OMESH Networks

OPM15 Application Note: Address Configuration

Version: 0.0.1

Date: November 10, 2011

Email: info@omeshnet.com
Web: http://www.omeshnet.com/omesh/

Contents

1.0 Introduction

OPM15 is a large-scale cognitive wireless networking module, providing great flexibility for a wide range of applications. Powered by the OPM optimized radio design and networking stack, the result is a fully integrated module providing a complete system for dynamic wireless networking with real-time and high-performance communications. The module has the following attributes: 1) dynamic drop-and-play (supporting station mobility); 2) real-time communications over unlimited number of wireless hops; 3) low power consumption and small footprint; 4) compatible with the 802.15.4 standard; 5) tolerant of interference in unlicensed spectrum.

This document describes the address configuration of OPM15 radio. The API to configure network address is described in [1].

2.0 Specification

The Host is responsible for configuring the network address of the Module: the first byte contains a Network ID (the first 2 bit) and a Node ID (the last 6 bit). The second and third bytes (0-255) are representing the X and Y grid coordinates of the node in the network respectively (except for "0xFF (255)" which has a special definition as to be described later). Any valid network address must have a non-zero first byte. A Module must have a valid network address in order to send or receive packets. And any two nodes in a network cannot have identical network address.

A network address with the second and third bytes as "0xFF (255)" cannot be relaying unicast packets, nor be the destination of any "multi-hop (larger than 1 hop)" unicast packets (i.e., no unicast packets with such destination address can be relayed). No unicast packets can be relayed by a relay node with Network ID different from the destination node.

For reliable performance of unicasting, the following rules about network address configuration shall be observed. Broadcasting and Multi-hop broadcasting do not necessarily have such requirements.

The network address can either be pre-configured or be dynamically configured by processing the node's network neighborhood information. Under the same Network ID, the Manhattan distance between any two nodes within a single-hop range can be configured between 0 and 6, depending on the mapping of mutual RSSI; the typical RSSI range is -25 to 25. The higher the RSSI, the smaller the mutual Manhattan distance should be.

The Manhanttan distance between any two nodes 1 and 2 is defined by |X1-X2|+ |Y1-Y2|, where X1, Y1 are the last two bytes of node one network address, and X2, Y2 are the last two bytes of node two network address. Unicast packets could be transmitted from a transmitter node (pervious-hop relay or source node) to a candidate relay node, if any one of the following conditions can be met:

- Transmitter node address has a Network ID different from destination node address; relay node address has the same Network ID as destination node address.

- Transmitter, relay, and destination nodes have their network address under the same Network ID. The Manhanttan distance between transmitter and destination nodes is greater than the Manhanttan distance between relay and destination nodes.

ADDITIONAL NOTES:

1. The network address configuration does not necessarily relate to the physical geometry of a deployed network.

2. Unicast "dead-end" shall be prevented in network address configuration where a relay node does not have a neighbor that is further closer to unicast destination in terms of Manhanttan distance (to be further elaborated in Section 6). Such a packet would be dropped by the dead-end relay node.

3.0 Stationary Networks

If the networking nodes are all stationary, the network address shall be configured upon deployment and remain constant. All networking nodes can have a same Network ID: this gives an address space of 64X255X255 or 4,161,600 nodes in a single network.

The network address can be pre-configured in the network planning (as convenient in most cases); or dynamically configured when it is actually being deployment and powered on.

In the dynamic address configuration, the newly deployed node could initialize the network address with the known network ID and random node ID, for the non-zero first byte; and the second and third bytes of network address could be both "0xFF". The node can then use Command Query [1] to obtain the addresses of neighboring nodes in a single-hop range and the RSSI to every neighboring node.

It is recommended that the new node shall send the information to one neighbor node; the neighbor node can act as a communication proxy between the newly deployed node and a cloud server. The server then processes the information with global network knowledge, and send/set network address configuration to the new node.

When a communication proxy is used, application protocol needs to be implemented in the Host MCU, where the proxy protocol header shall be placed in unicast payload and include the actual source/destination addresses.

4.0 Stationary & Mobile Networks

If the network is composed of both stationary and mobile nodes, the stationary nodes can be configured with network address according to Section 3.0.
The mobile nodes configuration can take two design options:

1. Mobile nodes do not periodically update their network addresses. The mobile nodes can initialize with a network address under the same Network ID as stationary nodes, but with the second/third bytes as "0xFF"; or otherwise any address under a different Network ID to stationary nodes. The mobile nodes then periodically use Command Query [1] to discover neighboring stationary nodes, and select the one with strongest RSSI as its communication proxy. In this option, the stationary nodes virtually function as "access points" to mobile nodes.

