INTERNET-DRAFT
IETF MANET Working Group
Expiration: 31 July 2005

Thomas Clausen
Emmanuel Baccelli
LIX, Ecole Polytechnique, France

31 January 2005

# Simple MANET Address Autoconfiguration
## draft-clausen-manet-address-autoconf-00.txt

Status of this Memo

This document is a submission to the Network Mobility Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the nemo@ietf.org mailing list.

Distribution of this memo is unlimited.



Abstract

In this draft, a simple autoconfiguration mechanism for MANETs is developed. The mechanism aims at solving the simple, but common, problem of one or more new nodes emerging in an existing network. A solution is proposed, which allows these new nodes to acquire an address and participate in the network. The method is simple, both algorithmically and in the requirements to the network. While this is a partial solution to the general autoconfiguration problem, the

mechanism described in this draft can satisfy the requirements for a great number of real-world situations. Though examples are given with OLSR [1] [11] being the routing protocol in use, nothing prevents the described mechanisms to work along with other routing protocols.

Table of Contents

## 1. Introduction

A Mobile Ad-hoc NETwork (MANET) is a collection of nodes which are able to connect on a wireless medium forming an arbitrary and dynamic network, routing traffic through multi-hop-paths in order to ensure connectivity between any two nodes in the network. Implicitly herein is the ability for the network topology to change over time as links in the network appear and disappear.

In order to enable communication between any two nodes in such a MANET, a routing protocol is employed. The abstract task of the routing protocol is to discover the topology (and, as the the network is dynamic, continuing changes to the topology) to ensure that each node is able to acquire a recent image of the network topology for constructing routes.

An issue, complementary to that of routing, emerges with respect to bootstrapping of the network. Routing protocols accomplish the task of discovering paths in a MANET, however a prerequisite to the correct functioning of routing protocols is that all nodes are identifiable by an unique IP-address. Subsequently, a mechanism for assigning (unique) addresses to MANET nodes is required.

A particularity of MANETs is, that the roles of ``terminal'' and ``network forming node'' (router) are not clearly separate. In principle, all nodes may act in both capacities simultaneously. An additional constraint is, that no assumptions with respect to a preexisting infrastructure can be made. Traditional mechanisms for host autoconfiguration, such as DHCP [7] or ZeroConf [10] or similar mechanisms all assume the presence of a ``server'', which can coordinate and assign addresses. Further, these mechanisms work on the assumption that direct communication between the ``server'' and all hosts in the local network is possible. Due to the multi-hop nature of MANETs, direct communication between an arbitrary host in the network and (any) server cannot be assumed.

In order to ensure the true autonomy of MANETs, a specific mechanism -- or adaptation of mechanism -- for address autoconfiguration of MANETs is required. Such a mechanism is described in the following.

### 1.1. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [5].

Several references are made to the OLSR terminology as described and employed in [1]. This document uses the following terminology:

- Node: a device capable of participating in a MANET.

- Neighbor Node: A node X is a neighbor node of node Y if node Y can hear node X.

- Multipoint Relay (MPR): A node which is selected by its neighbor, node X, to "re-transmit" all the broadcast messages that it receives from X, provided that the message is not a duplicate, and that the time to live field of the message is greater than one.

- Hello Messages: An OLSR node periodically broadcasts a Hello Message listing its neighbors. These messages are not forwarded, and serve the purpose of local neighborhood discovery and maintenance, as well as setting up Multipoint Relays.

- TC Messages: An OLSR node periodically broadcasts a TC Message listing its neighborhood link status. These messages are forwarded throughout the MANET, using MPR flooding, and serve the purpose of MANET topology discovery and maintenance.

### 1.2. Applicability

This document describes a simple address autoconfiguration mechanism aiming at solving a number of real-world situations with one or more new nodes emerging in an existing network. It is assumed that either at least one node in the network (typically, this might be a node providing Internet connectivity) is already configured or that, absent a previously configured node, an election can be undertaken to allow one node to self-configure and thereby initiate a network-wide autoconfiguration as described in this specification.

Even though examples are given with OSLR [1] [11] being the routing protocol in use, nothing prevents the described mechanism to work along with other routing protocols.

