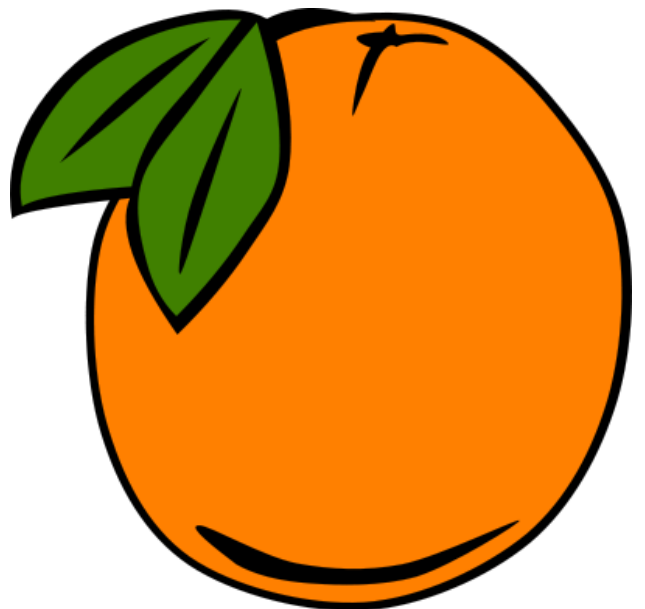


OrangeMesh Network Management Dashboard



User Manual

OM Release 0.2a Revision 160



Table of Contents



Section I: Network Installation

- Mesh Networking Introduction..... 3
 - Mesh Networking Advantages..... 4
 - Mesh Networking Disadvantages..... 4
- Orangemesh Server Installation..... 4
 - Requirements..... 4
 - Database Setup..... 4
 - Dashboard Installation and Configuration..... 5
 - Linux-Only Expert Feature..... 5
 - Web server Configuration..... 5
 - Network Migration..... 6
- Node Hardware..... 7
 - How many nodes do I need?..... 7
 - Indoor vs Outdoor installation?..... 7
 - Node Installation..... 8
 - Where to put them?..... 8
 - Sample Deployment..... 8
 - Getting Ready..... 10
 - Pre-Test..... 11
- Testing your network..... 11

Section II: Administrator Dashboard Interface

- Home Page..... 14
 - Configuring the Home Screen..... 14
- Create Network Page..... 15
- Manage Network Page..... 16
 - Network Account Settings..... 16
 - Network Notifications..... 16
 - Access Point 1 (Public) Configuration..... 17
 - Splash Page Configuration..... 18
 - Access Point 2 (Private) Configuration..... 19
 - Advanced Settings..... 19
- Node Map Page..... 20
- Node Status List Page..... 21
 - Information Categories..... 21
- Node Info List Page..... 22
- Node Info Editing Screen..... 23
- Add/Edit Nodes Page..... 24

Section III: Public Dashboard Interface

- View Network Pages..... 26
- Node Map..... 26
- Node List Page..... 27
 - Information Categories..... 27
- My Nodes..... 28
- Add Network Page..... 29
- Logout..... 29

Appendices

- Appendix A: Basic Troubleshooting..... 31
 - Node Issues:..... 31
 - No Internet Connectivity..... 31
 - Dashboard Navigation Issues..... 31
- Appendix B: Network Deployment Check-List..... 32
- Appendix C: GNU Affero GPL Notice..... 33

Documentation Valid as of OM Release 0.2a Revision 160

***Section I:
Network Installation***



Mesh Networking Introduction

This section briefly explains the concepts of Mesh Networking and important considerations when physically deploying a network for optimal results.

How does wireless networking usually work?

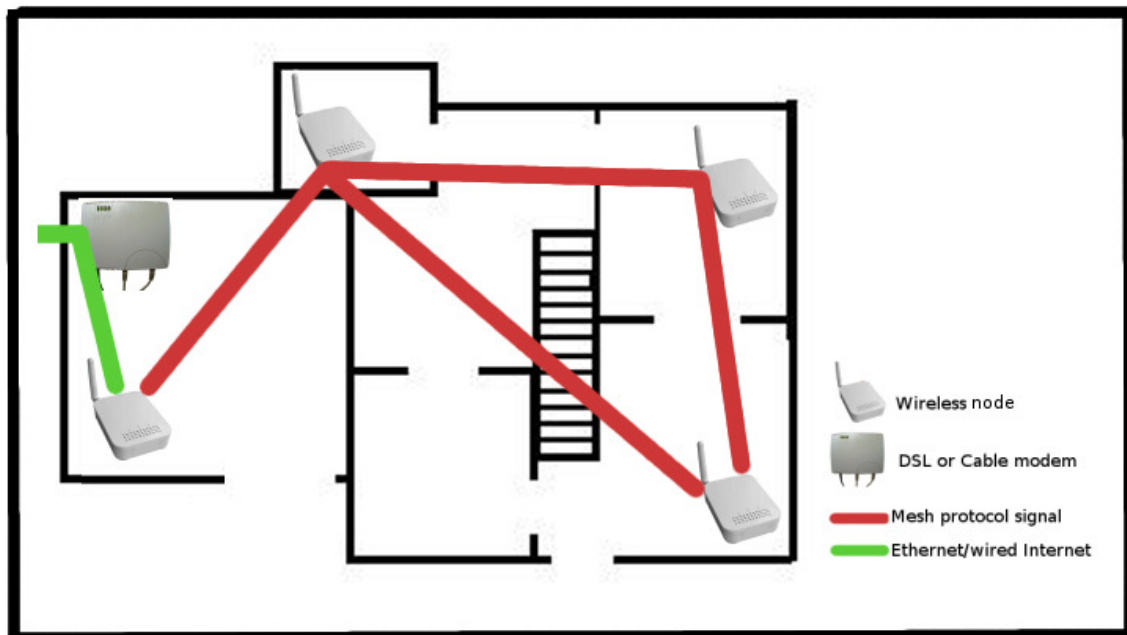
A normal wireless network is created when a wireless router directly connected to the internet shares its connection with wirelessly connected users.

Large wireless networks are created when many routers are deployed over a large area. Each router must physically connect to the Internet

What is different about a wireless mesh network?

In a wireless mesh network, each "router", called a node, does not need to be physically connected to the Internet. That is what makes wireless mesh networking special.

Rather, only one or a few nodes--called gateways--are physically plugged into the Internet. They share the connection with users and other nodes--called repeaters--which carry the signal far and wide.



Mesh Network with Routing to Internet Gateway Displayed

Mesh Networking Advantages

A few of the major advantages of using a Mesh Network:

- Rapid deployment
- No need to install new cables in walls
- Low cost
- Easy to monitor usage and change network settings.

Mesh Networking Disadvantages

There are also a few inherent disadvantages:

- Nodes must be close enough to communicate with one another in order to share a single internet connection. Traditional networks use Ethernet or other physical connections to ensure all routers have internet connectivity.
- Because nodes share a connection to the Internet, bandwidth must be shared among multiple nodes resulting in possible slow downs.

OrangeMesh Server Installation

Requirements

- A copy of OrangeMesh (available at <http://meshnet.googlecode.com>)

- XAMPP (available for Linux, Windows, Mac, and Solaris)

Note: XAMPP isn't required, but this manual assumes it has been installed. If you choose not to, then you'll need to have a working installation of Apache, MySQL, PHP + PEAR, and sendmail. These can be quite difficult to configure so use of XAMPP is encouraged. OrangeMesh has been tested using Linux XAMPP on Ubuntu 7.10.

Database Setup

The recommended method of setting up an OrangeMesh capable database is to use phpMyAdmin. Under "Privileges" create a new user called 'orangemesh' with a password that is recorded for future use and then select the option to "Create a database with same name and all privileges".

