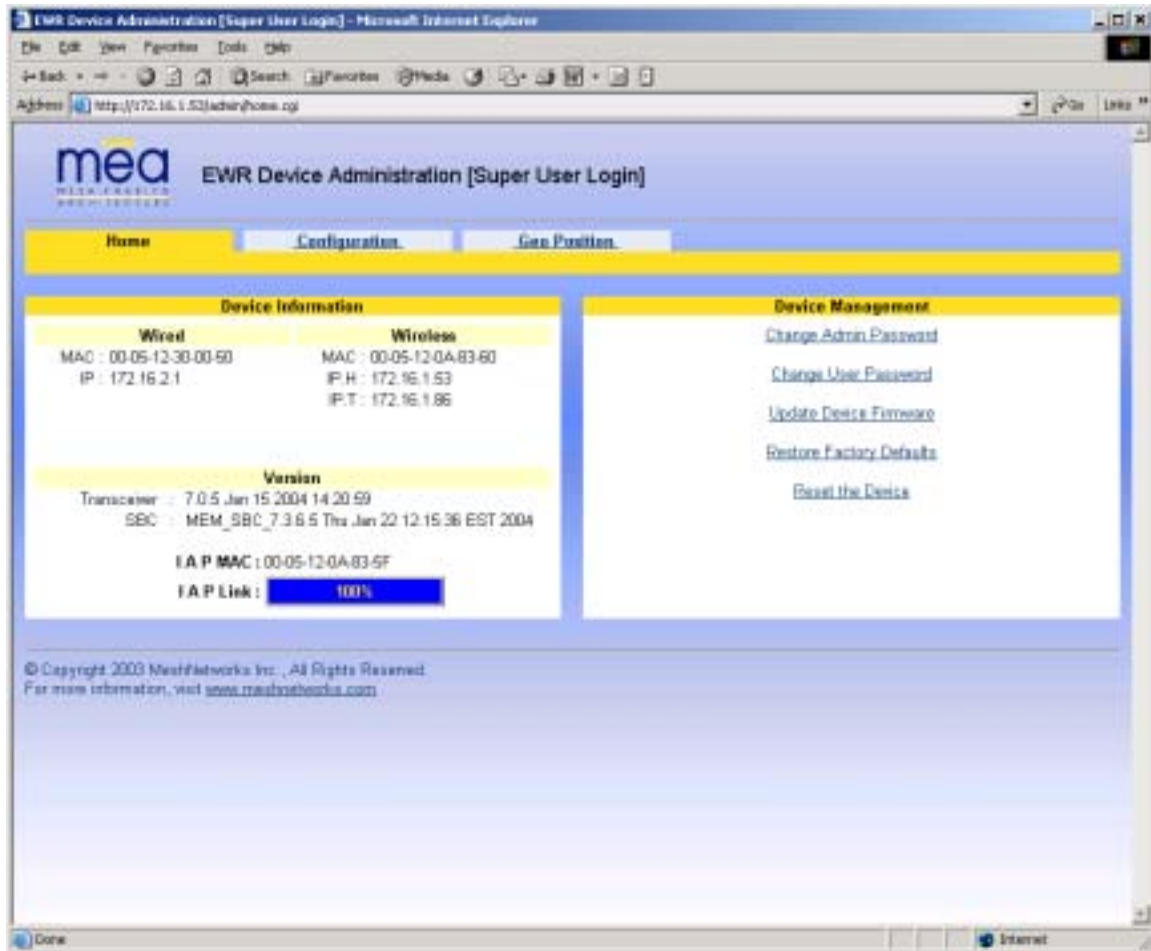


Figure 3-3. MEA Device Administration Home Page (Super User Login)

The MEA Device Administration home page provides you with some basic information about the device, including the IP addresses assigned to the device, the MAC addresses of the device, the firmware revision number, and the reported link quality for the link to the IAP. In addition, links are provided to web pages for device configuration, password management, firmware upgrades, device reset, and restoring the factory default configuration.

3.1.2 Configuring the Device

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

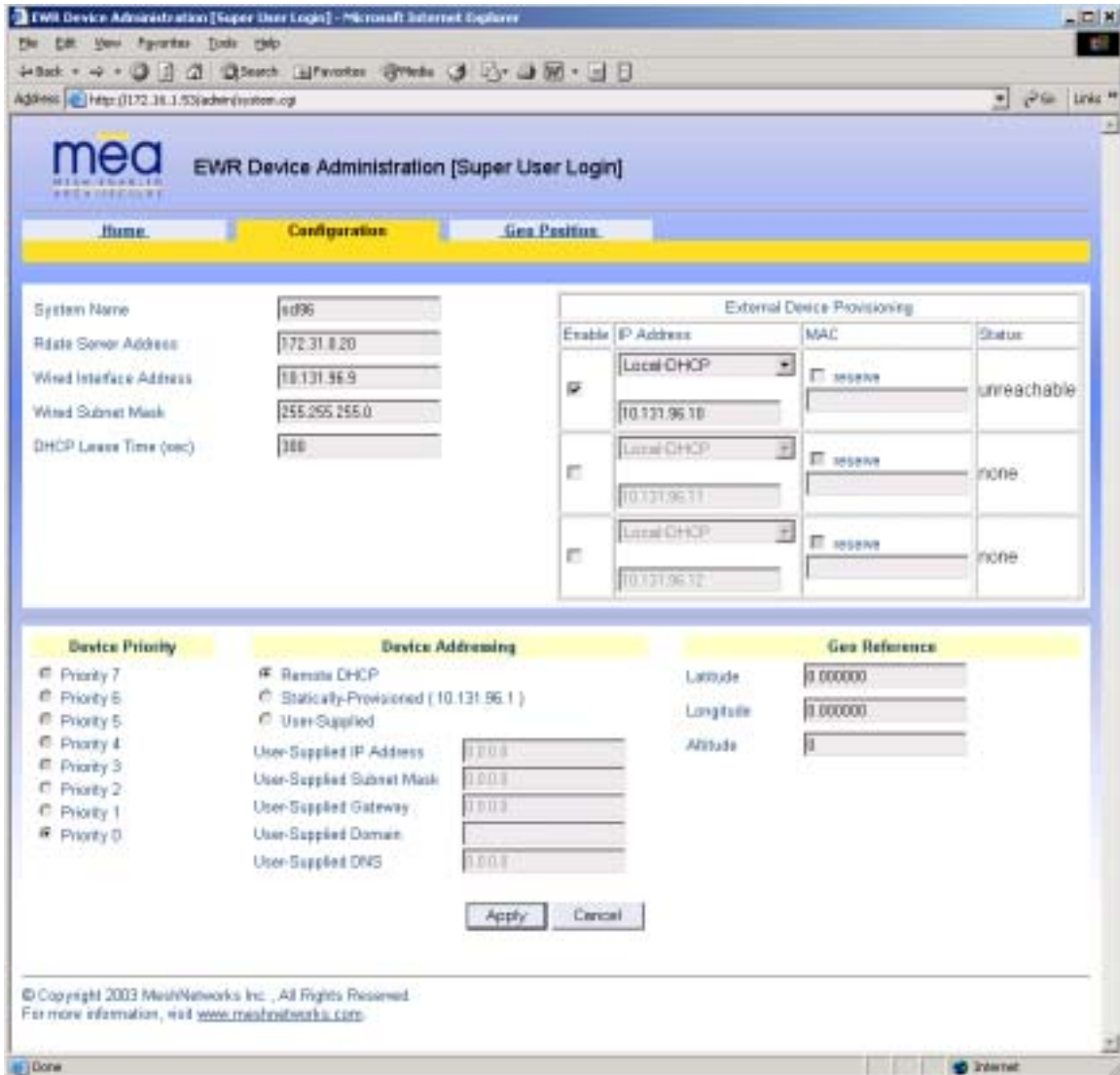


Figure 3-4. EWR Device Administration Configuration Page (Super User Login)

The *EWR Device Administration (Super User Login)* page will allow you to change the configuration of the EWR. The fields displayed on this page are described below.

