autoconf
Internet-Draft
Expires: December 10, 2005

S. Ruffino
P. Stupar
TILAB
June 8, 2005

Automatic configuration of IPv6 addresses for nodes in a MANET with multiple gateways
draft-ruffino-manet-autoconf-multigw-00

Abstract

This Internet Draft relates to Mobile Ad-hoc Networks (MANETs) connected to an external network by means of one or more gateways. A solution that enables MANET nodes to automatically discover a global address is proposed. The proposed solution aims at reducing the latency introduced by a global address change and exposes two algorithms a node may adopt to discover if the used address has to be changed.

Table of Contents

1. Introduction 3
2. Terminology 4
3. Applicability Scenario 5
4. Problem Statement 7
5. Autoconfiguration Method Overview 9
5.1 Advantages of the proposed method 10
5.2 Examples of operations 11
5.2.1 Bootstrapping of a node 11
5.2.2 Gateway change 12
6. Data structures 15
6.1 Prefix Information base 15
6.2 Delegated Prefixes Information Base 15
6.3 Secondary Addresses Information Base 16
6.4 Multiple Interface Association Information Base 16
7. Detailed operations 18
7.1 IPv6 Addresses generation 18
7.2 Primary Address configuration 18
7.3 Prefix Advertisement 18
7.3.1 Prefix Advertisement (PA) messages format 18
7.3.2 PA message generation 20
7.3.3 PA message forwarding 20
7.3.4 PA message processing 21
7.3.5 Secondary Addresses Information Base Management . . . 21
7.4 MID messages 22
7.4.1 MID message generation 22
7.4.2 MID message forwarding 22
7.4.3 MID message processing 22
7.5 Global IPv6 Address configuration for MANET nodes 23
7.5.1 Best Prefix Selection Algorithm 24
7.5.2 Address change 25
7.6 Gateway operations 25
8. Mobile IPv6 Considerations 27
9. Proposed Values for Constants 28
9.1 Emission Intervals 28
9.2 Holding Time 28
10. Security Considerations 29
11. IANA Considerations 30
12. References 31
12.1 Normative references 31
12.2 Informative References 31
Authors' Addresses 33
A. Acknowledgments 35
Intellectual Property and Copyright Statements 36

1. Introduction

MANETs are wireless networks characterized by the absence of any infrastructure: nodes of a MANET function both as hosts (i.e. they are end-points of a communication) and as routers. In fact packets which can not be directly delivered between two nodes are routed through other intermediate nodes following a multi-hop path to reach their destination. Routing within a MANET is guaranteed by a routing protocol, which enables nodes calculate the optimal path that data packets must follow within the MANET itself. If the MANET is connected to an external network (e.g. the global Internet), nodes can communicate towards hosts located in such network: in this case, global connectivity has to be guaranteed, i.e. MANET nodes have to be identified by a valid IP address through which packets transmitted by hosts located outside the MANET can be received.

This document presents a mechanism for automatic configuration of a topologically correct, globally valid IPv6 address on nodes in a MANET connected to the Internet through one or more gateways. The routing protocol considered in this document is Optimized Link State Routing (OLSR) [RFC3626]. With the solution presented in this document, nodes can effectively exploit all the active gateways in the MANET: a new OLSR message type is introduced, to enable gateways to announce IP prefixes within MANET. When nodes receive such prefixes, they build a set of global addresses and, in turn, advertise them to other MANET nodes. Global addresses announcement enables node to dynamically choose another valid address, among those announced, and to continue to communicate with external IP hosts, without experiencing significant delay. The node can decide to change the global address in use basically for two reasons: after the failure of the gateway announcing the prefix from which it derived its used global address or for performance reasons, e.g. to optimize downlink data traffic path.

This document is organized as follows: Section 3 describes the reference scenario and its main features; Section 4 exposes the problem statement regarding global address configuration in the reference scenario; Section 5 outlines the proposed solution, which is detailed in Section 6 and Section 7.

2. Terminology

Valid IPv6 Global Address
: An IPv6 address which is globally routable, i.e. it is topologically correct and it is reachable from all hosts and routers located in external networks (e.g. the Internet).

Main Address
: In OLSR [RFC3626], an IPv6 address used as identifier of the node, inserted in the 'Originator Address' field in OLSR control messages.

Primary Address (PADD)
: The identifier used by MANET nodes to partecipate to routing protocol, i.e. it is used as OLSR main address. One MANET node owns exactly one primary address, which must be configured at bootstrapping. In this proposal, such address is MANET-scoped, i.e. it is routable within the MANET only.

Secondary Address (SADD)
: A valid IPv6 global address that can be used as IPv6 source address in datagrams transmitted from a MANET node to internal nodes or external hosts. More than one secondary address can be bound to one node's primary address.

Designated Secondary Address (DSADD)
: A SADD used by the node to communicate with a generic host, namely an address used as IPv6 source address of transmitted packets. This address may change during the lifetime of a node.

3. Applicability Scenario

The reference scenario to which the mechanism described in this specification applies is shown in Figure 1. In this scenario, MANETs are connected to other external networks by means of one or more gateways that provide Internet connectivity. Nodes that are not directly linked to the external network can use a multihop wireless connection to reach the gateways and forward outbound traffic. An in-depth description of such scenario can be found in [I-D.ruffino-conn-scenarios].