The database structure is stored in orangemesh.sql. Import this file into the database. It will create the "orangemesh" database with two tables "network" and "node". The "network" table contains information about all the network accounts stored on this dashboard server. The "node" table contains information about every node for every network on the server.

Next, to ensure that the OrangeMesh installation is able access the database server, the administrator should configure OrangeMesh with the database

password. Open the file `/lib/connectDB.php` in the OrangeMesh directory using a text editor. Under "Database Configuration Options" change the value of "dbPass" to whatever the password was used when creating the dashboard. Ensure changes have been saved and exit the utility changes are complete.

Dashboard Installation and Configuration

Copy the files contained within the OrangeMesh installation archive into the web server root directory (under XAMPP, this is `htdocs`). If correctly installed, the web server will now be functional. In a web browser, visit `http://localhost` (or user selected directory the dashboard files have been installed to), and the administrator will see the main page if the installation is functioning properly.

Additionally, it is necessary to sign up for a Google Maps key for the dashboard: `http://code.google.com/apis/maps/signup.html`. Use the address typed into the browser used to access the Orangemesh server (don't include the `http://`). Put the key received from Google in the `/lib/mapkeys.php` file. There are only two lines to change -- they are at the top of the file.

Linux-Only Expert Feature

Email alerts are a non-supported expert feature in this release and require a Linux cron job to work properly. It requires knowledge of cron jobs and how to properly configure them under Linux. The administrator must configure a cron job to run the `/lib/mailalerts.php` script every 30 minutes. If not using Linux, cron jobs won't be available but any way of scheduling a script to run at a certain interval will work. Additionally, it is necessary to set SMTP server settings in `/lib/mailalerts.php` so that the dashboard can send emails. The settings are located at the top of the script; the most important one is 'host', which the administrator should change to the address of the desired SMTP server.

Web server Configuration

Once server configuration is complete, start XAMPP. In Linux, just run `/opt/lampp/lampp start` to start XAMPP. In Windows, XAMPP probably was started automatically, but the administrator can start using the XAMPP Control Panel (Start > Programs > Apache Friends > XAMPP > XAMPP Control Panel). Be sure that at least Apache and MySQL running. None of the other services are required for OrangeMesh.

Before completing installation, it is important to secure the server since it is publically accessible across the network running a web server. If using XAMPP, a security script is included with the install that will lock down many vulnerabilities. The administrator can run this script from the console or through the web at `http://localhost/security/xamppsecurity.php`.

Depending upon the desired level of security, the administrator may need to take further steps to adequately secure the server depending upon its configuration (i.e., disable directory listings in Apache). A detailed explanation of how to secure a web server is outside the scope of this document, but there are many good resources available online. One geared towards XAMPP is <http://robsnotebook.com/xampp-security-hardening>.

Network Migration

Note: Network Migration is considered a very advanced feature and should be used with great caution as it can seriously damage or corrupt an OrangeMesh installation if used incorrectly

The Network Migration feature is used to transfer an OrangeMesh Network profile between different OrangeMesh installations. It is a multistep process that requires a source server with a pre-existing network that the administrator desires to transfer and a destination server that will serve as the new home for the network.

The first step is to create a new Network on the destination server and record the network name and OrangeMesh installation path for future reference during the process. The migration mode must be enabled in the configuration page.

The second step involves preparing the existing network to be transferred. Under the advanced options section in the configuration page, the Migrate to Remote host option should be selected. The administrator will then be prompted to enter the network name and OrangeMesh installation path recorded in step one.

The administrator should then select the transfer button and begin the transfer process. Important steps when the network settings and node information is transferred will be noted when completed. The administrator should inspect the final out for any possible error messages for future diagnostic use.

The administrator must configure the nodes to report to the new OrangeMesh server by changing the Alternate Control Server on the open-mesh.com network profile.

IT IS VITAL THE MIGRATION FEATURE BE DISABLED ON THE DESTINATION SERVER ONCE THE TRANSFER IS COMPLETE OR UNEXPECTED CONSEQUENCES CAN OCCUR

Node Hardware

How many nodes do I need?

If using the nodes in apartments or hotels, one node is used for every two to four average sized units that coverage is desired. Required node installation density will vary depending upon the type of apartment building construction. If concrete, brick, stone, or other “dense” materials are present, one node may be required for every one or two residential units.

If using the nodes in a residential neighborhood, it is recommend that each house have its own set of node as houses are typically larger than apartments and yards create much more separation between nodes than present in apartment complexes. In large buildings, multiple nodes may be necessary through the structure to provide even coverage.

To bridge multiple structures, it is important to situate the nodes as close as possible and establish a line of sight free of obstructions. Using the supplied antennas under ideal conditions, it is possible for nodes to communicate over 100-200 feet if both are placed in exterior windows with a clear line of sight. After market directional antennas may solve connection issues between buildings but are an unsupported feature.

Indoor vs. Outdoor installation?

Important Considerations:

- Outdoor nodes are expensive to install
- Can require an electrician to install power for remote nodes
- May involve using ladders or rooftops to access high mounts
- Long Ethernet cables need to be installed to supply internet to nodes
- Alternate power supply is recommended (Typically Power-over-Ethernet)
- Lightning protection needed in many areas
- Outdoor antennas and power amplifiers are expensive
- They are unsightly and often violate leases or home owner’s agreements

Outdoor nodes can be used to create long distance backhaul connections between separate structures or subnets, but offer few advantages for the typical single compound installation. Indoor nodes are recommended for most installations.

Historically outdoor nodes have been used because mesh repeaters were expensive so minimizing the number of installed nodes was an important consideration. A few centralized routers using large antennas to both broadcast

and receive incoming wireless signals minimized the number of nodes required to provide coverage across a wide area. A side effect of using outdoor nodes was that a significant portion of the signal was wasted proving signal to outdoor areas that an internet connection isn't required. Outdoor nodes also typically required labor intensive installation on towers or other high points that didn't have preexisting power or data access.

The advent of very low cost mesh technology has reduced the need to minimize the total number of nodes using a few large outdoor nodes. This allows networks to be created using smaller nodes indoors with a smaller wireless foot print that more precisely covers a structure with less wireless signal being wasted outdoors. It is also typically faster and cheaper to install nodes indoors as they can be placed in easily accessible areas that have preexisting data and power connections available.

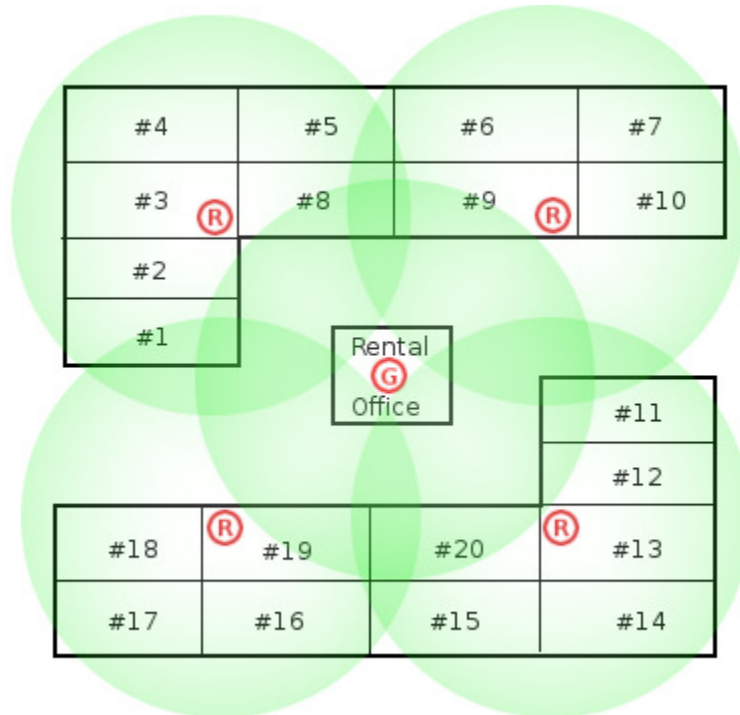
Node Installation

Where to put them?