Field Name	Field Description	Field Default Value
System Name	This is the name of the device as shown by MeshManager	

MeshNetworks

Field Name	Field Description	Field Default Value
	MeshManager	
RDATE Server IP Address	The IP address of the RDATE server. This is usually the MiSC when operating in infrastructure mode. The RDATE server provides the current date to the EWR. The EWR can operate without an RDATE server.	172.31.0.20
Wired Interface Address	The EWR will tell the attached Ethernet devices to use this address for the default gateway, and the EWR will use the address when accessing the local Ethernet segment.	MAC-derived
Wired Interface Subnet Mask	This is the subnet mask for the local Ethernet segment.	255.255.0.0
DHCP Lease Time	This is the duration (in seconds) of the DHCP leases that the EWR offers to the attached Ethernet devices.	300
Device Priority	The <i>Device Priority</i> provisioning area allows the operator to set the priority assigned to wireless messages transmitted by this device.	
Geo Reference	The <i>Geo Reference</i> area allows the operator to provision the exact location of the EWR so that it can serve as a geographical reference for the mea network. Enter the <i>Latitude</i> and <i>Longitude</i> in degrees and the <i>Altitude</i> in feet.	

The *External Device Provisioning* frame of this web page is described in [Section 3.2](#).

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

3.1.2.1 Device Addressing

With mea Release 3.0, the concept of modes has been replaced by a Unified Modes of operation addressing scheme. The concept of unified modes of operation centers on the current state of network communication: Associated State and Unassociated State. There are three addressing schemes which allow the IT manager increased flexibility in deployment.

3.1.2.2 Network DHCP Scheme

Operation under the Network DHCP scheme is similar to that of Release 2 in Infrastructure Mode. The primary difference is that loss of infrastructure does not force loss of connectivity.

Network DHCP requires that the EWR device be configured to request an address from a DHCP server and the inclusion of a DHCP server in the core network configuration to answer these requests. With Network DHCP selected, the EWR will send DHCP requests for its own address to the core network once it becomes associated and establishes communications with the infrastructure.

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

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

3.1.2.3 Statically Provisioned Scheme

Operation under the Statically Provisioned scheme is similar to that of Release 2 in Peer-to-Peer Mode. The primary difference is that addresses are configured by the network operator rather than hashed from the MAC address. This serves to eliminate the 10.x.x.x limitation on the network range.

When operating under the Statically Provisioned scheme, the EWR device will use provisioned DHCP-like information to establish an IP address for use in the wireless network.

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

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

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

3.1.2.4 User Supplied Scheme

Operating under the *User Supplied* scheme, the EWR 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.

3.1.2.5 Setting the User Supplied IP Address

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

Note that this configures the user-supplied address for the EWR device. To configure addresses for ethernet clients, please refer to the description of the *External Device Provisioning* frame of this web page in [Section 3.2](#).