## 2. Problem Statement

The issue of autoconfiguration in MANETs is complex since, for a complete solution, issues such as ensuring uniqueness of addresses in independent MANETs which later merge, must be addressed: independent MANET must somehow select non-overlapping address-spaces, duplicate

address detection, conflict resolution -- and the issue of how to deal with ongoing data streams without loosing data or the requirement of specific application behavior.

In this draft, we aim for a simple solution to a simple problem: the connected case. A common situation occurs, in which an efficient and simple address autoconfiguration mechanism is desirable and sufficient. This situation is, where a MANET acts as an edge-extension to the Internet. I.e., nodes are interested in maintaining connection to each other and to the Internet. The implication is also, that nodes join or leave the MANET, but do not migrate (alone or in groups) between different MANETs with the expectation of maintaining connectivity. The topic of nodes migrating between different MANETs may better be addressed through mechanisms such as NEMO [6].

The mechanism, developed in this draft, is therefore targeted explicitly at the connected case described above. While this is a particular solution to a particular problem, there is indeed a need to develop a simple and light-weight mechanism efficient for these stated scenarios.

The address autoconfiguration mechanism in this draft is specified as an extension to OLSR [1]. However, nothing prevents the mechanism to be work with other routing protocols as well.

## 3. Simple Address Autoconfiguration Solution Overview

This section will outline the functioning of the address autoconfiguration mechanism.

The following two terms will be used for the remainder of this draft: a "new node" is a node which is not yet assigned an address, and thus not is part of a MANET. An "MANET node" is a node which is assigned an address and which is part of the network. A "configurating node" is an MANET node, which is currently assisting a new node in acquireing an address.

- MANET nodes behave as specified by the routing protocol in use, say OLSR [1]. Additionally, they emit ADDR_BEACON messages, to signal to new nodes that they may act as configurating nodes. This is detailed in the following section.

- New nodes do not participate with the routing protocol in use: for example with OLSR, they do not emit HELLO and TC messages. However they listen for ADDR_BEACON messages.

- From among the MANET nodes emitting ADDR_BEACON messages, one configurating node is selected, and a request for address configuration is issued through an ADDR_CONFIG message. The goal is for the configurating node to provide the new node with first a temporary local address, then a permanent global address.

This process of acquiring a local, temporary address, and the task of acquiring a global address are detailed in the following sections. Packet formats are proposed in the case of OLSR.

## 4. Local Beaconing

Each MANET node, must ensure that it has the ability to provide temporary addresses from a private address space to new nodes. It is important that, within a region, these temporary addresses are unique, i.e. that no two new nodes within the same neighborhood are assigned the same temporary address. In order to ensure this, a predefined address space is allocated to use for ``temporary addresses''. The task is to ensure that this address space is divided, without overlap, between nodes in a region of the network:

- Each MANET node will, independently, select a continuous address sequence from the address space allocated for ``temporary addresses''.

- Each MANET node will signal, with periodic ADDR_BEACON messages, this selected sequence. ADDR_BEACON messages are transmitted to neighbor nodes only, i.e. are not forwarded.

- Each node will record the address sequences, selected by all its neighbor nodes.

If, upon receiving an ADDR_BEACON message, a node detects that there is a conflicting address sequence selection, arbitration must happen. In this case:

- If no nodes in the conflict are acting as configurating nodes, arbitration is carried out simply by having the conflicting node with the lowest ID (IP-address) select a new, unused address-sequence.

- If one or more conflicting nodes are acting as configurating node(s), arbitration must aim at allowing ongoing configuration sessions to complete.

In order to accommodate this, all configuration nodes ``narrow'' their selected address-sequence to contain only the address(es) which are currently assigned to new nodes. This is included in the next ADDR_BEACON. Nodes which are not currently acting as configuration nodes, select non-conflicting address sequences. If a conflict between two configurating nodes remains, the node which has the lowest ID (IP address) must yield.

If OLSR is the routing protocol in use, the ADDR_BEACON message can use the format specified in the following figure. [1] specifies the values of Message Size, Originator Address, Message Sequence Number and Vtime.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  ADDR_BEACON  |     Vtime     |         Message Size          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Originator Address                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |       1       |       0       |    Message Sequence Number    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Address Sequence Start                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Address Sequence Stop                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   :                    Currently Used Addresses                   :
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

In case of ``narrowing down'' the address-sequence to only currently used addresses, the ``Address Sequence Start'' and ``Address Sequence Stop'' are both set to zero.