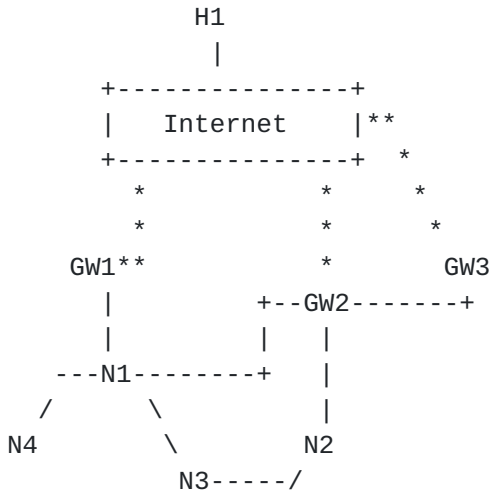

Figure 1: MANET interconnected to an external network

An example of the applicability scenario can be a mobile operator cellular network extended by means of ad-hoc "clouds". In this case, mobile nodes are equipped with two interfaces, for example an UMTS interface and an IEEE 802.11g interface. The first one enables nodes to directly set-up a radio link towards the external network and receive a valid global IPv6 address, while the second one is used to participate to a MANET. This is typically achieved by running a MANET routing protocol, s.a. AODV [RFC3561], OLSR [RFC3626], TBRPF [RFC3684] and DSR [DSR]. A node located in the coverage area of the cellular network can act as gateway for the MANET: in this way, nodes that are not in the coverage area of the mobile network can use other MANET nodes to reach the gateways and forward outbound traffic.

It is also assumed that gateways own one or more IPv6 prefixes which can be advertised within the MANET. The mechanism by which gateways retrieve this information is out of scope of this specification: it can be manually configured by administrators or dynamically set up, during link establishment towards the Internet, e.g. using DHCP with Prefix Delegation Option ([RFC3633]). It is also assumed that

different gateways advertise different prefixes, in order not to require special configuration both on gateways themselves and on Internet routers. As a consequence, traffic directed to an IPv6 address derived by one of the prefixes advertised within the MANET is univocally routed towards the gateway owning such prefix.

4. Problem Statement

Standard configuration methods for IPv6, i.e. stateful ([RFC3315]) and stateless ([RFC2462]) IPv6 autoconfiguration, cannot be applied to MANETs, as outlined by previous work ([PERKINS], [WAKI-GLOBAL6], [I-D.singh-autoconf-adp], [I-D.wakikawa-manet-ipv6-support]). Standard methods have been designed for single-hop link (e.g. a single LAN segment, where all hosts and routers are on the same Layer 2 link) and don't address MANET intrinsic characteristics, such as multi-hop connections, partitions and mergers.

In the past, a number of solutions has been proposed, to solve automatic configuration of IPv6 addresses in a MANET and the global IPv6 connectivity problem: e.g. [WAKI-GLOBAL6], [CHA], [JELGER], [JEONG], [PAAKKONEN]. Technical issues addressed by these proposals can be summarized as follows:

Bootstrapping of a node
: Actually, there is no standardized method enabling a node to automatically configure a unique address by means of which it can participate to the routing protocol. MANET routing protocols have been defined implicitly assuming that nodes already own a unique address configured on their MANET interface. Moreover, there is not any standard DAD mechanism for MANET, through which a node can verify the uniqueness of its address.

Global Connectivity
: In a MANET endowed with gateways global connectivity problem arises: nodes need a valid global IPv6 address enabling them receive data traffic coming from hosts located outside the MANET.

It is worth noting that in the applicability scenario, a number of technical issues arise, besides those described by previous work. In fact, gateways can freely move and they may also leave the MANET: in this case, global prefixes associated to such gateways are no more valid, as the traffic would be routed by external network routers towards a link which is no more active. As a consequence, MANET nodes using global addresses derived from such (no more valid) prefixes are no more reachable from the external network. Nodes must therefore acquire a new valid IPv6 address, derived from a valid prefix which is advertised by an available gateway.

The technical issues specific to the applicability scenario described in Section 3 are the following:

IPv6 address change

Routing protocols (e.g. OLSR) assume that each node configures on its MANET interface only one address, which identifies the node itself and all its related topological information collected by routing protocol. When the node changes such address (named main address in OLSR), all topological information diffused by the node to the MANET is no more valid as it is associated to an address which is not used by any node. From the point of view of the MANET, an address change is similar to the failure of the node. Therefore, after the change of its configured address, a node will experience a period of absence of connectivity as the other MANET nodes don't own a route towards it. Such period will last until the node has transmitted enough topological information bound to its new configured address.

Sub-optimal path

The choice of the global address defines the path that downlink traffic coming from the Internet will follow to reach a MANET node. Indeed, external hosts will send packets to the global address used by the node: such packets will be delivered to the gateway owning the global prefix from which the global (configured) address was derived and will then follow a path connecting such gateway to the node. If a node doesn't change the global address in use as long as this is valid, the downlink path followed by (return) traffic within the MANET will always start from the same gateway. This doesn't assure that such used path is the best one, according to a predefined metric. Indeed, after a change of MANET topology, there may be a better gateway whose use optimizes download traffic reception: the node doesn't exploit such gateway as long as the global address in use is derived from another gateway's global prefix.

It is a non-goal of this specification to solve application session survivability, after a node changes its global address. It is authors' belief that IETF standard method for IPv6 mobility, namely Mobile IPv6 [RFC3775], can be applied to this environment. Section 8 elaborates on this. Similarly, this specification does not propose any new Duplicate Address Detection method. A generic DAD procedure (e.g. [PERKINS]) can be used, in order to verify uniqueness of MANET-local and global addresses.