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

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

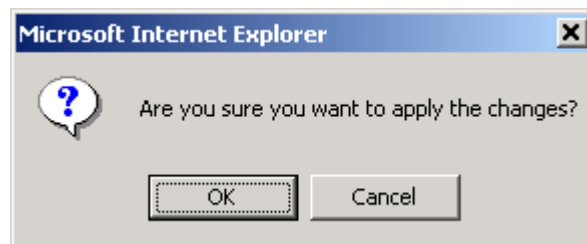


Figure 3-5. Configuration Change Verification

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

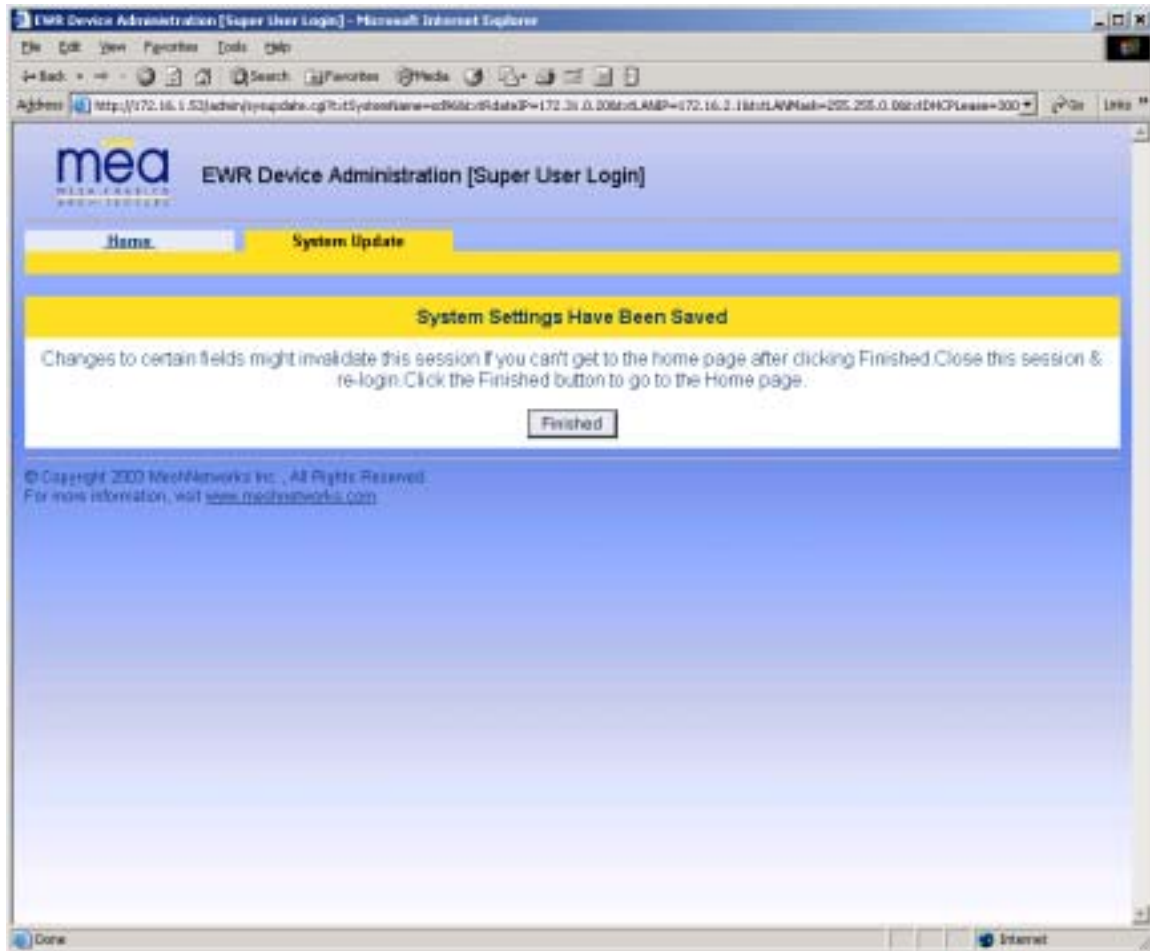


Figure 3-6. System Update Save Completed Web Page

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

3.1.3 Resetting the EWR

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

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

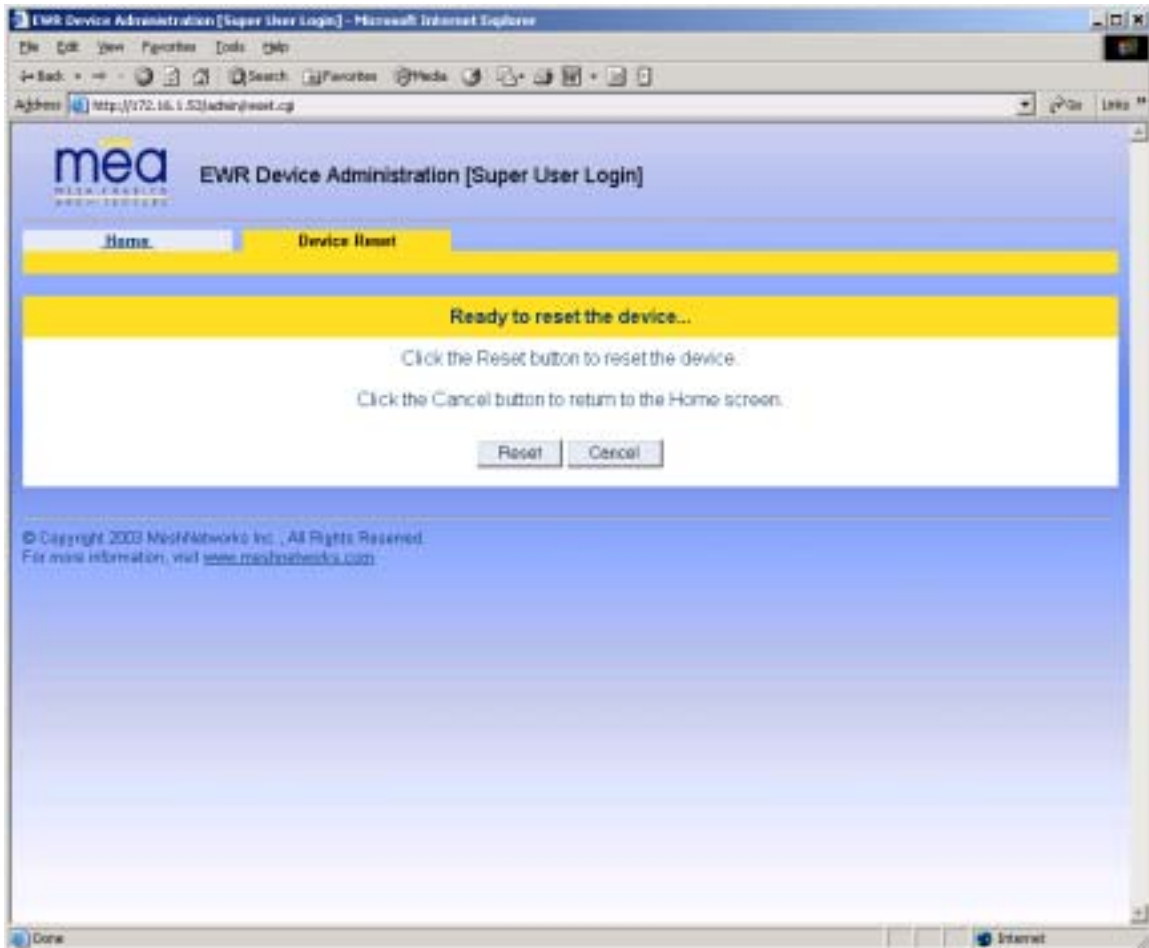


Figure 3-7. Device Reset Prompt Web Page

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

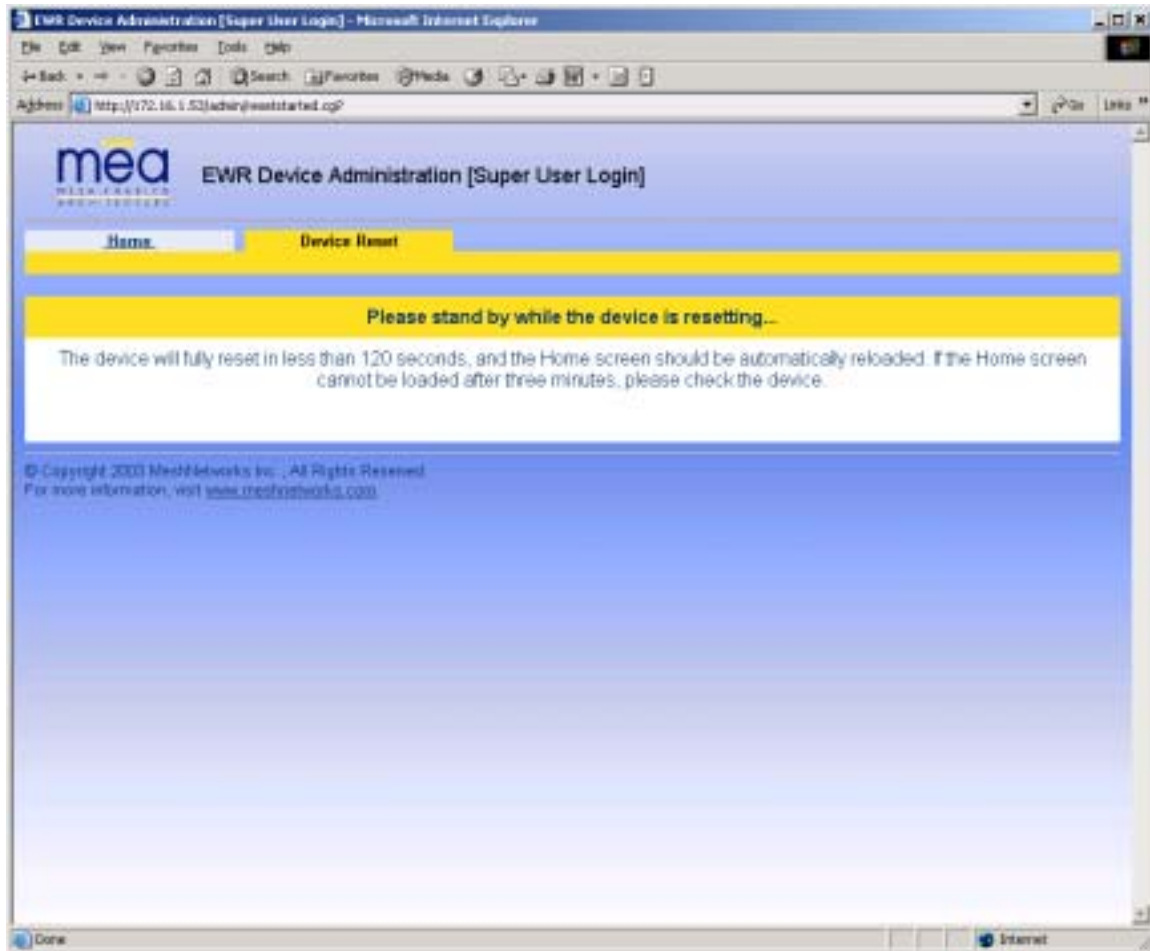


Figure 3-8. Device Reset in Progress Web Page

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

3.1.4 Restoring Factory Settings – User Supplied Mode Limitations

NOTE: In Release 3.0, there is a known issue that arises if the selected device addressing mode is *User-Supplied* when the user restores the factory default settings for the EWR. The following options are offered as a way to recover from this limitation.

3.1.4.1 *EWR Reset-to-Default Recovery In User-Supplied Mode*

The factory default settings for the *User-Supplied* parameters cannot be routed (i.e. 0.0.0.0). *When the non-routable values are applied, the network connection between the attached ethernet devices and the core network becomes disabled.*

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

3.1.4.2 *Reset the Device Addressing Mode Using DeviceManager*

DeviceManager will be able to manage some but not all of the device parameters at this time. The network operator may change the selected device addressing mode via DeviceManager to either *Remote-DHCP* or *Statically-Provisioned*.

