

Adh-Hoc Network Autoconfiguration
(AUTOCONF)
Internet-Draft
Intended status: Informational
Expires: December 20, 2010

CJ. Bernardos
M. Calderon
UC3M
H. Moustafa
France Telecom
June 18, 2010

Survey of IP address autoconfiguration mechanisms for MANETs
draft-bernardos-manet-autoconf-survey-05

Abstract

This Internet Draft provides a detailed description of most of the existing IP autoconfiguration solutions proposed so far. The main aim of this document is to serve as a general reference for the AUTOCONF solution space. We present most of the previously proposed IP AUTOCONF mechanisms in MANETs, showing their key characteristics. Furthermore, each solution is analysed based on a number of evaluation considerations.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on December 20, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

Internet-Draft

MANET autoconf survey

June 2010

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Draft

MANET autoconf survey

June 2010

Table of Contents

1.	Introduction and motivation	5
2.	IP address auto-configuration protocols	7
2.1.	Solutions for Standalone MANET scenarios	7
2.1.1.	No merging support	7
2.1.1.1.	IP address Autoconfiguration for Ad Hoc Networks (Perkins et al.)	7
2.1.2.	Merging support	9
2.1.2.1.	IPv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks (Weniger et al.)	9
2.1.2.2.	Ad Hoc IP Address Autoconfiguration (Jeong et al.)	10
2.1.2.3.	IP Address Assignment in a Mobile Ad Hoc Network (Mohsin et al.)	12
2.1.2.4.	An Address Assignment for the Automatic Configuration of Mobile Ad Hoc Networks (Tayal et al.)	14
2.1.2.5.	No Overhead Autoconfiguration OLSR (Mase et al.)	15
2.1.2.6.	PDAD-OLSR: Passive Duplicate Address Detection for OLSR (Weniger et al.)	17
2.1.2.7.	Passive Duplicate Address Detection for On-demand Routing Protocols (Jeong et al.)	20
2.1.2.8.	Prophet Address Allocation for Large Scale MANETs (Zhou et al.)	22
2.1.2.9.	MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network (Nesargi et al.)	23
2.2.	Solutions for Connected MANET scenarios	25
2.2.1.	No merging support	25
2.2.1.1.	Automatic Configuration of IPv6 Addresses for Nodes in a MANET with Multiple Gateways (Ruffino et al.)	25
2.2.1.2.	Simple MANET Address Autoconfiguration (Clausen et al.)	26
2.2.1.3.	Extensible MANET Auto-configuration Protocol	

	(EMAP) (Ros et al.)	28
2.2.1.4.	Global Connectivity for IPv6 Mobile Ad Hoc Networks (Wakikawa et al.)	30
2.2.1.5.	Multihop Radio Access Network (MRAN) Protocol Specification (Hofmann)	32
2.2.1.6.	Automatic IP Address Configuration in VANETs (Fazio et al.)	34
2.2.1.7.	Address Configuration Using Address Pool (Ahn et al.)	36
2.2.1.8.	Address Autoconfiguration for MANET with Multiple MBRs (Lee et al.)	38
2.2.1.9.	Border Router Discovery Protocol (BRDP) based	

	Address Autoconfiguration (Boot et al.)	39
2.2.2.	Merging support	41
2.2.2.1.	Address Autoconfiguration in Optimized Link State Routing Protocol (Adjih et al.)	41
2.2.2.2.	Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks (Cha et al.)	43
2.2.2.3.	Gateway and Address Autoconfiguration for IPv6 Adhoc Networks (Jelger et al.)	44
2.2.2.4.	VET, SEAL, RANGER (Templin et al.)	46
2.2.2.5.	A DHCP-based IP address autoconfiguration for MANETs (Bernardos et al.)	47
3.	Security Considerations	49
4.	IANA Considerations	50
5.	Acknowledgements	51
6.	References	52
6.1.	Normative References	52
6.2.	Informative References	52
Appendix A.	Change Log	56
	Authors' Addresses	57

1. Introduction and motivation

Multi-hop communication in ad hoc networks presents some interesting advantages, where no permanent infrastructure is required. Also, the coverage area of an existing infrastructure can be extended through multi-hop ad hoc communication. Several MANET routing protocol specifications have been developed by the IETF MANET WG. In order to allow wide deployment of ad hoc networks, in which IP routing is the most candidate approach, IP configuration of nodes is a strong requirement that need to be satisfied. In this context, the AUTOCONF WG is working towards standard specifications and solutions for IP address autoconfiguration within different MANET environments.

Ad hoc networks present particular characteristics that should be taken into account when designing address auto-configuration protocols. Since existing solutions for IP infrastructure-based networks (e.g., RFCs 4861, 4862, 3315 etc.) were designed for a different scope than MANETs, there are several issues that need to be tackled, mainly (but not only) the following: 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 first (and so far unique) goal of the AUTOCONF WG has been to describe a practical addressing model for ad hoc networks and how nodes in these networks configure their IP addresses [2]. Now it is the time to start working on solutions (the WG is currently considering to re-charter to work on actual solutions). In previous discussions, the group has identified two possible scenarios of MANET where IP address auto-configuration is required:

- o Standalone MANETs: these networks 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 this scenario, nodes may join or leave randomly. Besides, most likely no pre-established nor reliable address or prefix allocation agency will be present in the network.
- o Connected MANETs. These networks have connectivity to one or more external networks, typically the Internet, by means of one or more gateways that are also known as MBRs (MANET Border Routers). These networks may be connected to the Internet in permanent fashion or in intermittent fashion.

This draft aims at providing a survey on most of the previously proposed IP autoconfiguration solutions, trying to serve as a useful reference for the AUTOCONF WG during the problem space analysis and

solution design phases.

In the following section, we provide a description of several existing AUTOCONF solution proposals. In order to present the analysed solutions in a structured way, two major classification levels are used: i) standalone/connected, and ii) partitioning/merging support. Note that this is just one of the many possible solution classifications that could have been followed. In order to provide additional information, we evaluate each of the analysed solutions against some of the evaluation considerations proposed in [1].

[2.](#) IP address auto-configuration protocols

In this section we briefly describe some of the existing proposals for IP address autoconfiguration, classifying them according to some of the evaluation considerations introduced in [\[1\]](#).

[2.1.](#) Solutions for Standalone MANET scenarios

2.1.1. No merging support

2.1.1.1. IP address Autoconfiguration for Ad Hoc Networks (Perkins et al.)

This address autoconfiguration mechanism -- proposed in [3] -- basically consists in choosing an address randomly from an address pool (i.e., a network prefix) available to the MANET and then performing a Duplicate Address Detection procedure within the MANET.

Assumptions: It is assumed that nodes performing this autoconfiguration protocol obtain a non-link-local prefix (it cannot be link-local, since the addresses have to be valid over a multiple-hop distance) from which to configure an address. The method to obtain a globally routable prefix is not specified in the solution and, in case it is not possible to obtain any suitable one, a reserved IPv6 prefix, called MANET_PREFIX, is used: fec0:0:0:ffff::/64.

Approach description: This solution basically works as follows: a node first selects a random address from the non-link-local prefix that is deployed in the MANET and then performs a Non-unique Address Detection procedure to check for its uniqueness across the MANET. To perform this uniqueness check, the node sends an Address Request (AREQ) message, including the randomly chosen tentative non-link-local IP address. This message is broadcast to its neighbours, by sending the message using the all-nodes multicast IPv6 address as destination of the packet. The source address used by the node to send the AREQ message is another temporary IP address, acquired only for the purpose of sending these messages. This temporary IPv6 address belongs to a different non-overlapping prefix -- called MANET_INITIAL_PREFIX -- so the probability of this address to be duplicated in the network is very low, given its short lifetime (this address is only used in this message exchange and discarded thereafter). When a node receives an AREQ message, it creates a reverse route entry for the temporary IPv6 address of the node. If the tentative address contained in the AREQ message does not match the address of the receiving node, it rebroadcasts the message to its neighbours. If the IP address of the receiving node matches the tentative address contained in the AREQ message it sends an Address

Reply (AREP) message to the sender, indicating that the address is

already in use. The route created by the AREQ messages is used to route the message back to the source node.

A node waits for a certain amount of time after sending an AREQ message, for the reception of an AREP message. The process is repeated if no answer is received, and if after a number of attempts no AREP has been received, the node assumes that the tentatively chosen IPv6 address is unique and starts using it. The values configured for the involved timers and retry parameters have an impact on the maximum size of the MANET where the solution would properly work. Additionally, since the Non-unique Address Detection procedure is performed only when the node initially chooses the tentative IPv6 address to use, this mechanism does not support merging of MANETs.

AREQ and AREP are a modification of the standard ICMPv6 Neighbour Advertisement and Neighbour Solicitation messages, respectively.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: the solution targets standalone MANETs, although it considers the possibility of being applied to connected scenarios in those cases in which nodes are provided with the non-link-local prefix to be used in the MANET.
- o Routing protocols' dependency: the solution is routing protocol independent.
- o Address uniqueness: the proposed solution makes use of Non-unique Address Detection in the initial address assignment phase.
- o Distributed/centralised approach: the solution does not make use of any centralised server.
- o Merging support: the solution does not support merging.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the solution requires additional message flooding (AREQ messages) to verify if an IP address is being used in the MANET.

[2.1.2.](#) Merging support

[2.1.2.1.](#) IPv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks (Weniger et al.)

The solution described in [\[4\]](#) extends the Neighbour Discovery and IPv6 Stateless Address Autoconfiguration mechanisms to work in multi-hop wireless networks.

Assumptions: The solution assumes a hierarchical approach, where there are two different types of participating nodes: those that obtain IPv6 addresses by using a modified version of IPv6 Neighbour Discovery, and special nodes -- called leader nodes --, that are responsible for parts of the address configuration of other nodes.

Approach description: The solution basically extends IPv6 Neighbour Discovery to provide nodes within a multi-hop environment with IPv6 address autoconfiguration capabilities. To do so, the following modifications to the IPv6 Neighbour Discovery protocol are proposed:

- o The Neighbour Solicitation message is modified to allow it to be broadcast to a bounded area of radius *r_s* hops (instead of only a single hop). In addition, a new option for Neighbour Discovery is defined (called MANET option) which contains a Random Source ID (RS-ID) field, that is used to distinguish different nodes. Nodes use the all-nodes multicast address instead of the solicited-node multicast address. This mechanism guarantees link-local addresses to be unique within the scope (limited by *r_s*) of each node.
- o To enable the configuration of unique site-local addresses, a hierarchy is established by special nodes (called leader nodes) that configure a group of nodes by issuing Router Advertisements (RA) within their scope, containing the subnet ID (i.e., network prefix) and its link-local address as source address. The subnet ID has to be unique for each leader node, so Non-unique Address Detection has to be performed between the leader nodes within the entire Ad hoc network. An algorithm is provided for the election of leader nodes.

It should be noted that because of the nature of the solution, it would be possible to have multihomed nodes -- that is, nodes with more than one IPv6 address -- if a node is within the scope of more than one leader node.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: the solution targets standalone MANETs, although it could be possible to extend it to support the assignment of

global IPv6 addresses.