5. Autoconfiguration Method Overview

This section gives an overview of the proposed IPv6 address autoconfiguration solution, which is specified for nodes running OLSR protocol in Section 6 and Section 7.

Each node is characterized by two types of addresses:

- its Primary Address (PADD), which does not change during node's life in the MANET and is independent from the prefixes announced by gateways; PADD can be, for example, an IPv6 ULA [I-D.ULA];

- one or more Secondary Addresses (SADD), built using the global prefixes announced by gateways; each node can use one of such addresses as source address of the outgoing traffic, i.e. the Designated Secondary Address (DSADD).

A new OSLR message type, named Prefix Advertisements (PA), is defined, to advertise global prefixes. Gateways periodically disseminate PA messages, which contain their delegated prefixes. More details on PA messages format and processing are described in section Section 7.3. PA messages can be considered complementary to OLSR HNA (Host and Network Association) messages, whose content is used by OLSR nodes to perform gateway discovery and default route set-up.

Basic operations for a generic node can be summarized as follows:

- At bootstrap, node builds and configures a PADD and uses it as main address in OLSR messages.

- Node participates to OLSR, sending and receiving topology information. After a transitory period, the node receives Prefix Advertisement (PA) messages from the gateways in the MANET.

- It uses the prefixes, received from gateways, to build a set of global IPv6 addresses: at least, it derives an address from each received prefix (i.e. a SADD). Among them, node chooses the "best" address, corresponding to the "best" prefix, according to some method (e.g. Default Gateway method, described in Section 7.5.1), and starts using it as DSADD.

- Node inserts all (or a subset) of the addresses (including DSADD) built in the previous step into OLSR MID messages and starts broadcasting them. After a transitory period, all nodes own a route towards the DSADD and all the other SADDs of the node, proactively announced using MID messages.

- Topological information regarding gateways announcing global prefixes is constantly monitored by node to know at any time which is the best prefix and therefore the current best global address. Such address is chosen as DSADD. As a consequence, the node changes its DSADD after one of the following events:

  * The gateway which advertises the prefix used by the node to derive its DSADD is no more reachable.

  * Node experiences a significant topological change (e.g. it moves) after which the prefix used to derive the DSADD is no more the best one.

Since a node inserts into MID messages multiple SADDs, besides those which it is actually using as DSADDs, a node can transparently use a new Secondary Address without bootstrapping the routing protocol every time this happens. Indeed, the traffic destined to any of the Secondary Addresses is immediately routable within the MANET and, in particular, from the gateways to the nodes.

In case the considered gateway has several associated prefixes, the node will choose one of these prefixes according to a predetermined rule, for example it may choose the first one it has received, but may also decide to configure many DSADDs (one for each prefix).

Section 5.1 exposes the benefits of the solution proposed in this document and Section 5.2 gives two examples of the sequence of operations executed by a node when the proposed solution is adopted.

5.1 Advantages of the proposed method

The main advantages of the proposed solution are the following:

- The downlink path followed by traffic coming from external network can be optimized, with respect to the hop-count metric. This can be achieved when using a best prefix selection method that enables MANET nodes always to use as DSADD an address derived from a prefix announced by the gateway indicated as the best one by

routing protocol.

- After changing its DSADD, a node can immedately exchange data traffic with hosts located both within and outside the MANET: no significant delay is experienced. This because the local topological information is bound to a PADD and therefore independent from the DSADD currently used. This address has been already announced with MID messages: all other MANET nodes already know the correct path to reach the node by this address.

- A gateway which becomes a node, e.g. as the result of losing connectivity towards the external network, can immediately receive downlink traffic by using another active gateway.

5.2 Examples of operations

5.2.1 Bootstrapping of a node

This section gives an overview of the operations executed by a node N that joins a MANET for the first time (i.e. it is bootstrapping).

As shown in Figure 2, the node configures its Primary Address and participates to the routing protocol, sending Hellos and TCs. The participation to the routing protocol lets the node to be informed of the network topology (Hello and TC messages), of the gateways addresses (HNA messages) and of the correspondent delegated prefixes (PA messages).

HNA messages reception enables the node to choose its default gateway, which will be used to send uplink traffic, while PA messages reception enables the node to receive all the available global prefixes. Among those, it chooses the best prefix and uses it to build the DSADD, which is then configured on the interface. It builds also a set of SADDs, one for each received prefix. At this point the node is not reachable from the external network yet, as no routes towards any of its SADDs have been set up by the MANET nodes. The node starts sending MID messages containing the whole list of the SADDs.

Only after MID messages diffusion, the node can receive traffic incoming from the external network (as all MANET nodes own a route to its global address) and can therefore start transmitting data to external hosts.