3.1.4.3 *Reset the Device Addressing Mode via the Configuration Web Page*

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

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

3.1.4.4 *Reset the User-Supplied Parameters via the Configuration Web Page*

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

3.1.5 Restoring Factory Defaults – Normal Operations

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

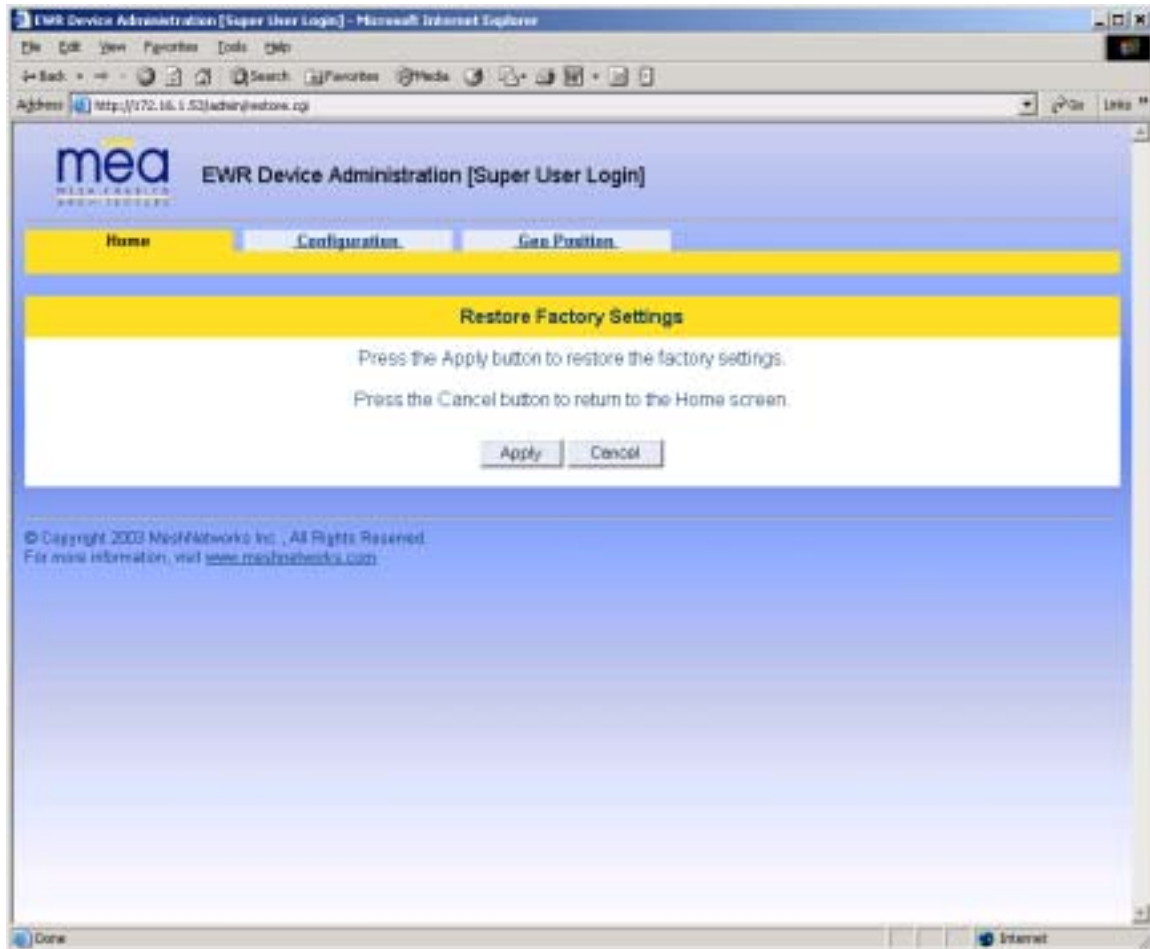


Figure 3-9. Restore Factory Settings Web Page

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

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

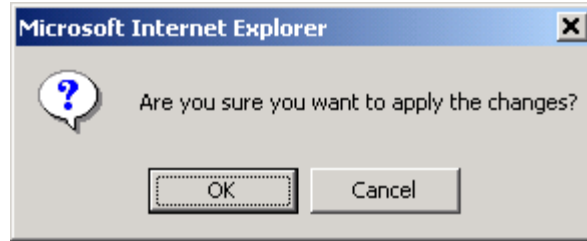


Figure 3-10. Confirm Changes Window for Restore Factory Settings

The *Factory Settings Restored* page will be displayed.

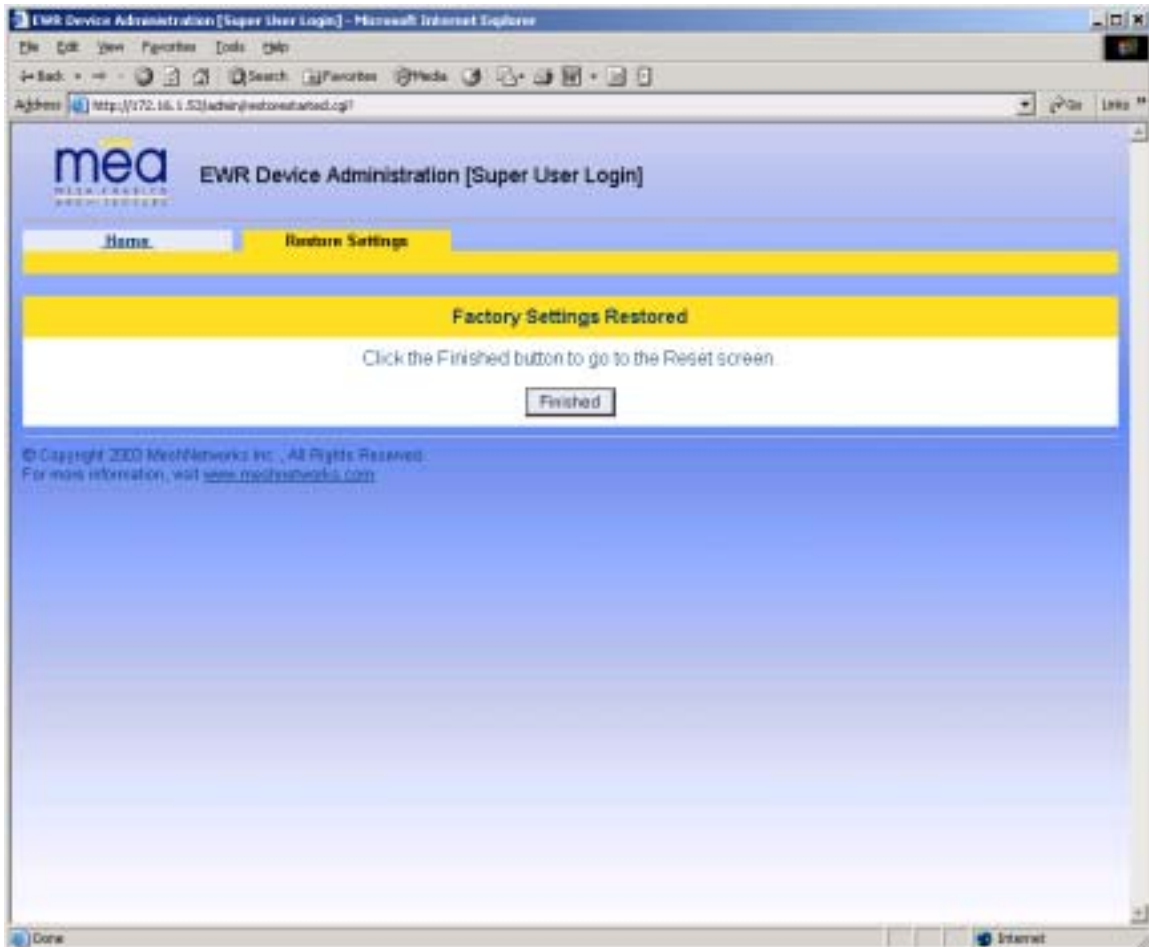


Figure 3-11. Factory Settings Restored Web Page

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

3.1.6 Changing the Web Password

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

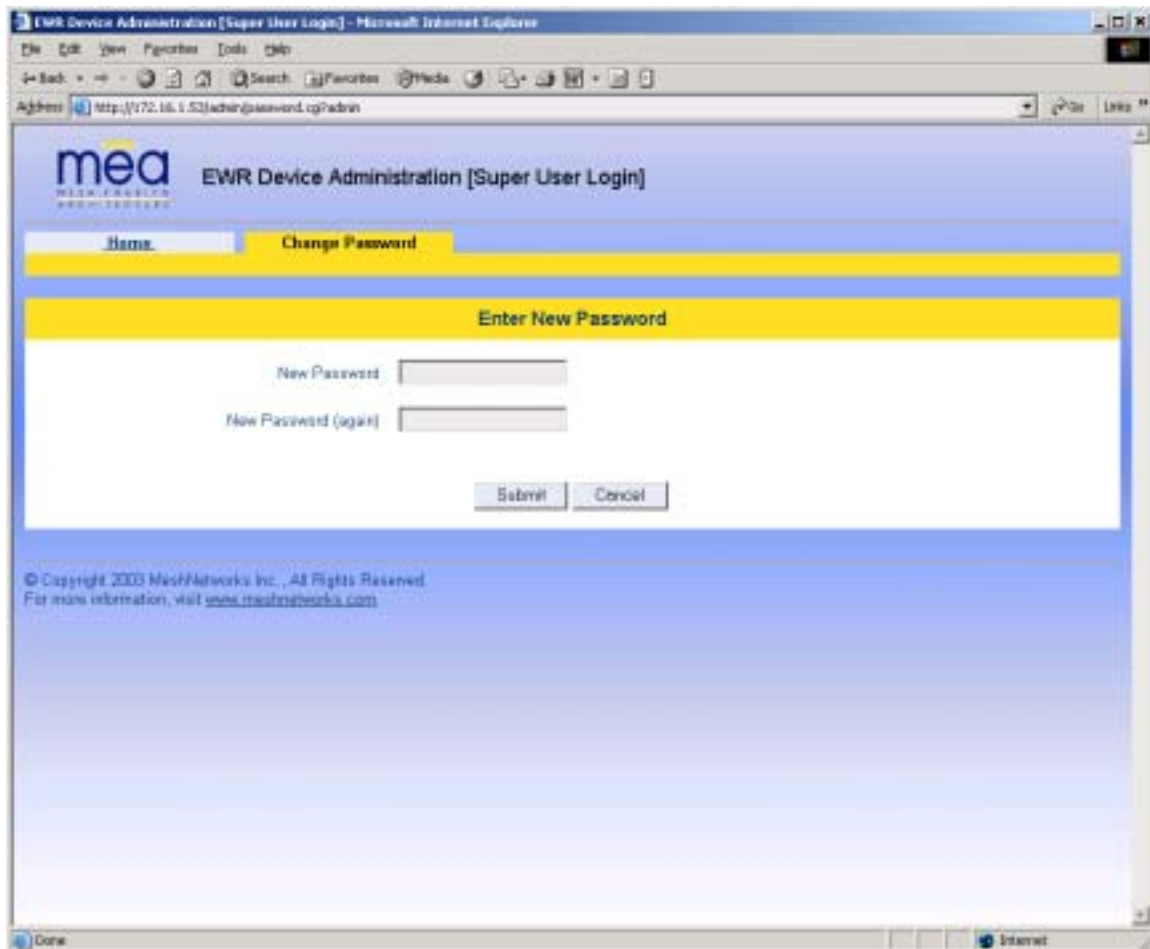
The image shows a screenshot of a web browser window displaying the EWR Device Administration interface. The browser's address bar shows the URL: http://172.16.1.53/admin/passwd.cgi/admin. The page title is "EWR Device Administration [Super User Login]". The main content area has a blue header with the "mea" logo and the text "EWR Device Administration [Super User Login]". Below the header, there are two tabs: "Home" and "Change Password", with "Change Password" being the active tab. The main section is titled "Enter New Password" and contains two text input fields: "New Password" and "New Password (again)". Below these fields are two buttons: "Submit" and "Cancel". At the bottom of the page, there is a copyright notice: "© Copyright 2003 MeshNetworks Inc., All Rights Reserved. For more information, visit www.meshnetworks.com".

