

MANET Autoconfiguration (AUTOCONF)
Internet-Draft
Intended status: Informational
Expires: May 6, 2009

H. Moustafa
France Telecom
C. Bernardos
M. Calderon
UC3M
November 2, 2008

Evaluation Considerations for IP Autoconfiguration Mechanisms in MANETs
[draft-bernardos-autoconf-evaluation-considerations-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 May 6, 2009.

Abstract

This Internet Draft aims at providing general guidelines for the AUTOCONF solution space, through providing a set of evaluation considerations for IP autoconfiguration mechanisms in MANETs. These evaluation considerations conform to the AUTOCONF problem statement draft and the MANET architecture draft. The main objective of this draft is to illustrate some key features and highlight some important behaviours for the different autoconf mechanisms, and thus aiming to help solution developers during mechanisms' design and to help implementers in the choice of the autoconf mechanism that fits better their particular requirements, taking into consideration a number of

important factors that are discussed in this draft.

Table of Contents

1.	Introduction and motivation	3
2.	Evaluation Considerations	3
2.1.	Node/Network Characteristics	3
2.1.1.	MANET Scenarios	4
2.1.2.	Mobility type	4
2.2.	Functional Characteristics	5
2.2.1.	Address Uniqueness	5
2.2.2.	Merging support	6
2.2.3.	Partitioning support	6
2.2.4.	Prefix delegation support	6
2.3.	Performance Characteristics	7
2.3.1.	Protocol overhead	7
2.3.2.	Robustness	7
2.3.3.	Convergence time	8
2.3.4.	Scalability	8
2.3.5.	Address space utilisation	9
2.4.	Nodes' Behaviour Characteristics	9
2.4.1.	Distributed/Centralised approach	9
2.4.2.	Trust and Security	10
2.5.	Architectural Characteristics	10
2.5.1.	Integration with standard IPv6 nodes	10
2.5.2.	Gateway involvement	11
2.6.	Usability Characteristics	11
2.6.1.	Routing Protocol Dependency	11
3.	Security Considerations	12
4.	IANA Considerations	12
5.	Acknowledgements	12
6.	References	12
6.1.	Normative References	12
6.2.	Informative References	13
Appendix A.	Change Log	13
	Authors' Addresses	13
	Intellectual Property and Copyright Statements	15

1. Introduction and motivation

Ad hoc networks present particular characteristics that should be taken into account when designing address auto-configuration protocols. These unique characteristics make existing solutions for IP infrastructure-based networks (e.g., RFCs 2461, 2462, 3315 etc.) difficult to be applied, as is, in MANETs. Some limitations of these existing solutions are stated in [[1](#)] and they mainly concern: the lack of multi-hop support, the lack of dynamic topology support, the lack of network merging support and the lack of network partitioning support.

The AUTOCONF WG is working to develop and standardise IP autoconfiguration mechanisms for MANETs. The dynamic and random nature of MANETs together with the different environmental behaviour, results in different autoconfiguration mechanisms functionalities and characteristics. The problem statement draft [[1](#)] highlights the importance of some solution considerations that should be taken in mind, mainly focusing on low overhead, low delay, different link type's applicability, interaction with the existing protocols and security issues. In this context, this document discusses some evaluation considerations for IP autoconfiguration mechanisms in MANETs, giving a useful reference for the solutions' space as well as guidelines for solution developers during mechanisms' design and implementers in the choice of the autoconf mechanism. These considerations will help to decide which of the available autoconf mechanisms fits better a particular scenario.

The evaluation considerations developed in this draft refer to the previous study, carried out in [[3](#)], in which an analysis of several evaluation criteria for MANET autoconf mechanisms is done. The evaluation considerations presented in this draft are generally classified according to a number of characteristics, namely: node/network characteristics, nodes' behaviour characteristics, functional characteristics, performance characteristics, and usability characteristics.

[2.](#) Evaluation Considerations

[2.1.](#) Node/Network Characteristics

The node/network characteristics basically deal with the special features and constraints that a MANET environment might have. This includes the applicability scenarios as well as some nodes' characteristics, like the type of mobility.

