MANET Autoconfiguration (Autoconf)
Internet-Draft
Expires: August 28, 2008

E. Baccelli (Ed.)
INRIA

February 25, 2008

Address Autoconfiguration for MANET: Terminology and Problem Statement
draft-ietf-autoconf-statement-04

Status of this Memo

Copyright Notice

Abstract

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

Table of Contents

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.

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 its interfaces, or other nodes.

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 disconnected 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.

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.

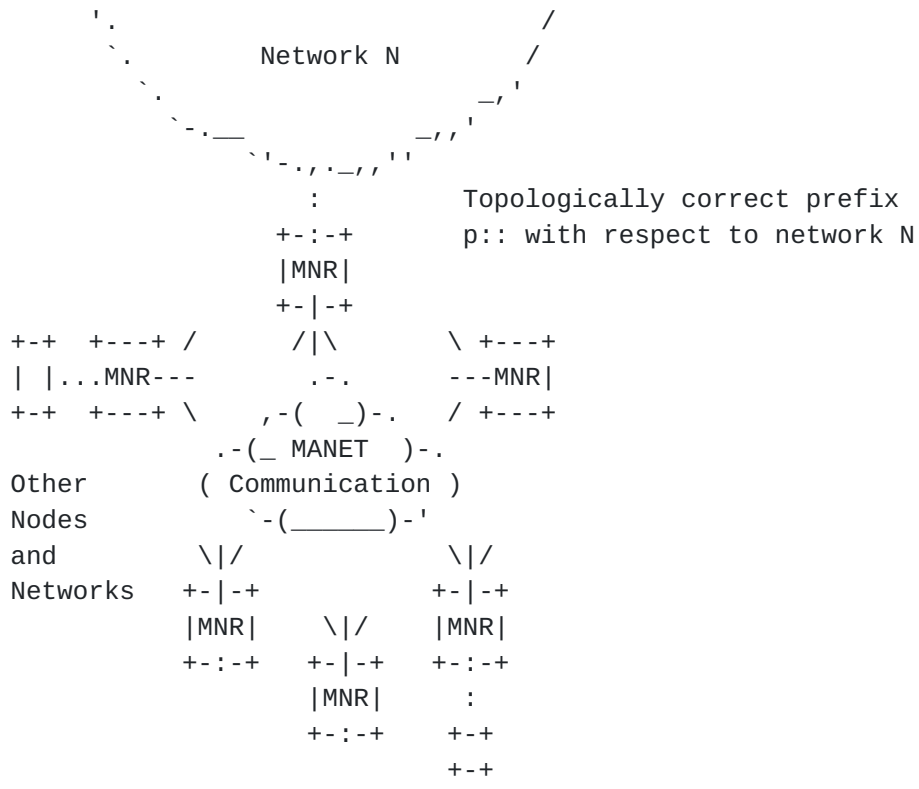

Figure 1: Subordinate MANET. Imposed address hierarchy by external network N.

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.

Vehicle 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.

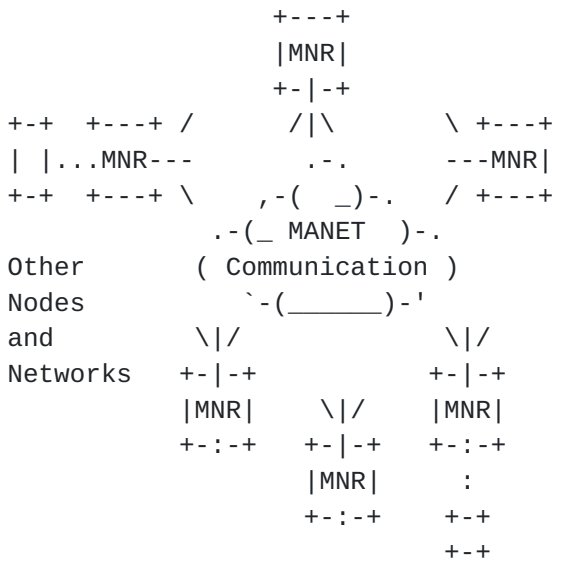

Figure 2: Autonomous MANET. No subordination to an addressing scheme imposed by an external network.