Once nodes flashed with OrangeMesh compatible firmware and an internet connection has been acquired, the network is ready for physical deployment. It is important to carefully consider node placement for optimal results. The nodes should be placed to maximize their signal coverage of location where connectivity is desired.

Sample Deployment

In this example, let's take a hypothetical 20-unit apartment complex with a central community center or rental office building. Using five nodes, one is configured as a gateway and the other four as repeaters to propagate the signal. Remember that a Gateway node is the one that is plugged into the available internet connection. In this case, the Rental Office contains the internet connection in the form of a DSL modem.



In the above diagram, the Gateway node is in the Rental Office and is marked with a **G**. If the Rental Office already has an internet connection as most offices typically do, this connection can be shared with residents for NO additional cost. The green circles show the approximate coverage range of each node. Repeaters are marked as **R** on the map. As shown above, five nodes were able to completely cover all rental units. Coverage results will vary based upon unit construction and any other factors which influence wireless signals.

Here are some important installation suggestions:

- A centrally located internet connection will offer the most even distribution performance across a site since users and repeaters located farther from the gateway will require more hops to reach gateway with a corresponding performance penalty for each hop.
- Make sure the Repeaters are located as closely to the Gateway as possible within their apartments. Placing them on the wall facing the Gateway is generally a good place to start but further experimentation can be used to fine tune location. For reliable usage, it is very important they have a dependable connection to the Gateway.
- Each node can cover an indoor circular area with roughly a 50-100 foot radius depending upon the number of walls and their construction. For reliability, it is desirable to have multiple coverage footprints overlap so that each node has multiple neighbors it can talk to. A node should have at least one neighbor node with good signal quality, but preferably two or

more for redundancy in the case one neighbor node goes down and the network needs to reroute communication.

- When planning a deployment within a multi-story building, it is important to consider the vertical coverage footprint as well. Signal propagation between floors is very dependant upon how the building is constructed and the density between floors. When providing coverage to a multistory building, nodes located on central floors may be able to provide coverage to floors above and below them which will minimize the number of nodes required to cover a building. If a building has more than three floors, then repeating the installation on every other floor will usually do the trick.
- A building that uses brick, cement or stone construction on exterior walls can greatly limit signal range. When planning these types of installation, it is desirable keep all of the network hardware within the structure and reduce reliance on outdoor nodes to minimize the number of wireless links that must be made through signal disrupting exterior walls.
- In order to mesh the network connection between different buildings, it is recommended that users install nodes at the closest feasible point between the two locations to minimize the effects of signal degradation having to travel through multiple exterior walls.
- Public internal hallways within apartment complexes are often ideal deployment locations for nodes. Being a common space mean that physical access to node will be possible without disturbing residents. Also, placing the several nodes within a long corridor means they can all communicate without having to link through signal disrupting walls. This allows greater signal quality between the nodes and minimizes potential "hops" that will slow down the network.

Getting Ready

Important: Nodes should be plugged into your DSL or other internet connection via their Ethernet cables for at least 30 minutes before being deployed. This is to make sure they are running the latest firmware. This only needs to be done once. After the first time, they will update wirelessly reliably. You can use a hub or switch to connect many nodes at once rather than connecting one at a time.

Before installing nodes in individual apartments or hallways, it is a good idea to record the location where each one is placed. In a large deployment, it can be difficult to match nodes and their MAC addresses without a centralized list of nodes and their locations.

It is also recommended that the node themselves be labeled before proceeding with the install for future identification purposes. A typical approach is to write (using a Sharpie pen that can write on plastic) the location on each node and record the MAC address for future reference before deploying to the installation site.

Pre-Test

Note: Nodes must have upgraded to current firmware for this test to work.

Nodes have a built-in self diagnostic feature once connected to a functioning network. The WLAN light will power on and start blinking 4-5 minutes after supplying power to a node if it has successfully connected to a gateway. If after 5 minutes, there is no WLAN light, it is likely the node is located too far from a gateway or other repeater for a viable connection and should be moved to a location with better signal reception or an intermediate node placed to bridge the signal gap.

Testing your network

The easiest way to test a network is to use a laptop to survey each apartment and test the usability of the detected wireless signal. A simple test procedure is detailed below that will yield fairly consistent results and a general idea of how well the connection will work for users. A more detailed site survey can be conducting using specialized wireless spectrum scanners but is beyond the scope of this manual.

The first step in conducting a wireless network test is to set the laptop to connect to the SSID of the network being tested. "open-mesh" is the default name for OrangeMesh network installations until changed by an administrator. On Windows XP, this connection can be set by right-clicking on the wireless network icon in the taskbar "notification area" (the small icons near the date/time display on the right). Then select "View Available Wireless Networks" from the pop-up Menu. A dialog box will appear.

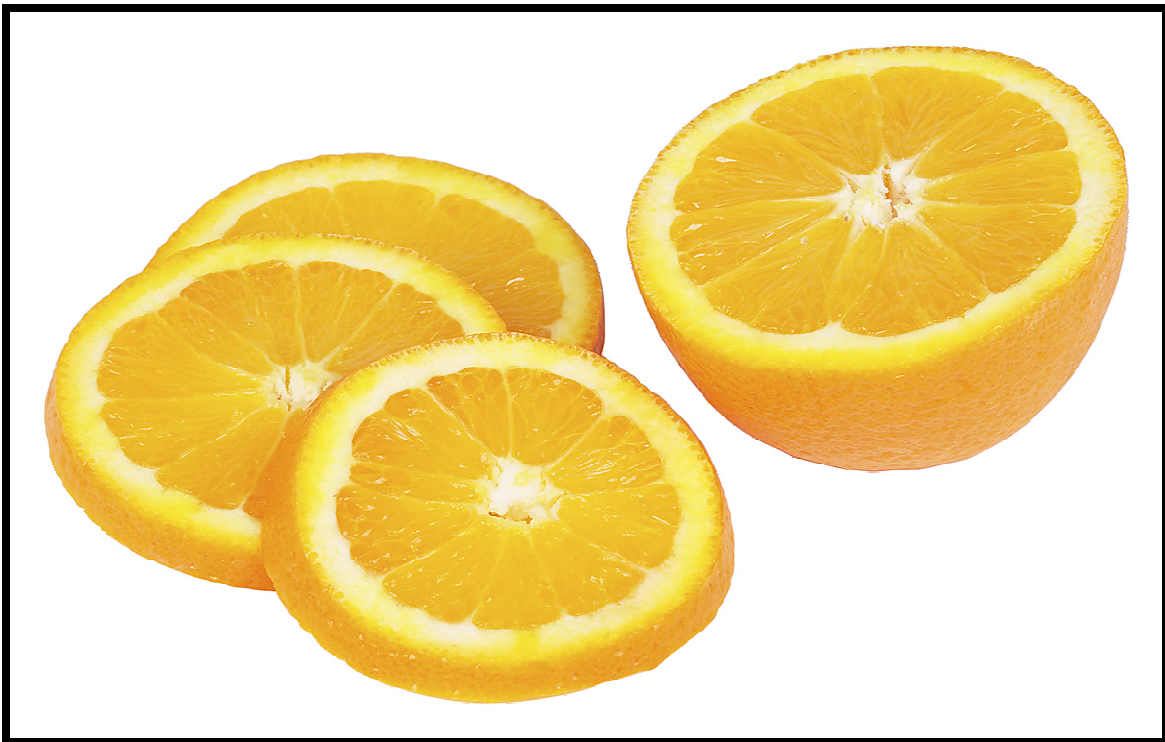
For the purposes of this test, make sure it isn't possible to connect to anything networks except the one being tested to ensure no accidental connections to other networks resulting in erroneous test results. Select "Change the order of preferred networks" link on the left of the wireless menu to see a list of networks that the computer will attempt to connect to. Remove any SSIDs that appear in this list by clicking "remove" until the list is empty then click "add" to add the name of network to be test. Select "OK" twice to save and close this settings page once the name has been added.