- o Routing protocols' dependency: the solution does not depend on any particular ad-hoc routing protocol, but it may be advantageous the routing protocol follows a hierarchical structure. Besides, it is also preferable that nodes move in logical groups. Otherwise, the cost of maintaining the hierarchical structure may be considerable.
- o Address uniqueness: the proposed solution makes use of a periodic Non-unique Address Detection for ensuring the address uniqueness within the scope of the leader node. Since each leader node makes use of a different Subnet ID, the uniqueness of the assigned address within the entire MANET is ensured.
- o Distributed/centralised approach: the solution does not make use of any centralised server, but considers the existence of special nodes (leader nodes) that participate in the mechanism in a distributed fashion.
- o Merging support: the solution support merging, by leader nodes performing periodic Non-unique Address Detection that ensures the uniqueness of Subnet IDs.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the solution requires additional message flooding within a bounded area of radius r_s hops.

[2.1.2.2](#). Ad Hoc IP Address Autoconfiguration (Jeong et al.)

The solution described in [5] proposes two Non-unique Address Detection mechanisms. The first one -- called "strong DAD" -- is done in the initial phase when the ad hoc node does not have an IP address configured yet, it relates to the fact that before a randomly generated address is assigned and used, it should be verified that it will not create an address conflict. On the other hand the second Non-unique Address Detection mechanism -- called "weak DAD" -- is

always executed by nodes taking part in ad hoc routing in order to prevent any address conflicts due to mergers.

Assumptions: The solution assumes that initially a random address is selected by ad hoc nodes using the reserved IPv6 prefix MANET_PREFIX.

Approach description: This approach includes two different Non-unique Address Detection mechanisms:

- o Strong DAD: based on [3]. Strong DAD is done initially after an ad hoc node has chosen randomly an IP address and it is trying to find out whether there is a duplication conflict or not. AREQ message for Strong DAD is broadcast in site-local scoped all node multicast address, IPV6_MANET_BROADCAST_ADDRESS. The ad hoc node waits for an AREP message -- indicating the selected address has already been utilised -- until the timer for Strong DAD expires. In the case an AREP message arrives it chooses a new address and executes Strong DAD mechanism again. [5] describes the message format, using ICMPv6 messages (new types are defined). [6] describes the message format for AODV.
- o Weak DAD: based on [7]. During ad hoc routing, weak DAD is used to find out whether address duplication, due to merging has occurred or not. The concept of ``Virtual IP address'', which is the combination of an 'IP address' and an 'Key', is used, which is selected to be unique by each mobile ad hoc node. This 'key' is appended to control packets of ad hoc routing protocol, such as route discovery messages or hello messages. Intermediate routing points must store the 'key' value for each address in its routing table. Using these 'keys', duplication conflicts can be found out during ad hoc routing process. An AERR message is sent during Weak DAD for the purpose of indicating that an address duplication happened. The ad hoc node that receives an AERR message should autoconfigure a new IPv6 address through Strong DAD. The same AERR message is used to inform each peer node that its address has been changed. In order to keep ongoing sessions after an address duplication episode, data packets are sent to the new address through IP tunnelling. The destination address in outer IP header is the new IP address of the node that announced duplicate address and the inner IP header contains the duplicate IP address of the node, i.e. the old address of the

node. The match duplicate address and new address is done in an Address Mapping Cache.

Based on [1], this solution has the following key features:

- o MANET scenario: the solution targets standalone MANETs.
- o Routing protocols' dependency: the solution does not depend on any particular ad-hoc routing protocol.
- o Address uniqueness: the proposed solution makes use of two different Non-unique Address Detection mechanisms.
- o Distributed/centralised approach: the solution is distributed. It does not make use of either any centralised servers or special nodes.

Bernardos, et al.

Expires December 20, 2010

[Page 11]

Internet-Draft

MANET autoconf survey

June 2010

- o Merging support: the solution supports merging by looking for duplicate addresses on an ongoing basis.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: The Strong DAD mechanism requires additional message flooding (AREQ messages) to find out whether there is a duplication conflict or not. The Weak DAD mechanism introduces also some protocol overhead since the Key extension (20 bytes) is appended to each control packet of the ad hoc routing protocol.

[2.1.2.3](#). IP Address Assignment in a Mobile Ad Hoc Network (Mohsin et al.)

This proposed solution [8] is based on a dynamic allocation of IP addresses in MANETs using the concept of binary split. A proactive approach is used, in the sense that each node can independently assign a new IP address without consulting any other node in the network. Partitioning and merging as well as nodes abrupt departures are supported in this solution.

Assumptions: It is assumed that all nodes collectively perform the DHCP functionality; where each node is capable of configuring a new node and providing it with a new IP address. It is also assumed that

one MANET node have the entire pool of IP addresses at the beginning.

Approach description: In this proposed solution the concept of Buddy Systems is used. This is a type of segregated lists used in memory allocation and supports efficient splitting and coalescing. In the context of the proposed solution, binary buddies are used, where all buddy sizes are a power of two, and each size is divided into two equal parts. Thus, every node has a disjoint set of IP addresses that it can assign to a new node without consulting any other node in the network. When a new unconfigured mobile node (B) joins the network, it requests the nearest neighbour (A) an IP address. Node (A) divides its IP address set into two, giving one half to the requesting node (B). The new node assigns itself an IP address from the acquired pool of addresses, storing the rest of addresses to configure other nodes afterwards. The new node (B) is now configured and is considered as the Buddy of node (A). The scheme of the IP address assignment can be seen as a handshaking protocol between the server and the client, where the node requesting the IP address is considered as the client node and the node that actually assigns the IP address is considered as the server node.

Nodes synchronise the IP blocks which they store to keep track of the assigned IP addresses and detect any IP leakage, where every node

keeps a record of all the IP address blocks in the network by maintaining a corresponding table. Each node sends its IP address pool to all other nodes in the network, and each node receiving an IP pool from another node records the received information in its IP address table. Through this approach, the network has among its nodes the available IP addresses organised in the form of a binary tree with a division of two identical blocks (Buddies) per level.

Two mechanisms are proposed for releasing the node's IP address pool when the node leaves the network: i) graceful leave, in which the leaving node gives its IP address pool to any nearby node. This nearby node may keep the IP address pool for itself or may search in its IP address table the Buddy of the leaving node and forward to it the IP pool. ii) abrupt leave, in which the node leaves with its IP address pool that leads to IP leakage. In such a case, a pool of IP addresses that is not assigned to any node is not available. IP leakage is detected from the IP address table stored at each node. Each node scans from time to time its IP address table for the IP

pool of its Buddy node, if it does not find it, it concludes that the node has left and it merges this missing IP block to itself.

Based on [1], this solution has the following key features:

- o MANET scenario: This proposed solution targets standalone MANETs.
- o Routing protocols' dependency: This proposed solution is independent of the underlying routing protocol.
- o Address uniqueness: The proposed solution does not use any Non-unique Address Detection mechanism.
- o Distributed/Centralised approach: Although this solution is based on IP address pools assignment and splitting, it has a distributed approach, where all nodes collectively perform the functionality of a DHCP server.
- o Merging support: Thanks to employing the buddy systems, the proposed solution supports merging. In case of merging, the process of buddies splitting allows the merging node to be assigned an IP address and an IP pool.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the solution requires a kind of flooding so that each node sends its IP address block to all other nodes in the network. Furthermore, other control messages are required in the form of request-reply messages to enable a new joining node to

be assigned an IP address, or in the form of announcement in the case of IP release.

2.1.2.4. An Address Assignment for the Automatic Configuration of Mobile Ad Hoc Networks (Tayal et al.)

The solution described in [9] is very similar to the previous one ([8]), sharing the idea (also used by others) of nodes assignment of half of their address pools to newly arrived nodes that request IP addresses.

In a more recent work [10] it has been proposed a different way of managing the address pool. The authors propose to take advantage of node mobility and make the system achieve roughly even distribution of the free addresses amongs all nodes in the MANET. In order to achieve this goal a redistribution is performed everytime there is a process of address allocation, the new joining node redistributes evenly among its neighbors and itself the free addresses that were previously held by its neighbors.

Assumptions: It is assumed that initially there is one node that configures itself as initiator node (when there is no other node in the network), configuring itself with a default IP address and starting to manage a default address pool.

Approach description: The solution basically works as follows: when a new node *i* (called requester node) is willing to join the MANET, it has to contact an existing node *j* in the network. If node *j* has the address pool, it divides it into two parts and allocates one part to node *i*. The starting address of the allocated pool is the address of node *i*. In case node *j* does not have the address pool, *j* starts searching for nodes that might have an address pool, by broadcasting a message (called SEARCH_ADDR). The search message is forwarded by all the nodes which do not have an address pool. A node receiving the search message, either replies with the address pool or with negative ACK. If a node replies with its address pool, it marks half of its addresses as under allocation and wait for a POOL_ACCEPTED message from node *j*. Node *j* replies with POOL_ACCEPTED message to the node whose address pool it received first, and allocates the received address pool to node *i*.

This solution defines mechanisms to handle different scenarios, such as network partitioning and merging, message loss, etc. More details can be found in [9].

Based on [1], this solution has the following key features:

- o MANET scenario: This proposed solution targets standalone scenarios.
- o Routing protocols' dependency: This proposed solution is

independent of the underlying routing protocol.

- o Address uniqueness: The proposed solution does not use any Non-unique Address Detection mechanism, since the uniqueness of the solution is based on the split of the initially available IP address pool.
- o Distributed/Centralised approach: the solution is based on IP address pools assignment and splitting, where all nodes collectively perform the functionality of assigning addresses to newcomers.
- o Merging support: the solution defines a mechanism to detect merging, through redistributing information about assigned addresses and pools. If an address collision is detected, then the solution defines a mechanism to solve that, based on giving up/shrinking the address pool used by one of the nodes detecting the conflict.
- o Prefix assignment support: Since the solution supports the assignment of address pools, it can be possible to use it to assign prefixes to nodes, although it is not explicitly covered by the mechanism.
- o Protocol overhead: the solution requires some message flooding to search nodes that have an address pool available.

[2.1.2.5](#). No Overhead Autoconfiguration OLSR (Mase et al.)

This solution [[11](#)] proposes some passive Non-unique Address Detection techniques to be used in MANETs running the OLSR protocol. It utilises the Passive Duplicate Address Detection concept [[12](#)], [[13](#)], which enables nodes to passively detect duplicate addresses in the network (e.g., occurring after network merging) by analysing received routing protocol messages. The basic idea of PDAD is to exploit the fact that some protocol events occur in case of duplicate address, but (almost) never in case of a unique address. The proposed techniques may be used to ensure uniqueness of an address when it is initially generated before being assigned to an interface and the solution also performs to ensure uniqueness of addresses which have been assigned and used, and then a network merger happens.

This is one of the multiple drafts proposing the use of PDAD for OLSR [[14](#)], [[15](#)].

Assumptions: The protocol assumes the existence of a Non-unique Address Detection-based IP address generation mechanism.

Approach description: The solution proposes an ongoing duplicate address detection mechanism, checking for inconsistencies in the routing protocol messages to diagnose duplicate address detection. The first kind of inconsistency is based on information included in OLSR messages (such as HELLO messages and TC messages) and the second kind of inconsistency is based on sequence numbers (when two nodes -- which selected the same IP address -- are present in a network, they would send control messages that will be inconsistent).

Different Non-unique Address Detection rules -- twelve in total -- are proposed to handle the cases where the distance between conflicting nodes is one hop, two hops and, three hops or more. In the two first cases the detection is done by means of HELLO messages and in the last case -- three hops or more -- the detection is fulfilled by using information inside TC messages. Also, an additional case is taken into account: this is a specific multihop address conflict case, where the address conflict results in deficiencies in the MPR selection.