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 case of network merging).

4. be allocated topologically correct prefixes, in the subordinate MANET scenario.

5. Applicability of standard configuration solutions

This section reviews the applicability of existing standard protocols for the purposes listed in Section 4. Note that MANET routers are assumed to also run these standard protocols as usual over non-MANET interfaces, if any.

5.1. Applicability of DHCP

DHCP [4] enables automatic allocation of an IP address to a node by a DHCP server. A node requiring an IP address contacts a DHCP server and requests an address. The DHCP server will dynamically assign an address from a certain pool of addresses, and allocate a so called ''lease'' of that address to the client. The client can then use the address for a certain time. If the client wants to keep the address for a longer time, it has to prolong the lease. If the DHCP server is not on the same link as the DHCP client, it is possible to use one or more DHCP relay agent to forward the messages to a different subnet.

5.1.1. Issues with DHCP Fundamental Assumptions

DHCP works on the basic assumption that every node in the MANET can directly communicate with either (i) the DHCP server, or (ii) a DHCP relay which can communicate with either the DHCP server or another relay.

As described in [1], part (i) of this assumption is often wrong in a MANET, as each node may see a different set of neighboring MANET nodes. On the other hand, part (ii) of this assumption relies on the guarantee that the recursion will end at some point (by reaching the root, i.e. the DHCP server). Because of the dynamics in MANET topology and MANET membership described in [1], there is no such assurance in a MANET, as the DHCP server may be unreachable, or a loop may have appeared along the path.

Moreover, DHCP works with the assumption that either (a) there is a unique DHCP server in the network, or (b) if there are several DHCP servers in the network, they are manually configured accordingly. Because of the dynamics in MANET membership described in [1], there is no such assurance in a MANET, as topology changes may produce a situation where several servers with conflicting configuration parameters (e.g. managing non-disjoint pools of local addresses) become part of the same MANET. Servers may thus require dynamic (re)configuration.

Similarly, DHCP works with the assumption that should there be DHCP relays, they benefit from appropriate manual configuration. Because

of the dynamics in MANET membership and topology described in [1], there is no such assurance in a MANET. Configuration may not remain appropriate over time, and relays may thus require dynamic (re)configuration.

5.1.2. What DHCP Can and Cannot Do in MANETs

DHCP "as is" could be used to some extent for address configuration purposes (goal 1, listed in Section 4). However DHCP's applicability in this context is limited. Indeed, if the topology is or becomes such that a MANET router does not have access to a DHCP server directly nor through a relay, DHCP is not operational.

DHCP "as is" could also be used to some extent for uniqueness maintenance purposes (goal 3, listed in Section 4). However DHCP's applicability in this context is limited. Since different DHCP servers will not automatically check the disjoint character of the pools of addresses they provide leases from, if the topology is or becomes such that several DHCP servers with conflicting configuration lease addresses in the same MANET, there is no guarantee that configured addresses will indeed be unique.

5.2. Applicability of SLAAC/NDP

Stateless Address Autoconfiguration (SLAAC [5]) enables automatic configuration of an IP address to a host without contacting any kind of server. A host first constructs a tentative IPv6 address by attaching its host identifier (in most cases its MAC address) to the well-known link-local prefix. It then operates duplicate address detection, that verifies that no other host on the link has the same address by broadcasting NDP messages [3]. If the address is not unique, the autoconfiguration process will abort. Upon a successful address uniqueness test, a host may request a prefix from any router on the link by an exchange of NDP messages. It will again attach its host identifier to that router prefix and repeats the address uniqueness test sequence.

5.2.1. Issues with SLAAC/NDP Fundamental Assumptions

SLAAC relies on NDP signalling, which works on the basic assumption that each node in the MANET can communicate directly with every other node in the MANET, i.e. all the nodes are connected to a single multicast-enabled link. As described in [1], this assumption is often wrong in a MANET, as each node may see a different set of neighboring MANET nodes.

