

MANET Autoconfiguration (Autoconf)
Internet-Draft
Expires: October 5, 2007

E. Baccelli (Ed.)
INRIA
K. Mase
Niigata University
S. Ruffino
Telecom Italia
S. Singh
Samsung
April 3, 2007

**Address Autoconfiguration for MANET: Terminology and Problem Statement
draft-baccelli-autoconf-statement-03**

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 October 5, 2007.

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

1.	Introduction	3
2.	Terminology	4
3.	Deployment Scenarios	5
3.1.	Standalone MANET	5
3.2.	Connected MANET	5
3.3.	Deployment Scenarios Selection	5
4.	Problem Statement	6
4.1.	MANET Autoconfiguration Goals	6
4.2.	Existing Solutions' Shortcomings	6
4.2.1.	Lack of Multi-hop Support	6
4.2.2.	Lack of Dynamic Topology Support	7
4.2.3.	Lack of Network Merging Support	7
4.2.4.	Lack of Network Partitionning Support	7
4.3.	MANET Autoconfiguration Issues	8
4.3.1.	Address and Prefix Generation	8
4.3.2.	Address Uniqueness Requirements	8
4.3.3.	MANET Border Routers Related Issues	9
5.	Security Considerations	11
6.	IANA Considerations	12
7.	Informative References	13
	Contributors	14
	Authors' Addresses	15
	Intellectual Property and Copyright Statements	16

1. Introduction

Mobile ad hoc networks (also known as MANETs [\[2\]](#) [\[1\]](#)) are networks composed of mobile devices that communicate over wireless media, which dynamically self-organize multi-hop IP communication between each other, and such regardless of the availability of a connection to any infrastructure.

However, prior to participation in IP communication, each MANET interface 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.

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

2. Terminology

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. The key words "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](#)].

In addition, this document uses the MANET architecture terminology defined in [[2](#)], as well as the following terms :

Local address - An IP address configured on an interface of a router in a MANET and valid for communication inside this MANET. A local address MUST NOT be used for communication including routers outside the 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 at this given point in time, within a given scope.

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, as the address is 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 MANET nodes and destined to nodes 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 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, typically the Internet, by means of one or more MBR (Manet Border Router, see [2]). MANET routers may generate traffic destined to remote hosts accross 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 (i) 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 MBRs. 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" scenario and "Connected MANET" scenarii are to be addressed by solutions for MANET autoconfiguration.

4. Problem Statement

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

4.1. MANET Autoconfiguration Goals

A MANET router needs to configure an IPv6 prefix(es) on its host interface and/or an IPv6 address on its loopback interface. Besides, it needs to configure a /128 and/or a link local address on its MANET interface. A MANET router may also configure a 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.

These mechanisms 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.

Solutions must achieve their task with (i) low overhead, due to scarce bandwidth, and (ii) low delay, due to the dynamicity of the topology.

4.2. Existing Solutions' Shortcomings

Traditional dynamic IP address assignment solutions, 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 network, 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 an MBR.

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 an MBR. The MANET must thus function without traditional 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. Moreover, [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 is required in most cases of MANET interface address assignment (see [Section 4.3.2](#)).



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 central 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.](#) Address Uniqueness Requirements

If 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 uniqueness requirements are called pre-service issues. Conceptually, they relate to the fact that before a generated address 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 uniqueness are called in-service issues. They come from the fact that even if an assigned address 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 can bring the need for checking the uniqueness (within the specified scope) of addresses that are already assigned and used, if in-service address uniqueness is required.

4.3.3. MANET Border Routers Related Issues

Another category of problems concern MBR management.

MBR Mobility -- Some addresses may be configured by servers available through MBRs that may themselves be mobile and that may therefore leave the MANET. In this case, global addresses used by routers in the MANET may no longer be valid.

MBR Multiplicity -- In the case where multiple MBRs 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 invalid routes in the Internet towards MANET routers. On the other hand, use of multiple network prefixes guarantees traffic is unambiguously routed towards the MBR responsible for one particular prefix, but asymmetry in the routers' choice of ingress/egress MBR can lead to non-optimal paths followed by inbound/outbound data traffic. When a device changes its MBR attachment, some routes may be broken, affecting MANET packet forwarding performance and applications.

IPv6 Specifications -- Additional problems come from issues with current IPv6 specifications. For example, the strict application of [5] may lead to check every IPv6 unicast address for uniqueness: in a multiple-MBR / multiple-prefixes MANET, this could bring to a large amount of control signalling, due to frequent reconfiguration.

Moreover, IPv6 does not currently specify an address scope that is appropriate to fit the scope of a MANET, which could lead to undesirable behavior such as MBRs leaking MANET local traffic outside the MANET.

5. Security Considerations

Address configuration in MANET could be prone to security attacks, as in other type of IPv6 networks. Security threats to IPv6 neighbor discovery are discussed in [6]: in particular, analysis includes trust model and threats for a specific ad hoc network scenario, where all the routers share a common link (i.e. they are one hop away from each other, full-meshed connectivity is available). Although the document does not explicitly address MANETs, where routers can be multiple hop away from each other, the trust model it provides could be valid also in the context of MANET autoconfiguration. It is also worth noting that, in case of MANET connected to the Internet, other threats defined in [6] could apply here, e.g. attacks involving routers and DoS attacks on Duplicate Address Detection procedures.

The security analysis has to be further extended to include threats, specific to multi-hop networks and related to the address configuration process in particular. However, general security issues of ad hoc routing protocols' operations are not in the scope of MANET autoconfiguration.

6. IANA Considerations

This document does currently not specify IANA considerations.

7. 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.

Contributors

This document is the result of joint efforts, including those of the following contributors, listed in alphabetical order: C. Adjih (INRIA), T. Clausen (Ecole Polytechnique), C. Perkins (Nokia), P. Ruiz (University of Murcia), P. Stupar (Telecom Italia), D. Thaler (Microsoft).

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.

Acknowledgment

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

