

MANET Autoconfiguration (Autoconf)  
Internet-Draft  
Expires: February 2, 2008

E. Baccelli (Ed.)  
INRIA  
K. Mase  
Niigata University  
S. Ruffino  
Telecom Italia  
S. Singh  
Samsung  
August 2007

**Address Autoconfiguration for MANET: Terminology and Problem Statement**  
**draft-ietf-autoconf-statement-01**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on February 2, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

## Abstract

Traditional dynamic IPv6 address assignment solutions are not adapted to mobile ad hoc networks. This document elaborates on this problem, states the need for new solutions, and requirements to these solutions.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Terminology . . . . .</a>	<a href="#">4</a>
<a href="#">3.</a>	<a href="#">Deployment Scenarios . . . . .</a>	<a href="#">5</a>
<a href="#">3.1.</a>	<a href="#">Standalone MANET . . . . .</a>	<a href="#">5</a>
<a href="#">3.2.</a>	<a href="#">Connected MANET . . . . .</a>	<a href="#">5</a>
<a href="#">3.3.</a>	<a href="#">Deployment Scenarios Selection . . . . .</a>	<a href="#">5</a>
<a href="#">4.</a>	<a href="#">Problem Statement . . . . .</a>	<a href="#">7</a>
<a href="#">4.1.</a>	<a href="#">MANET Autoconfiguration Goals . . . . .</a>	<a href="#">7</a>
<a href="#">4.2.</a>	<a href="#">Existing Protocols' Shortcomings . . . . .</a>	<a href="#">7</a>
<a href="#">4.2.1.</a>	<a href="#">Lack of Multi-hop Support . . . . .</a>	<a href="#">7</a>
<a href="#">4.2.2.</a>	<a href="#">Lack of Dynamic Topology Support . . . . .</a>	<a href="#">8</a>
<a href="#">4.2.3.</a>	<a href="#">Lack of Network Merging Support . . . . .</a>	<a href="#">8</a>
<a href="#">4.2.4.</a>	<a href="#">Lack of Network Partitioning Support . . . . .</a>	<a href="#">9</a>
<a href="#">4.3.</a>	<a href="#">MANET Autoconfiguration Issues . . . . .</a>	<a href="#">9</a>
<a href="#">4.3.1.</a>	<a href="#">Address and Prefix Generation . . . . .</a>	<a href="#">9</a>
<a href="#">4.3.2.</a>	<a href="#">Prefix and Address Uniqueness Requirements . . . . .</a>	<a href="#">10</a>
<a href="#">4.3.3.</a>	<a href="#">MANET Border Routers Related Issues . . . . .</a>	<a href="#">10</a>
<a href="#">5.</a>	<a href="#">Solutions Considerations . . . . .</a>	<a href="#">12</a>
<a href="#">6.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">13</a>
<a href="#">7.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">14</a>
<a href="#">8.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">15</a>
	<a href="#">Contributors . . . . .</a>	<a href="#">16</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">17</a>
	<a href="#">Intellectual Property and Copyright Statements . . . . .</a>	<a href="#">18</a>



## **1. Introduction**

A Mobile Ad hoc NETwork (also known as a MANET [2] [1]) consists of a loosely connected set of MANET routers. Each MANET router embodies IP routing/forwarding functionality and may also incorporate host functionality. These routers dynamically self-organize and maintain a routing structure among themselves, regardless of the availability of a connection to any infrastructure. MANET routers may be mobile and may communicate over symmetric or assymetric wireless links. They may thus join and leave the MANET at any time.

However, prior to participation in IP communication, each MANET router that does not benefit from appropriate static configuration needs to automatically acquire at least one IP address, that may be required to be unique within a given scope, or to be topologically appropriate.

Standard automatic IPv6 address/prefix assignment solutions [5], [3] [4] do not work "as-is" on MANETs due to ad hoc networks' unique characteristics [2], therefore new or modified mechanisms are needed. This document thus details and categorizes the issues that need to be addressed.



## **2. Terminology**

This document uses the MANET architecture terminology defined in [2], as well as the following terms :

MANET Local address (MLA) - An IP address configured on an interface of a router in a MANET and valid for communication inside this MANET.

Global address - An IP address configured on a MANET router and valid for communication with routers in the Internet, as well as internally within the MANET.

Standalone MANET - An independent ad hoc network, which does not contain a border router through which it is connected to the Internet.

Network merger - The process by which two or more previously disjoint ad hoc networks get connected.

Network partitioning - The process by which an ad hoc network splits into two or more disconnected ad hoc networks.

Address generation - The process of selecting a tentative address in view to configure an interface.

Address assignment - The process of configuring a generated address on an interface.

Pre-service address uniqueness - The property of an address which is assigned at most once within a given scope, and which is unique, before it is being used.