Each node has an "autoconfiguration state". This state is an indicator of how long the node has been in the network. The central idea, is that each time a node generates a tentative address, it should enter the network gradually, running a restrained version of the OLSR protocol. In this way, the node can detect which addresses are being used, checking for duplicates of its own address, while avoiding to disrupt the routing tables of the other nodes, in the event that its address is actually found to be in conflict.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: This Non-unique Address Detection technique is to be used in standalone MANETs.
- o Routing protocols' dependency: this mechanism depends on OLSR, since the Non-unique Address Detection technique is designed for MANETs running the OLSR protocol.
- o Address uniqueness: The proposed mechanism assumes the existence of a Non-unique Address Detection-based address assignment mechanism.
- o Distributed/centralised approach: the proposed solution follows a distributed approach given that all nodes have the same responsibility detecting address conflicts.

- o Merging support: The proposed solution supports merging, enabling nodes to continuously detect duplicate addresses by analysing received routing protocol messages.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the proposed mechanism does not add any additional messages but it checks for inconsistencies in the routing protocol messages to diagnose duplicate address detection.

[2.1.2.6](#). PDAD-OLSR: Passive Duplicate Address Detection for OLSR (Weniger et al.)

This solution [[14](#)] proposes a passive Non-unique Address Detection mechanism for configured address uniqueness maintenance in MANETs running the OLSR protocol.

Assumptions: The protocol assumes the existence of a Non-unique Address Detection-based address generation mechanism.

Approach description: The proposed solution is made up of a set of algorithms which specify how to detect duplicate addresses based on incoming routing protocol messages. The algorithms utilise different parameters in TC and HELLO messages such as link states (i.e., neighbour interface addresses), link codes, (message) sequence numbers, and addresses in OLSR routing protocol messages as well as addresses in the IP header. PDAD-OLSR allows the detection of conflicts by intermediate nodes that have unique addresses.

Each node conceptually maintains two tables for PDAD: a Last received Protocol Messages (LRM) table and a Neighbour History (NH) table. LRM table contains information about the last TC and HELLO protocol message received from a specific originator address (e.g., originator address, message type, sequence number, neighbour interface addresses, receive time). NH table contains the history of neighbouring node addresses and is built from received HELLO messages (e.g., neighbour interface address, last time the receiver has selected this neighbour interface address as MPR, Last time the receiver has been selected as MPR by this neighbour interface

address, reception time).

The solution proposes eight different algorithms for conflict detection:

- o PDAD-Source Address (SA). Whenever a node receives a TC or HELLO message, it compares the source address in the IP header to its own address (the IP source address is always the address of the

last forwarder). This mechanism (e.g., Both addresses coincide) allows nodes to detect conflicts with its neighbouring nodes.

- o PDAD-Sequence Numbers (SN): If a node receives a TC or HELLO message, it compares the originator address with its own address. If they are equal and the sequence number in the message is higher than the receiver's sequence number, a conflict of the originator address is detected. This mechanism allows to detect conflicts between nodes that are any number of hops away from each other.
- o PDAD-Sequence Number Difference (SND): If a node receives a TC or HELLO message, it compares the sequence number in the message with the sequence number in the previously received message from the same originator address and with the same message type (there is a relation between the time a node has originated two TC messages and the sequence number in those TC messages). This mechanism allows to detect conflicts between nodes that are any number of hops away from each other.
- o PDAD-Sequence Numbers Equal (SNE): If an intermediate node receives a TC or HELLO message, it searches its LRM table for a message with the same type value and the same tuple < sequence number, originator address > (the tuple < sequence number, originator address > uniquely identifies messages originated by a specific node. This mechanism allows to detect conflicts between nodes that are any number of hops away from each other.
- o PDAD-SNs Always Increment (SNI): If a node receives a HELLO message, it compares the sequence number in the message with the sequence number in the previous HELLO message from the same originator address (HELLO messages sent by a specific node are received in the order they are sent). This mechanism only allows to detect conflicts between nodes that are at most two hops away

from each other.

- o PDAD-Neighbourhood History (NH): If a node receives a TC message, it checks whether its own address is part of the neighbour interface addresses in the TC message. If this is the case and the link code indicates a bi-directional link, the node searches the originator address in its NH table (a TC message only contains neighbours that have selected the originator address as MPRs and that requires a bi-directional link). This mechanism allows to detect conflicts between nodes that are any number of hops away from each other.
- o PDAD-Link States (LS): If a node receives a TC message with its own address as originator address, it searches in its NH table for each of the neighbour interface addresses (if the message has been

originated by the receiver, it must only contain addresses of recent neighbour interfaces). This mechanism allows to conflicts between nodes that are any number of hops away from each other.

- o PDAD-extended Neighbourhood History (eNH): If a node receives a TC message, it checks for each neighbour interface address in the message if it is a neighbour. This algorithm is basically the PAD-NH algorithm executed on behalf of a neighbouring node. Minimal additional signalling is needed. This mechanism allows to detect conflicts between nodes that are any number of hops away from each other.

For some of the above mechanisms it is crucial to detect a possible sequence number wrap-around, so a mechanism to detect this kind of events is proposed.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: The solution targets standalone MANETs. Although it proposes a Non-unique Address Detection mechanism suitable for any kind of addresses exchanged in routing protocol messages, be it MANET-local or globally routable addresses, the solution does not address the issue of how to obtain global IPv6 addresses.
- o Routing protocols' dependency: this solution requires OLSR, since the set of proposed techniques are applicable to MANETs running

the OLSR protocol.

- o Address uniqueness: The proposed mechanism assume the existence of an address assignment mechanism which may assign duplicate addresses.
- o Distributed/centralised approach: The solution follows a completely distributed approach, every node has the same responsibility in detecting duplicate addresses and does the same processing.
- o Merging support: The proposed solution supports merging given that it enables nodes to continuously detect duplicate addresses in the network by analysing received routing protocol messages.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the solution enables nodes to passively detect duplicate addresses in the network by analysing received routing protocol messages and thus does not cause any overhead.

[2.1.2.7](#). Passive Duplicate Address Detection for On-demand Routing Protocols (Jeong et al.)

This solution [16] proposes a set of Non-unique Address Detection techniques to be used jointly with an on-demand routing protocol. In this proposal passive duplicate address detection is performed by analysing incoming on-demand routing protocol packets.

Assumptions: The protocol assumes the existence of an on-demand routing protocol and a Non-unique Address Detection-based IP address configuration mechanism.

Approach description: In this proposal passive duplicate address detection is performed by analysing incoming on-demand routing protocol packets. Additional information included in routing protocol packets allows end-points of a communication -- source or destination -- to detect that the other end-point is using an address which is duplicated in the MANET.

This additional information is included into routing control packets exchanged for route discovery and it may be: the node location when it configured its IP address, the node's neighbour list when it configured its IP address, or a sequence number in RREP packets (increased whenever a destination node sends a new RREP packet).

The authors propose different mechanisms for detecting address conflicts:

- o PDAD-RREQ-with-Location-information Technique (RQL): This technique includes location information in RREQ packets to differentiate between RREQ packets which contain the same source address but are generated by different nodes.
- o PDAD-RREQ-with-Neighbour-knowledge Technique (RQN): This technique includes a list of neighbour nodes (this list is captured and recorded when the node's IP address is configured) in RREQ packets to differentiate between RREQ packets which contain the same source address but are generated by different nodes.
- o PDAD-RREP-with-SEQ Technique (RPS) : This technique requires an incremental PDAD-sequence number to be included in each RREP packet transmitted by a destination node. Therefore, when a source node receives more than one RREP packet with the same PDAD-sequence number and the same destination address, the source node can detect the address conflict of destination nodes.
- o PDAD-RREP-with-Location-information Technique (RPL): This technique includes location information into RREP packets to

differentiate between RREP packets which contain the same source address (the source address of RREP packets is the destination address of RREQ packets) but are generated by different nodes.

- o PDAD-RREP-with-Neighbour-knowledge Technique (RPN): When a destination node replies with an RREP packet, a list of neighbour nodes of the destination node (this list is captured and recorded when the node's IP address is configured) is included in the RREP packet.

The document does not include how to perform address conflict resolution.

Based on [1], this solution has the following key features:

- o MANET scenario: The solution targets standalone MANETs. Although the proposed Non-unique Address Detection mechanism is suitable for any kind of addresses exchanged in routing protocol messages, be it MANET-local or globally routable addresses, it does not define any mechanism to obtain global IPv6 addresses.
- o Routing protocols' dependency: The set of proposed techniques supposes the existence of an on-demand ad-hoc routing protocol.
- o Address uniqueness: The proposed mechanism assumes the existence of a Non-unique Address Detection-based address assignment mechanism.
- o Distributed/centralised approach: The solution follows a completely distributed approach, every node has the same responsibility in detecting duplicate addresses and does the same processing.
- o Merging support: The proposed solution supports merging given that it enables nodes to continuously detect duplicate addresses in the network by analysing received routing protocol messages.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the solution enables nodes to passively detect duplicate addresses in the network by analysing received routing protocol messages and thus does not cause any overhead.

[2.1.2.8](#). Prophet Address Allocation for Large Scale MANETs (Zhou et al.)

The mechanism defined in [17] is based on the use of a special type of function to derive the IPv6 addresses of nodes, so the probability

of address duplication is very low, and therefore the use of a Non-unique Address Detection mechanism can be avoided.

Another proposal sharing the idea of avoiding duplication is presented in [18] where to avoid address duplication it is assumed that the IPv6 address of a node includes its Home Subnet identifier (i.e., a subnet where the node originally belongs to) as part of the 64-bit Host identifier. This is because "at home administration" guarantees that nodes belonging to the same home subnet have different Host identifier.

Assumptions: This solution is based on the use of a stateful function $f(n)$ (where the initial state of $f(n)$ is the seed) that produces as output an integer sequence of numbers. Different seeds lead to different sequences, and the state of $f(n)$ is updated. This function can be used to generate IP addresses, since it satisfies the following properties:

- o The interval between two occurrences of the same number in a sequence is extremely long.
- o The probability of more than one occurrence of the same number in a limited number of different sequences initiated by different seeds during some interval is extremely low.

These properties may be satisfied if the space of available addresses is large, so it is relatively easy to achieve in IPv6.

Approach description: The mechanism basically work as follows: the first node in the MANET chooses a random number as its IP address and uses a random or default state value as the seed for its $f(n)$. When a different node approaches, the first node uses its $f(n)$ to obtain a different number and state. This number is used by the second node as its IP address, and the state is used as the seed for its $f(n)$. After that both nodes are able to assign IP addresses to other nodes.

Authors of the mechanism propose different mechanisms to support partitioning/merging, such as for example including the seed used in the MANET in the messages of the routing protocol. By doing that, nodes of different merging MANETs can easily detect the merge (if different seeds are received, that would mean that a merge has happened) and start checking if there are potential IP address conflicts. Given the characteristics of the function $f(n)$ if a MANET

gets partitioned and later merges, IP address conflicts are very unlikely to occur.

