

MANET Autoconfiguration (Autoconf)
Internet-Draft
Expires: August 3, 2008

E. Baccelli (Ed.)
INRIA
K. Mase
Niigata University
S. Ruffino
Telecom Italia
S. Singh
Samsung
January 31, 2008

Address Autoconfiguration for MANET: Terminology and Problem Statement
draft-ietf-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/lid-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 August 3, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Internet-Draft

MANET Autoconf Problem Statement

January 2008

Abstract

This document states the problems pertaining to automatic IPv6 address configuration and prefix allocation in MANETs.

This draft currently contains terminology, target scenarios and goals for MANET autoconfiguration. Future versions of this document will also review the applicability of existing IPv6 address autoconfiguration and prefix allocation mechanisms, and security considerations.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	MANET Categories	5
3.1.	Subordinate MANET	5
3.1.1.	Scenarios of Subordinate MANETs	6
3.2.	Autonomous MANET	6
3.2.1.	Scenarios of Autonomous MANETs	7
4.	MANET Autoconfiguration Goals	8
5.	Security Considerations	9
6.	IANA Considerations	10
7.	References	11
7.1.	Normative References	11
7.2.	Informative References	11
	Contributors	13
	Authors' Addresses	14
	Intellectual Property and Copyright Statements	15

Internet-Draft

MANET Autoconf Problem Statement

January 2008

1. Introduction

As defined in [[1](#)], a MANET is a network composed of MANET routers, each of which has at least one MANET interface. This document states the goals of autoconfiguration mechanism(s) for MANETs, with respect to the necessary parameters for basic IP identification. Specifically, this document thus states the requirements for:

- autoconfiguring MANET interfaces with IPv6 addresses;
- automatic allocation of IPv6 prefixes to MANET routers.

This draft currently contains terminology, target scenarios and goals for MANET autoconfiguration. Future versions of this document will also review the applicability of existing IPv6 address autoconfiguration and prefix allocation mechanisms, and security considerations.

2. Terminology

This document uses the terminology defined in [\[1\]](#), as well as the following terms :

External Network - a network connected to the MANET, through an interface that is not part of this MANET.

Subordinate MANET - a MANET, which is connected to one or more external network(s), and where such external network(s) are imposing an addressing hierarchy scheme on the MANET.

Autonomous MANET - a MANET upon which no external network imposes an addressing hierarchy.

Address autoconfiguration - the process of configuring an interface with a given address, using an automatic mechanism (contrary to manual configuration).

Prefix allocation - the process of providing a router with authority over an aggregatable pool of addresses (i.e. a prefix), for the purpose of configuring interfaces or other routers.

Disjoint prefixes - two prefixes are said to be disjoint if and only if their respective address ranges do not overlap.

Network merging - the process by which two or more previously disjoint MANETs get connected.

Network partitioning - the process by which a MANET splits into two or more disconnected MANETs.

[3.](#) MANET Categories

IP address autoconfiguration on MANET interfaces and prefix allocation for MANET routers may be used in a number of deployment scenarios. This section outlines the different types of scenarios that are to be addressed by solutions for MANET autoconfiguration.

Note that solutions should also aim at coping with special cases such as a MANET transiting from one type of scenario to an other, or such as routers pre-configured with IP addresses (or prefixes) joining the MANET.

[3.1.](#) Subordinate MANET

A subordinate MANET, as shown in Fig. 1, is a MANET which is connected to at least one external network N that imposes a specific addressing hierarchy on the MANET. In a subordinate MANET, this addressing hierarchy yields the use of specific prefixes for communications between nodes in the MANET and nodes in or across network N. For instance, in Fig. 1, these prefixes need to be topologically correct, i.e. allocated from within a prefix $p::$, over which the point of attachment to network N has authority.