[2.1.1.](#) MANET Scenarios

This characteristic concerns the MANET environment. In this context, two possible scenarios of MANET are identified in [\[1\]](#):

1. Standalone MANETs, which are autonomous ad hoc networks that are not connected to any external network. All traffic is generated by MANET nodes and destined to nodes in the same MANET. Examples of these networks are conference networks, battlefield networks, surveillance networks, etc. In standalone MANET scenarios, nodes may join or leave randomly. Most likely, there is neither pre-established nor reliable address or prefix allocation agency is present in such type of networks.
2. Connected MANETs, which are ad hoc networks having connectivity to one or more external networks, typically the Internet, by means of one or more gateways. It is noticed that these networks may be connected to the Internet in a permanent fashion or an intermittent fashion.

This characteristic is an important and basic one that should be considered during the design phase of any autoconfiguration mechanism. Different mechanisms functionalities will be required according to the scenario type, where for example, solutions designed for connected MANET scenarios have to deal with the issue of getting global IPv6 addresses that allow nodes to get Internet connectivity. In fact, contributions designated for connected MANETs can mostly be general for both types of scenarios. Indeed, an autoconfiguration mechanism should take into account the case of scenario transition, where a connected MANET can converge to a standalone MANET if it loses its attachment with the infrastructure, or a partially

standalone manner if sub-network(s) exist(s) due to partitioning.

2.1.2. Mobility type

This characteristic concerns the nodes behaviour in MANETs. In fact, nodes' mobility type depends on the MANET application type. It is also noticed that MANET nodes (or some of them) could be fixed or present low mobility patterns in certain applications (e.g. mesh networks).

This characteristic impacts the performance of autoconfiguration mechanisms. Particularly, the transmission reliability of autoconfiguration messages differs from low to high mobility scenarios. It is noticed that this characteristic impacts the autoconfiguration mechanisms performance, especially the convergence time and the scalability. Indeed, high mobility can lead to frequent subnet change by mobile nodes and hence requires a change in the nodes' address. The design of any autoconfiguration mechanism should take into account the nodes mobility type, where employing periodic

functionalities is more suitable for high nodes' mobility scenarios. Furthermore, the size of messages' exchange should adapt to the mobility types of nodes. A complex problem under this issue is the co-existence of different mobility types within the same MANET, where we can have different types of mobility ranging from low to high among the communicating nodes in a given MANET.

An additional issue, related to network partitioning and merging, is the movement detection, that is specially relevant in high mobility scenarios. Additionally, movement detection can be hard to achieve in MANET scenarios and therefore should also be taken into account when analysing a particular autoconf solution.

2.2. Functional Characteristics

The functional characteristics describe the functionalities that a mechanism must aim at featuring [3]. An autoconfiguration mechanism can implement one or several of these functionalities. Such functionalities can vary according to the MANET environment and the autoconfiguration approach. There should be a trade-off between the number of functionalities that an autoconfiguration mechanism implements and the network performance. The increase in the number

of functionalities, provided that they are correctly designed, should not harm the network performance.

[2.2.1.](#) Address Uniqueness

The Address Uniqueness characteristic concerns two points: i) Duplicate Address Avoidance, and ii) Non-unique Address Detection. Duplicate address avoidance is a mandatory characteristic in any autoconfiguration mechanism. It consists in making all autoconfiguration mechanisms' functionalities assign addresses only after checking their uniqueness. Hence, this principle must be the core of any design of an autoconfiguration mechanism [3]. On the other hand, Non-unique Address Detection is the process used to detect address collisions and resolve them. This might be a heavy process in any MANET IP autoconfiguration mechanism, requiring a considerable number of control messages.

The Duplicate Address Avoidance is the only mandatory functionality in an autoconfiguration mechanism, as it reflects the assumption of uniqueness upon which the routing protocol is based [1].

As for Non-unique Address Detection, most of the existing contributions employ such a procedure, whether through developing a Non-unique Address Detection mechanism or through using an existing one. Due to MANETs' merging and separation, this process should take place in a continuous manner before the IP assignment (Pre-service)

as well as after the IP assignment (In-service) [2]. However, there are some contributions that are Non-unique Address Detection-free, which do not use any of such mechanisms while being capable of assuring the IP address uniqueness. Employing a Non-unique Address Detection mechanism adds overhead to the autoconfiguration mechanism and has an impact on its scalability.

[2.2.2.](#) Merging support

The merging characteristic presents the ability of the autoconfiguration mechanism to detect MANETs' merging and provide functionalities to avoid IP address conflicts and connectivity problems in such case.