It is important when testing different locations to power cycle the wireless adapter on the laptop (most laptops have a switch for this so they can be used on airplanes where wireless isn't allowed) to ensure consistent test conditions. A more detailed explanation why this is necessary is offered in the section below. Laptops generally offer a software option or hardware switch to turn wireless adapters off to conserve power which can be used to cycle the network card. Upon entering a new apartment or room that is being surveyed, turn the wireless switch or software utility to the "off" position, wait a few seconds and then turn it on again. It will usually take a few moments to find the network again and once it says "connected" in the taskbar (if you are using a Windows Laptop), then begin testing. If the network is functioning properly, the SSID should be detected in the list of available networks. Upon successful connection to the network at each location, it's a good idea to refresh a page with lots of graphics a few times. A recommended test page is <http://www.yahoo.com> as it typically has several images. Each page should load in under 5 seconds with no missing images if the connection is functioning properly.

It is important to power cycle the wireless adapter in the laptop being used because they typically they like to stay "locked" onto the wireless access point (During testing, it will probably lock onto one of the mesh nodes) unless the signal gets really bad. Since testing involves moving around and using many different access points, false positives may result as the network card may be trying to talk to a node that is now farther away than another node which would offer a better signal. Users typically don't change position like this, so by power cycling your wireless adapter will offer a better idea of the typical user experience.

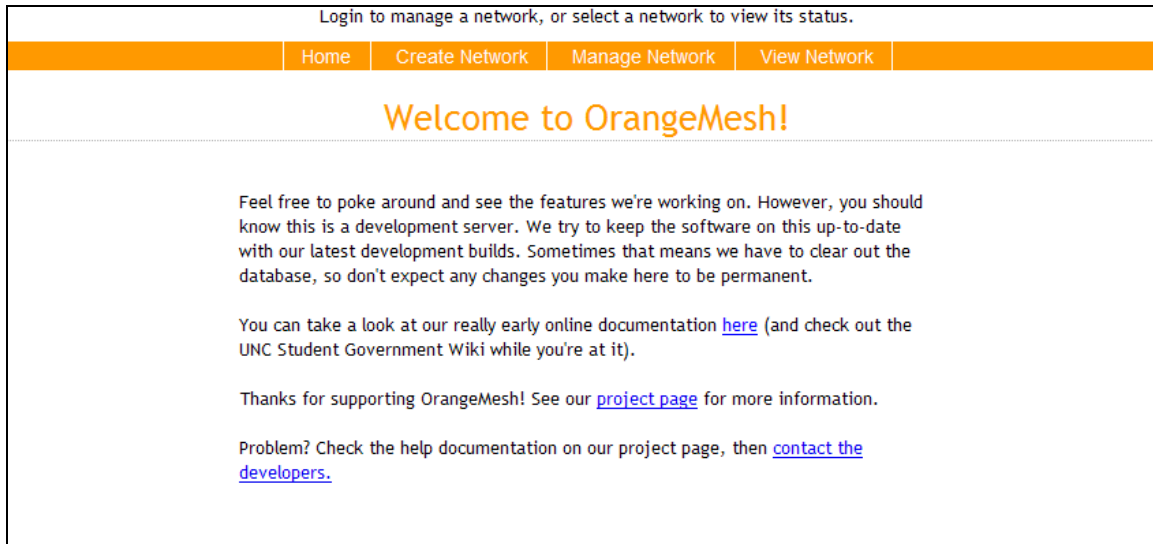
If any locations are found during testing with connectivity issues or an overall failure to connect, it is recommended additional nodes are added to cover the gap in wireless coverage or reposition existing nodes to offer better coverage.

***Section II:
Administrator Dashboard
Interface***



Home Page

The Home tab is the central navigation hub of the management dashboard. It offers a central site all users of the dashboard will be able to access and can serve as a central communication point by updating the welcome message.



Default Home Screen

Configuring the Home Screen

The welcome message can be altered by editing the file *index.php* within the root directory of the dashboard software. The message is stored as commented HTML that is editable within any standard text or HTML editor. A word processor can be used, but users must ensure they save their output as plain ASCII text instead of a formatted word processing document.

Create Network Page

The Create Network page is the first step in creating a new OrangeMesh managed network. The information on this page serves as the basic contact information for a new network. Daily network summaries alerting the administrator of nodes connectivity issues will be sent to the supplied email notification address. The network location will anchor the Google Maps interface to the network location. A user desiring to notify multiple individuals can supply the address of an email listserv to have the daily alert disseminated to multiple users.

Login to manage a network, or select a network to view its status.

Home	Create Network	Manage Network	View Network
----------------------	--------------------------------	--------------------------------	------------------------------

Please fill in the following information to register a new network. Fields outlined in red have errors.

* Network Name (no spaces, please)	<input style="border: 1px solid red;" type="text"/>	The login name for your network account. This is NOT the SSID of your network.
* Password	<input style="border: 1px solid red;" type="password"/>	The password for your network account, used to log into this server. This is NOT the network key for your network.
* Confirm Password	<input style="border: 1px solid red;" type="password"/>	Confirm your password.
* Primary email address	<input style="border: 1px solid red;" type="text"/>	Your email address, used for network alerts.
* Network Location	<input style="border: 1px solid red;" type="text"/>	The physical location of your network. You can enter a street address, postal code, or city/state name.

*** Required Field**

Create Network Page

Manage Network Page

The Networking management screen centralizes all of the options and settings needed to configure and administer the Mesh network. It should be noted that the navigation options change when logged into the management section and allow access to administrator specific pages.

You are logged in to the "foo" network.

[Network Settings](#) | [Node Map](#) | [Node Status List](#) | [Node Info List](#) | [Add/Edit Nodes](#) | [Logout](#)

Test Network

Network Account Settings

Network Name	<input type="text" value="foo"/>	Login ID for this network.
Display name	<input type="text" value="Test Network"/>	The name to use on reports and the splash page.
	Change Password	Administrator password for this network.
Primary Email Address	<input type="text" value="qw0ntum@gmail.com"/>	Your email in case we need to contact you. We will not share this with others.

Network Notifications

Additional Notification Emails	<input type="text"/>	Separate multiple email addresses with spaces. Gateway outages will be sent on the hour, repeater outages will be sent daily.
Enable/Disable/Configure notifications...	Coming soon!	Enable or disable status notifications for this network.

Sample Network Management Screen

Network Account Settings

This configuration sections contains the network owner and name information supplied during the initial network configuration. It allows the administrator to update this information with current information and edit his account information. It should be noted that the Network Name supplied in this section is only used within OrangeMesh to access network information; the SSID of the network is altered in the Access Point 1 & 2 configuration sections below.

Network Notifications

This section allows the user to configure the alerts issued by the dashboard. It allows additional addresses to be specified to receive daily email alerts listing nodes with issues or connectivity problems.