Figure 3-12. Enter New Password Web Page

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

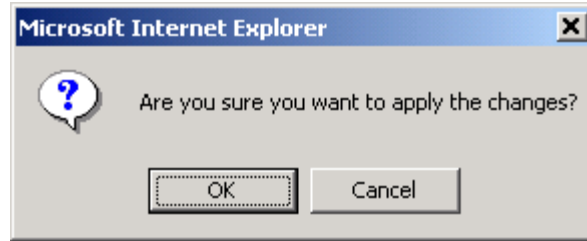


Figure 3-13. Confirm Changes Window for Enter New Password

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

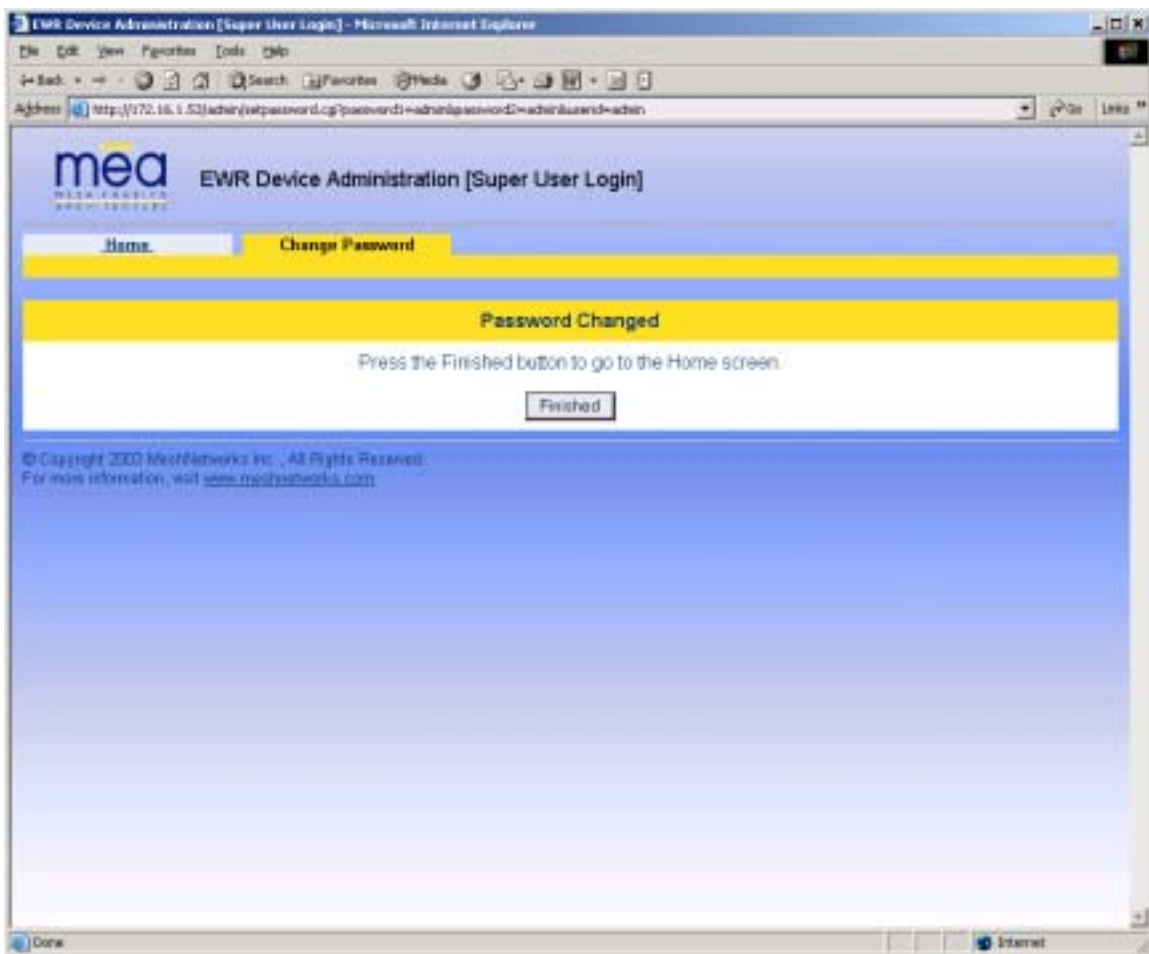


Figure 3-14. Password Changed Confirmation Web Page

3.1.7 Upgrading the Device Firmware

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

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

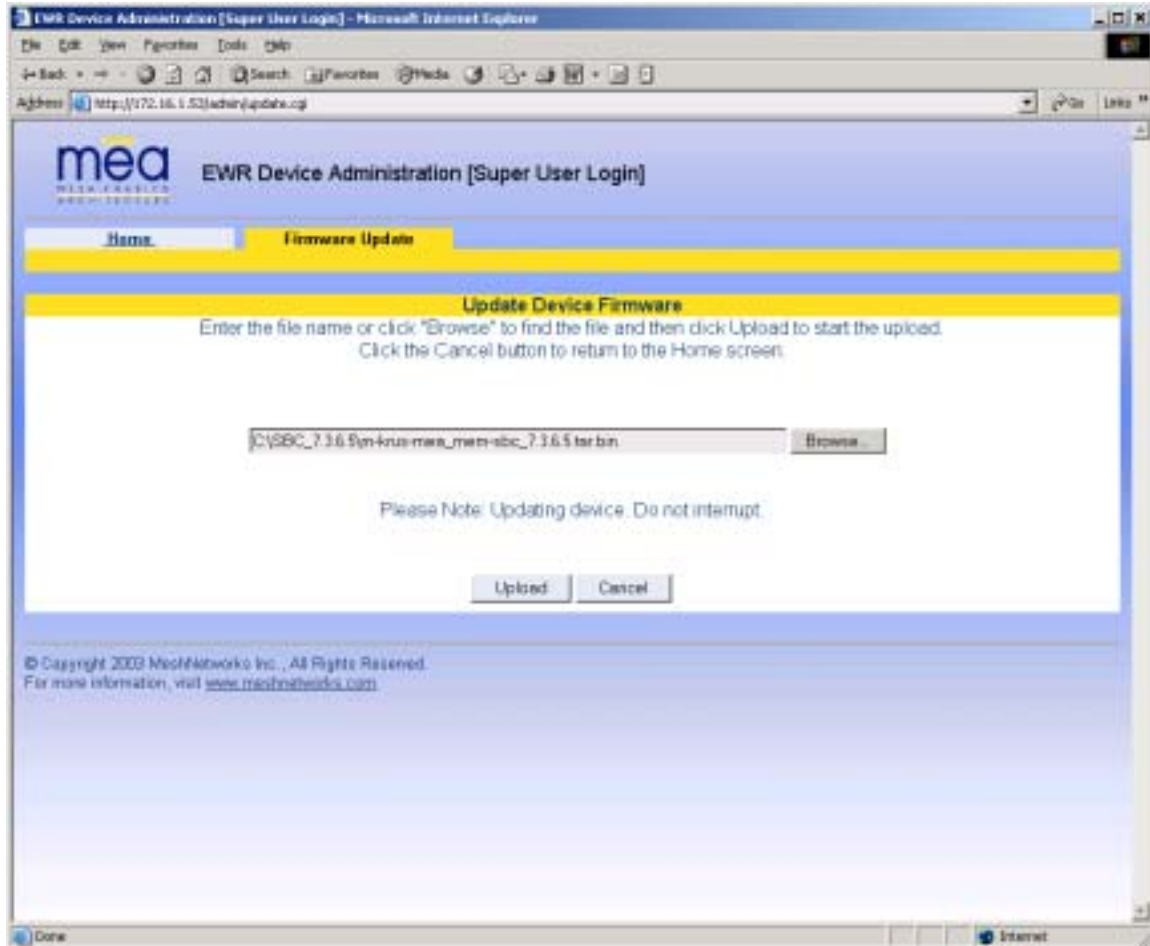


Figure 3-15. Update Device Firmware Web Page

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