2. Mobile nodes periodically update their network addresses. A mobile node can periodically uses Command Query [1] to discover neighboring stationary nodes, and processes the information at a remote server (i.e., with global network knowledge) or locally (depending on application environment) to re-configure its own network address. In this option, the mobile nodes and stationary nodes shall have the same Network ID and can relay unicast packets for each other. The mobile nodes may also use the "previous address" mode by setting the ADDRESS bit in Command CONFIG, so that packets sent to previous address can still be retrieved by the mobile.

5.0 All Mobile Networks

If the network is composed of all mobile nodes, at least a portion of nodes shall rely on another infrastructure such as GPS and/or cellular towers to configure network addresses. Other mobile nodes use the first portion of nodes as virtual "stationary nodes" to configure their own network addresses. It is however desired that the virtual stationary nodes are accessible to the rest mobile nodes.

6.0 Dynamic Address Configuration

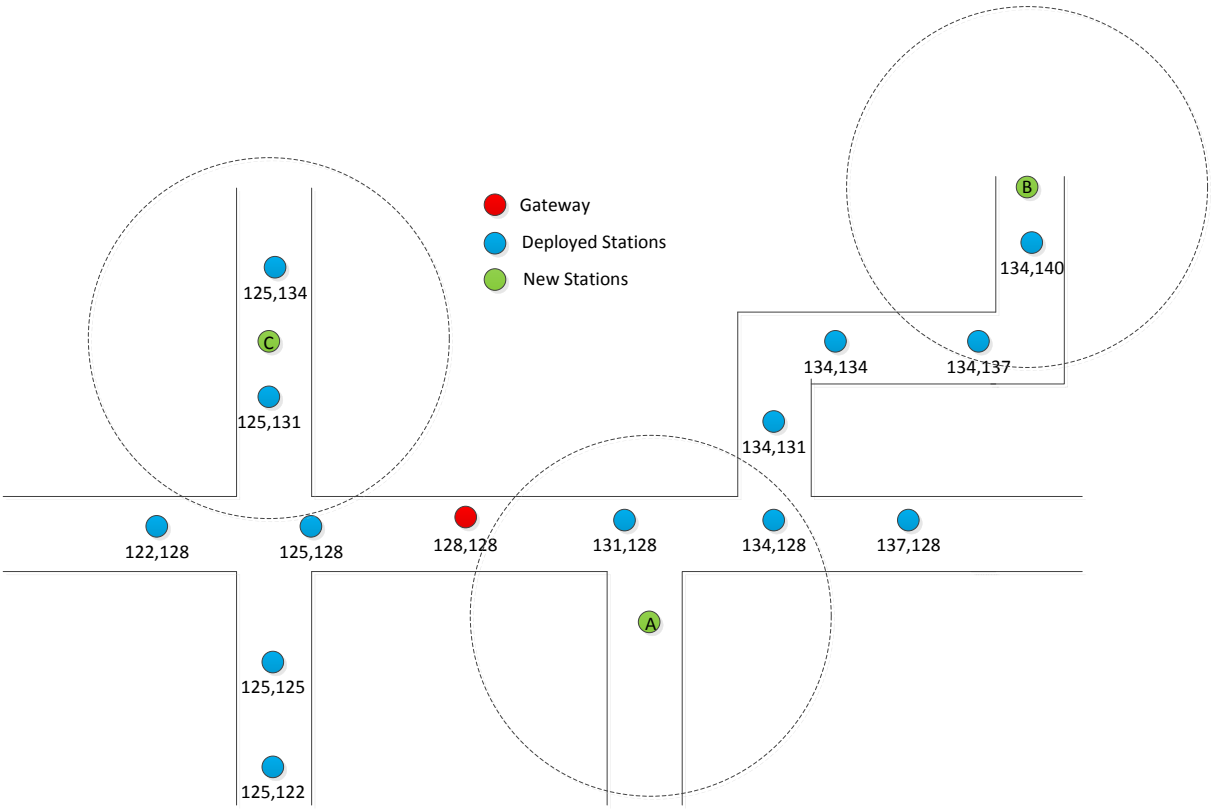

Figure 1: Typical Address Configuration with Both Stationary and Mobile Nodes

Here we further discusses how to dynamically configure the network address of a mobile or (new) stationary node given the information of its neighboring stationary nodes (network address and RSSI etc.), under the same Network ID.