Based on [1], this solution has the following key features:

- o MANET scenario: the solution targets standalone MANETs.
- o Routing protocols' dependency: the solution is routing protocol independent.
- o Address uniqueness: the proposed solution does not define any Non-unique Address Detection mechanism. The address uniqueness is ensured by using a "prophet" allocation with a very low probability of collision.
- o Distributed/centralised approach: the solution does not make use of any centralised server.
- o Merging support: the solution proposes different mechanisms to support merging.
- o Prefix assignment support: the solution supports the assignment of IPv6 prefixes to nodes, by using the DHCP prefix delegation.
- o Protocol overhead: only few additional messages are required to assign addresses to new nodes.

2.1.2.9. MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network (Nesargi et al.)

In this autoconfiguration mechanism -- proposed in [19] -- each node maintains a list of all IP addresses in use in the network and a new node (i.e., requester) obtains a candidate IP address through an existing node in the network (i.e., initiator). If the proposal is accepted by all the nodes that are part of the MANET, the proposed address is assigned to the newly arrived node. Otherwise, another candidate IP address is chosen and the process is repeated (for a finite number of times).

Assumptions: It assumes that the MANET starts with a single node initiating the configuration process.

Approach description: This solution basically works as follows: Each node maintains a list of all the addresses in use in the network. When a node joins the system, it requests an address through one of its neighbours that have joined the system. This neighbour (i.e., the initiator) chooses an address that is free according to its address list and query through the network for the permission to

Internet-Draft

MANET autoconf survey

June 2010

assign the chosen address. If at least one response is negative, another address is selected and another query is distributed. The assignment is granted only if a positive ack is received from all known nodes. The initiator makes this allocation permanent by flooding a second message sent once it has received confirmation from all known nodes. So, IP address allocation is similar to a two-phase commit.

In order to detect partitions and merges every node remember its address and its MANET (i.e., partition) identifier. A network partition is detected when a initiator fails to obtain permission for an address assignment for a new node from all the other nodes in the network (i.e., one or more nodes do not answer). After the detection, every node in each partition cleans up the addresses in other partitions. The nodes then agree on a new partition identifier.

This partition identifier is used to detect merges when two previously distant nodes come within communication range of each other and exchanger their partition identities. When partitions merge, nodes in different partitions are required to exchange their set of allocated addresses so that duplicates can be detected.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: the solution targets standalone MANETs.
- o Routing protocols' dependency: the solution assume the existence of a proactive routing protocol to handle network partitions and merges.
- o Address uniqueness: the proposed solution makes use of Non-unique Address Detection every time a new address is assigned to a node.
- o Distributed/centralised approach: the solution does not make use of any centralised server.
- o Merging support: nodes detect merges by receiving messages from nodes with a different partition identifier.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.

- o Protocol overhead: the solution requires at least flooding two messages along the address assignment process. One asking if a candidate address is perceived as unallocated by the rest of the nodes, and a second one making the assignation permanent.

[2.2.](#) Solutions for Connected MANET scenarios

[2.2.1.](#) No merging support

[2.2.1.1.](#) Automatic Configuration of IPv6 Addresses for Nodes in a MANET with Multiple Gateways (Ruffino et al.)

This proposed solution [[20](#)] describes a mechanism enabling nodes belonging to a MANET connected to the infrastructure -- by means of one or more gateways -- to obtain global IPv6 addresses that could be used to communicate with external nodes.

Assumptions: This mechanism assumes the existence of one or more gateways that provide MANET nodes with connectivity to external networks (e.g., the Internet). It is also assumed that nodes running this solution obtain at the bootstrapping phase a MANET local IPv6 address (which is the address that the node uses when it participates in the routing protocol, which is assumed to be OLSR). The uniqueness of the obtained address should be ensured by means of a Non-unique Address Detection method. Neither the procedure followed to obtain this address, nor the Non-unique Address Detection method used to check its uniqueness, are defined in this solution.

Approach description: The mechanism basically works as follows: at bootstrap, a node configures a Primary Address (PADD) that is MANET-scoped and is used as main address in OLSR messages. The node then is able to start participating to OLSR and receiving topology information. Each of the gateways available at the MANET has a global IPv6 prefix that is announced using a new OLSR message type, called Prefix Advertisement (PA).

With the prefix information received in the PA messages, a node is able to build a set of global IPv6 addresses (called Secondary Addresses: SADDs). Among them, the node chooses the "best" prefix and starts using the address formed from this prefix (called,

Designated Secondary Address: DSADD). The node introduces all (or a subset) of the SADDs (including the DSADD) in OLSR messages and starts broadcasting them, enabling these addresses to be routable and reachable within the MANET. It should be noted, that this solution does not define any new Non-unique Address Detection mechanism, while it is suggested to use a generic MANET Non-unique Address Detection procedure, such as [3], to verify the uniqueness of MANET-local and global addresses.

Based on [1], this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs.

- o Routing protocols' dependency: the solution requires OLSR to be run in the network.
- o Address uniqueness: the proposed solution does not define any Non-unique Address Detection mechanism, although requires some generic one to be used to ensure the uniqueness of MANET-local and global addresses.
- o Distributed/centralised approach: the solution does not make use of any centralised server, but requires gateways to announce the global IPv6 prefixes that can be used by MANET nodes in the configuration of their IPv6 addresses.
- o Merging support: the solution partially supports merging, since the scenario in which new gateways join the network as a result of a merger is considered. However, since no Non-unique Address Detection mechanism is defined, the solution does not describe how to deal with IPv6 address duplication after merging of different MANETs.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the solution adds some overhead. Since Gateways broadcast prefix information.

[2.2.1.2.](#) Simple MANET Address Autoconfiguration (Clausen et al.)

This proposed solution [21] aims to provide a simple IP autoconfiguration mechanism for mobile nodes joining an existing MANET. This mechanism is designed for MANETs that act as an edge-extension to the Internet, where mobile nodes need to maintain the connections with each other and with the Internet.

Assumptions: It is assumed that at least one node in the network is already configured with a permanent address. In the absence of a configured node, it is assumed that an election mechanism is undertaken allowing a selected node to be self-configured.

Approach description: In this proposed solution, only configured nodes can participate in the MANET and are considered as MANET nodes. These nodes are also considered as "configuring nodes" aiding the new joining nodes to acquire an IP address. Actually, each new joining node is firstly assigned a temporary local address then a permanent global address. The configuring nodes emit periodical ADDR_BEACON messages to their neighbours in order to signal their existence to new nodes. A new node joining the network selects a configuring node from its neighbours, then sends an Address Request (AREQ) to this

selected configuring node and waits for a reply. The process of sending AREQ may be repeated for a number of trials until either receiving a reply or selecting a new configuring node. The configuring node replies by an Addr-Config message, containing a local temporary address, and keeps track of the link existence with the new joining node through local routing messages exchange on this link. If this link disappears then the configuring node gives up, otherwise the configuring node assigns a global address to the new joining node.

The process of obtaining a temporary address consists of having an address space, where each MANET node independently selects an address sequence from this space and signals it to its neighbours (through beacons). Each MANET node records the address sequence received from its neighbours to avoid conflicts in the chosen addresses. If a conflict is detected between two nodes, the node with the lowest ID should select a new sequence if both nodes are not configuring nodes (MANET nodes that are not yet engaged in configuring a new node). Otherwise, if one or more configuring nodes are involved in the conflict, each configuring node should narrow its sequence of addresses to contain only the address that is currently assigned (in

order to keep on the configuring session). On the other hand two options exist for global addresses allocation. One option is that the configuring node acts as a modified DHCP proxy and transmits a request to a DHCP server to acquire a global address for each new node it configures. Another option is that the configuring node consults the nodes' topology tables (containing destinations and thus network addresses), and then picks up an unused address. It then sends an advertisement to all MANET nodes to be sure that this address is not used. If a node detects that its address is being used, it can signal the conflict to the originator of the advertisement.

Based on [1], this solution has the following key features:

- o MANET scenario: This proposed solution targets connected MANET scenarios.
- o Routing protocols' dependency: This proposed solution uses OLSR, typically extending OLSR messages, however it is not dependent on the routing protocol. Although the proposed solution is open to any routing protocol, the fact that periodical beacons are used requires a proactive routing protocol.
- o Address uniqueness: The proposed solution uses a Non-unique Address Detection mechanism to avoid conflicts in IP address assignment. In global address allocation, using a Non-unique Address Detection mechanism is an option but the proposed solution

can function without a Non-unique Address Detection mechanism if the modified DHCP proxy approach is followed. While in temporary address allocation, a limited Non-unique Address Detection mechanism is used with the neighbourhood to resolve any conflict when assigning temporary addresses sequences to MANET nodes.

- o Distributed/Centralised approach: The proposed solution is distributed in the sense that it can employ a decentralised DHCP server using the concept of proxy DHCP to reach the server.
- o Merging support: This proposed solution has no merging support.
- o Prefix assignment support: The proposed solution allows prefix assignment through using DHCP.

- o Protocol overhead: the solution requires a considerable number of signalling. This is mainly during the advertisement messages for global addresses flooded to all nodes in the network for verifying the global address uniqueness, the periodical ADDR_BEACON messages that are transmitted by each configuring nodes to its neighbours, and the Beacon messages signalling the selected address space by each configuring node during the process of temporary address assignment. Furthermore, AREQ messages are used by each new joining node while communicating a neighbour configuring node, which in turn replies by an Addr-config message.

2.2.1.3. Extensible MANET Auto-configuration Protocol (EMAP) (Ros et al.)

The Extensible MANET Auto-configuration Protocol (EMAP) [22] provides an autoconfiguration solution for isolated as well as hybrid MANETs. EMAP is envisioned to be integrated within unicast routing protocols as DYM0 or OLSRv2. The notion of intermediate proxies is used in the autoconfiguration process. The general EMAP framework may be used as a service discovery protocol for MANETs, however the approach is extensible to other services. An optional feature in EMAP includes DNS discovery, where nodes can discover DNS servers reachable from the MANET, and this feature can be extended to services like SIP, proxies, and authentication entities.

Assumptions: It is assumed that at least one element must act as a gateway between the MANET and the fixed network. This element is called an Internet Gateway (IGW).

Approach description: EMAP allows MANET nodes to configure unique IP local addresses and globally routable IP addresses. The local configuration allows a MANET node to communicate with other nodes in the same MANET. To configure a local address, the MANET node picks

an IP address and asks the network if it is already being used, thus avoiding address duplication. In this process, a node generates a pair of IP addresses: temporary and tentative ones. The temporary address is used as the originator-address, where it can be a mobile IP home address or another sort of highly likely unique address. While the tentative address is the one which is being requested and is used as the requested address in the DAD_REQ messages and the

originator-address in DAD_REP messages. Thanks to the proxy functionality, intermediate nodes can also answer with a DAD_REP message if they do not own the requested address but they do know that it is being used by another node. If the MANET node sending the DAD_REQ receives no DAD_REP messages, then it understands that there is no address conflict and it considers that the tentative address is its local address.

On the other hand, global configuration takes place through using the Internet Gateway (IGW), which may be a fixed element belonging to each network, or a mobile one which detects the presence of an attachment point to the Internet (e.g. a wireless router). The mobile node requesting a global address either waits for advertisements sent by the IGW (mainly advertising its prefix) to configure its global address or floods a global configuration request (GC_REQ) message. When an IGW receives a GC_REQ message, it sends a global configuration reply message (GC_REP) to the originator-address through unicast. Thus, the originating node is able to auto-configure a global address by substituting the first bits of the requested local address by the prefix advertised by the IGW. When there are multiple IGWs announcing their own information, the MANET node selects one, and the selection rules are implementation-dependent.