Access Point 1 (Public)

Network Name	<input style="width: 90%;" type="text" value="open-mesh"/>	The SSID to use to connect to this access point.
Network Key	<input style="width: 90%;" type="text"/>	Password (key) for the this access point. Leave blank for an open network. KEYS MUST BE 8 CHARACTERS OR LONGER.
Download Limit	<input style="width: 90%;" type="text" value="400"/>	Download limit (throttling) in Kbits/sec.
Upload Limit	<input style="width: 90%;" type="text" value="100"/>	Upload limit (throttling) in Kbits/sec.
Whitelist	<input style="width: 90%; height: 40px;" type="text"/>	MAC address allowed to use this Access Point, one per line. All other users (MAC addresses) will not be able to browse on this access point. Leave blank to allow all MAC addresses.

Splash Page

Splash Redirect URL	<input style="width: 90%;" type="text"/>	The page to display after the Splash page. Leave blank to display the user's requested page.
Idle Splash Page Timeout	<input style="width: 90%;" type="text" value="1440"/>	Minutes client is idle before showing Splash Page
Require Splash Page Timeout	<input style="width: 90%;" type="text" value="1440"/>	Minutes to show splash page regardless of activity

Sample Network Management Screen (Cont.)

Access Point 1 (Public) Configuration

This section allows the administrator to configure the settings of Access Point 1. It is the interface that is generally used as a publically accessible network if open access to the network is desired. The Network name is the publically broadcasted SSID that identifies the network to users wishing to connect. The network key is the encryption key used to secure the interface if the administrator wishes to keep access private to AP1, longer keys are more secure with a minimum of 8 characters.

Download and Upload limits allow the user to determine how much bandwidth each user will be allowed to use. AP1 offers more configuration and throttling options than AP2. If users are consuming too much bandwidth engaging in activities such as file sharing or watching videos, it can degrade the network experience for all users. Setting lower download speeds will limit the ability of a user to consume too much bandwidth. Often called "throttling", these are the maximum speeds users will get when attached to the network. It is a good idea to set these to between 10% and 25% of the speed of the internet connection. This will make sure that one or two users can't bring the network to halt by

consuming the entire bandwidth. So, if the internet connection is a 4mb DSL, a download speed of 400 to 1000 kb/s would be ideal in most cases. Upload speeds are often far less than download, so limiting the upload speed to 10% of the download speed is a good idea.

Splash Page Configuration

A redirect URL is a page that users will see before other pages they might visit. A few examples of this feature utilized would be linking to a Terms of Service agreement page or a central community portal. Unlike the splash page, a redirect URL can be ANY internet page (such as yahoo.com, google.com or a personal blog. Redirect URLs do not have an "enter" concept. Users will see this page first, and then can click the "home" button in their browser to go to their home page.

The idle splash page timeout is an administrator configurable interval until a user who isn't actively using their connection is redirected to the initial splash screen. The Require Splash Page timeout is the interval in which all connections are redirected to the splash screen regardless of user activity.

Access Point 2 (Private)

Enable	<input checked="" type="checkbox"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">Uncheck to disable this access point.</div>
Network Name	<input type="text" value="mySecure"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">The SSID to use to connect to this access point.</div>
Network Key	<input type="text" value="0p3nm35h"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">Password (key) for this access point. It is NOT possible to leave this field blank and have this be an open AP. MUST BE 8 CHARACTERS OR LONGER.</div>

Advanced Settings

[show](#)
[hide](#)

Root Password for Nodes	<input type="text" value="0p3nm35h"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">Root password for all nodes on your network used for ssh. You should change this for security.</div>
LAN Block	<input checked="" type="checkbox"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">Checking this box will prevent users on the wireless networks from accessing your wired LAN</div>
AP1 Isolation	<input checked="" type="checkbox"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">Check this box to prevent your AP#1 users from being able to access each other's computers.</div>
AP2 Isolation	<input type="checkbox"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">Check this box to prevent your AP#2 users from being able to access each other's computers.</div>
Enable Migration	<input type="checkbox"/>	<div style="background-color: #f39c12; padding: 5px; border-radius: 5px;">Allow remote servers to send network data (settings and nodes) to this network account. Turn this off if you are not in the process of moving your network from one server to another!</div>

[Migrate this network to another Oranagemesh Server](#)

Send this network's settings and associated nodes to another network account on a remote server.

Save Settings

Sample Network Management Screen (Cont.)

Access Point 2 (Private) Configuration

Access Point 2 is typically used as the private network when used in conjunction with AP1. It doesn't offer as many advanced configuration options to throttle and shape user traffic. It is recommended an administrator use AP1 for any networks that require these configuration options or used as an open access network.

Advanced Settings

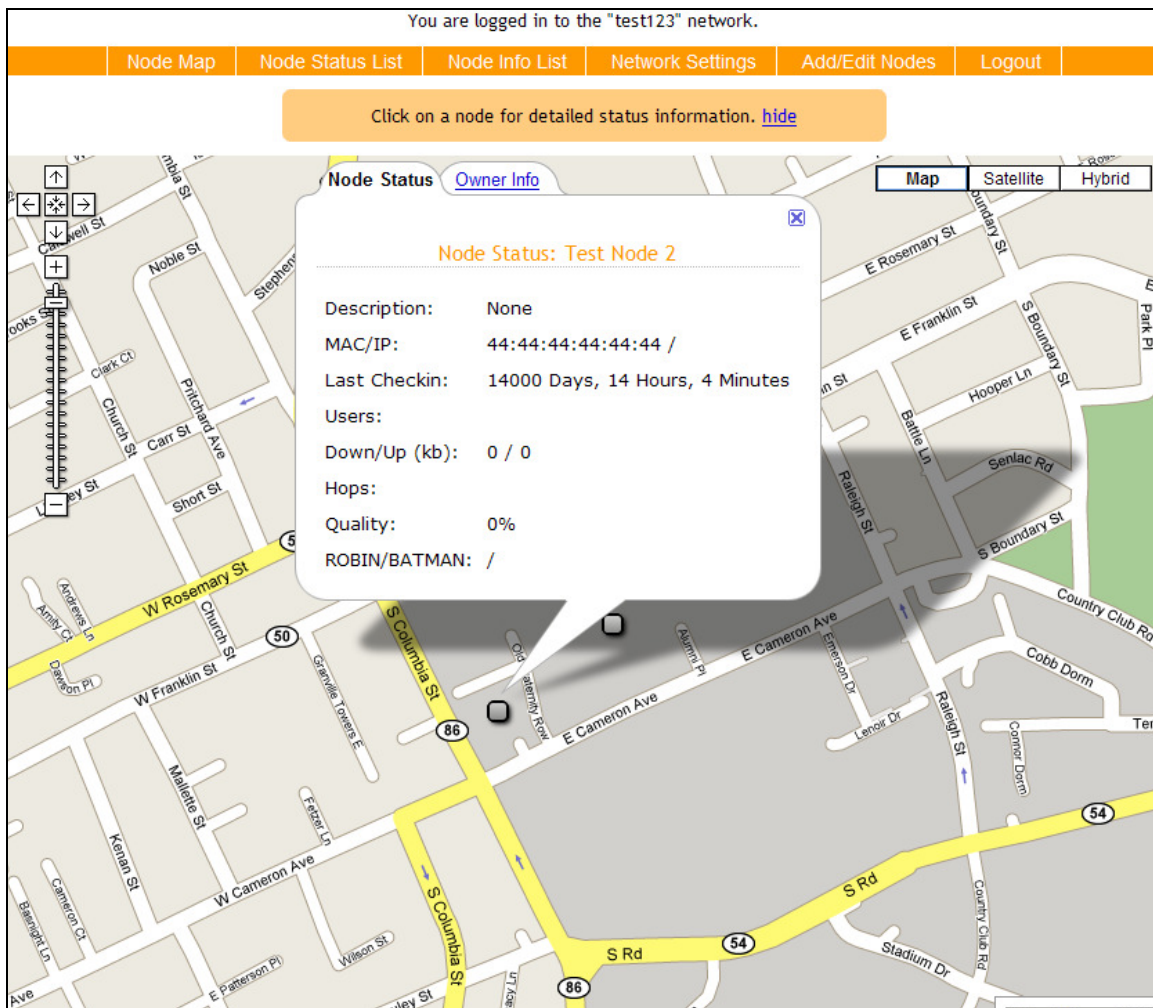
This section offers advanced settings for administrators. The root password for nodes is when connecting directly to an individual node with SSH and interfacing through a console account. Although it is not recommended, it is possible to skip this step and manually change the configuration settings on each node. To do this, it is necessary to establish an SSH connection to the node, using 'root' as the user name and '0p3nm35h' as the default password. Details about changing this

setting area available in the ROBIN firmware documentation:
<http://www.blogin.it/howtorobin/node96.html>

The Block and Isolation features are a security enhancement that will reduce users' vulnerability to unwanted access from other users on the network. It will remove the ability of users to directly interact with each other across the network.