Each node will periodically send ADDR_BEACON messages, listing both its address sequence and the addresses which are currently in use. In case of a conflict, a recipient node can detect if the node with which it is conflicting is active as configurating node. If both nodes are active as configurating nodes, the nodes can detect a conflict in the addresses actually selected.

If OLSR is the routing protocol in use, ADDR_BEACON messages are transmitted piggybacked in the same OLSR packet as OLSR HELLO messages.

## 5. Aquireing a Local Address

The first task of a new node is to associate itself with a MANET node. Thus, the new node listens for ADDR_BEACON messages and selects one ``configurating node''. An ADDR_CONFIG message is then created and transmitted, in order to request address configuration from the selected configurating node. Absent an IP address, the MAC address of the new node must be included, in order to uniquely identify the new node.

Upon receiving an ADDR_CONFIG message, the configurating node assigns a local address to the new node, and signals this assignment through another ADDR_CONFIG message. Additionally, the configurating node marks the assigned address as ``used'' in its ADDR_BEACON messages.

Upon receiving a local address through an ADDR_CONFIG message, the new node can slowly start participating locally with the routing protocol in use.  For example, if OLSR is used, it can start sending HELLO messages, including only the configurating node as neighbor. The goal is to allow the new and configurating node to track each other (i.e. it allows both nodes to ``reset'', should the link disappear before a global address was assigned to the new node), while not causing the new node to be advertised to the network. Advertising a node with a non-unique address might lead to data loss, routing loops etc.

If a new node does not receive an ADDR_CONFIG reply, it may either (i) retransmit the ADDR_CONFIG to the same configurating node, or (ii) give up and select an alternative configuration node. Absent the local participation of the new node in the routing protocol (i.e. with OLSR, the HELLO message exchange described above) the configurating node may (i) retransmit its ADDR_CONFIG reply, or (ii) give up, in which case any temporarilly assigned addresses will be reclaimed.

If OLSR is the routing protocol in use, the ADDR_CONFIG message can use the format specified in following figure.  [1] specifies the values of Message Size, Originator Address, Message Sequence Number and Vtime.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  ADDR_CONFIG  |     Vtime     |         Message Size          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                      Originator Address                       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |       1       |       0       |    Message Sequence Number    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                 Configurating Node Address                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    :                        MAC Addresses                          :
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                    Assigned Local Address                     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                   Assigned Global Address                     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

If the ``Assigned Local Address'', ``Assigned Global Address'' and ``Originator Address'' fields are all set to zero, the ADDR_CONFIG message is a request to the ``Configurating Node'' to perform local address assignment.

If the ``Assigned Local Address'' is non-zero (i.e. contains an actual address) and ``Originator Address'' is non-zero, but the ``Assigned Global Address'' field is set to zero, the ADDR_CONFIG message is an assignment of a temporary local address. I.e. this is the reply to a new node, generated by a configurating node.

The ``Assigned Global Address'' field is discussed in the next section.

## 6. Global Address Assignment

When local participation of the new node in the routing protocol has started (i.e. with OLSR, the HELLO message exchange commences between the new and configurating node), local address assignment is completed, and the task of acquireing a global address can commence. The configurating node is in charge of acting on behalf of the new node, with respect to acquireing this global address. Since the configurating node is already part of the MANET, a multitude of different mechanisms can be employed. One such mechanism for acquiring a global address would be for the configurating node to act as a modified DHCP

proxy [8] and transmit a request to an existing DHCP server in the network.

Another option would be to consult the nodes' topology table. This table (in a relatively stable state) contains all destinations (thus addresses) of the network. The configurating node can thus pick a non-used address and assign to the new node. In that case, in order to prevent duplicate address assignment, the configurating node advertises the selected address to the MANET. If a node detects that its address is being re-used, it can signal the conflict to the originator of the ``offending'' advertisement.

If OLSR is the routing protocol in use, the configurating node includes the selected address in a few TCs. If a node receives a TC containing its own address (or an address, which the node has claimed for a new node) AND if the originator of the message is not the node itself nor an MPR of the node, a duplicate address assignment is detected. The detecting node can then communicate this to the originator of the offending TC, with the purpose of resolving the conflict.