5.2.2. What SLAAC/NDP Can and Cannot Do in MANETs

SLAAC "as is" could be used to some extent for address configuration and uniqueness maintenance purposes (goal 1 and 3, listed in Section 4), for instance when no DHCP server is available. However SLAAC's applicability in this context is limited, since NDP messages are not relayed beyond the ''link'' (or in MANET terms, beyond the first hop). If topology is or becomes such that the MANET is not contained in a single hop, there is no guarantee that the configured addresses will indeed be unique, since signalling will not reach all the concerned nodes.

5.3. Applicability of DHCP-PD

DCHP-PD [17] is a DHCP option that enables automatic allocation of IPv6 prefixes to routers using DHCP. A router may request a prefix allocation from a DHCP server by sending a DHCP request including the Prefix Delegation option. The server may then delegate a sub-prefix (i.e. a subset of its address pool) to the router. The DHCP message containing the Prefix Delegation option may be relayed through one or more DHCP relays, as per [4].

5.3.1. Issues with DHCP-PD Fundamental Assumptions

DHCP-PD is based on DHCP, and thus encounters the fundamental issues described in Section 5.1.1, with respect to server reachability, and dynamic (re)configuration of servers and relays.

5.3.2. What DHCP-PD Can and Cannot Do in MANETs

DHCP-PD "as is" could be used to some extent for prefix allocation purposes (goals 2 and 4 listed in Section 4) and for uniqueness maintenance purposes (goal 3, listed in Section 4). However DHCP-PD's applicability in this context is limited. If topology is or becomes such that the MANET router cannot communicate with a DHCP server, DHCP-PD is not operational. Moreover, if topology is or becomes such that several servers with conflicting configuration become part of the same MANET, there are no automatic (re)configuration mechanisms available in order for servers to dynamically adapt to the situation.

6. Problem Statement

SLAAC, NDP, DHCP and DHCP-PD provide only a partial solution with respect to the goals listed in Section 4. As explained in Section 5.1, Section 5.2, and Section 5.3, existing protocols "as is" cannot deal with the specific dynamic, multi-hop and distributed nature of MANETs. Additional solutions are thus needed to complete the goals of MANET IPv6 autoconfiguration.

6.1. Solutions Requirements

The following list presents the requirements for potential IPv6 address autoconfiguration solutions:

R 01. Solutions must configure MANET interfaces with IPv6 addresses that are unique within the MANET.

R 02. Solutions must configure routers within the same MANET with disjoint prefixes.

R 03. Solution must work even without a MANET routing protocol. However, solutions may leverage the presence of routing protocols, for optimization purposes.

R 04. Solutions must provide a mechanism to prevent and deal with address or prefix conflicts (due for instance to network merging, change in MANET membership, preconfiguration or misconfiguration).

R 05. Solutions must be designed taking into account the particular characteristics of MANETs [1], including their multi-hop nature, and the potential asymetry of links.

R 06. Solutions must achieve their goal(s) with low control overhead.

R 07. Solutions must achieve their goal(s) with low delay or convergence time.

R 08. Solutions must ensure backward compatibility with other standards defined by the IETF.

R 09. Solutions must not require modifications of existing protocols on non-MANET interfaces and non-MANET routers.

R 10. Solutions should address security threats considered in existing IPv6 autoconfiguration mechanisms. In addition, solutions should address potential MANET-specific threats (see Section 7).

R 11. Solutions should work in MANETs connected to an external network via multiple border routers, as well as in MANETs connected to multiple external networks.

R 12. In the case of subordinate MANETs, solutions should have a minimal impact on the routing system of the external network(s) to which a MANET is connected. In particular, this includes the following:

R 12.1. Solutions should not preclude prefix aggregation at the edge of the subordinate MANETs.

R 13. Solutions should support transitioning from one MANET scenario to another (e.g. from subordinate to autonomous or vice-versa).