A given option in EMAP allows a MANET node to issue a query to find DNS Server Advertisers, which provide IP addresses of available DNS servers. This feature may be quite useful in situations where a high degree of auto-configuration is desired.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: This proposed solution is designed for standalone MANETs and connected MANETs.
- o Routing protocols' dependency: Although EMAP is envisioned to be integrated with unicast routing protocols like DYM0 or OLSRv2, it may be implemented as a standalone daemon.
- o Address uniqueness: The proposed solution uses a Non-unique Address Detection mechanism during the autoconfiguration of MANET local addresses.

- o Distributed/Centralised approach: The proposed solution is a distributed solution in the sense of not being based on any DHCP servers.
- o Merging support: No special merging mechanisms are explained in this solution. However, no in-service Non-unique Address Detection is used which makes the merging support not feasible.
- o Prefix assignment support: This solution employs IPv6 prefixes, where gateway nodes are responsible for advertising their prefixes.
- o Protocol overhead: the solution adds certain overhead, depending on the network size, the number of IGWs, and the applied option in global address configuration. The resulting overhead in this solution mainly concerns: flooding of the local address selected by each joining node to verify its uniqueness through the DAD_REQ messages, prefix advertisement by IGWs during global address configuration (this has more impact on the overhead when the number of IGWs increases), and flooding of GC_REQ messages by the node requesting a global address (in case that no prefix advertisement is taking place by the IGWs) where in this case GC_REP messages are sent by IGWs through unicast. Furthermore, DAD_REPLY messages could take place in case of address conflicts detection.

2.2.1.4. Global Connectivity for IPv6 Mobile Ad Hoc Networks (Wakikawa et al.)

The solution described in [23] proposes how to provide Internet connectivity with mobile ad hoc networks. It describes how to obtain a globally routable IPv6 address from an Internet gateway. The Internet access method is not dependent on a particular MANET routing protocol.

Assumptions: The solution assumes that before configuring a global IPv6 address, the node has configured a routable address (i.e. MANET-local address or a Mobile IPv6 home address). The routable address is used for initial configuration when a node boots up and joins the MANET.

Approach description: This mechanism [23] is similar to [24] from the point of view of how IPv6 addresses are configured. Global prefix information is obtained from Internet gateways. Two methods are proposed for the Internet gateway discovery: one method periodically disseminates gateway advertisements to all nodes in the MANET; the other method utilises solicitation and advertisement signalling between a MANET node and the gateway. Extended router solicitation

Internet-Draft

MANET autoconf survey

June 2010

and advertisements of the Neighbour Discovery Protocol (NDP) or extended control message of each MANET routing protocol can be used for this signalling. The proposed methods target all MANET protocols regardless of whether they are reactive or proactive. Internet gateways supply their own global prefix information and IPv6 global address to MANET nodes somehow, either proactively or reactively. In this way, the reactive and proactive route discovery features of each MANET routing protocol are not disturbed. An advertisement from the Internet gateway provides prefix information -- IP routing prefix and prefix length -- and lifetime.

After accepting an advertisement from the Internet gateway inserts the Internet gateway address as an Internet route and the MANET node configures a global address from the prefix of the Internet gateway. It uses the 64-bit interface ID in order to construct a valid address with the acquired prefix. It is assumed that before configuring a global IPv6 address, the node has configured a routable local address (i.e. MANET-local address), and a Non-unique Address Detection mechanism has been performed for that routable local address (e.g. using the mechanism defined in [3] and [25]), so it is assumed that the global address would be also unique. If not, the node may perform another Non-unique Address Detection mechanism for this global address.

If the destination of a packet is inside the MANET even though a global routable address is used as destination address, the gateway prevents this packet from being forwarded to the Internet. It returns the packet back to the MANET if it has a MANET route for the destination. The source node receives an ICMP Redirect message from the Internet Gateway warning that it should use a host route (MANET-local address) instead of a default route (Internet route). To do so, each Internet gateway may manage a list of IP addresses of all the associated MANET nodes (mainly if a reactive ad hoc routing protocol is being used). So, each MANET node must contact the Internet gateway at least once it establishes an Internet route through the Internet Gateway in order to communicate its global routable address to the Internet Gateway.

Based on [1], this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs.
- o Routing protocols' dependency: Not restricted to any particular ad

hoc routing solution, and it is designed to work properly with both proactive and reactive protocols.

- o Address uniqueness: It is assumed that the global address would be also unique. If not, the node may perform a Non-unique Address

Detection mechanism for this global address. In any case the Non-unique Address Detection mechanism is considered out of scope.

- o Distributed/centralised approach: The proposed solution uses a distributed approach where nodes do not solicit any centralised server for IP address assignment.
- o Merging support: No special merging mechanisms are discussed in this solution. Also, no in-service Non-unique Address Detection is used which makes the merging support not feasible.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: depends on the approach utilised. If extended control messages of the MANET routing protocol -- including global prefix information -- are used the solution introduces low overhead, but if gateway advertisement messages are periodically flooded (with the hop limit field set to an appropriate value in the MANET) then the solution introduces high overhead.

[2.2.1.5](#). Multihop Radio Access Network (MRAN) Protocol Specification (Hofmann)

This proposed solution [\[26\]](#) presents the Multihop Radio Access Network (MRAN) protocol, which is an IPv6-based protocol for the interconnection of ad hoc networks and the Internet. MRAN proposes an approach that enables mobile ad hoc nodes to communicate with correspondent nodes on the Internet. The application scenario of this protocol is mainly when multiple gateways are available and mobile nodes are frequently changing these gateways. The gateways are supposed to be fixed and advertising different prefixes. MRAN treats the gateways discovery and selection, the autoconfiguration of global addresses, and the packet forwarding to/from the fixed network.

Assumptions: It is assumed that mobile nodes (MNs) and Gateways (GWs) use local addresses for communication within the MANET and that routing is performed by a MANET routing protocol. It is also assumed that a flooding protocol is used for broadcasting certain MRAN control messages, where the flooding functionality may be provided by the routing protocol.

Approach description: The operation of MRAN involves several functions: GW discovery, GW selection, address autoconfiguration, registration with the GW, packet forwarding and multi-hop handovers. Three modes of GW discovery are proposed and the choice between them depends on the application scenario. In proactive GW discovery, all

GWs periodically broadcast advertisement messages "GW_ADV", where MNs in proactive mode requiring Internet access waits until they receive such a message. The reactive mode discovery allows MNs to discover the available GWs when needed through broadcasting a GW solicitation message. A GW receiving such a message replies by unicast solicited GW advertisement message "sol_GW_ADV" to the MN. Hybrid GW discovery mode is a combination of both proactive and reactive discovery, where the GW is in proactive mode and the MN is in reactive one. All GW advertisement messages contain the GW globally valid prefix of 64 bits length. The GW selection process allows each MN to select the closet GW with respect to the number of hops. Other additional metrics may be included in the selection process. After the GW selection, the MN uses the selected GW's prefix and its own EUI-64 to autoconfigure the global address. It may subsequently perform a Non-unique Address Detection. Registration with the selected GW should take place, where the MN sends a registration request message "MN_REG" to the selected GW. A GW receiving this message replies by a registration acknowledgement message "MN_REG_ACK" indicating the successful registration. The MN then periodically repeats the registration process and the registration may be used for other purposes as well (for instance the AAA). To assure appropriate packet forwarding between each MN and its selected GW, payload packets are tunnelled between MNs and GWs in both directions. The tunnelling approach uses IP-in-IP encapsulation thus allowing using local addresses for intra-MANET communication. In the tunnel from the GW to the MN, the destination address of the inner IP header is the MN global address and the destination address of the outer header is the local address of the MN. On the other hand, in the tunnel from the MN to the GW, the destination address of the inner IP header

is the CN global address, whereas the destination address of the outer header is the local address of the GW. In the case of MN's disconnection from its current GW while communicating with a CN in the Internet, multihop handover takes place. Thus, the MN has to discover, select and register with another GW. This is called a "forced multihop handover". For optimisation reasons, the MN may also select a new GW that could be more close than the current GW. In this case, the MN performs the registration with the new GW while it is connected to the current one. This is known as "optimised multihop handover", and is much faster than the forced one.

Maintenance takes place through creating two tables: i) GW table, and ii) MN table. MNs maintain a GW table storing information about the available GWs (local address, prefix, expiration time, registration expiration). A table entry is created when the MN receives a GW_ADV or Sol_GW_ADV messages. On the other hand, GWs maintain MN tables storing information about mobile nodes having a valid registration, where each entry in this table stores the following information on MNs (local address, global address, registration expiration time).

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: This proposed solution targets connected MANET scenarios enabling mobile nodes to communicate with correspondent nodes in the Internet.
- o Routing protocols' dependency: This proposed solution works independent of the MANET routing protocol.
- o Address uniqueness: The proposed solution may use a Non-unique Address Detection mechanism.
- o Distributed/Centralised approach: The proposed solution uses a distributed approach, where it does not solicit any centralised server for IP address assignment.
- o Merging support: No special merging mechanisms are discussed in this solution. Also, no in-service Non-unique Address Detection is used which makes the merging support not feasible.
- o Prefix assignment support: This proposed solution supports prefixes assignment, where the different gateways are responsible

for IPv6 prefixes advertisements.

- o Protocol overhead: the solution integrates several mechanisms and there is a number of flooding used to achieve the proper mechanisms' functioning. The overhead in this solution mainly lies in the assumption of an existing flooding protocol for broadcasting certain MRAN control messages, and GWs periodical broadcast of GW_ADV messages (containing the GW prefix) when proactive GW discovery is applied. Also, GW_Solicitation messages are broadcast on-demand when reactive GWs discovery is applied, and periodical MN_REG messages are sent to the selected GWs by each node requesting an IP address which is acknowledged by a MN_REG_ACK by the selected GW. Furthermore, additional messages are used for maintenance.

2.2.1.6. Automatic IP Address Configuration in VANETs (Fazio et al.)

Automatic IP address configuration is a challenging and still unexplored issue in vehicular ad hoc networks (VANETs) environments, where the vehicles' high mobility and variant density impede the direct utilisation of traditional networking techniques and protocols. Aiming at integrating VANETs within the Internet and providing passengers with any kind of Internet applications, the IP address represents the natural identifier in the system. This work [27] proposes an IP autoconfiguration solution in VANETs environment, exploiting the VANETs topology and an enhanced DHCP service with

dynamically elected leaders to provide a fast and reliable IP address configuration.

Assumptions: It is assumed that the network topology is linear and that a group of nodes move following a track with an internal mobility with respect to each other. It is also assumed that the relative speed between nodes is low.

Approach description: This work proposes a novel automatic IP address configuration protocol named Vehicular Address Autoconfiguration (VAC), that is characterised by a low configuration time. VAC represents the first protocol for IP address configuration in VANETs. It exploits the VANET topology and a distributed dynamic host configuration protocol (DHCP) runs by dynamically elected leader vehicles to quickly provide unique identifiers and reduce the

frequency of IP address re-configurations due to mobility. VAC organises leaders in a connected chain such that every node (vehicle) lies in the communication range of at least one leader. This hierarchical organisation allows limiting the signal overhead for the address management tasks. Only leaders communicate with each others to maintain updated information on configured addresses in the network. Leaders act as servers of a distributed DHCP protocol and normal nodes ask leaders for a valid IP address whenever they need to be configured.