Migration is used to transfer network information from one hosting dashboard to another. Refer to the migration feature of the manual for more information on this advanced feature.

Node Map Page



The screenshot displays the 'Node Map Page' for a network named 'test123'. The page features a navigation bar with tabs for 'Node Map', 'Node Status List', 'Node Info List', 'Network Settings', 'Add/Edit Nodes', and 'Logout'. A central instruction box says 'Click on a node for detailed status information. [hide](#)'. Below this is a map with a 'Node Status' popup for 'Test Node 2'. The popup shows the following details:

Node Status: Test Node 2	
Description:	None
MAC/IP:	44:44:44:44:44:44 /
Last Checkin:	14000 Days, 14 Hours, 4 Minutes
Users:	
Down/Up (kb):	0 / 0
Hops:	
Quality:	0%
ROBIN/BATMAN:	/

The map background shows a street grid with several nodes marked as small black squares. A yellow line highlights a path through the network, and various street names like 'W Rosemary St', 'S Columbia St', and 'S Rd' are visible.

Status Map Example

The Status Map page is a Google maps based visualization designed to allow a network administrator to easily survey the physical lay out of his network while

quickly accessing information on individual nodes. Selecting a node opens a pop up that displays traffic, user numbers and connectivity statistics of the individual nodes. An owner information tab is also accessible listing the contact information supplied during the node registration process. The categories listed are the same as used on the Node Status List Page; refer below for further explanation on each statistic reported.

Node Status List Page

You are logged in to the "test123" network.										
Node Map	Node Status List	Node Info List	Network Settings	Add/Edit Nodes	Logout					
Node Status List for test123										
<p style="color: red; margin: 0;">Nodes in red need attention.</p> <p style="margin: 0;">Names of gateway nodes appear in bold. hide</p>										
Node Name	Description	Uptime	Quality	Hops	Down kb	Up kb	Users	Max Users	Last Checkin	MAC
Test	Test Node		0%		0	0			14000 Days, 14 Hours, 5 Minutes	33:33:33:33:33:33
Test Node 2	None		0%		0	0			14000 Days, 14 Hours, 5 Minutes	44:44:44:44:44:44

Node Status List Page

The Node Status Page is a view that quickly lists all the nodes present on the network and their current status.

Information Categories

Uptime: Total Amount of Time the Node has Been Functional

Quality: Wireless Signal Strength to the Gateway

Hops: The number of routing steps between node and internet gateway

Down kb: Amount of data downloaded through node the previous day

Up kb: The total amount of data uploaded through node the previous day

Users: The number of current users

Max Users: The largest historical number of simultaneous users

Last Check in: Last time the node reported status to the dashboard

MAC: The unique hardware serial number

Node Info List Page

You are logged in to the "test123" network.

Node Map	Node Status List	Node Info List	Network Settings	Add/Edit Nodes	Logout
--------------------------	----------------------------------	--------------------------------	----------------------------------	--------------------------------	------------------------

Node Information List for test123

You can edit node information by clicking on the node's name. [hide](#)

Node Name	MAC	Description	Owner Name	Owner Email	Owner Phone	Owner Address	Activation Status
Test	33:33:33:33:33:33	Test Node	Joe Public	Noone@false.com	555-555-5555	123 Nowhere Ln	Activated
Test Node 2	44:44:44:44:44:44	None	Jenny	no@tutone.com	555-867-5309	123 Musik St	Activated

Node Info List Page

The Node Information page allows an administrator to view the contact information for all the nodes on the network. It also allows an administrator to quickly view the status of pending and approved nodes. Selecting a node name loads a page that allows an administrator to alter or update the stored information.

Node Info Editing Screen

You are logged in to the "test123" network.

Node Map	Node Status List	Node Info List	Network Settings	Add/Edit Nodes	Logout
----------	------------------	----------------	------------------	----------------	--------

Edit Node Information for 33:33:33:33:33:33

Node Information

Node Name	<input type="text" value="Test"/>	A useful name for the node.
Description	<input type="text" value="TestNode"/>	A useful description of the node.
Node Owner Name	<input type="text" value="Joe Public"/>	Name of the node owner. Only visible to the administrator.
Node Owner Email	<input type="text" value="Noone@false.com"/>	Owner's email address. Only visible to the administrator.
Node Owner Phone Number	<input type="text" value="555-555-5555"/>	Owner's phone number. Only visible to the administrator.
Node Owner Address	<input type="text" value="123 Nowhere Ln"/>	Owner's address. Only visible to the administrator.
Activation Flag	<input type="text" value="Activated"/>	If your node is deactivated, it will not appear in the dashboard until you reactivate it. This is the default setting for nodes added by community members. If your node is deleted, you will not be able to reactivate it.

Node Info Edit Page

The edit screen allows the administrator to change all of a node's configuration options. The node name is the name that is used to reference the node in all other dashboard screens. The node description allows the administrator to store information about a node such as a note about its location or other relevant fact. The node owner information allows the administrator to track and contact the node owner or individual physically responsible for the node in question. The activation flag allows individual nodes to be activated or deactivated. Any nodes added by community users through the View Network navigation options must be manually enabled by the administrator before becoming active on the network.

Add/Edit Nodes Page

You are logged in to the "test123" network.

Node Map	Node Status List	Node Info List	Network Settings	Add/Edit Nodes	Logout
----------	------------------	----------------	------------------	----------------	--------

Click anywhere on the map to add a new node to this network.
Drag an existing node to a new location, or click on it to change its settings. [hide](#)

Add Node ✕

Name:

MAC: *

Description:

Latitude:

Longitude:

Owner Name:

Owner Email:

Owner Phone:

Owner Address:

*Use MAC address in form xx:xx:xx:xx:xx:xx.