R 14. Solutions may be designed in a modular way, each module addressing a specific subset of the requirements or scenarios.

7. Security Considerations

A significant security issue is that of maintaining the confidentiality and the integrity of some data being exchanged between communication end-points in the MANET (e.g. between a server and a client). This task is equivalent to that of ensuring end-to-end security in other types of networks, and existing techniques are therefore applicable.

An orthogonal issue with respect to securing MANET protocols is ensuring network integrity. So far, MANET protocols in general allow any node to participate in the network - the assumption being that all nodes are well-behaving and welcome. If that assumption fails, i.e. if the network may count malicious nodes, the integrity of the network may fail. Specific malicious behaviour include, but are not limited to, jamming (resulting in DoS), incorrect traffic generation (e.g. server, router or address spoofing), incorrect traffic relaying (e.g. "man in the middle"), or replay attacks. Most of these threats are already taken into account in RFC 3756, RFC 3971, and the security sections of RFC 4861 and RFC 3315.

DoS attacks can highly penalize the operation of IP autoconfiguration solutions, through increasing the signalling overhead and hence harming the solutions' convergence time. "Man-in-the-middle" attacks can cause (i) interception of the IP autoconfiguration messages and hence operation failure, (ii) messages' modifications leading for example to changing assigned IP addresses or prefixes during their transfer and hence causing address or prefix conflicts, (iii) impersonation, which allows a non-legitimate MANET router to participate in the IP autoconfiguration process in place of a legitimate node, and may lead to DoS. On the other hand, IP spoofing can also lead to impersonation, whereby an IP address can be spoofed by a non-legitimate node during transfer.

Existing security solutions usually protect network integrity through authentication guaranteed by a "higher" authority, trusted a priori, which typically issues the cryptographic keys used to authenticate. However, for instance in autonomous MANET scenarios, there may not be any "higher" authority, or if there is, it may not be trusted a priori by every node in the MANET.

Encryption is thus essential to many existing security mechanisms. However it may affect convergence time or require a process that is too heavy in the context of MANETs, since a significant part of the nodes in a MANET may have limited resources.

Another issue specific to MANETs is related to the potential selfishness behaviour of some MANET nodes, a.k.a. "the selfish node

problem". This behaviour can cause non-cooperation between MANET nodes during the IP autoconfiguration process, and hence affect the operation of autoconfiguration mechanisms.

In the context of MANET IPv6 autoconfiguration, such MANET characteristics are to be considered in addition to general characteristics supported by existing IPv6 autoconfiguration solutions.

8. IANA Considerations

This document does not specify IANA considerations.

9. References

9.1. Normative References

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

9.2. 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] Troan, O. and R. Droms, "IPv6 Prefix Options for DHCPv6", RFC 3633, 2003.

Contributors

Shubhranshu Singh, Samsung.
Email: Shubranshu@gmail.com

Kenichi Mase, Niigata University.
Email: Mase@ie.niigata-u.ac.jp

Simone Ruffino, Telecom Italia.
Email: Simone.Ruffino@telecomitalia.it

Carlos J. Bernardos, Universidad Carlos III de Madrid.
Email: cjbc@it.uc3m.es

Hassnaa Moustafa, France Telecom.
Email: Hassnaa.Moustafa@orange-ftgroup.com

Emmanuel Baccelli, INRIA.
Email: Emmanuel.Baccelli@inria.fr

Thomas Heide Clausen, LIX, Ecole Polytechnique.
Email: T.Clausen@computer.org

Acknowledgements

This document benefited from specific feedback, and helpful discussions with C. Adjih, T. Boot, C. Dearlove, U. Herberg, G. Montenegro, C. Perkins, A. Petrescu, P. Ruiz, P. Stupar, F. Templin, D. Thaler, R. Wakikawa, K. Weniger.

Editor's Address

Emmanuel Baccelli
INRIA

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

Full Copyright Statement

Intellectual Property

Acknowledgment

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