VAC guarantees unique IP addresses within a defined SCOPE around the leader, where the SCOPE of the leader A is the set of leaders whose distance from A is less or equal to SCOPE hops. Considering the normal node Y that received the IPy address from A, IPy will be unique as long as Y moves within the SCOPE of A. If Y goes out of the SCOPE of A, in order to still ensure the address uniqueness, Y has to ask the new leader for another address. Considering that the relative speed between the nodes is low, changes in the address configuration due to having left the own leader's SCOPE are not frequent.

Based on [1], this solution has the following key features:

- o MANET scenario: The proposed solution targets connected MANET scenarios, enabling mobile nodes (vehicles) to communicate with correspondent nodes on the Internet.
- o Routing protocols' dependency: Apparently VAC does not depend on a special routing protocol. However no clear definition is given on how and what control messages are exchanged in order to configure each node requiring an IP address.

- o Address uniqueness: The proposed solution does not employ any Non-unique Address Detection mechanisms, however it guarantees address uniqueness for each configured node.
- o Distributed/Centralised approach: The proposed solution employs a partially distributed approach, where distributed DHCP run by some mobile nodes (vehicles) that are elected in a dynamic manner to assign IP addresses to the requesting nodes.

- o Merging support: No special merging mechanisms are explained in this proposed solution, however it could support merging. The SCOPE principle together with the distributed DHCP permit the nodes to join/leave different SCOPES while acquiring a new address from the SCOPE leader.
- o Prefix assignment support: This proposed solution does not employ any IPv6 prefix assignment to nodes.
- o Protocol overhead: the hierarchical organisation in this solution limits the signalling overhead and avoids flooding. The overhead in this solution mainly concerns: the signalling messages for communication between leaders nodes, the request messages sent by mobile nodes requesting an IP address from their leaders (this takes place in a limited scope), and the reply messages from the leaders to the requesting mobile nodes for assigning IP addresses (this also takes place in a limited scope). It is noticed that this solution does not use Non-unique Address Detection mechanisms due to the distributed DHCP functionality among leader nodes, which helps in limiting the signalling overhead.

2.2.1.7. Address Configuration Using Address Pool (Ahn et al.)

This address autoconfiguration mechanism -- proposed in [28] -- is based on the concept of address pool allocation in connected MANETs scenarios. This mechanism allows stable and fast global IP address configuration based on the DHCP.

Assumptions: It is assumed that the Internet gateway acts a DHCP server having the pool of IP addresses and assigning a part of this IP address pool to each node requesting an IP address. It is also assumed that each node having an address pool could assign a part of this address pool to other IP address requesting nodes. Each node then plays the role of a DHCP server. The lifetime of the address pool is assumed to be infinite.

Approach description: This solution basically works as follows: the Internet gateway periodically broadcasts Router Advertisement (RA) messages to the entire MANET and each MANET node receiving the RA

message can request for IP addresses through sending a unicast

DHCP_Request message to the Internet gateway. When the Internet gateway received the DHCP_Request message, it allocates a part of its address pool and sends it to the address requesting node in a DHCP_Reply message. At the same time, any intermediate node receiving the DHCP_Request message and having a big address pool intercepts the message and allocates a part of its address pool instead of the Internet gateway and sends it to the address requesting node in a DHCP_Reply message. Each node with the allocated address pool assigns one address to its interface and keeps the rest of the address pool for later allocation to other MANET nodes requesting addresses.

No renewal takes place for the allocated address pool, as the valid-lifetime field in the DHCP_Reply message is set to an infinite value reflecting an infinite use of the address pool. However, the Internet gateway broadcasts to the entire MANET an Address Pool Release Request (APRR) message when the size of its address pool arrives below a pre-defined threshold. Each node receiving the APRR message replies by an Address Pool Release Reply (APRP) message allowing the Internet gateway to know which addresses are being used or assigned.

Based on [1], this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs, however, it could be applied to standalone MANETs if some dedicated nodes are previously allocated address pools in order to allocate part of these pools to other IP requesting nodes in a standalone MANET.
- o Routing protocols' dependency: the solution is routing protocol independent.
- o Address uniqueness: the proposed solution guarantees address uniqueness since each node is assigned an address from an address pool allocated from a global address pool.
- o Distributed/Centralised approach: the solution is partially distributed, where it relies on a centralised DHCP server and at the same time each node plays the role of a DHCP server.
- o Merging support: the solution does not support merging.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes.
- o Protocol overhead: the solution requires additional messages flooding by the Internet gateway for announcing its address pool

and to get information on the different address pools assignment.

[2.2.1.8](#). Address Autoconfiguration for MANET with Multiple MBRs (Lee et al.)

This address autoconfiguration mechanism -- proposed in [\[29\]](#) -- is based on PMIPv6 (Proxy Mobile IPv6) mechanism in which a Local Mobility Anchor (LMA) is located and acts as a Home Agent (HA) while multiple MBRs (MANET Border Router) are used for scalable and reliable communication between each MANET node and the external network. The proposed solution prevents against the session termination or the non-optimal paths use during packet transmission when the MANET node changes the MBR.

Assumptions: It is assumed that all MBRs advertise the same network prefix in the connected MANET, and that each node configures its IP address using the stateless address autoconfiguration mechanism making use of the advertised network prefix.

Approach description: This solution basically works as follows: since all MBRs advertise the same network prefix, when a node moves it can still use its pre-configured address. This allows for maintaining the existing sessions even with node movement and allows for finding an optimised path by the node without changing the IP address. Each MBR periodically advertises Scope-Extended Router Advertisement (SERA) messages to the entire MANET. This message includes the network prefix assigned to the MANET and the address of the MBR originating the message. A MANET node connecting for the first time receives the SERA message and configures the IPv6 address of its MANET interface using the stateless address autoconfiguration mechanism based on the node MAC address, the obtained network prefix and the network prefix length. Then the node sets the originating MBR as its default gateway and stores in its routing table the distance from this MBR as well as the next-hop to this MBR (which is extracted from the source IP address field of the received message). The node then sends a Registration Request (RR) message to this MBR, where this latter sends a Proxy Binding Update (PBU) message with the MANET node to the LMA. After that, a tunnel between the LMA and MBR is established for the MANET node.

Since SERA messages are periodically advertised by each MBR, a node can receive multiple SERA messages advertised by the same MBR but through more optimal paths or advertised by new MBR than the default one. In the former case, the node could update the next-hop to its default MBR with no need to change the node address. In the latter case, the node can update its default MBR without changing its IP

address since all MBRs advertise the same network prefix. The node only needs to send an RR message to the new MBR for the binding with

this it following the same binding process explained above.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs.
- o Routing protocols' dependency: the solution is routing protocol independent, however the routing table is used to store information about the default gateway, the distance from it and the next hop to it.
- o Address uniqueness: the proposed solution guarantees address uniqueness since each node constitutes its IP address using the stateless IP autoconfiguration approach, employing its MAC address, the network prefix, and the prefix length.
- o Distributed/Centralised approach: the solution does not make use of any centralised server, however distributed gateways are involved.
- o Merging support: the solution does not support merging.
- o Prefix assignment support: the solution allows the assignment of IPv6 prefixes, where the same IPv6 prefix is broadcast by the different gateway nodes (MBRs).
- o Protocol overhead: the solution requires additional messages flooding by MBRs nodes (Scope Extended Router Advertisement 'SERA' message).

[2.2.1.9](#). Border Router Discovery Protocol (BRDP) based Address Autoconfiguration (Boot et al.)

This address autoconfiguration mechanism -- proposed in [\[30\]](#) -- describes a solution for configuring valid global IPv6 addresses for ad hoc nodes. It is based on the discovery of MANET Border Routers (MBRs), which are responsible of advertising topologically valid IPv6 prefixes, which can then be used by the ad hoc nodes.

Assumptions: It is assumed that there is at least one MBR advertising a valid global IPv6 address. The Border Router Discovery Protocol (BRDP) is defined for Border Router discovery. For standalone MANETs, the solution derives in the use of Unique Local Addresses (ULAs) generated by the individual MANET routers.

Approach description: This solution basically uses two phases: a) the initial discovery of one or more Border Routers, and b) the selection of a Border Router and address autoconfiguration of globally routable

IPv6 addresses to be used in conjunction with that Border Router. The BRDP is a simple distance vector protocol that distributes Border Router information, where each MANET router selects one or more Border Routers and forwards the Border Router information in the MANET. It basically extends the IPv6 Neighbor Discovery Protocol (NDP) to make it carry the required information (e.g., prefix information).

BRDP is a derivative of Tree Discovery [31]. BRDP uses ICMP Router Advertisement (RA) messages in NDP to distribute Border Router information by extending it with the Border Router Information Option (BRIO). BRDP allows MANET Routers to advertise Border Router reachability, including information for selecting a preferred Border Router. A MANET Router selects at least one BRIO from its cache, for dissemination in the MANET.

The address generated has a /128 prefix. It is constructed from a 64-bit Interface Identifier -- which is assumed to be unique (it is not specified how the MANET router generates this identifier, although several alternative approaches are proposed) -- and a 64-bit prefix (advertise in the BRIO). The generated 128-bit address is advertised in the MANET routing system.

Based on [1], this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs.
- o Routing protocols' dependency: the solution is routing protocol independent. A companion document [32] can be used in a multi-homed scenario (i.e. multiple MBRs available) to replace the default route mechanism.

- o Address uniqueness: address uniqueness is assured by the IPv6 address generation mechanisms used. However, details on how to handle a duplicate address condition are stated as out-of-scope for the document describing this solution.
- o Distributed/Centralised approach: the solution does not make use of any centralised server, however distributed gateways are involved.
- o Merging support: the solution does not support merging (as it is not specified how to handle duplicate addresses).
- o Prefix assignment support: the solution does not allow the assignment of IPv6 prefixes.

- o Protocol overhead: the solution requires additional messages flooding by MBRs nodes (BRIOs).

[2.2.2.](#) Merging support

[2.2.2.1.](#) Address Autoconfiguration in Optimized Link State Routing Protocol (Adjih et al.)

This proposed solution [[33](#)] is based on the concept of conflict detection. Each node periodically sends its address and an identifier. The node identifier is a sequence of bits, of fixed length (L), that is randomly generated. An address conflict is detected when the identifier mismatches. This proposed solution is suitable for OLSR routing protocol with a light increase of control message overhead, however, it might be used with any MANET protocol. Two issues are addressed in this solution, an IPv6 stateless autoconfiguration mechanism and a mechanism promoting address uniqueness in the situation where different ad hoc networks merge.

Assumptions: Two assumptions are mainly considered in this proposed solution. Firstly, it is assumed that the identifier of each node is globally unique in the network. Secondly, it is assumed that a MANET may be isolated.

Approach description: In this proposed solution, a new mobile node

joining the network is assigned an IP address then it carries out a conflict detection procedure through running a Non-unique Address Detection mechanism. If another node is detected to have the same address, the new joining node selects a new address. The address assignment process takes place as follows: i) consulting a neighbour node that should configure an address for the new node. The neighbour node then selects an IP address and sends it to the new node. This takes place by control messages exchange. ii) picking up a random address inside a given subnet with MANET_prefix either from a pool of allocated addresses or through a set of addresses advertised by each MANET node and are believed not used. In case of address pool existence, this pool could be reserved by the IANA for local use only (i.e. not forwarded outside MANET). In addition, in case of MANETs connected to the Internet, nodes acting as gateways diffuse IPv6 router advertisement messages. In this case each address in the pool would be a global address that can be seen from the outside.