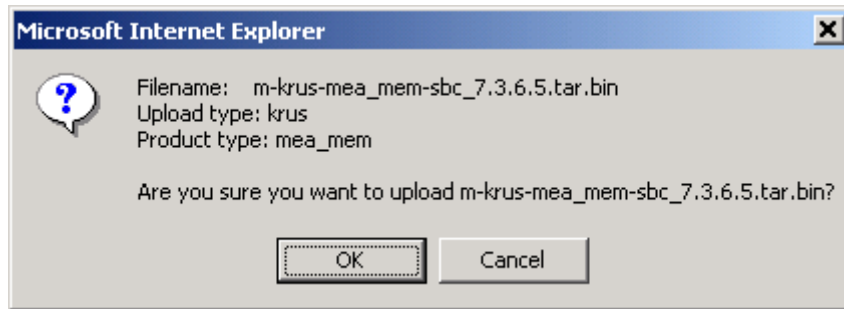


Figure 3-16. Confirm Upload Window for Firmware Update

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

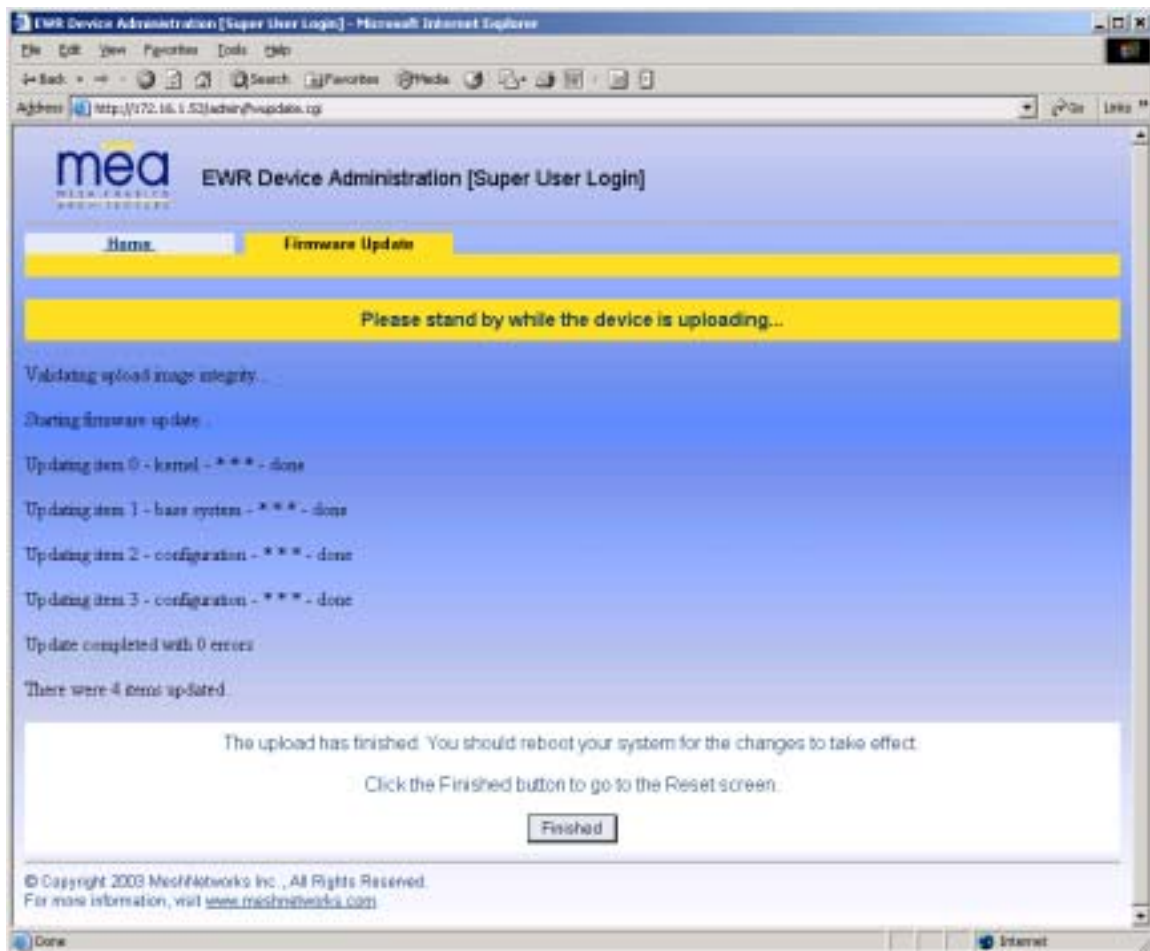


Figure 3-17. Firmware Upload Progress Web Page

Once the upgrade is completed, the device must be reset. The **Finished** button will transition the web browser to the reset screen.

3.2 External Device Provisioning

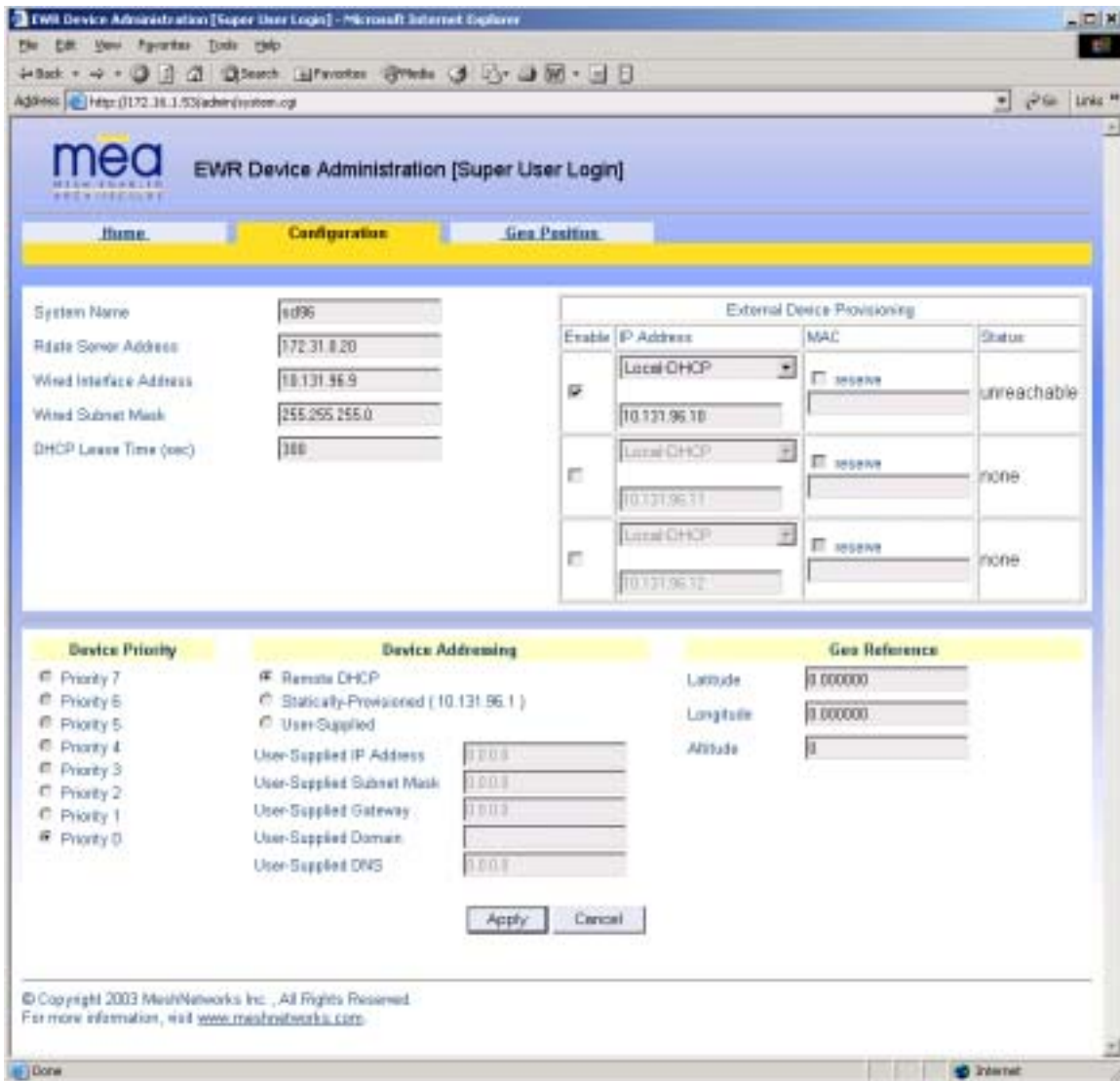


Figure 3-18. External Device Provisioning Table

The *External Device Provisioning* table is used to configure addresses for the attached nodes on the local ethernet segment. Up to three addresses are provisioned.