In-service address uniqueness - The property of an address which was assigned at most once within a given scope, and which remains unique over time, after the address has started being used.



### **3. Deployment Scenarios**

Automatic configuration of IP addresses and/or prefixes on MANET interfaces is necessary in a number of deployment scenarios. This section outlines the different categories of scenarios that are considered.

#### **3.1. Standalone MANET**

Standalone MANETs are not connected to any external network: all traffic is generated by routers and hosts in the MANET and destined to routers or hosts in the same MANET.

Routers joining a standalone MANET may either have (i) no previous configuration, or (ii) pre-configured local or global IP addresses (or prefixes). Due to potential network partitions and mergers, standalone MANETs may be composed of routers of either types.

Typical instances of this scenario include private or temporary networks, set-up in areas where neither wireless coverage nor network infrastructure exist (e.g. emergency networks for disaster recovery, or conference-room networks).

#### **3.2. Connected MANET**

Connected MANETs have, contrary to standalone MANETs, connectivity to one or more external networks (leaf networks, or other networks that provide Internet connectivity) by means of one or more MANET border router [2]. MANET routers may generate traffic destined to remote hosts across these external networks, as well as to destination inside the MANET.

Again, routers joining a connected MANET may either (i) have no previous configuration, or (ii) already own pre-configured local or global IP addresses (or prefixes).

Typical instances of this scenario include public wireless networks of scattered fixed WLAN Access Points participating in a MANET of mobile users, and acting as MANET border routers. Another example of such a scenario is coverage extension of a fixed wide-area wireless network, where one or more mobile routers in the MANET are connected to the Internet through technologies such as UMTS or WiMAX.

#### **3.3. Deployment Scenarios Selection**

Both "Standalone MANET" and "Connected MANET" scenarios are to be addressed by solutions for MANET autoconfiguration. Note that solutions should also aim at addressing cases where a MANET transits





from one scenario to an other.

## **4. Problem Statement**

This section details the goals of MANET autoconfiguration, and highlights the shortcomings of existing autoconfiguration protocols. A taxonomy of autoconfiguration issues on MANETs is then elaborated.

### **4.1. MANET Autoconfiguration Goals**

A MANET router needs to configure IP addresses and/or prefixes on its non-MANET interfaces. In addition, it needs to configure a link local address, a /128 and/or an MLA on its MANET interface. A MANET router may also configure a IP prefix shorter than /128 on its MANET interface, provided prefix uniqueness is guaranteed [2].

The primary goal of MANET autoconfiguration is thus to provide mechanisms for IPv6 prefix allocation and address assignment, that are suited for mobile ad hoc environments. Note that this task is distinct from that of propagating knowledge about address or prefix location, as a routing protocol does (see for example [8], [9]), or as described in [7].

The mechanisms employed by solutions to be designed must address the distributed, multi-hop nature of MANETs [2], and be able to follow topology and connectivity changes by (re)configuring addresses and/or prefixes accordingly.

### **4.2. Existing Protocols' Shortcomings**

Traditional dynamic IP address assignment protocols, such as [5], [3] or [4], do not work as-is on MANETs due to these networks' unique properties. This section overviews the shortcomings of these solutions in mobile ad hoc environments.

#### **4.2.1. Lack of Multi-hop Support**

Traditional solutions assume that a broadcast directly reaches every router or host on the subnetwork, whereas this generally is not the case in MANETs (see [2]). Some routers in the MANET will typically assume multihop broadcast, and expect to receive through several intermediate relayings by peer MANET routers. For example, in Fig. 1, the MANET router MR3 cannot communicate directly with a DHCP server [4] that would be available through a MANET border router, since the server and the MANET router are not located on the same logical link. While some DHCP extensions (such as the relay-agent [11]) overcome this issue in a static network, it is not the case in a dynamic topology, as explained below.



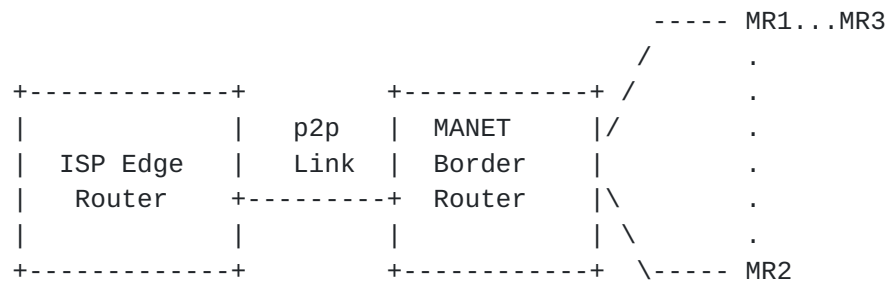


Fig. 1. Connected MANET router topology.