The Non-unique Address Detection algorithm uses a single special control message to perform conflict detection. Each node periodically diffuses to the entire network a special message called MAD (Multiple Address Declaration). This message contains the node address and a unique identifier for the node. Several mechanisms are

proposed for MAD messages propagation. When using OLSR, propagation of MAD messages mainly relies on the MPR flooding, where a number of MPR selection rules are explained, presenting different options. If another routing protocol is used, default pure flooding is used for MAD messages propagation. In case of IP conflict discovery, this is resolved by the node with the smaller identifier in each conflicting pair. This node should change its IP, selecting a new IP at random (that is believed to be free) following the same approach of IP address assignment.

When OLSR routing protocol is used, an additional proposed option is using Passive Duplicate Detection. In this case, the topological information diffused by the OLSR routing protocol is sufficient to detect address conflict. However, some MPR selection mechanisms are used to ensure that the control messages are properly propagated.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: This proposed solution targets both standalone and connected MANETs scenarios.
- o Routing protocols' dependency: This proposed solution depends on the underlying routing protocol.
- o Address uniqueness: the proposed solution comprises a Non-unique Address Detection mechanism. The notion of passive duplicate detection is also used, where the solution makes use of the routing protocol messages propagation to detect the address conflicts.
- o Distributed/Centralised approach: The proposed solution uses a distributed approach in the sense of not communicating with a centralised DHCP server to acquire IP addresses.
- o Merging support: This proposed solution has a merging support, since the conflict detection process is periodically carried out by mobile nodes. Thus, this solution assures address uniqueness in case of ad hoc networks merge.
- o Prefix assignment support: This solution does not support IPv6 prefix assignment to nodes.
- o Protocol overhead: the solution adds low protocol overhead, since this solution benefits from the OLSR routing protocol signalling and MPRs concept to verify the address conflicts. The signalling in this solution is limited to a single control message (MAD message) to perform conflicts detection. If passive duplicate detection option is applied with OLSR, the overhead is almost

none, as the topological information diffused by OLSR is sufficient to detect address conflict. However, if another routing protocol is used (which is an option), the MAD messages have to be flooded resulting in a 'medium' overhead since the flooding is limited to only one message in this case.

2.2.2.2. Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks (Cha et al.)

The solution described in [34] proposes a stateful global IP autoconfiguration for MANETs with the goal of providing enhanced

Internet connectivity to mobile ad-hoc networks. This stateful autoconfiguration is performed through the exchange of extended control messages of MANET routing protocols. The protocol is devised as an extension to AODV, but the concept may be applicable to proactive routing protocols.

Assumptions: The solution assumes that each node has a local_IP_address configured.

Approach description: The protocol basically consists in nodes requesting global addresses to a gateway, which assigns a non-used address to the requesting node. When an ad hoc node needs a global IP address it sends an Internet-gateway solicitation message (GW_SOL message). The Gateway uses an Internet-gateway advertisement (GW_ADV message) to assign the solicited global IP address to the ad hoc node.

Given the event that an ad hoc node which has a Global IP address (e.g., G-A1) assigned by a gateway (e.g., GW1) cannot reach GW1 anymore due to a partition in the MANET but this ad hoc node has Internet connectivity through a different gateway (e.g., GW2), the ad hoc node gets another global IP address from GW2 (e.g., G-A2) and it performs a Locator Registration Procedure with GW1. This locator registration procedure is similar to Binding Updates in Mobile IPv6. Using this procedure the ad hoc node registers G-A2 as CoA -- Care of Address in Mobile IPv6 terminology -- of G-A1, so that ongoing communications are kept.

More details can be found in [\[34\]](#).

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs.
- o Routing protocols' dependency: although the protocol is devised as an extension to AODV, it could be applicable to proactive routing protocols.

- o Address uniqueness: since non-duplicate addresses are assigned to ad hoc nodes, the proposed solution is Non-unique Address Detection-free.

- o Distributed/centralised approach: the solution makes use of centralised servers (gateways) in order to assign IP global addresses.
- o Merging support: given that the proposed solution assigns global IP addresses avoiding duplicates, merging is supported. On the other hand it supports partitions through the Locator Registration Procedure.
- o Prefix assignment support: the solution does not support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: the solution adds certain protocol overhead, since the mechanism appends some fields to AODV routing protocol (RREQ message) to ask for a global IP address and gateway information, and the replay (GW-ADV message) is unicast to the originator MANET node. The solution includes the possibility of gratuitous GW-ADV broadcast periodically.

2.2.2.3. Gateway and Address Autoconfiguration for IPv6 Adhoc Networks (Jelger et al.)

This proposed solution [24] allows nodes in an ad hoc network to proactively discover a gateway/prefix pair to be used in building an IPv6 global address and to maintain a default route towards the Internet. The core element of this proposed solution is the concept of "Prefix Continuity". With prefix continuity, any node A that selected a given prefix P has at least one neighbour with prefix P on its path to the selected gateway G, thus assuring that each node on the path between node A and the Gateway G uses the same prefix P.

Assumptions: It is assumed that each node can find a Gateway to connect with and that each node can be assigned a global address through this gateway. It is also assumed that one (or possibly more) nodes of the ad hoc network should provide connectivity to the Internet, thus acting as Gateways to other nodes.

Approach description: In this proposed solution, each Gateway (GW) periodically sends a GW_INFO message notifying nodes in the ad hoc network about its existence as well as the prefix it uses. Some information in the GW_INFO message allows nodes to select the more appropriate GW when more than one GW exist. Other information contained in this message concerns: the GW global address, the length of the prefix part of the address, and the distance to the gateway as

perceived by the node sending the message. The node receiving the GW_INFO message forwards it to its 1-hop neighbourhood, where the forwarder node is considered as the upstream node for each node that receives the message. Among the transmitted GW-Info messages, each mobile node selects (through a selection algorithm) only one neighbour as its upstream neighbour and receives the GW_INFO messages from this neighbour (i.e. consider this upstream as an intermediate node to the gateway), then it forwards the message. A node must not forward a GW_INFO message sent by a node that is not its upstream neighbour. The destination address of the IPv6 header of the packet containing the GW_INFO message must be FF02::1 (all nodes), while the source address of such a packet must be the link local address of the sender. Thanks to the prefix continuity, the routing via the GW can be achieved without the need of an IPv6 routing header. Each mobile node creates its IPv6 global address as follows: {Extended Unique Identifier (EUI) of the interface from which the GW_INFO message is received + prefix contained in the message}. No Non-unique Address Detection mechanism is needed in this approach, as there is a very little probability of address duplication when EUI is used.

More details can be found in [\[35\]](#).

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: This proposed solution targets connected MANETs scenarios.
- o Routing protocols' dependency: This proposed solution is independent (in terms of message semantics) of the underlying routing protocol. Thus, it can be integrated in the operation of the routing protocol or it can run as standalone daemon.
- o Address uniqueness: The proposed solution does not depend on a Non-unique Address Detection procedure or mechanism.
- o Distributed/Centralised approach: The proposed solution is distributed in the sense of not employing any centralised DHCP server.
- o Merging support: Although no Non-unique Address Detection mechanism is used, this proposed solution supports networking partitioning and merging as it is based on generating an IPv6 address for each node based on the prefix advertisements.
- o Prefix assignment support: This proposed solution is based on the prefix continuity and is thus supporting prefix assignment. Each gateway advertises the IPv6 prefix that it uses.

Internet-Draft

MANET autoconf survey

June 2010

- o Protocol overhead: depends on the network size and the number of GWs. The main signalling in this solution mainly concerns the GW_INFO messages that are periodically sent by each GW notifying its existence as well as its prefix. Since no Non-unique Address Detection mechanism is needed in this solution, this helps in limiting the signalling and hence the overhead.

2.2.2.4. VET, SEAL, RANGER (Templin et al.)

NOTE from authors: this section needs further revision to catch up with all the updates of Templin proposals.

Here we refer to a set of different documents that provide functionalities that can be used to enable IPv6 address autoconfiguration in MANETs. [RFC5558](#) [36] specifies a Virtual Enterprise Traversal (VET) abstraction for autoconfiguration and operation of routers in enterprise networks. Enterprise networks connect routers over various link types. Since certain MANETs can be considered as a challenging example of an enterprise network, the mechanisms described in this document can be applied to provide MANETs with IP address autoconfiguration capabilities. This document has evolved a lot from its previous versions (and companion documents, such as [37] and [38], in which the author started to define an architecture in which MANET Routers were attached to an imaginary shared link (called "virtual ethernet") that connected all the MRs in the MANET. Other documents that complement VET are SEAL [39] and RANGER [40].

Assumptions: It is assumed the existence of Enterprise Border Gateways (EBRs), that are routers that connect the enterprise network to provider networks and can delegate addresses/prefixes to other EBRs within the enterprise.

Approach description: Regarding the applicability of the document to MANETs, it defines the Virtual Enterprise Traversal (VET), which is an abstraction that uses IP-in-IP encapsulation to span a multi-link enterprise in a single (inner) IP hop. VET interfaces are Non-Broadcast, Multiple Access interface used for VET, which encapsulate each inner IP packet in any mid-layer headers plus an outer IP header then forwards it on an underlying interface such that the TTL/Hop

Limit in the inner header is not decremented as the packet traverses the enterprise network. In this way, the VET interface presents an automatic tunnelling abstraction that represents the enterprise as a single IP hop.

In order to autoconfigure a VET interface, the interface is first initialised (a link-local address is configured on the interface), then border routers (Enterprise Border Gateways, EBGs) are

discovered, and last, IPv6 SLAAC is run on top of the VET. EBGs plays the role of access routers (i.e., send Router Advertisements), so standard IPv6 SLAAC mechanisms can be used to configure VET interfaces. DHCPv6 prefix delegation can also be used to configure a VET interface.

Based on [\[1\]](#), this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs.
- o Routing protocols' dependency: the solution is routing protocol independent.
- o Address uniqueness: the proposed solution reuses SLAAC and DHCP mechanisms, by providing an abstraction that represents the enterprise network as a single IP hop.
- o Distributed/centralised approach: the solution makes use of border routers (EBRs) in a similar way that routers sending Router Advertisements are used by SLAAC, or DHCPv6 servers are used when DHCPv6 prefix delegation is used.
- o Merging support: the solution supports merging.
- o Prefix assignment support: the solution supports the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: it does not add much overhead compared with SLAAC and DHCPv6. It adds some overhead in terms of tunneling headers due to the VET approach.

[2.2.2.5](#). A DHCP-based IP address autoconfiguration for MANETs (Bernardos et al.)

In this autoconfiguration mechanism -- proposed in [41] -- the first node that falls into the radio coverage of an access network uses DHCPv6 to get a global IPv6 prefix to be shared in the MANET.

Assumptions: It assumes the existence of a DHCP server in the access router giving access to the Internet.

Approach description: This solution basically works as follows: The first step is obtaining a global IPv6 prefix to be shared in the MANET (i.e., the MANET prefix). This task is done by the first node in the coverage of an access network (i.e., the initiator), using DHCPv6. The initiator node gets from this MANET prefix a /64 for itself and starts sending routers advertisements through its ad hoc interface. Each RA contains a new option (MANET DHCP Prefix

Delegation Information) that indicates to the receivers that the sender of the RA is able to delegate prefixes using DHCPv6.