Figure 1 shows a typical network address configuration with stationary and mobile nodes. In the figure, the red dot denotes the network gateway; the blue dots denote the deployed stationary nodes; and the green dots denote the new stationary nodes or mobile nodes.

For the gateway and deployed stationary nodes, the two bytes underneath the corresponding dot denotes the second (X) and third (Y) bytes of its network address. In an enclosed environment as shown in Figure 1, nodes {[125,122], [125,125], [125, 131], [125,134]} shall also be configured by Command SETROUTELIM [1], so that they won't route packets for nodes on any other "column". For example, [125, 134] won't relay packets with destination [134, 140]; otherwise unicast dead-end would be resulted and the packet would be dropped since [125, 134] does not

have any one-hop neighbor that is closer to [134, 140] in terms of Manhanttan distance in addressing.

The [Centre_X, Centre_Y, Delta_X, Delta_Y] of the nodes {[125,122], [125,125], [125, 131], [125,134]} can be configured as [125, 128, 1, 1], so that the "width" of gateway row and the columns is 3. Similarly, {[134,131], [134,134], [134,137], [134,140]} can be configured by Command SETROUTELIM as [134, 128, 1, 1].

For any new stationary node deployed or mobile nodes, it shall first collect the information of 2 neighboring stationary nodes with the strongest RSSI that are located on the same row or column.

For example, a new stationary node A finds the node [131, 128] as the strongest neighbor, and the node [134, 128] as the second strongest neighbor. The address configuration server also decides that the RSSI from A to [134, 128] is weaker than the RSSI from [131, 128] to [134, 128]; and the RSSI from A to [128, 128] is weaker than the RSSI from [131, 128] to [128, 128]. So the new node A can be configured with network address [131, 131] (second and third bytes) with SETTOUTELIM [Centre_X, Centre_Y, Delta_X, Delta_Y] as [131, 128, 1, 1].

For another example, a new stationary node B finds the node [134, 140] as the strongest neighbor, and the node [134, 137] as the second strongest neighbor. The address configuration server also decides that the RSSI from B to [134, 137] is weaker than the RSSI from [134, 140] to [134, 137]. So the new node B can be configured with network address [134, 143] as dependent on the RSSI from B to [134, 140]. The SETROUTELIM [Centre_X, Centre_Y, Delta_X, Delta_Y] shall also be configured the same as [134, 128, 1, 1].

For any mobile node, it can periodically update its network address configuration. For example, a mobile node C finds the node [125, 131] as the strongest neighbor, and the node [125, 134] as the second strongest neighbor. Node C can be configured with an address in-between, for example [125, 132], or [126, 132], [124, 132] given that the "width" of the column is 3. A mobile node is recommended to have a different X byte than stationary nodes on the column, and a different Y byte than stationary nodes on the row, in the use of address space. The SETROUTELIM [Centre_X, Centre_Y, Delta_X, Delta_Y] shall also be configured the same as [125, 128, 1, 1].

For the above nodes A, B and C, some global network information is required in the dynamic address configuration, where the new nodes can extend the contour of currently deployed nodes. As such the address configuration shall be done in a remote server and then sent to the required node. However, the address configuration can also be processed locally as dependent on the application, where the address of new nodes shall stay in the contour of currently deployed nodes (e.g., node C in the example).

In an open environment instead of enclosed environment, the Command SETROUTELIM may not be necessary. When used appropriately, the SETROUTELIM can prevent dead-ends of unicast packets in the address configurations as explained in above.

7.0 References

[1] OMESH Networks, “OPM15 Software API Guide”, version 3.2.0, available from **http://www.omeshnet.com/omesh**, Oct 10, 2011.

DISCLAIMER: THE DOCUMENTATION OR SOFTWARE IS PROVIDED TO YOU "AS IS," AND OMESH NETWORKS MAKE NO EXPRESS OR IMPLIED WARRANTIES WHATSOEVER WITH RESPECT TO ITS FUNCTIONALITY, OPERABILITY, OR USE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR INFRINGEMENT. WE EXPRESSLY DISCLAIM ANY LIABILITY WHATSOEVER FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR SPECIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST REVENUES, LOST PROFITS, LOSSES RESULTING FROM BUSINESS INTERRUPTION OR LOSS OF DATA, REGARDLESS OF THE FORM OF ACTION OR LEGAL THEORY UNDER WHICH THE LIABILITY MAY BE ASSERTED, EVEN IF ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.