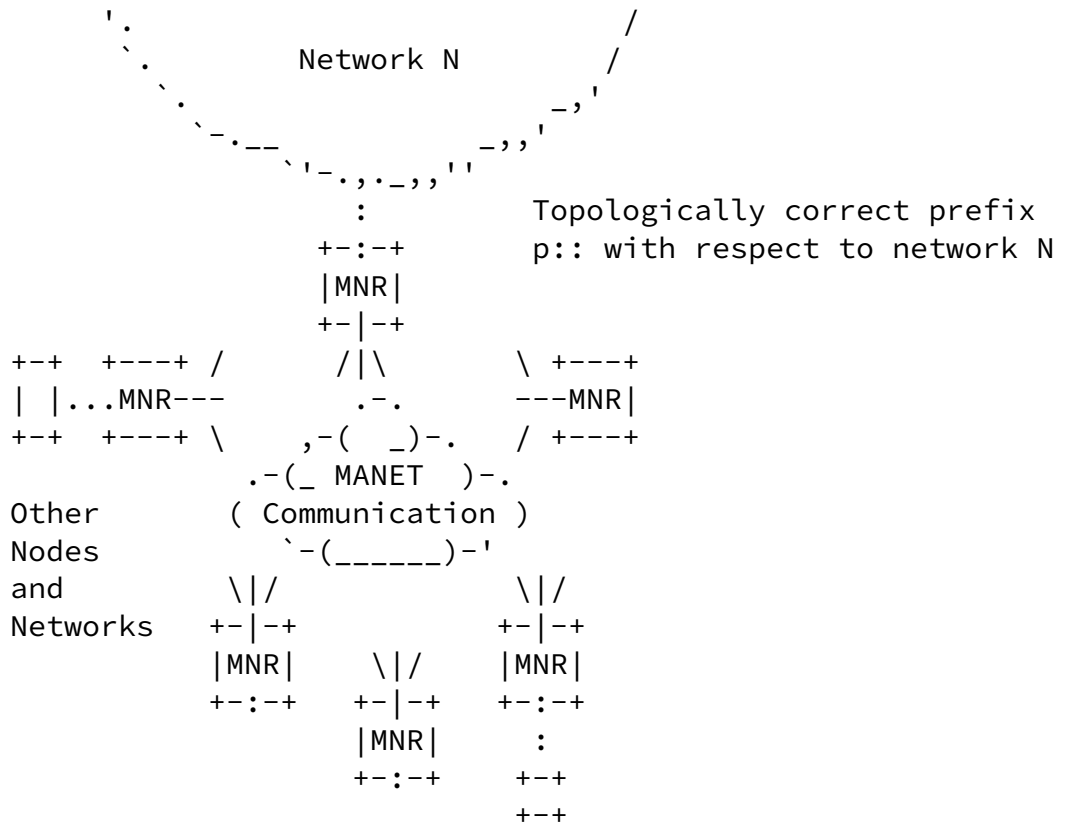


Figure 1: Subordinate MANET. Imposed address hierarchy by external network N.

3.1.1. Scenarios of Subordinate MANETs

This section contains a non-exhaustive list of examples of MANETs falling in the subordinate category.

A typical example of subordinate MANET is a MANET that is part of the Internet, which yields the use of topologically correct IP addresses in order to communicate over the Internet. For instance public wireless mesh networks, i.e. scattered fixed WLAN access routers participating in a MANET of mobile users, and acting as border routers.

Another typical example is the coverage extension of a fixed wide-area wireless network, where one or more MANET router(s) are connected to the Internet through technologies such as UMTS or WiMAX.

Car-to-car communication networks connected to an external infrastructure may also be understood as an instance of subordinate MANET.

3.2. Autonomous MANET

Autonomous MANETs are MANETs upon which no external network imposes an addressing hierarchy. This is shown in Fig. 2, as opposed to the subordinate MANET category described in [Section 3.1](#).

```

                                +----+
                                |MNR|
                                +-|-+-
++  +----+ /      /|\      \ +----+
| |...MNR---      .-.      ---MNR|
++  +----+ \      ,-( _)-.  / +----+
                                .-( _ MANET )-.
Other      ( Communication )

```

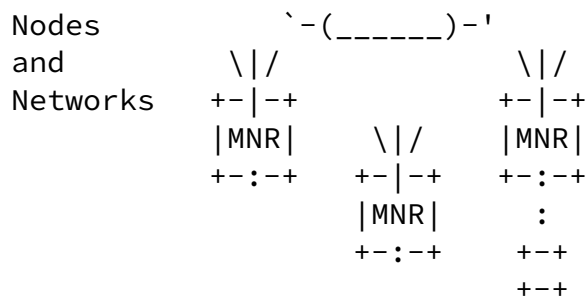


Figure 2: Autonomous MANET. No subordination to an addressing scheme imposed by an external network.

3.2.1. Scenarios of Autonomous MANETs

This section contains a non-exhaustive list of instances of MANETs falling in the autonomous category.

Typical examples of autonomous MANETs are networks set-up in areas where infrastructure is unavailable or inappropriate. For instance, car-to-car communication for sharing traffic and safety-related information, on-site emergency communication among rescue team members for disaster recovery, file sharing in conference or class rooms.

4. MANET Autoconfiguration Goals

The goals of AUTOCONF is to provide autoconfiguration mechanisms which allow each MANET router to:

1. configure IPv6 addresses that are unique within the MANET, on their MANET interface(s).
2. be allocated IPv6 prefixes that are disjoint from prefixes allocated to other routers within the MANET.
3. maintain, within the MANET, the uniqueness of configured addresses and the disjoint character of allocated prefixes (even in face of network merging).
4. be allocated topologically correct prefixes, in the subordinate MANET scenario.

5. Security Considerations

This document does not currently introduce security considerations beyond those captured by [\[1\]](#).

[6.](#) IANA Considerations

This document does not specify IANA considerations.

7. References

7.1. Normative References

- [1] Macker, J., Chakeres, I., and T. Clausen, "Mobile Ad hoc Network Architecture", ID [draft-ietf-autoconf-manetarch](#), February 2007.

7.2. Informative References

- [2] Macker, J. and S. Corson, "MANET Routing Protocol Performance Issues and Evaluation Considerations", [RFC 2501](#), January 1999.
- [3] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IPv6", [RFC 4861](#), September 2007.
- [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., Thomson, S., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.
- [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.
- [12] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 3041](#), 2001.
- [13] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), 2005.
- [14] Aura, T., "Cryptographically Generated Addresses (CGA)",

[RFC 3972](#), 2005.

- [15] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", [RFC 4429](#), 2006.
- [16] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", [RFC 4193](#), 2005.
- [17] Thubert, P. and TJ. Kniveton, "Mobile Network Prefix Delegation", ID [draft-ietf-nemo-prefix-delegation](#), August 2007.
- [18] Troan, O. and R. Droms, "IPv6 Prefix Options for DHCPv6", [RFC 3633](#), 2003.

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, U. Herberg, G. Montenegro, H. Moustafa, C. Perkins, A. Petrescu, P. Ruiz, P. Stupar, F. Templin, D. Thaler, R. Wakikawa, 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

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).