Receivers of these RAs, that is, new arriving nodes, may then configure an IPv6 address from the prefix contained in the RA (i.e., performing normal IPv6 stateless address auto-configuration). These nodes may then request an IPv6 prefix for themselves using, using DHCPv6. The initiator node delegates each of them a /64 prefix, keeping track of how many /64 prefixes from the MANET preix are still available for distribution.

These MANET nodes configure their interfaces with addresses from the prefix they have just obtained and start sending RAs containing this prefix. This enables other nodes that are within the radio coverage of these MANET nodes to obtain IPv6 addresses and request IPv6 prefixes. When a MANET node, other than the initiator node, receives a DHCPv6 prefix request, it generates a new request and sends it to one node capable of delegating prefixes. In this way requests are recursively generated until they reach the initiator node, which then generates a DHCPv6 reply with the delegated prefix. Again, replies are recursively sent backwards until they reach the unconfigured nodes that requested the prefixes.

Based on [1], this solution has the following key features:

- o MANET scenario: the solution targets connected MANETs.

- o Routing protocols' dependency: the solution is routing independent.
- o Address uniqueness: The solution reuses SLAAC and DHCP mechanisms.
- o Distributed/centralised approach: the MANET does not make use of any centralised server, but all the nodes have the potential to ask for a prefix to the DHCP server on the infrastructure, and becomes a router sending Router Advertisements are used by SLAAC.
- o Merging support: given that the proposed solution assigns global IP addresses avoiding duplicates, merging is supported.
- o Prefix assignment support: the solution support the assignment of IPv6 prefixes to nodes.
- o Protocol overhead: it does not add much overhead compared with SLAAC and DHCPv6. RAs include a new option that indicates to receivers that the sender of the RA is able to delegate prefixes using DHCPv6.

[3.](#) Security Considerations

Due to the open wireless environment of ad hoc networks, IP autoconfiguration mechanisms are susceptible to a number of attacks.

[4.](#) IANA Considerations

This document has no actions for IANA.

[5.](#) Acknowledgements

We would like to thank all the AUTOCONF ML people that provided comments to the previous version of the I-D. We would also like to thank Kilian Weniger for his useful review of this draft, and Thomas

Clausen for his review and support on the continuity of this draft in another shape.

The work of Carlos J. Bernardos and Maria Calderon has been partially supported by the Ministry of Science and Innovation of Spain under the QUARTET project (TIN2009-13992-C02-01).

The work of Carlos J. Bernardos has also been partially supported 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] Moustafa, H., Bernardos, C., and M. Calderon, "Evaluation Considerations for IP Autoconfiguration Mechanisms in MANETs", [draft-bernardos-autoconf-evaluation-considerations-03](#) (work in progress), November 2008.

6.2. Informative References

- [2] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", [draft-ietf-autoconf-adhoc-addr-model-03](#) (work in progress), March 2010.
- [3] Perkins, C., "IP Address Autoconfiguration for Ad Hoc Networks", [draft-perkins-manet-autoconf-01](#) (work in progress), November 2001.
- [4] Weniger, K. and M. Zitterbart, "IPv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks", European Wireless 2002 , 2002.
- [5] Jeong, J., "Ad Hoc IP Address Autoconfiguration", [draft-jeong-adhoc-ip-addr-autoconf-06](#) (work in progress), January 2006.
- [6] Jeong, J., "Ad Hoc IP Address Autoconfiguration for AODV", [draft-jeong-manet-aodv-addr-autoconf-01](#) (work in progress), July 2004.
- [7] Vaidya, N., "Weak Duplicate Address Detection in Mobile Ad Hoc Networks", MOBIHOC'02 , 2002.
- [8] Mohsin, M. and R. Prakash, "IP Address Assignment in a Mobile Ad Hoc Network", MILCOM 2002 , 2002.
- [9] Tayal, A. and L. Patnaik, "An address assignment for the automatic configuration of mobile ad hoc networks", Personal Ubiquitous Computing , 2004.
- [10] Chen, Y., Fleury, E., and T. Razanfindralambo, "Scalable Address Allocation Protocol for Mobile Ad Hoc Networks", Fifth International Conference on Mobile Ad-hoc and Sensor Networks , 2009.
- [11] Mase, K. and C. Adjih, "No Overhead Autoconfiguration OLSR", [draft-mase-manet-autoconf-noolsr-01](#) (work in progress), April 2006.

Internet-Draft

MANET autoconf survey

June 2010

-
- [12] Weniger, K., "Passive Duplicate Address Detection in Mobile Ad hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC) , 2003.
 - [13] Weniger, K., "PACMAN: Passive autoconfiguration for mobile ad hoc networks", IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, Mar 2005 pp. 507-519 , 2005.
 - [14] Mase, K. and K. Weniger, "PDAD-OLSR: Passive Duplicate Address Detection for OLSR", [draft-weniger-autoconf-pdad-olsr-01](#) (work in progress), June 2006.
 - [15] Baccelli, E., "OLSR Passive Duplicate Address Detection", [draft-clausen-olsr-passive-dad-00](#) (work in progress), July 2005.
 - [16] Jeong, H., "Passive Duplicate Address Detection for On-demand Routing Protocols", [draft-jeong-autoconf-pdad-on-demand-01](#) (work in progress), April 2007.
 - [17] Zhou, H., Ni, L., and M. Mutka, "Prophet Address Allocation for Large Scale MANETs", Proceedings of INFOCOM 2003 , 2003.
 - [18] Pongpaibool, P., Siriwong Na Ayutaya, K., Kachanasut, K., and H. Tazaki, "Rapid IPv6 Address Autoconfiguration for Heterogeneous Mobile Technologies", Proceedings of the 8th International Conference of ITS Telecommunications (ITST 2008), Phuket, Thailand , 2008.
 - [19] Nesargi, S. and R. Prakash, "MANETconf: configuration of hosts in a mobile ad hoc network", INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Volume: 2 Page(s): 1059 - 1068 vol.2. 2002 , 2002.
 - [20] Ruffino, S. and P. Stupar, "Automatic configuration of IPv6 addresses for MANET with multiple gateways (AMG)", [draft-ruffino-manet-autoconf-multigw-03](#) (work in progress), June 2006.
 - [21] Clausen, T. and E. Baccelli, "Simple MANET Address Autoconfiguration", [draft-clausen-manet-address-autoconf-00](#)

(work in progress), February 2005.

- [22] Ruiz, P. and F. Ros, "Extensible MANET Auto-configuration Protocol (EMAP)", [draft-ros-autoconf-emap-02](#) (work in progress), March 2006.

- [23] Wakikawa, R., "Global connectivity for IPv6 Mobile Ad Hoc Networks", [draft-wakikawa-manet-globalv6-05](#) (work in progress), March 2006.
- [24] Jelger, C., "Gateway and address autoconfiguration for IPv6 adhoc networks", [draft-jelger-manet-gateway-autoconf-v6-02](#) (work in progress), April 2004.
- [25] Sun, Y., Belding-Royer, E., and C. Perkins, "Internet Connectivity for Ad hoc Mobile Networks", International Journal of Wireless Information Networks special issue on 'Mobile Ad Hoc Networks (MANETs): Standards, Research, Applications' , 2002.
- [26] Hofmann, P., "Multihop Radio Access Network (MRAN) Protocol Specification", [draft-hofmann-autoconf-mran-00](#) (work in progress), March 2006.
- [27] Fazio, F., Palazzi, C., Das, S., and M. Gerla, "Automatic IP Address Configuration in VANETs", ACM VANET 2006 Workshop co-located with Mobicom 2006 , 2006.
- [28] Ahn, S. and Y. Lim, "MANET Address Configuration using Address Pool", [draft-ahn-autoconf-addresspool-00](#) (work in progress), December 2009.
- [29] Lee, J., Ahn, S., and Y. Kim, "Address Autoconfiguration for MANET with Multiple MBRs", [draft-jaehwoon-autoconf-mmbr-02](#) (work in progress), February 2010.
- [30] Boot, T. and A. Holtzer, "Border Router Discovery Protocol (BRDP) based Address Autoconfiguration", [draft-boot-autoconf-brdp-02](#) (work in progress), July 2009.
- [31] Thubert, P., "Nested Nemo Tree Discovery",

[draft-thubert-tree-discovery-08](#) (work in progress), June 2009.

- [32] Boot, T., "Border Router Discovery Protocol (BRDP) Based Routing", [draft-boot-brdp-based-routing-00](#) (work in progress), November 2008.
- [33] Laouiti, A., "Address autoconfiguration in Optimized Link State Routing Protocol", [draft-laouiti-manet-olsr-address-autoconf-01](#) (work in progress), July 2005.
- [34] Cha, H., Park, J., and H. Kim, "Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks", [draft-cha-manet-extended-support-globalv6-00](#) (work in

progress), October 2003.

- [35] Jelger, C. and T. Noel, "Prefix Continuity and Global Address Autoconfiguration in IPv6 Ad Hoc Networks", Proceedings of the 4th Mediterranean Ad Hoc Networking Workshop (MedHocNet'05), June 2005, Porquerolles, France , 2005.
- [36] Templin, F., "Virtual Enterprise Traversal (VET)", [RFC 5558](#), February 2010.
- [37] Templin, F., "MANET Autoconfiguration over Multilink Sites", [draft-templin-autoconf-multilink-00](#) (work in progress), February 2007.
- [38] Templin, F., "MANET Autoconfiguration over Virtual Ethernets", [draft-templin-autoconf-virtual-00](#) (work in progress), February 2007.
- [39] Templin, F., "The Subnetwork Encapsulation and Adaptation Layer (SEAL)", [RFC 5320](#), February 2010.
- [40] Templin, F., "Routing and Addressing in Networks with Global Enterprise Recursion (RANGER)", [RFC 5720](#), February 2010.
- [41] Bernardos, C. and M. Calderon, "A DHCP-based IP address autoconfiguration for MANETs", I International Conference on Ubiquitous Computing: Applications, Technology and Social Issues (ICUC 2006), Alcalá de Henares, Spain , 2006.

Internet-Draft MANET autoconf survey June 2010

[Appendix A](#). Change Log

Changes from -04 to -05:

- o Removal of references to old autoconf problem statement draft and MANET architecture drafts.
- o Update of the document, adding new solutions.

Changes from -03 to -04:

- o New release to keep the document alive.
- o Update of some references and the associated solution description.

Changes from -02 to -03:

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

Changes from -01 to -02:

- o The classification criteria section has been removed, since it is now part of the evaluation considerations in [1]. Solutions are now analysed conforming to some of these evaluation considerations in [1].
- o The Conclusions section has been removed.
- o The Terminology section has been removed.
- o The term "DAD" has been removed in the document (when possible), using Non-unique Address Detection instead.
- o Many editorial changes.

Changes from -00 to -01:

- o The structure of the I-D has modified, classifying the analysed solutions according to a number of useful criteria, conforming to the AUTOCONF problem statement draft and the MANET architecture draft.
- o More solutions have been added to the I-D.
- o Adding of a security consideration section.

Bernardos, et al.

Expires December 20, 2010

[Page 56]

Internet-Draft

MANET autoconf survey

June 2010

Authors' Addresses

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

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: <http://www.it.uc3m.es/cjbc/>

Maria Calder<F3>n

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

Phone: +34 91624 8780
Email: maria@it.uc3m.es

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