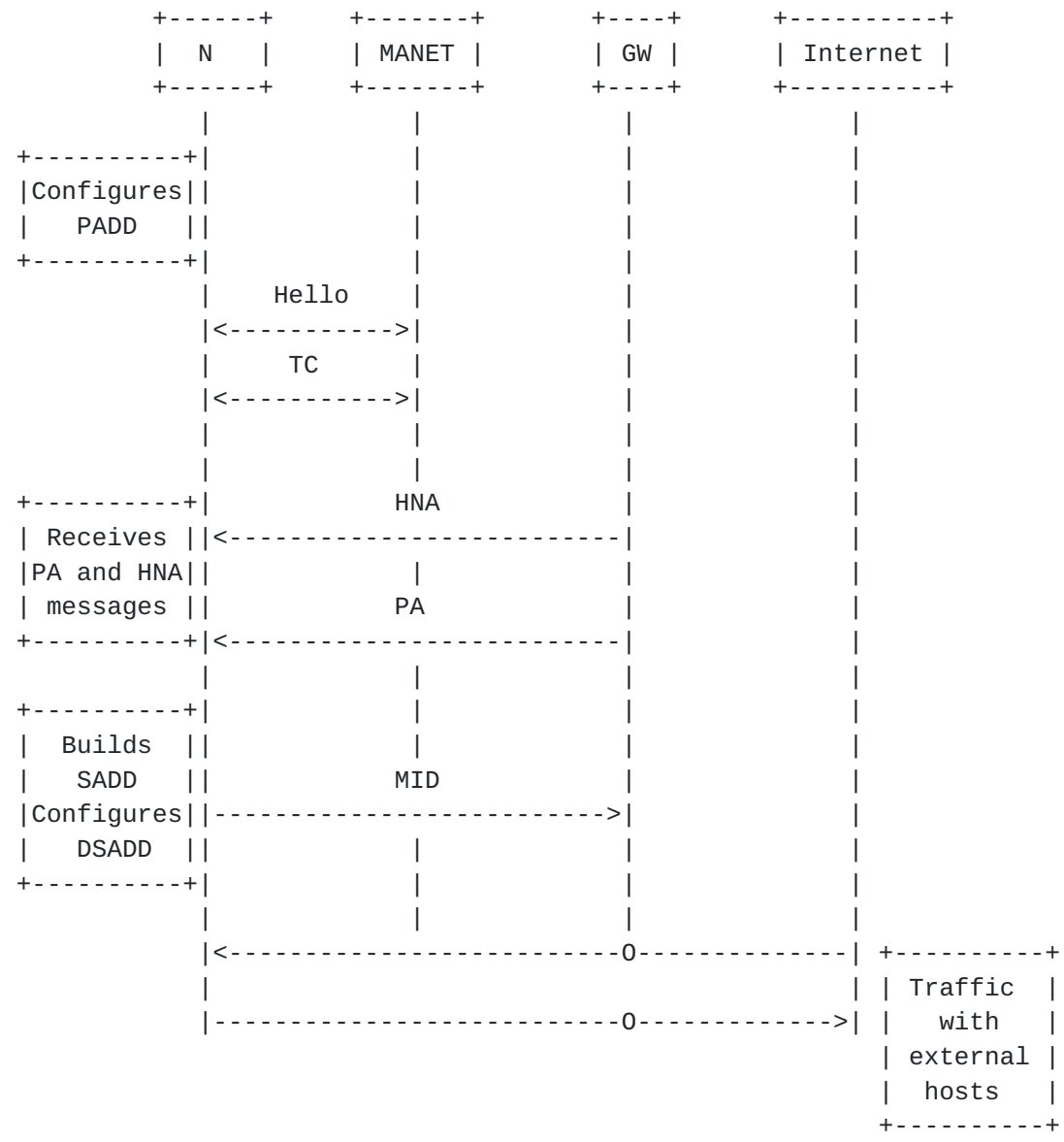

Figure 2: Bootstrapping of a node

5.2.2 Gateway change

In Figure 3 it is represented the message flow triggered by a node N, connected to a MANET endowed with two gateways GW1 and GW2. The Secondary Addresses built by node N are two: SADD1 (derived by gateway GW1 delegated prefix) and SADD2 (derived by gateway GW2 delegated prefix). It is assumed that the node is using SADD1 (according to a best prefix selection method not specified). It is worth noting that as soon as node N receives PA messages, it can start using SADD1 and sending MID messages at the same time.

After the failure of GW1, the Secondary Address SADD1 used by node N is no more valid: node N then stops using SADD1 and starts using the other globally valid Secondary Address, i.e. SADD2: all the other MANET nodes already own a route towards such address as it was inserted into MID messages generated by N, which can start a new communication towards the internet without experiencing significant delay due to the address change.