The *Enable* checkbox indicates this row contains a valid address. Any address can be disabled by clearing the checkbox. The pull-down menu options indicate whether this address will be offered via the local DHCP service (“Local-DHCP”) or not (“Statically-Provisioned”).

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

The MAC address field is used for *Local-DHCP* addresses, so that the IP address can be reserved for a specific device. The *reserved* checkbox must be marked for this kind of IP address reservation. The *Status* field indicates whether the provisioned IP address was detected (via a ping) when the web page was brought up.

MeshNetworks

The IP addresses default to values based on the transceiver MAC address of the device. The derivation is described below. By default, only the first IP address is enabled (for *local-DHCP*), and no addresses are reserved for specific MAC addresses.

Please make sure to check the checkbox for the client IP addresses you have entered. Client 2 and Client 3 are not enabled by default. In this example, the EWR wired interface is assigned the IP address 172.16.2.1. This address is hidden from the core network and the IAP will not route for this address. The core network must use the 172.16.1.37 address to access the EWR (which is the address obtained via MeshManager).

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

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

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

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

Derived MAC addresses:

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

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

The user is encouraged to change these addresses upon installation.

3.2.1 Connecting to the Ethernet Port

If only one device is to be connected to the EWR, you will need to connect the device using a crossover cable.

If you are going to connect more than one device to the EWR, you will need to connect a hub to the EWR and connect the other devices to the hub. A straight through cable will be used between an EWR and a hub.

3.3 Infrastructure Requirements

The EWR requires an associated IAP load to support the additional addresses the EWR makes available. All IAPs must have the appropriate software installed to support the EWR.

3.4 EWR6300 Mounting Bracket

The mounting bracket for the IAP6300 and the MWR6300 are identical to mounting bracket for the EWR6300. The bracket is robust secure; and can be used for horizontal, vertical, and off-angle pole mounted installations. The mounting bracket is preinstalled and supplied with two 3 1/2 x 1/4 inch stainless steel bolts. The mounting bracket can accommodate up to a 3 1/4 inch diameter mounting pole. Substitute for the 1/4-inch bolts supplied with the bracket may be used to accommodate mounting poles smaller than 3 inches.

MeshNetworks strongly recommends the use of stainless steel mounting hardware to prevent corrosion. The standard mounting hardware supplied with the bracket is stainless steel. The bracket is made of aluminum.

The following procedure outlines the required steps for installing a MEA EWR6300 the bracket shown in [Figure 3-19](#).



Figure 3-19. EWR6300 Mounting Bracket

1. Using the deployment guidelines described in the *mea Setup and Deployment User's Guide*, locate an appropriate mounting pole such as a streetlight cobra arm or a metal post. The mounting pole can be vertical, horizontal, or project at almost any angle.
2. Remove one of the C-Clamp Bracket bolts so that the bracket can be positioned around the mounting pole. If necessary, remove the second bolt. When the two halves of the Clamp Bracket are correctly positioned, reinstall the bracket bolts.

Note: The C-Clamp Bracket Assembly requires two 3 1/2 x 1/4 inch stainless steel bolts to secure the C-Clamp to a mounting pole. Each bolt is supplied with (2) stainless steel flat washers, (1) lock washer, and (1) stainless steel nut. The bracket hardware should be installed as indicated in [Figure 3-17](#).

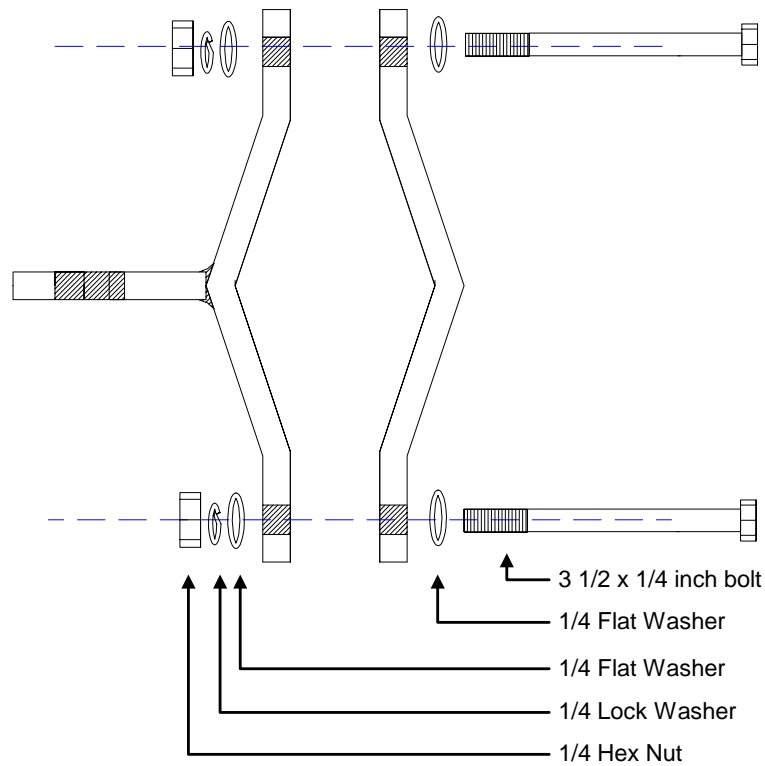


Figure 3-20. C-Clamp Bracket Assembly

3. Position the bracket in the desired location and securely tighten the two bracket bolts.
4. If required, loosen the Pivot Bolt and the Angle Locking Bolt ([Figure 3-18](#)) so that the antenna connector is positioned vertically.
5. Tighten the Angle Locking Bolt using a #1 Phillips screwdriver.
6. Ensure that the antenna connector is still vertical and tighten the Pivot Bolt using a 7/16-inch open-end wrench or socket wrench.

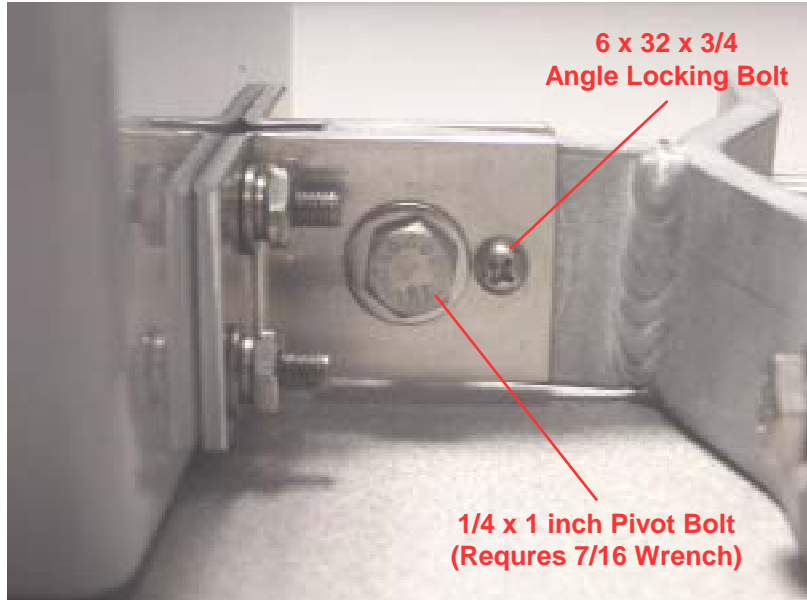


Figure 3-21. EWR Pivot and Angle Locking Bolts

NOTE: Some IAP6300 and MWR6300 enclosures may have a bolt or plug in the center of the back of the box. To maintain the integrity of the box, **DO NOT REMOVE THIS PLUG.**

3.4.1 EWR MAC Addresses

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.