Merging support is important in the case where two previously

disjoint ad hoc networks get connected, since there might be nodes with duplicated address in the merged network, and therefore it is needed to make some nodes change the IP addresses they are using to avoid the conflict (this can be achieved for example by using in-service Non-unique Address Detection mechanisms).

[2.2.3.](#) Partitioning support

The partitioning characteristic presents the ability of the autoconfiguration mechanism to detect MANETs' partitioning and provide functionalities to avoid IP address conflicts and connectivity problems in such case.

Partitioning support is important, especially in connected scenarios, in which as a result of a network split, some nodes of the ad hoc network might lose the connectivity to the node that they were using as gateway to the fixed infrastructure and to the Internet. Additionally, it is also important to analyse how an autoconf solution deal with the issue of re-use or re-claiming of resources (such as IP addresses) once a node has left a particular network.

[2.2.4.](#) Prefix delegation support

The MANET architecture document [2] considers nodes of a MANET as routers (MANET Routers) that can have attached "traditional" hosts, and that therefore need to acquire IPv6 prefixes instead of just single addresses.

It is important to analyse if a particular AUTOCONF solution supports the delegation of IPv6 prefixes to nodes.

[2.3.](#) Performance Characteristics

Performance is always a critical issue in communication protocols. In the case of autoconf, performance might be specially relevant in certain scenarios (for example, in constrained devices). The performance of an autoconfiguration mechanism can be evaluated through a number of characteristics, as mentioned below.

2.3.1. Protocol overhead

This characteristic concerns the additional signalling required by the autoconfiguration mechanism. Such signalling is considered as protocol overhead that might have a significant performance impact.

Several cases may be considered:

- o The IP autoconfiguration mechanism (not the ad-hoc routing protocol) requires additional message flooding. This message flooding may be optimised using existing techniques.
- o The IP address autoconfiguration mechanism requires some protocol messages (besides the normal routing protocol messages) to be exchanged locally or it modifies existing routing protocol messages to add (piggybacking) some information (e.g., prefix or GW information). The size of the added information and how often this information is sent can vary depending on the particular autoconf solution and the applicability scenario.
- o The IP address autoconfiguration mechanism does not require any special signalling to function (that is, it works in a passive way).

This characteristic might have an impact on the convergence time and thus the scalability of the autoconfiguration mechanism.

2.3.2. Robustness

One important characteristic/property of an autoconf mechanism is its robustness. Given the particular multi-hop characteristics of MANET scenarios, it might be important to analyse the underlying assumptions that an autoconf mechanism might make.

For example, certain autoconf solutions may assume that the underlying physical layer is reliable and messages are never lost, while another autoconf mechanism may need to provide additional mechanisms that deal with the reliability of the message transmission. Obviously, in certain scenarios the former assumption makes no sense, and therefore, autoconf solutions may need to implement some procedures to ensure that a certain protocol message -- needed for the correct operation of the autoconf mechanism -- has actually reached its intended destination(s). Additionally, an

autoconf solution may be designed in such a way that certain message

loos are supported without disrupting the correct operation of the autoconf mechanism.

The same kind of reasoning than above can be applied for solutions that assume an ordered delivery of signalling messages or the integrity of the received messages .

[2.3.3.](#) Convergence time

Another important characteristic, that can be related to the robustness as well, is the convergence time of an autoconf solution. Depending on the scenario and/or the application, we may define the convergence time as the time required by a single node to get a usable (and unique) IPv6 address or as the time required by the whole network to have all its nodes configured with correct addresses. For several scenarios, it might not be important for an autoconf solution to take a long time to finish its operation (e.g., several minutes), for example because the autoconf mechanism is only run once and then the nodes remain stable. However, for other scenarios, it might be required that the autoconf solution should take less to converge than a given amount of time.

In relation to the convergence time, it might be also important for an autoconf mechanism not to assume at any time an upper limit on the time required for a certain message to reach any node of the MANET, since this may have an impact on the global convergence time. Besides, this kind of assumptions might lead to a solution not to work properly in a particular scenario (where the time required for a message sent from a node A to reach a node B is longer than the assumed upper limit).

[2.3.4.](#) Scalability

An important issue to deal with during autoconfiguration mechanisms design is the scalability of mechanisms to different networks sizes. The MANET Architecture I-D [\[2\]](#) defines as Small a MANET composed of 2-30 peer MANET routers, Moderate a MANET composed of 30-100 peer MANET routers, Large a MANET composed of 100-1000 peer MANET routers, and Very Large those MANETs larger than 1000 peer MANET routers.