#### 4.2.2. Lack of Dynamic Topology Support

A significant proportion of the routers in the MANET may be mobile with wireless interface(s), leading to ever changing neighbor sets for most MANET routers (see [1]). Therefore, network topology may change rather dynamically compared to traditional networks, which invalidates traditional delegation solutions that were developed for infrastructure-based networks, such as [11], which do not assume intermittent reachability of configuration server(s), and a potentially ever changing hierarchy among devices. For instance, in Fig. 1, even if MR1 would be able to delegate prefixes to MR3 with DHCP [4], it cannot be assumed that MR1 and MR3 will not move and become unable to communicate directly.

#### 4.2.3. Lack of Network Merging Support

Network merging is a potential event that was not considered in the design of traditional solutions, and that may greatly disrupt the autoconfiguration mechanisms in use (see [2]). Examples of network merging related issues include cases where a MANET A may feature routers and hosts that use IP addresses that are locally unique within MANET A, but this uniqueness is not guaranteed anymore if MANET A merges with another MANET B. If address uniqueness is required within the MANET (see [Section 4.3.2](#)), issues arise that were not accounted for in traditional networks and solutions. For instance, [5] and [3] test address uniqueness via messages that are sent to neighbors only, and as such cannot detect the presence of duplicate addresses configured within the network but located several hops away. However, since MANETs are generally multi-hop, detection of duplicate addresses over several hops is a feature that may be required for MANET interface address assignment (see [Section 4.3.2](#)).



#### **4.2.4. Lack of Network Partitioning Support**

Network partitioning is a potential event that was not considered in the design of traditional solutions, and that may invalidate usual autoconfiguration mechanisms (see [2]). Examples of related issues include cases such as a standalone MANET, whereby connection to the infrastructure is not available, possibly due to network partitioning and loss of connectivity to a MANET border router. The MANET must thus function without traditional address allocation server availability. While stateless protocols such as [5] and [3] could provide IP address configuration (for MANET interfaces, loopback interfaces), these solutions do not provide any mechanism for allocating "unique prefix(es)" to routers in order to enable the configuration of host interfaces.



Fig. 2. Standalone MANET router topology.

### **4.3. MANET Autoconfiguration Issues**

Taking into account the shortcomings of traditional solutions, this section categorizes general issues with regards to MANET autoconfiguration.

#### **4.3.1. Address and Prefix Generation**

The distributed nature of MANETs brings the need for address generation algorithms that are not always based on traditional "client-server" schemes and hierarchies to provide MANET routers with addresses and prefixes. In addition, the multi-hop aspect of mobile ad hoc networking makes it difficult to totally avoid address and prefix duplication a priori over all the MANET.





#### **4.3.2. Prefix and Address Uniqueness Requirements**

If prefix or address uniqueness is required within a specific scope, and if the address/prefix generation mechanism in use does not totally avoid address/prefix duplication, then additional issues arise. This section overviews these problems.

Pre-service Issues -- One category of problems due to address or prefix uniqueness requirements are called pre-service issues. Conceptually, they relate to the fact that before a generated address or prefix is assigned and used, it should be verified that it will not create an address conflict within the specified scope. This is essential in the context of routing, where it is desirable to reduce the risks of loops due to routing table pollution with duplicate addresses.

In-Service Issues -- Another category of problems due to address and prefix uniqueness are called in-service issues. They come from the fact that even if an assigned address or prefix is currently unique within the specified scope, it cannot be ensured that it will indeed remain unique over time.

Phenomena such as MANET merging and MANET partitioning may bring the need for checking the uniqueness (within the specified scope) of addresses or prefixes that are already assigned and used. This need may depend on (i) the probability of address conflicts, (ii) the amount of the overhead for checking uniqueness of addresses, and (iii) address/prefix uniqueness requirements from applications.

For instance, if (i) is extremely low and (ii) significant, checking uniqueness of addresses and prefixes may not be used. If on the other hand (i) is not extremely low, checking uniqueness of addresses and prefixes should be used. In any case, if the application has a hard requirement for address uniqueness assurance, checking uniqueness of addresses and prefixes should always be used, no matter how unlikely is the event of address conflict.

#### **4.3.3. MANET Border Routers Related Issues**

Another category of problems concern MANET border router(s) management.

In the case where multiple MANET border routers are available in the MANET, providing access to multiple address configuration servers, specific problems arise. One problem is the way in which global prefixes are managed within the MANET. If one prefix is used for the whole MANET, partitioning of the MANET may result in invalid routes towards MANET routers, over the Internet. On the other hand, the use



of multiple network prefixes guarantees traffic is unambiguously routed from the hosts/routers in the Internet towards the MANET border router responsible for one particular prefix. However, asymmetry in the routers' choice of ingress/egress MANET border router can lead to non-optimal paths followed by inbound/outbound data traffic, or to broken connectivity, if egress filtering is being done.