EWR MAC Address 00-05-12-0A-xx-yy	EWR ETH MAC Address 00-05-12-30-xx-yy

4 License and Warranty Information

4.1 Important Information

PLEASE READ CAREFULLY THE FOLLOWING BEFORE INSTALLING OR USING THIS HARDWARE, CONSISTING OF A CD ROM AND PCMCIA CARD, AND THE SOFTWARE (COLLECTIVELY, THE "PRODUCT"). IF YOU AGREE WITH ALL OF THE TERMS OF THIS LICENSE AGREEMENT & LIMITED WARRANTY, PROCEED WITH THE INSTALLATION AND USE OF THE PRODUCT FOLLOWING THE ONSCREEN INSTRUCTIONS. IF YOU DO NOT AGREE, DO NOT INSTALL OR USE THE PRODUCT. BY INSTALLING OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUND BY ALL OF THE TERMS OF THIS LICENSE AGREEMENT & LIMITED WARRANTY. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE AGREEMENT & LIMITED WARRANTY, PROMPTLY RETURN THE UNUSED PRODUCT AND DOCUMENTATION TO THE SOURCE (AS DEFINED BELOW) FOR A FULL REFUND OF THE PURCHASE PRICE.

License Agreement & Limited Warranty

LICENSE GRANT

MeshNetworks, Inc. ("MeshNetworks"), by and through its resellers and suppliers (collectively, the "Source") hereby licenses to the end-user ("You") the software accompanying this Product ("Software"). You have right of possession to the CD ROM on which the Software is recorded (in accordance with your arrangement with the Source), but MeshNetworks retains title to the Software and related documentation. The license is non-exclusive, non-transferable, non-sublicensable and confers a right to use only the machine-readable, object code form of the Software for its normal and intended purpose by a single-user. You may make one backup copy of the Software in machine-readable form, provided the backup copy is not installed or used on any electronic device. You must reproduce on the backup copy the MeshNetworks' copyright notice and any other proprietary legends that were on the original copy of the Software.

RESTRICTIONS

You acknowledge that the Product contains copyrighted material, trade secrets and other proprietary material owned by MeshNetworks, and that unauthorized use of such material may cause serious loss or damage to MeshNetworks. You agree that You will not:

- decompile, reverse engineer, disassemble, translate or reduce the Product to a human-perceivable form.
- modify, adapt, pledge, lease, rent, share, lend, distribute, disclose or create derivative works based upon the Product in whole or in part.
- electronically transmit the Software from one computer to another or over a network.
- transfer any of your rights in the Software, the backup copy of the Software, the media, the documentation, or this License Agreement & Limited Warranty to another party.
- use the Product for any unlawful or harmful purpose.

TERM, TERMINATION

This license is effective until terminated. You may terminate this license at any time by destroying the Software, related documentation and all copies thereof. This license will terminate immediately without notice from MeshNetworks if You fail to comply with any provision of this License Agreement & Limited Warranty. Upon termination You must destroy the Software, related documentation and all copies thereof.

HARDWARE WARRANTY

MeshNetworks warrants to You that the hardware elements of the Product will be substantially free from material defects in workmanship and materials, under normal use and service, for a period of one (1) year from the date of acquisition from the Source.

Our sole obligation under this express warranty will be, at our option and expense, (1) to repair the defective hardware element or, (2) deliver to You an equivalent hardware element to replace the defective item. Any hardware element that is replaced will become our property. Replacement hardware elements may be new or reconditioned. We warrant any replaced or repaired hardware elements for the greater of ninety (90) days from shipment, or the remainder of the initial warranty period.

SOFTWARE WARRANTY

MeshNetworks warrants to You that the Software, except as noted below, will perform in substantial conformance to its published program specifications, for a period of ninety (90) days from the date of acquisition from the Source. No updates are provided under this warranty. Our sole obligation under this express warranty will be, at our option and expense, to replace any defective software product, with software which substantially conforms to applicable MeshNetworks' published program specifications.

You assume responsibility for the selection of the appropriate applications program and associated reference materials. MeshNetworks makes no warranty or representation that the Software will meet your requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the Software will be uninterrupted or error free, or that all defects in the Software will be corrected.

WARRANTY SERVICE

You must contact the Source of the Product within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase may be required. A Return Material Authorization (RMA) number will be issued. This number must be marked on the outside of the package. The Product must be packaged appropriately for safe shipment and sent prepaid. It is recommended that returned Products be insured or sent by a method that provides for tracking of the package. Responsibility for loss or damage does not transfer to the intended recipient until the returned item is received by such party. We will make commercially reasonable efforts to ship the repaired or replaced item to You, at our expense, not later than ten (10) business days after receipt of the defective Product. We will retain risk of loss or damage until the Product is delivered to You.

We will not be responsible for any software, firmware, information, or Memory data belonging to You contained in, stored on, or integrated with any Products returned to the Source for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE, WARRANTY DISCLAIMER

TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, INFORMATIONAL CONTENT, ACCURACY, SYSTEM INTEGRATION, NON-INFRINGEMENT AND QUIET ENJOYMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. WE DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE PRODUCT WILL MEET YOUR REQUIREMENTS, THAT THE PRODUCT WILL BE COMPATIBLE WITH ANY OTHER SOFTWARE, HARDWARE OR OPERATING SYSTEM, THAT THE OPERATION OF THE PRODUCT WILL BE UNINTERRUPTED OR ERROR-FREE. WE NEITHER ASSUME NOR AUTHORIZE ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF THIS PRODUCT.

WE WILL NOT BE LIABLE UNDER THIS WARRANTY IF TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, MESHNETWORKS EXCLUDES FOR ITSELF, ITS RESELLERS AND SUPPLIERS AND THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS, ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR OR REPLACEMENT. AT OUR OPTION THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN WILL FAIL OF ITS ESSENTIAL PURPOSE.

Some jurisdictions do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for death or personal injury, so the above limitations and exclusions may be limited in their application to You. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives You specific legal rights which may vary depending on local law.

EXPORT COMPLIANCE

You agree and certify that the Product will be utilized only in the United States of America or in compliance with 22CFR125.4(b)(9).

GOVERNING LAW

This License Agreement & Limited Warranty will be governed by the laws of the state of Florida, U.S.A., and by the laws of the United States, excluding their conflicts of laws principles. Both the Uniform Computer Information Transactions Act and the United Nations Convention on Contracts for the International Sale of Goods are hereby excluded in their entirety from application to this License Agreement & Limited Warranty.

5 FCC Regulatory Information

5.1 *FCC Information*

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

The EWR6300 (Enhanced Wireless Router) is an infrastructure device that is positioned at a fixed location such as a building rooftop. The EWR6300 requires professional installation to ensure that the installation is performed in accordance with FCC licensing regulations.

The EWR6300 (Enhanced Wireless Router) is an infrastructure device positioned in a fixed location, such as on a pole, wall, or rooftop. The EWR6300 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 MeshNetworks could void the user's authority to operate the equipment.

5.2 *FCC RF Radiation Exposure Statement*

7. **CAUTION:** This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 2 meters between the antenna and your body.
8. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

6 Safety Information for the MEA Products

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

Do not touch or move the antenna(s) while the unit is transmitting or receiving.

Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.

Do not operate a portable transmitter near unshielded blasting caps or in an explosive environment unless it is a type especially qualified for such use (Intrinsically Safe).

Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio may be damaged.

Antenna use:

- In order to comply with FCC RF exposure limits, dipole antennas should be located at a minimum distance of 2 meters or more from the body of all persons.

7 Safety Certification



Conforms to UL STD ANSI/UL 60950 3rd Edition

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

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

7.1 CE Mark Certification

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

MeshNetworks Products are covered under the following product certification Europe:

ETSI EN 300 328 V 141 (2003-04)

MeshNetworks

Products covered - IAP6300, EWR6300 , WMC6300, and MWR6300
ETSI EN 301 489-1 (2002-08) and 301 489-17

Products covered - IAP6300, EWR6300 , WMC6300, and MWR6300
EN 55022:1998 and EN 55024:1998

Products covered - IAP6300, EWR6300 , WMC6300, and MWR6300
CENELEC EN 50360 and EN50371 – Specific Absorption Test - SAR

Products covered - WMC6300

The following countries are covered under the CE Mark:

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

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

An example of the CE Marking on a product label:



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