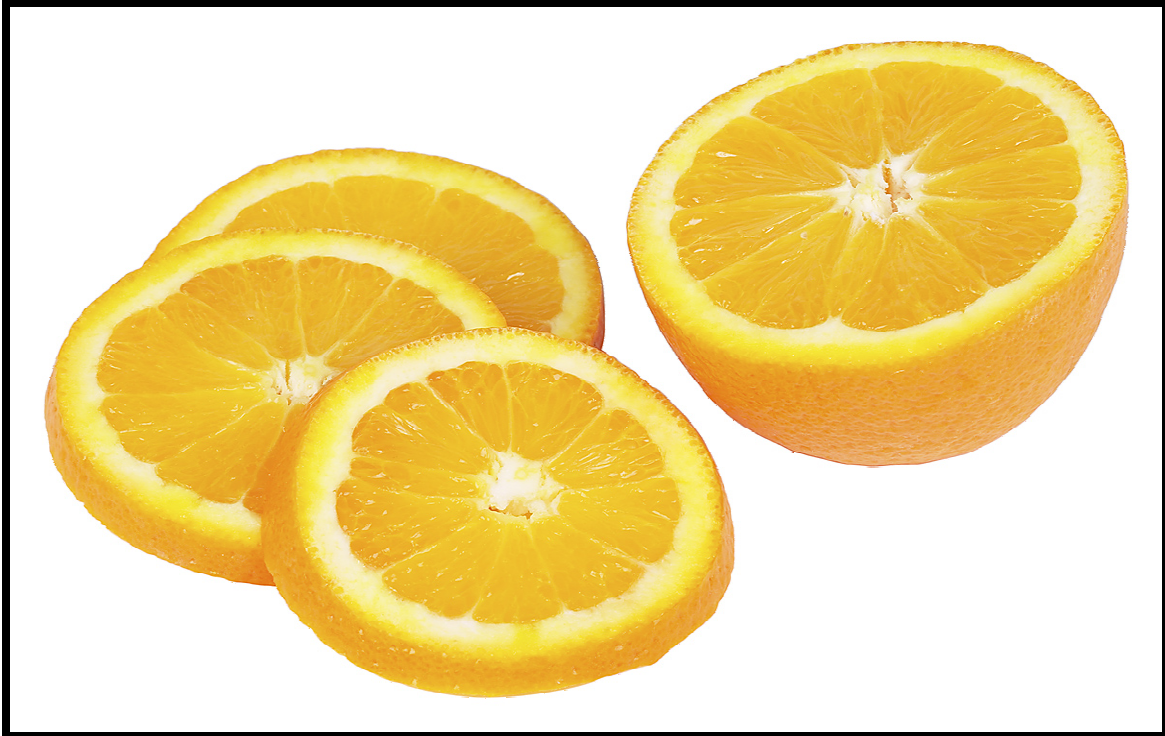
Add/Edit Node Page

The Add/Edit Page allows an administrator to add new nodes to the network and drop them into position on the Google map display. The MAC address must be entered correctly for the node to properly communicate with the dashboard. The Owner information must also be set correctly to properly reflect ownership in the dashboard listings.

Logout

The logout button allows a user or administrator to terminate their current dashboard session and return to the home page. They will have to log in to access network statistics again.

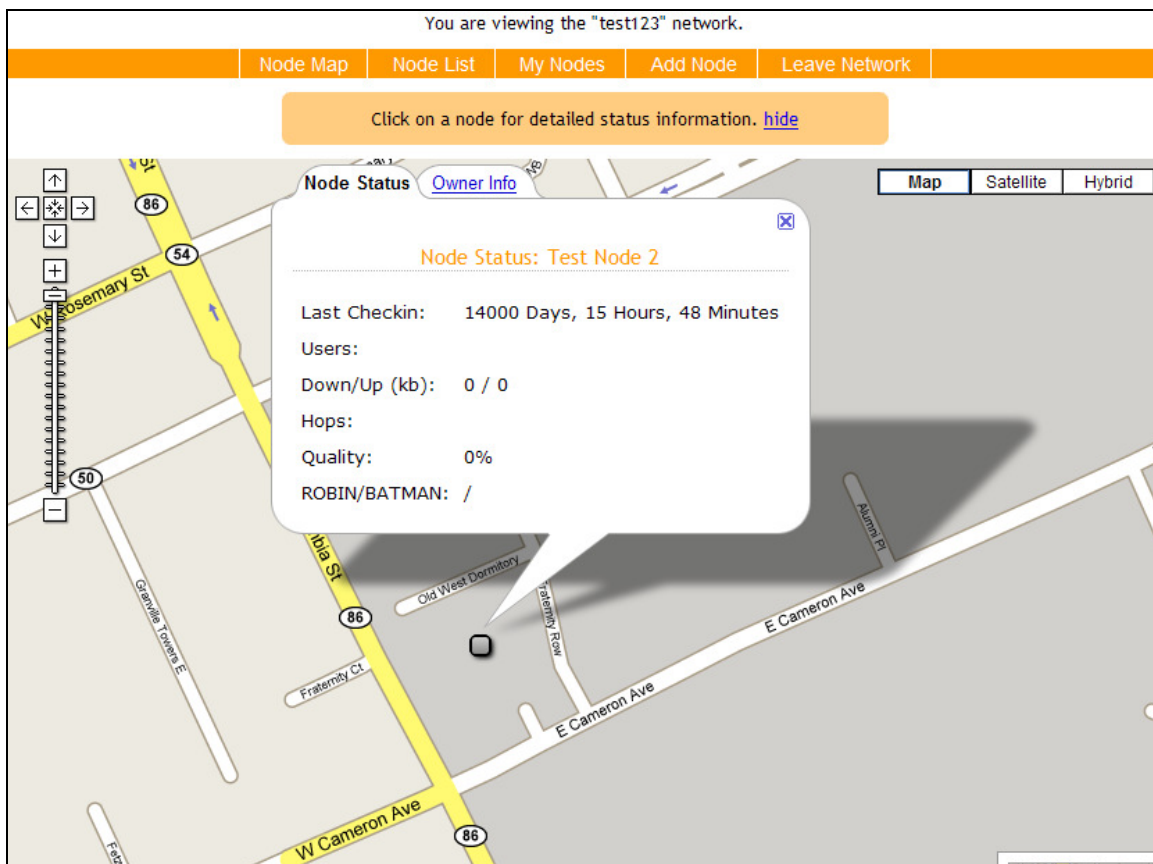
***Section III:
Public Dashboard Interface***



View Network Pages

The View Network pages are series of publicly available status pages; it shares several pages with the administrator views discussed in early sections. There is no authentication required to view the basic status of a hosted network. However, the user is unable to make and changes and is limited to viewing statistics. The user can elect to add a node to the approval process for an administrator to review and approve or disapprove later.

Node Map



View Network Page

The Node Map page is a Google maps based visualization designed to allow a user to easily survey the physical lay out of the network while quickly accessing limited information on individual nodes. Selecting a node opens a pop up that displays traffic, user numbers and connectivity statistics of the individual nodes. An owner information tab is also accessible listing the contact information supplied during the node registration process. The categories listed are the same

as used on the Node Status List Page; refer below for further explanation on each statistic reported.

Node List Page

You are viewing the "test123" network.										
		Node Map	Node List	My Nodes	Add Node	Leave Network				
Node Status List for test123										
<div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p style="margin: 0;">Nodes in red need attention. Names of gateway nodes appear in bold. hide</p> </div>										
Node Name	Description	Uptime	Quality	Hops	Down kb	Up kb	Users	Max Users	Last Checkin	MAC
Test	Test Node		0%		0	0			Never checked in.	33:33:33:33:33:33
Test Node 2	None		0%		0	0			Never checked in.	44:44:44:44:44:44

[View Network Page](#)

The Node Status Page is a publicly viewable page that quickly lists all the nodes present on the network and their current status.

Information Categories

Uptime: Total Amount of Time the Node has Been Functional

Quality: Wireless Signal Strength to the Gateway

Hops: The number of routing steps between node and internet gateway

Down kb: Amount of data downloaded through node the previous day

Up kb: The total amount of data uploaded through node the previous day

Users: The number of current users

Max Users: The largest historical number of simultaneous users

Last Check in: Last time the node reported status to the dashboard

My Nodes

You are viewing the "test123" network.