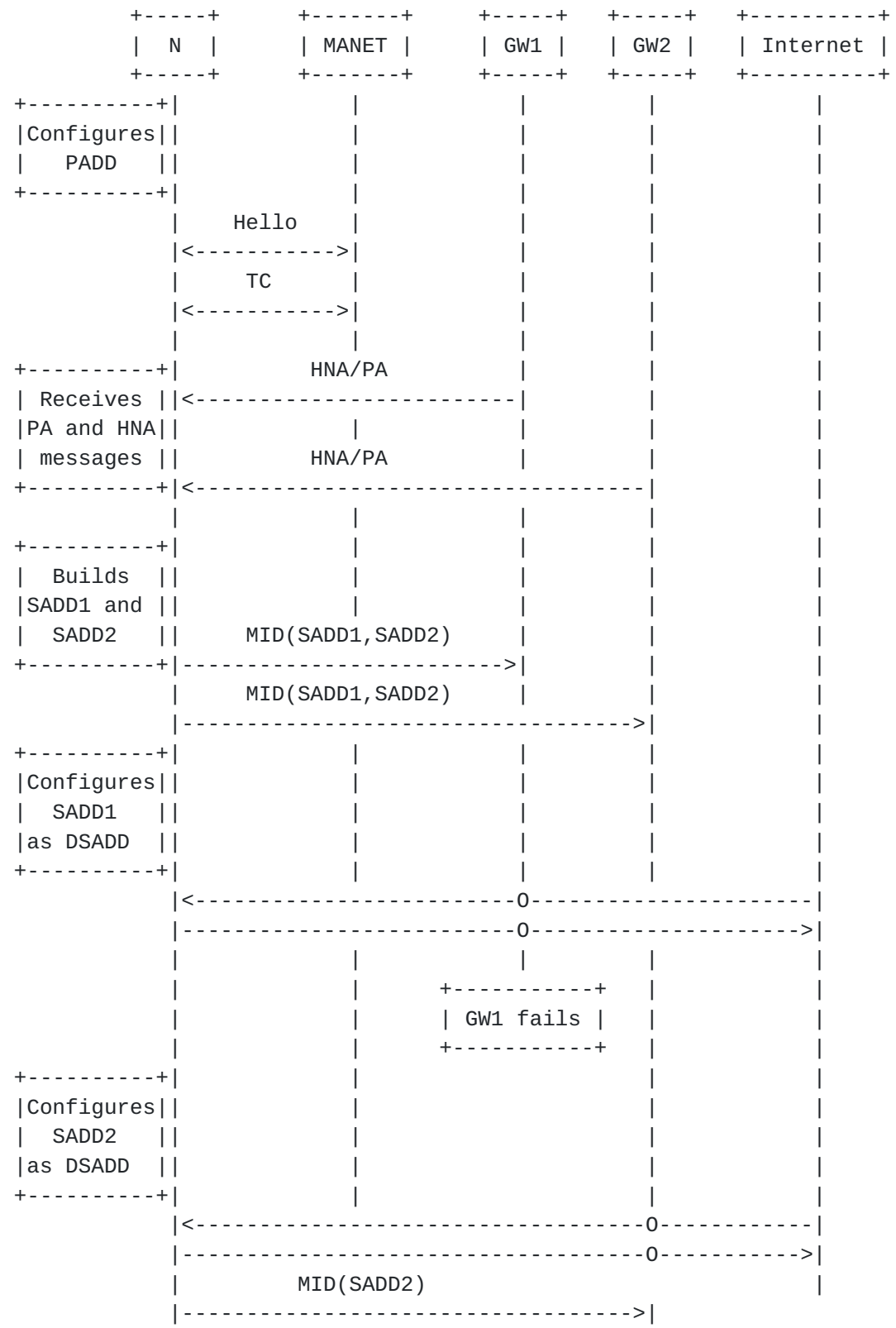

Figure 3: Gateway change

6. Data structures

In this section the OLSR data structures used by the proposed solution are detailed. One of these structures, namely the Multiple Interface Association Information Base, is defined in [RFC3626]: the present specification modifies the semantics of one of its fields.

6.1 Prefix Information base

The Prefix Information Base (PIB) contains the delegated prefixes announced by gateways within the MANET and it is filled processing Prefix Advertisements. It is maintained by each node and gateway.

Entries of the PIB have the following structure:

Field	Data
P_address	Primary Address of the gateway which sent the PA
P_network	A prefix owned by the gateway whose PADD is specified in P_address
P_prefix_length	Length of the prefix contained in P_network field
P_time	Validity time

Table 1: Prefix Information Base (PIB)

6.2 Delegated Prefixes Information Base

Each gateway owns one or more global prefixes to be announced within the MANET. Delegated Prefix Information Base, maintained only by gateways, contains such prefixes. How the table is filled is out of scope of this specification. Prefixes contained in this table are inserted in Prefix Advertisements, sent out by gateways.

Entries of the Delegated Prefixes Information Base have the following structure:

Field	Data
P_network	A prefix delegated to the gateway
P_prefix_length	Length of the prefix contained in P_network field

Table 2: Delegated Prefixes Information Base

6.3 Secondary Addresses Information Base

The Secondary Addresses Information Base (SAIB) is the set of the Secondary Addresses built by a node. It is maintained on each node and gateway. The Secondary Addresses stored by a node are those built processing Prefix Advertisements carrying global prefixes, i.e. using global prefixes contained into PIB. The refresh of its entries tightly depends on the state of the entries of PIB, as the validity of a Secondary Address is bound to the validity of the global prefix from which the Secondary Address has been derived.

Entries of the Secondary Addresses Information Base have the following structure:

Field	Data
S_Address	A valid global IPv6 address, owned by a node

Table 3: Secondary Addresses Information Base

DSADD is chosen among the addresses contained into this Base, using one of the algorithms detailed in Section 7.5.

6.4 Multiple Interface Association Information Base

Multiple Interface Association Information Base is defined in [RFC3626] and is filled processing MID messages. [RFC3626] mandates that these messages are generated by a MANET node only when it is equipped with multiple physical interfaces, through which it is connected to the MANET and participates to OLSR. MIDs contain the addresses configured on the node's physical interfaces. The node is

identified by multiple valid IPv6 addresses, one for each interface connected to the MANET: Multiple Interface Association Information Base contains bindings between such addresses and the main address of the node. Using this table, MANET nodes can set-up routes not only towards main address of other nodes, but also towards multiple interface addresses associated to main address. Following [RFC3626], a node connected to the MANET by means of a single interface MUST NOT generate MIDs.

In this specification, as described in Section 7.4, MID messages generated by a node contain the list of the Secondary Addresses, i.e. the list of all the global addresses the node may configure on its MANET interface. The Multiple Interface Association Information Base is maintained by each node and gateway and is used to store the bindings between the Secondary Addresses and Primary Addresses of other nodes.

