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

November 19, 2007

Address Autoconfiguration for MANET: Terminology and Problem Statement
draft-ietf-autoconf-statement-02

Status of this Memo

Copyright Notice

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

A Mobile Ad hoc NETwork (also known as a MANET [1]) consists of a loosely connected set of MANET routers. Each MANET router embodies IP routing/forwarding functionality and may also incorporate host functionality [2]. 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, at a rate that can be substantially higher than in usual networks.

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, and may also need to be delegated an IP prefix. This address or this prefix may be required to be unique within a given scope, or to be topologically appropriate.

Standard automatic IPv6 address assignment and prefix delegation 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 for operation within MANET scope, and this document thus details and categorizes the issues that need to be addressed.

2. Terminology

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

MANET Local Prefix (MLP) - An IP prefix delegated to a MANET router, consisting in chunks of IP addresses valid for communications inside the MANET.

MANET Local Address (MLA) - An IP address configured on a MANET interface, and valid for communications inside the MANET.

Global prefix - An IP prefix delegated to a MANET router, consisting in chunks of IP addresses valid for communications reaching outside the MANET (as well as communications within the MANET).

Global address - An IP address configured on an interface and valid for communications reaching outside the MANET (as well as communications within the MANET).

Internet Configuration Provider (ICP) - A router that can provide other routers requesting configuration with addresses or prefixes derived from a global prefix.

Connected MANET - A mobile ad hoc network, which contains at least one ICP.

Standalone MANET - A mobile ad hoc network, which does not contain any ICP.

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 with the purpose of configuring an interface.

Address assignment - The process of configuring an interface with a given address.

Prefix delegation - The process of providing a router with a set of contiguous addresses it may manage for the purpose of configuring interfaces or other routers.

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 on MANET interfaces and prefix delegation to MANET routers are necessary in a number of deployment scenarios. This section outlines the different categories of scenarios that are considered.

3.1. Connected MANET

Connected MANETs are mobile ad hoc networks which contain at least one ICP, i.e. a router that can provide other routers requesting configuration with addresses or prefixes derived from a global prefix. 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.

3.2. Standalone MANET

Standalone MANETs are mobile ad hoc networks which do not contain any ICP, i.e. which do not contain any router able to provide other routers requesting configuration with addresses or prefixes derived from a global prefix. Again, 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).

3.3. 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. A taxonomy of autoconfiguration issues specific to MANETs is then elaborated.

4.1. MANET Autoconfiguration Goals

A MANET router needs to configure IP addresses and prefixes as usual, on its non-MANET interfaces as well as its attached hosts and routers, if any. In addition, a MANET router needs to configure at least one IP address on its MANET interface, this being a link local address, an MLA or a global address. A MANET router may also require a delegated MLP, provided prefix uniqueness is guaranteed [2].

The primary goal of MANET autoconfiguration is thus to provide mechanisms for IPv6 prefix delegation and address assignment for operation on mobile ad hoc networks. 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.

Traditional dynamic IP address assignment protocols, such as [5], [3] or [4], do not work efficiently (if at all) on MANETs, due to these networks' unique properties. The following thus overviews what must be specifically supported for efficient operation on mobile ad hoc networks.

4.1.1. 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 DHCP can to some extent overcome this issue in a static network, it is not the case in a dynamic topology, as explained below.

```
                                                       ----- MR1...MR3
                                                      /      .
              +-------------+         +------------+ /       .
              |             |   p2p   |  MANET     |/        .
              |  ISP Edge   |   Link  |  Border    |         .
              |   Router    +---------+  Router    |\        .
              |             |         |            | \       .
              +-------------+         +------------+  \----- MR2
```

Fig. 1. Connected MANET router topology.

4.1.2. 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. Moreover, possible frequent reconfiguration due to intermittent reachability cause [5] to be less efficient than expected, due to large amounts of control signalling.

In particular, supporting multihop dynamic topologies means that even if some address configuration servers are present somewhere, it cannot be assumed that they are reachable most of the time, contrary to usual scenarios. Therefore, reusing "as-is" existing solutions (for instance [4]) using servers on a MANET would basically imply that "everyone is a server" in order to ensure server reachability. This implication is the specificity of MANETs that brings the requirement for new levels of service distribution, since the "everyone is a server" approach is essentially not functional.

4.1.3. 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 4.2.2), 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 4.2.2).

4.1.4. 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.

```
                          ----- MR1...MR3...MR5
                         /      .
                        /       .
                       /        .
                    MR4         .
                       \        .
                        \       .
                         \----- MR2
```

Fig. 2. Standalone MANET router topology.

4.2. MANET Autoconfiguration Issues

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

4.2.1. Address and Prefix Generation

The distributed nature of MANETs brings the need for address generation algorithms that can complement existing solutions by supporting operation outside "client-server" schemes and without fixed hierarchies to provide routers with appropriate addresses and prefixes. In addition, the multi-hop aspect of MANETs brings specific needs as far as address and prefix uniqueness is concerned, as detailed below.

4.2.2. 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 ensure address/prefix uniqueness, then additional issues arise. This section overviews these problems.

Pre-service Issues -- Address or prefix uniqueness problems in this category 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 desireable to reduce the risks of loops due to routing table pollution with duplicate addresses.

In-Service Issues -- Address or prefix uniqueness problems in this category 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, then checking pre-service uniqueness of addresses and prefixes may not be used. If on the other hand (i) is not extremely low, then checking pre-service and in-service uniqueness of addresses or prefixes may be required. In any case, if the application has a hard requirement for address uniqueness assurance, in-service uniqueness checks of addresses and prefixes should always be used, no matter how unlikely is the event of address conflict.

4.2.3. Internet Configuration Provider Related Issues

Another category of problems concern the management of Internet configuration providers (ICPs).

In the case where multiple ICPs 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 border router responsible for one particular prefix. However, asymmetry in the routers' choice of ingress/egress 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 router changes its ICP affiliation, 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).

5. Solutions Considerations

Solutions must achieve their task with (i) low overhead, due to scarse 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. However, it must be ensured that no modification of existing protocols is to be required outside of MANET scope.

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., 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 contributers, 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: Shubranshu@gmail.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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