Once the configurating node has acquired a globally unique address, it is assigned to the new node through an ADDR_CONFIG message, containing the same ``Assigned Local Address'' and ``Originator Address'' as before, but with a non-zero address in the ``Assigned Global Address'' field. This is then the ticket for the new node to participate fully in the MANET.

The configurating node will continue to transmit this ADDR_CONFIG message periodically until it detects that the new node has taken it into account. With OLSR, thw configurating node can detect this either when the HELLO messages from the new node's assigned local address cease, or when an ADDR_CONFIG message from the new node is received, listing the new nodes global address in both the originator field and the ``Assigned Global Address'' field, the ``Assigned Local Address'' and the ``MAC address'' fields.

## 7. Overhead Estimation

The overhead incurring from the mechanism specified in this draft comes from primarily three sources: (i) periodic beaconing of ADDR_BEACON messages, (ii) address request/replies through ADDRmessages, and (iii) discovery of a globally unique address.

ADDR_BEACON messages and ADDR_CONFIG messages are local, i.e. no flooding operations incur. ADDR_CONFIG messages are furthermore only

transmitted while nodes are being configured, and are of limited size (24 bytes + size of MAC address). Each configuration cycle incurs 4 messages. The overall overhead, incurred through this procedure, is therfore negligible.

With OLSR, ADDR_BEACON messages are transmitted in the same OLSR packets as OLSR HELLO messages (MTU permitting), thus the number of transmissions required remains constant as compared to OLSR. Except when an node configuration is ongoing, the additional overhead incurred from ADDR_BEACON amounts to 20 bytes.

on the other hand, the discovery of a globally unique message depends on the mechanism employed. Assuming a decentralized mechanism, where an unused address is picked from the topology table and is probed through including this address in a TC emission, the additional over-head per TC message for that node is 4 bytes. This is offset by the fact that if an address is assigned to the new node, topological information is already present in the network, allowing the node immediate participation.

## 8. Acknowledgements

The authors would like to thank Hitachi Labs Europe for their support.

## 9. Authors' Addresses

Thomas Heide Clausen,
Project PCRI
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: T.Clausen@computer.org

Emmanuel Baccelli
HITACHI Labs Europe/ Project PCRI,
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,

Email: Emmanuel.Baccelli@inria.fr

## 10. References

[1] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol. Request for Comments (Experimental) 3626, Internet Engineering Task Force, October 2003.

[2] T. Clausen, G. Hansen, L. Christensen, G. Behrmann, The Optimized Link State Routing Protocol - Evaluation Through Experiments and Simulation. Proceedings of the Fourth Wireless Personal Multimedia Communications, September 2001.

[3] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. Request for Comments (Best Current Practice) 2119, Internet Engineering Task Force, March 1997.

[4] R. Wakikawa et al. Global Connectivity for IPv6 Mobile Ad Hoc Networks (work in progress). Internet Draft (draft-wakikawa-manet-globalv6-03.txt), Internet Engineering Task Force, October 2003.

[5] T. Clausen, P. Jacquet, L. Viennot, Comparative study of routing protocols for mobile ad-hoc networks. Proceedings of IFIP Med-Hoc-Net 2002, September 2002.

[6] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Nemo Basic Support Protocol (work in progress). Internet Draft (draft-ietf-nemo-basic-support-02), Internet Engineering Task Force, December 2003.

[7] R. Droms, Dynamic host configuration protocol, RFC 2131, Internet Engineering Task Force, March 1997.

[8] M. Patrick, Dhcp Relay Agent Information Option, RFC 3046, Internet Engineering Task Force, January 2001.

[9] A. Qayyum, L. Viennot, A. Laouiti, Multipoint relaying: An Efficient Technique for Flooding in Mobile Wireless Networks. INRIA Research Report RR-3898, Project Hipercom, March 2000.

[10] A. Williams, Requirements for Automatic Configuration of IP Hosts. Internet Draft, draft-ietf-zeroconf-reqts-12.txt, September 2002, Work in progress.

[11] E. Baccelli, T. Clausen, A Simple Address Autoconfiguration Mechanism for OLSR, IEEE International Symposium on Circuits and Systems, ISCAS 2005.

## 11. Changes

This is the initial version of this specification.

## 12. IANA Considerations

This document does currently not specify IANA considerations.

## 13. Security Considerations

This document does not specify any security considerations.

## 14. Copyright