When a device changes its MANET border router attachment, some routes may be broken, affecting MANET packet forwarding performance and applications. In a multiple border router / multiple-prefixes MANET, frequent reconfiguration could cause a large amount of control signalling (for instance if [\[5\]](#) is used "as-is").



## **5. Solutions Considerations**

Solutions must achieve their task with (i) low overhead, due to scarce bandwidth, and (ii) low delay/convergence time, due to the dynamicity of the topology. The evaluation of such criteria may depend on the targeted network properties, which include (but are not limited to) node cardinality, node mobility characteristics, etc.

Solutions are to be designed to work at the network layer and thus to apply to all link types. However, in situations where link-layer multicast is needed it is possible that on some link types (e.g. NBMA links), alternative mechanisms or protocols specifying operation over a particular link type would be required.

Solutions must interact with existing protocols in a way that leverages as much as possible appropriate mechanisms that are deployed. For instance, besides the possible use of the well-known IPv6 multicast addresses defined for neighbor discovery in [3] (e.g. for Duplicate Address Detection), solutions may as well use some addresses defined in [10] for auto-configuration purposes.

Solutions must also take into account the security and trust issues that are specific to ad hoc networking (see [Section 6](#)).



## **6. Security Considerations**

Address configuration in MANET could be prone to security attacks, as in other types of IPv6 networks. Security threats to IPv6 neighbor discovery were discussed in SEND WG and described in [6]: three different trust models are specified, with varying levels of trust among network nodes and routers. Among them, the model by which no trust exists among nodes may be suitable a priori for most ad hoc networks. However, the other two models may be applicable in some cases, for example when a trust relationship exists between an operator and some MANET routers, or between military devices that are in the same unit. Although [6] does not explicitly address MANETs, the trust models it provides for ad hoc networks can be valid also in the context of MANET autoconfiguration.

It is worth noting that analysis of [6] is strictly related to Neighbor Discovery, Neighbor Unreachability Detection and Duplicate Address Detection procedures, as defined in [3] and [5]. As explained in the present document, current standard procedures cannot be used as-is in MANET context to achieve autoconfiguration of MANET routers and, therefore, design of new mechanisms can be foreseen.

In this case, although security threats and attacks defined in [6] could also apply in presence of new solutions, additional threats and attacks could be possible (e.g., non-cooperation in message forwarding in multi-hop communications). Therefore, the security analysis has to be further extended to include threats, specific to multi-hop networks and related to the particular address configuration solution.

General security issues of ad hoc routing protocols' operations are not in the scope of MANET autoconfiguration.





## **7. IANA Considerations**

This document does currently not specify IANA considerations.

## **8. Informative References**

- [1] Macker, J. and S. Corson, "MANET Routing Protocol Performance Issues and Evaluation Considerations", [RFC 2501](#), January 1999.
- [2] Macker, J., Chakeres, I., and T. Clausen, "Mobile Ad hoc Network Architecture", ID [draft-ietf-autoconf-manetarch](#), February 2007.
- [3] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IPv6", [RFC 2461](#), December 1998.
- [4] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6", [RFC 3315](#), July 2003.
- [5] Narten, T. and S. Thomson, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
- [6] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.
- [7] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", [RFC 4191](#), 2005.
- [8] Moy, J., "OSPF version 2", [RFC 2328](#), 1998.
- [9] Moy, J., Coltun, R., and D. Ferguson, "OSPF for IPv6", [RFC 2740](#), 1999.
- [10] Chakeres, I., "Internet Assigned Numbers Authority (IANA) Allocations for the Mobile Ad hoc Networks (MANET) Working Group", ID [draft-ietf-manet-iana](#), May 2007.
- [11] Patrick, M., "DHCP Relay Agent Information Option", [RFC 3046](#), 2001.



## Contributors

This document is the result of joint efforts, including those of the following contributors, listed in alphabetical order: C. Adjih, C. Bernardos, T. Boot, T. Clausen, C. Dearlove, H. Moustafa, C. Perkins, A. Petrescu, P. Ruiz, P. Stupar, F. Templin, D. Thaler, K. Weniger.

Authors' Addresses

Emmanuel Baccelli  
INRIA

Phone: +33 1 69 33 55 11  
Email: Emmanuel.Baccelli@inria.fr

Kenichi Mase  
Niigata University

Phone: +81 25 262 7446  
Email: Mase@ie.niigata-u.ac.jp

Simone Ruffino  
Telecom Italia

Phone: +39 011 228 7566  
Email: Simone.Ruffino@telecomitalia.it

Shubhranshu Singh  
Samsung

Phone: +82 31 280 9569  
Email: Shubhranshu@gmail.com



## Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