It is worth noting that the semantics of the entries in Multiple Interface Association Information Base, as well as of MID messages, is changed by this specification, since multiple Secondary Addresses can be configured on a single interface. This semantic change has no effect on the processing of MID messages and it is completely backward-compatible: in fact, from a node's perspective, addresses announced in MID messages can be single addresses configured on multiple interfaces, or multiple addresses configured on a single interface. Routing table construction rules are not changed: nodes build necessary routes to both primary and secondary addresses following [RFC3626].

Hence, Multiple Interface Association Information Base entries have the following semantics (same as specified in [RFC3626]):

Field	Data
I_iface_addr	a Secondary Address built (and possibly configured) by a node
I_main_addr	the Primary Address of the node which has built the Secondary Address contained into I_iface_addr field
I_time	Validity time

Table 4: Multiple Interface Association Information Base

7. Detailed operations

This section gives the complete description of the operations MANET devices must execute in order to build a SADD. Procedures are detailed for nodes running OLSR ([RFC3626]), but mechanism can though be generalized for other routing protocols.

7.1 IPv6 Addresses generation

An IPv6 address is obtained by a node by attaching a prefix (both local-scoped and global) to the unique 64-bit interface identifier. According to [RFC3513], this identifier can be an End-System Unique Identifier, EUI-64 identifier, e.g. derived from the MAC address of the node. In [I-D.dupont-ipv6-imei] the International Mobile Subscriber Identity of a SIM-card is used for this purpose.

7.2 Primary Address configuration

At bootstrap, each node builds an IPv6 address and uses it as Primary Address (PADD), i.e. PADD is the OLSR Main Address and will be inserted into the Originator Address field of all sent OLSR messages. The PADD can be generated as described in Section 7.1 using mechanism detailed in [I-D.ULA] to obtain the prefix. It is worth noting that uniqueness of ULAs is not guaranteed, especially if they are locally generated. Therefore, PADD uniqueness MUST be verified by the configuring node, by means of one DAD method, not specified in this document.

7.3 Prefix Advertisement

Prefix Advertisement messages are transmitted by gateways and contain their delegated prefixes. Such messages are received by nodes partecipating to routing protocol.

7.3.1 Prefix Advertisement (PA) messages format

The new message type defined to announce the delegated prefixes associated to the MANET is shown in Figure 4 together with OLSR message header

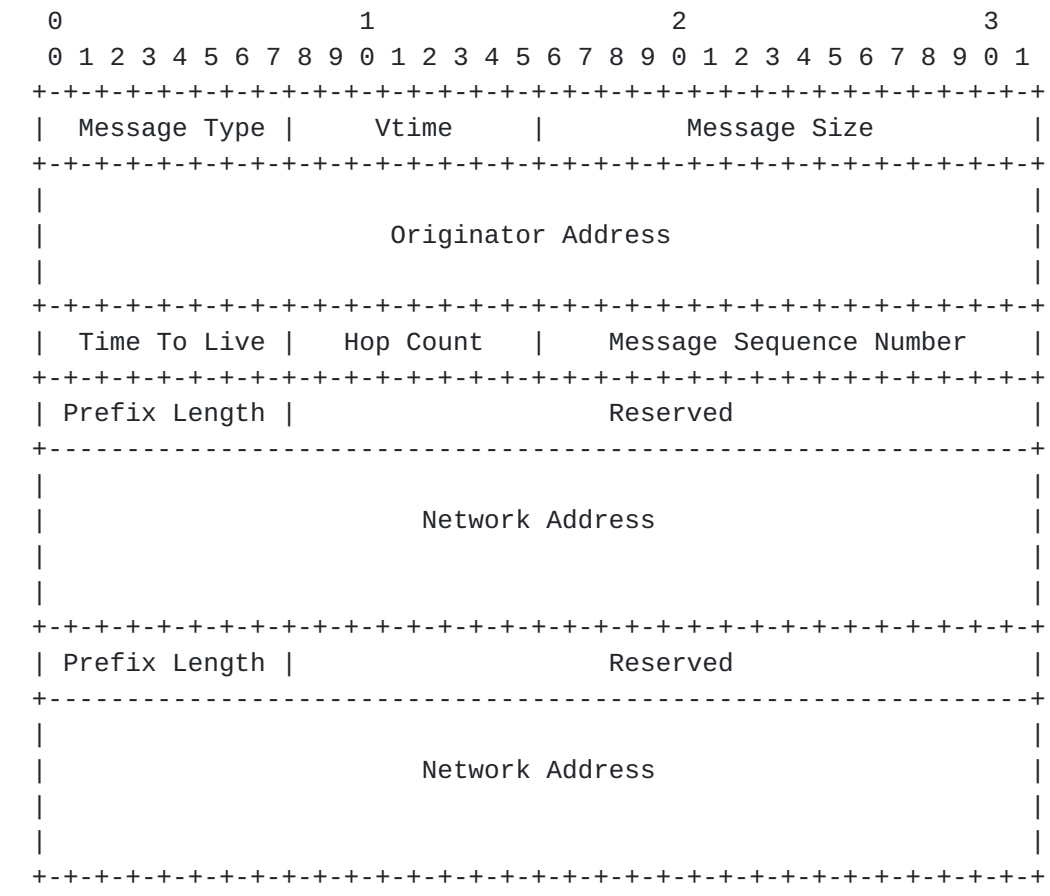

Figure 4: Format of Prefix Advertisement messages

Where each field of the message has the following meaning:

Field	Data
Message Type	[TBD]
Vtime	PA_HOLD_TIME
Message Size	see [RFC3626]
Originator Address	the Primary Address of the node (gateway) which generated the message
Time To Live	see [RFC3626]
Hop Count	see [RFC3626]
Message Sequence Number	see [RFC3626]
Prefix Length	the length of the prefix contained in Network Address field
Network Address	the delegated prefix of the gateway which generated the message

Table 5: Prefix Advertisement Fields

7.3.2 PA message generation

A PA message is sent by a gateway in the network to announce its delegated prefixes. I.e., the PA message contains the list of global prefixes which are associated to it. The list of prefixes can be partial in each PA message (e.g., due to message size limitations, imposed by the network), but parsing of all PA messages describing the interface set from a node MUST be complete within a certain refreshing period (PA_INTERVAL). The information contained in the PA messages is used by the nodes to build their Secondary Addresses.