An autoconfiguration mechanism, in its own, generates signalling overhead that may be high, thus impacting scalability. As mentioned in [\[3\]](#), information diffusion also suffers from a large size as the diffusion delay can increase such that information arrives at a node from distant parts of the network with a long delay.

Scalability is a very important characteristic that deserves

consideration. An autoconfiguration mechanism is not scalable, if its performance degrades significantly when the network size increases. This characteristic would be highly dependant on the particular usability scenario, since for example there might be an autoconf solution designed for a specific moderate-MANET application that works great for that particular MANET but this might not be the case when the same solution is used for very large network.

[2.3.5.](#) Address space utilisation

This characteristic basically analyses how an autoconf solution makes use of the available address space. For example, there are solutions that split the address space into ranges delegated to different nodes, that are responsible of the assignment of addresses from those ranges, whereas there are other solutions that keep the available address space common for all the MANET nodes. Obviously, the former approach might be more inefficient in terms of address space utilisation, compared to the latter. However, the first approach may present additional advantages that may make it better for certain scenarios.

This characteristic is important in networks that are assigned a short range of addresses, as well as in large and dense networks. If too many addresses are wasted by the autoconfiguration mechanism, such that all idle and accessible addresses are in use, an incoming node cannot be granted an address. This invalidates many of the functionalities [\[3\]](#).

[2.4.](#) Nodes' Behaviour Characteristics

The nodes' behaviour is an important point to be considered during autoconfiguration mechanisms design. It describes how the communicating nodes behave during the autoconfiguration process. Actually, nodes may behave in a distributed or centralised manner which affects the address assignment approach. In addition, trust is a pre-requisite behaviour among nodes and has a great impact on the correct functionalities of any autoconfiguration mechanism.

[2.4.1.](#) Distributed/Centralised approach

There are different possible approaches that an IP autoconfiguration mechanism might follow to assign IP addresses to all the nodes of a MANET. One possibility is to deploy a centralised server that is in charge of the IP address assignment (e.g., DHCPv6). The opposite approach is not to make use of any server, but to share the IP address assignment task among all the participant nodes. Between

these two extreme cases, intermediate approaches can be found, for example those that deploy several distributed servers within the

MANET and therefore can be considered as distributed solutions in one sense, while they can also be considered as centralised in a certain level, since they still make use of servers.

This characteristic has a direct impact on the performance of any autoconfiguration mechanism and is somewhat related to the MANET scenario, where, for example, a totally centralised approach is not suitable in a standalone MANET.

[2.4.2.](#) Trust and Security

A very important issue concerns securing communication, or assuring secure links existence, between the communicating nodes during the autoconfiguration process. So far, this issue is not considered within the ongoing mechanisms. To assure reliable messages' transmission and hence correct mechanisms functionalities, secure communication should exist between nodes. The main difficulty is mainly concerning the multi-hop environment.

In the design of autoconfiguration mechanisms, attacks in ad hoc multi-hop environments should be considered. Further, it is important to have a trust relationship between each communicating pair of nodes that are involved in the autoconfiguration process. This could assure secure and hence correct functioning of autoconfiguration mechanisms. Trust relationship can differ in standalone MANET compared to connected MANET, where a central authority can play the role of a trusted third party that could help in trust provision among the participating nodes. Also, cooperation between nodes is an important factor in order to assure the proper message forwarding during the autoconfiguration process. In this context, MANET nodes cooperation should be satisfied and also gateways should be enough cooperative.

[2.5.](#) Architectural Characteristics

The architectural characteristics concern the nodes architecture (especially, the interfaces architecture) as well as the topological architecture and network deployment, concerning special elements/entities (such as gateways).

[2.5.1.](#) Integration with standard IPv6 nodes

One characteristic that can be considered important in certain scenarios is the integration of the autoconf solution with standard IPv6 nodes. For example, certain autoconf mechanisms may allow/be compatible to support IPv6 nodes to get addresses using standard mechanisms defined in IPv6, while others may be totally incompatible with today's IPv6 nodes, therefore preventing these nodes to inter-

operate with these autoconf solutions, unless the IPv6 nodes are properly modified to support them.

