MANET Autoconfiguration (Autoconf)
Internet-Draft
Expires: December 20, 2007

E. Baccelli (Ed.)
INRIA
K. Mase
Niigata University
S. Ruffino
Telecom Italia
S. Singh
Samsung
June 18, 2007

Address Autoconfiguration for MANET: Terminology and Problem Statement
draft-ietf-autoconf-statement-00

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 [2] [1]) consists of a loosely connected set of MANET routers. Each MANET router embodies IP routing/forwarding functionality and may also incorporate host functionality. 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.

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. Note that this task is namely distinct from that of just vehiculing knowledge about address or prefix location such as a routing protocol does (see for example [8], [9]), or such 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.

Solutions must achieve their task with (i) low overhead, due to scarse bandwidth, and (ii) low delay, due to the dynamicity of the topology. Solutions are designed to work at the network layer and thus applies 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.

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 also use some addresses defined in [10] for auto-configuration purposes.

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 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 an MBR, since the server and the MANET router are not located on the same logical link. While some DHCP extensions (such as the relay-agent [11]) overcome this issue in a static network, it is not the case in a dynamic topology, as explained below.

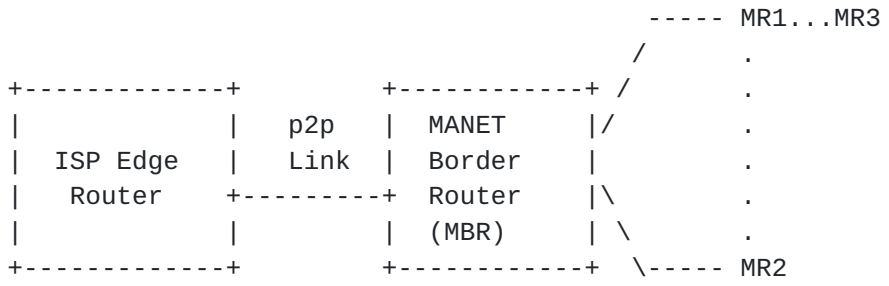

Fig. 1. Connected MANET router topology.

4.2.2. Lack of 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 assume the existence of a permanent hierarchy among devices and the permanent reachability of a configuration server. 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.

4.2.3. Lack of 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 4.3.2), issues arise that were not accounted for in traditional networks and solutions.

4.2.4. Lack of Network Partitionning Support

Network partinionning 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 partitnionning 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 "client-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 desireable 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 partitionning 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.

The need for checking uniqueness of addresses that are to be assigned or already assigned and used may depend on (i) the probability of address conflicts, (ii) the amount of the overhead for checking uniqueness of addresses, and (iii) address uniqueness requirements from applications.

For instance, if (i) is extremely low and (ii) significant, checking uniqueness of addresses may not be used. If on the other hand (i) is not extremely low, checking uniqueness of addresses should be used. In any case, if the application has a hard requirement for address uniqueness assurance, checking uniqueness of addresses should always be used, no matter how unlikely is the event of address conflict.

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 undesireable 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 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 is considered most suitable for ad hoc networks, although the other two models may also be applicable in some cases, for example when a trust relationship exists between an operator and some MANET routers. 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.

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.

[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.

Contributors

This document is the result of joint efforts, including those of the following contributers, listed in alphabetical order: C. Adjih, T. Boot, T. Clausen, C. Dearlove, 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).