7.3.3 PA message forwarding

Upon receiving a PA message, following the rules of Section 3 of [RFC3626], the message MUST be forwarded according to Section 3.4 of [RFC3626].

7.3.4 PA message processing

Upon processing a PA message, the P_time MUST be computed from the Vtime field of the message header (see [RFC3626]). The PIB SHOULD then be updated as follows:

1. If the sender interface (Note: not the originator) of this message is not in the symmetric 1-hop neighborhood of this node, the message MUST be discarded.

2. Otherwise, for each (Network Address, Prefix Length) pair in the message:

    1. if an entry in the association set already exists, where:

        P_addr == Originator Address

        P_network_addr == Network Address

        P_prefix_length == Prefix Length

      then the holding time for that entry MUST be set to:

        P_time = current time + validity time

    2. otherwise, a new entry MUST be recorded with:

        P_gateway_addr = Originator Address

        P_network_addr = Network Address

        P_prefix_length = Prefix Length

        P_time = current time + validity time

7.3.5 Secondary Addresses Information Base Management

For each (valid) prefix contained into Prefix Information Base, the node builds a Secondary Address as described in Section 7.1 and inserts it into the Secondary Address Information Base.

If a t-uple contained into Prefix Information Base is removed, e.g. after P_time expiration, the Secondary Address derived from the prefix contained into the removed t-uple MUST be removed from the Secondary Address Information Base.

7.4 MID messages

By means of standard MID messages processing, when OLSR eventually converges, the node is reachable at any of its Secondary Addresses : MANET nodes' routing tables contain a route for each secondary address listed into MID messages. A packet whose destination is one of the secondary addresses of a node (e.g. traffic from external hosts to MANET nodes) can therefore be routed within the MANET. Return traffic will be destined to such secondary address and will be routed within the MANET by means of the topological information inserted into MID messages.

7.4.1 MID message generation

A MID message is sent by a node in the network to announce its Secondary Addresses. I.e., the MID message contains the list of the Secondary Addresses which have been built by it and inserted into SAIB. The list of Addresses can be partial in each MID message (e.g., due to message size limitations, imposed by the network), but parsing of all MID messages describing the Secondary Information Base of a node MUST be complete within a certain refreshing period (MID_INTERVAL). The information contained in the MID messages is used by the nodes to route packets, which may be destined to one (or more) of the Secondary Addresses, chosen by a node to communicate with hosts located outside the MANET.

7.4.2 MID message forwarding

Upon receiving a MID message, following the rules of section 3 of [RFC3626], the message MUST be forwarded according to section 3.4 of [RFC3626].

7.4.3 MID message processing

MID messages are processed as described in [RFC3626]. The tuples in the multiple interface association set are recorded with the information that is exchanged through MID messages. Upon receiving a MID message, the "validity time" MUST be computed from the Vtime field of the message header (as described in Section 3.3.2 of [RFC3626]). The Multiple Interface Association Information Base SHOULD then be updated as follows:

1. If the sender interface (note: not the originator) of this message is not in the symmetric 1-hop neighborhood of this node, the message MUST be discarded.

2. For each Secondary Address listed in the MID message:

1. If there exist some tuple in the interface association set where:

   I_iface_addr == Secondary Address, AND

   I_main_addr == Originator Address,

   then the holding time of that tuple is set to:

   I_time = current time + validity time.

2. Otherwise, a new tuple is recorded in the interface association set where:

   I_iface_addr = Secondary Address,

   I_main_addr = Originator Address,

   I_time = current time + validity time.

7.5 Global IPv6 Address configuration for MANET nodes

A node uses one of the SADDs as its DSADD, i.e. the global IPv6 address used to exchange data traffic with other MANET nodes, as well as with external hosts. The choice of the global address must be executed at bootstrap time, after a node receives the first global prefixes. Nevertheless, this operation SHOULD also be executed when particular events trigger a topological change in the MANET. Such events have been cited in Section 5 and can be further detailed as follows:

1. The failure or the departure of the gateway owning the chosen prefix;

2. A partition, after which the node and the gateway owning the chosen prefix are connected to two different MANETs;

3. The gateway, which announces the chosen prefix, becomes a node, e.g. after shutting down the interface connecting it to the external network and stops announcing prefixes;

4. After a movement of one or more MANET devices, a gateway has a better metric than the gateway announcing the chosen prefix;

5. A merging occurs, after which a gateway previously not connected to the MANET may have the best metric value.

In case of events 1., 2. and 3. the global prefix, which the used SADD is derived from, is no more listed into PA messages and therefore is removed from Prefix Information Base: the node MUST change its global address, choosing one of the prefixes announced by active gateways. In case of 4. and 5., the node determines that its DSADD is derived from a prefix which is no more the best one, according to the the topological information it owns: in this cases, the node MAY change its DSADD, although it is still valid. A number of methods can be applied, to enable a node to choose its best prefix, among those announced by active gateways. Next section details two of such algorithms.