[2.5.2.](#) Gateway involvement

This characteristic concerns the role that Internet gateways could have in the IP address autoconfiguration process for incoming nodes. Indeed, in connected scenarios, Internet gateways are considered to provide the MANET with connectivity to the fixed infrastructure. However, these gateways might also have a role/involvement in the IP address assignment procedure (e.g., in some solutions, the gateway might only be responsible of forwarding packets to the infrastructure, while in other solutions it may also be involved in the task of providing nodes with addresses/prefixes).

This characteristic is interesting to be studied for each IP autoconfiguration mechanism and need to be considered during the mechanisms' design. Actually, gateway involvement depends somehow on whether the used approach is centralised or distributed. It can be also related to the address space usage.

[2.6.](#) Usability Characteristics

The usability characteristics describe how and under which circumstances an autoconf mechanism is able to be used. This means the adaptability to the whole environment including users and other protocols [3].

[2.6.1.](#) Routing Protocol Dependency

Typically, IP autoconfiguration mechanisms require special signalling and thus control overhead in order to assign a unique IP address for

each MANET node and, in a many cases, to verify the uniqueness of each assigned address. Consequently, some of the proposed IP autoconfiguration mechanisms are routing protocols dependent; making use of the ad hoc routing protocol in transmitting their own signals, especially benefiting from the routing discovery phase in the ad hoc routing protocol.

In this context, autoconfiguration mechanisms may be dependent on routing protocols and could not function without them (e.g., autoconfiguration mechanisms can be tailored for specific ad hoc routing protocols, because the use of the signalling of the routing protocol or because they make use of any kind of information provided by the routing protocol). On the other hand, autoconfiguration mechanisms can be routing protocols independent, not requiring the existence of any particular routing protocol to function. In between, autoconfiguration mechanisms may need a routing protocol,

where if a routing protocol exist this will optimise the mechanisms operation and if no routing protocol exist, the mechanism could also work.

[3.](#) Security Considerations

Due to the open wireless environment of ad hoc networks, IP autoconfiguration mechanisms are susceptible to a number of attacks. The autoconfiguration problem statement draft [\[1\]](#) states some security issues that worth consideration.

[4.](#) IANA Considerations

This document has no actions for IANA.

[5.](#) Acknowledgements

The authors would like to thank Charles Perkins and Joe Macker for their comments and suggestions during 69th IETF. We also like to thank Shubhranshu Singh and Thomas Clausen for their very valuable comments and suggestions on the content of this draft.

Authors also want to point out that some useful content of [3] has been used in several ways in the present draft.

The work of Carlos J. Bernardos and Maria Calderon has been partially supported by the Spanish Government under the POSEIDON (TSI2006-12507-C03-01) project.

The work of Carlos J. Bernardos and Maria Calderon has also been partially funded by the EU through the ICT FP7 European Project CARMEN (INFSO-ICT-214994). Apart from this, the European Commission has no responsibility for the content of this Internet-Draft. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

[6.](#) References

[6.1.](#) Normative References

- [1] Baccelli, E., Mase, K., Ruffino, S., and S. Singh, "Address Autoconfiguration for MANET: Terminology and Problem Statement",

Moustafa, et al.

Expires May 6, 2009

[Page 12]

Internet-Draft

AUTOCONF evaluation considerations

November 2008

[draft-ietf-autoconf-statement-04](#) (work in progress),
February 2008.

- [2] Chakeres, I., Macker, J., and T. Clausen, "Mobile Ad hoc Network Architecture", [draft-ietf-autoconf-manetarch-07](#) (work in progress), November 2007.

[6.2.](#) Informative References

- [3] Clausen, T., "Evaluation Criteria for MANET Autoconf Mechanisms", [draft-clausen-autoconf-criteria-00](#) (work in progress), July 2005.

[Appendix A.](#) Change Log

Changes from -02 to -03:

- o New release to keep the document alive.

Changes from -01 to -02:

- o New release to keep the document alive.
- o Update of some references.

Changes from -00 to -01:

- o Mainly editorial changes.

Authors' Addresses

Hassnaa Moustafa
France Telecom
38-40 rue du General Leclerc
Issy Les Moulineaux 92794 Cedex 9
France

Phone: +33 145296389

Email: hassnaa.moustafa@orange-ftgroup.com

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236

Email: cjbc@it.uc3m.es

Moustafa, et al.

Expires May 6, 2009

[Page 13]

Internet-Draft

AUTOCONF evaluation considerations

November 2008

Maria Calderon
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 8780

Email: maria@it.uc3m.es

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.