Node Map	Node List	My Nodes	Add Node	Leave Network
----------	-----------	----------	----------	---------------

Node Status List for no@tutone.com on test123

Nodes in red need attention.
Names of gateway nodes appear in bold. [hide](#)

Node Name	Description	Uptime	Quality	Hops	Down kb	Up kb	Users	Max Users	Last Checkin	MAC	Activation Status
Test Node 2	None		0%							44:44:44:44:44:44	Activated

My Nodes Page

The My Nodes page allows a user to retrieve all of the nodes registered to a requested email address. It offers the ability for a node owner to view the records of all his personally owned nodes and check their status.

Add Network Page

The screenshot displays the 'Add Node' page interface. At the top, there is a navigation bar with buttons for 'Node Map', 'Node List', 'My Nodes', 'Add Node', and 'Leave Network'. Below this, a yellow instruction box says 'Click anywhere on the map to add a new node to this network.' with a 'hide' link. The main area features a Google Map of a street grid. A white 'Add Node' form is overlaid on the map, containing the following fields: Name, MAC: *, Description, Latitude (pre-filled with 35.91156786422858), Longitude (pre-filled with -79.05093312263489), Owner Name, Owner Email, Owner Phone, and Owner Address. An 'Add' button is at the bottom right of the form. A note at the bottom of the form reads '*Use MAC address in form xx:xx:xx:xx:xx:xx.' The map shows streets like North St, E Rosemary St, E Franklin St, and S Columbia St.

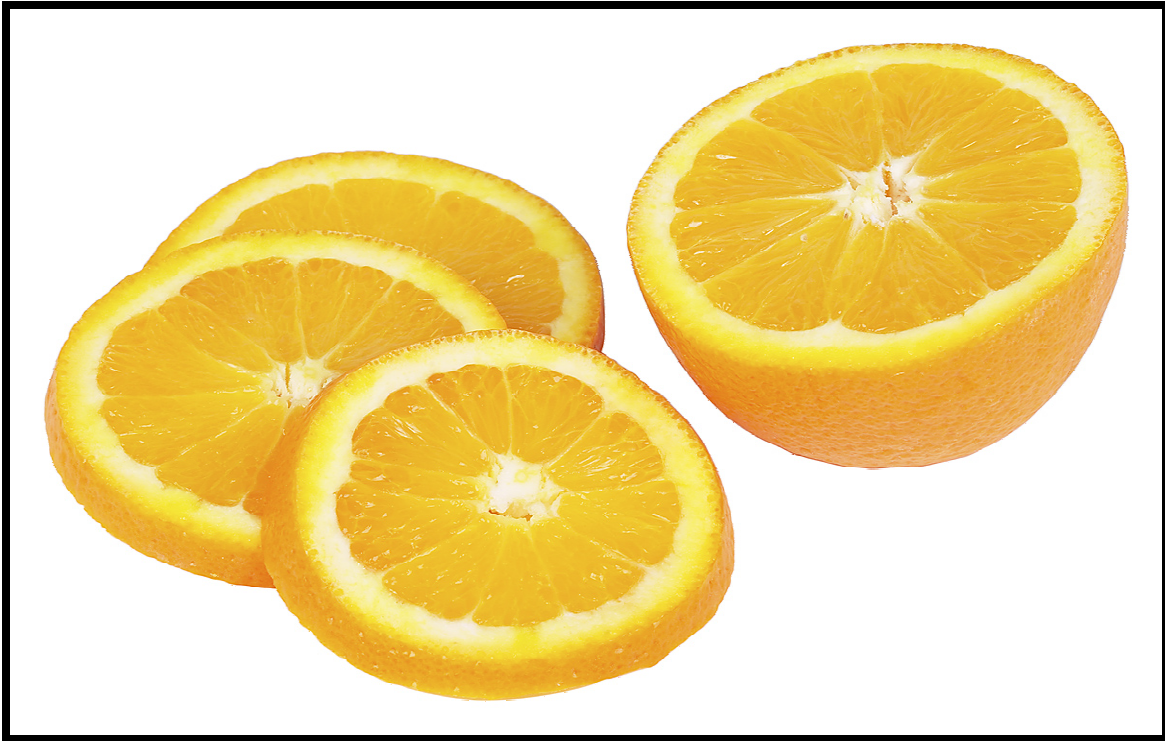
Add Node Page

The Add/Edit Page allows a user to add new nodes to the network and drop them into position on the Google map display. The MAC address must be entered correctly for the node to properly communicate with the dashboard. The Owner information must also be set correctly to properly reflect ownership in the dashboard listings. A user added node is automatically added as deactivated until an administrator reviews the new entry and enables it in the administrator node list.

Logout

The logout button allows a user to terminate their current dashboard session and return to the home page. They will have to log on to access network statistics again.

Appendices



Appendix A: Basic Troubleshooting

Node Issues: Restarting a node is one of the first steps in diagnosing a problematic node. Many common node issues will be resolved by a power cycle that causes a reboot. The node should be unplugged and remain disconnected for one to two minutes. It is important that the power remain off for at least a minute to prevent a power spike in the node which will prevent the node from properly booting and can only be resolved by removing power from the node for at least a minute.

No Internet Connectivity: If users are able to connect to the mesh network but don't have internet connectivity, make sure the internet Gateway node is working properly. If the gateway node is functioning properly, the middle status light should be flashing and the dashboard shouldn't indicate any issues with the node. If an internet gateway node does go down, it will take several minutes for the nodes to reroute their traffic to a functioning gateway, if one exists on the network.

Dashboard Navigation Issues: It is important for users to note that navigation options in the horizontal menu bar at the top of the screen change depending upon location with the dashboard and whether they are viewing a network as an administrator or as a user.

Appendix B: Network Deployment Check-List

- Buy pre-flashed nodes from www.open-mesh.com
- Open box when nodes arrive and Check Contents
- Go to www.open-mesh.com and create a network account.
- Add nodes to the Open-Mesh network, using that sites provided instructions.
- Update the firmware of your nodes. Follow the instructions provided by Open-Mesh. You'll need to connect at least one node to a reliable internet connection using its Ethernet port for at least half an hour. You can verify that the node or nodes you've connected have the latest firmware at Open-Mesh.com.
 - Instructions for the updating process are available here:
<http://www.open-mesh.com/activekb/questions/1/>
- Power on any other nodes you have. Make sure they are no more than a few feet away from one of the nodes you have connected to the internet. They will use the wireless connection to update their firmware as well. This process should take between 30 minutes to an hour. Just like the previous step, verify all your nodes have updated their firmware. If any node fails to update, try connecting it directly to an internet connection using its Ethernet port.
- On your Open-Mesh.com account, go to "Edit Network" > Advanced Settings. For the option "Alternate Control Server", enter the URL of your OrangeMesh server, including the path to where you installed OrangeMesh.
 - Example 1. If your server's address is www.example.com, and you have OrangeMesh installed in a folder called "dashboard", you would enter "www.example.com/dashboard".
 - Example 2. If you don't have a domain name, you can use an IP address. For instance, if your server's public IP address is 71.23.202.100, you would enter "71.23.202.100". You would use "71.23.202.100/dashboard" if you had installed OrangeMesh in a folder called "dashboard".
- Create a network account on your OrangeMesh server.
- Add your nodes to your new OrangeMesh network.
- You can configure your network settings any way you like from your OrangeMesh server. You have complete control over all settings from your OrangeMesh server.
- Once your nodes are all positioned where you want them to be and are powered on (following the setup instructions in this manual), you should begin to see your nodes "check in" to your OrangeMesh server with their status information in a few minutes. Check the troubleshooting section if you have any nodes that do not show up on your dashboard server within an hour!

Appendix C: GNU Affero GPL Notice

This file is part of the OrangeMesh Network Administration Dashboard.

OrangeMesh is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

OrangeMesh is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with OrangeMesh. If not, see <<http://www.gnu.org/licenses/>>.