7.5.1 Best Prefix Selection Algorithm

The best prefix selection algorithm must take into account factors related to MANET topology, e.g. the routing metrics of the gateways and external factors, e.g. the number and type of active data sessions. It is assumed that a node, inspecting the routing table, monitors the current metric value of every reachable gateway generating PA messages and always knows which is the current deafult gateway. In this section two alternative algorithms are proposed.

1. Default Gateway Method: a node always selects the prefix announced by the current Default Gateway.

   As in this document the solution is OLSR-based, the default gateway is the closest gateway in terms of number of hops. This algorithm solves the downlink path optimization problem described in Section 4. In fact, if the node uses a global IPv6 address derived from the prefix announced by the default gateway, traffic to and from the external network flows through the same gateway. As a disadvantage, if MANET topology frequently changes, a node using this algorithm may experience frequent address changes, which can cause disruption of data sessions.

2. Threshold Method: a node compares the metric value of the gateway announcing the prefix currently used with that of the best gateway (normally, the default gateway); if the absolute value of the difference of the two metrics is higher than a predefined threshold, an address change is triggered; the new address is derived from the prefix announced by the best gateway.

Choosing one value of the threshold for many deployment environments can be difficult: it highly depends on the chosen metric and other factors, which do not strictly depend on routing, e.g. Quality of Service required by applications, how many active data sessions the node will tear down after address change.

7.5.2 Address change

If an address change is triggered by one of the events listed in the previous Section, a node executes the following operations:

- It stops using the SADD which was previously used as DSADD

- Starts using as DSADD the SADD derived from the prefix announced by the new best gateway (this SADD has been already disseminated in the MANET using MIDs).

7.6 Gateway operations

As described in Section 3, a gateway is a MANET node, equipped with a MANET interface, and a second interface, connected to the external network. Therefore, gateways have at least one global IPv6 address, belonging to the external network and used on the external interface. While the mechanism, by which such address is acquired, is out of scope of this specification, the configuration of the global address used on the MANET interface is described in this section.

Gateways MUST configure the global IPv6 address of their MANET interface using the mechanism specified in Section 6 and Section 7: a gateway MUST execute the operations described in these sections for MANET nodes. Gateways MUST always select the prefix contained into Delegated Prefixes Information Base to derive global address they will use on MANET interface. Finally, gateways MUST process PAs received from other gateways, generate SADDs and disseminate them with MIDs.

As described in Section 5.1, a gateway can change its mode of operations, becoming a node, for a number of reasons, e.g. because it has lost connectivity with the external network or because of its secondary interface failure. When a gateway becomes a node, it stops generating PA messages and executes the operations described in Section 7.5.1 and Section 7.5.2. In particular, it chooses the secondary address corresponding to the best active gateway as DSADD.

Since the gateway has already disseminated its new global address as a SADD in MIDs, it can communicate with the hosts located outside the MANET with negligible latency.

8. Mobile IPv6 Considerations

According to the proposed solution (Section 7.5.1), a node can change its DSADD for many reasons, e.g. in order to optimize downlink traffic coming from external hosts: generally, such address change implies active sessions interruption. In order to cope with this, Mobile IPv6 [RFC3775] can be used.

It is worth noting that the reduction (ideally to zero) of the latency introduced by a DSADD change implies better performances when MANET nodes use MIPv6. In fact, if a node experiments a change from a gateway to a second gateway, then it chooses a secondary address as DSADD, associated to the second gateway, and it sends a Binding Update message, registering the new chosen address as the new Care-of Address. When the Binding Acknowledge message from the Home Agent arrives at the gateway, immediately a route to the node will be available, because the new Care-of Address was announced in the MANET using the MID messages. Therefore handover latency is reduced to the time needed to send a Binding Update message and receive the correspondent Binding Acknowledge message, because routing latency is negligible.

9. Proposed Values for Constants

9.1 Emission Intervals

PA_INTERVAL = 5 seconds

MID_INTERVAL = 5 seconds

9.2 Holding Time

PA_HOLD_TIME = 3 x PA_INTERVAL

MID_HOLD_TIME = 3 x MID_INTERVAL

10. Security Considerations

TBD.

11. IANA Considerations

This document has no actions for IANA.

12. References

12.1 Normative references

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[RFC3626] Clausen, T. and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

12.2 Informative References

[4G-INT] Siebert, M., "On Ad Hoc Networks in the 4G Integration Process", Med-Hoc 2004 , June 2004.

[AMBNET] "Ambient Networks", http://www.ambient-networks.org .

[BELDING] Sun, Y. and E. Belding-Royer, "A study of dynamic addressing techniques in mobile ad hoc networks", I-D Wireless communication and mobile computing, May 2004.

[CHA] Cha, H., Park, J., and H. Kim, "Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks", I-D draft-cha-manet-extended-support-globalv6-00.txt, October 2003.

[DSR] Johnson, D., Maltz, D., and Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", I-D draft-ietf-manet-dsr-10.txt, July 2004.

[ENGELSTAD] Engelstad, P., T?sen, A., Hafslund, A., and G. Egeland, "Internet Connectivity for Multi-Homed Proactive Ad Hoc Networks", First IEEE International Conference on Sensor

and Ad hoc Communications and Networks , October 2004.

[I-D.ULA] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", draft-hinden-ipv6-global-local-addr-09 (work in progress), January 2005.

[I-D.dupont-ipv6-imei]
Dupont, F. and L. Nuaymi, "IMEI-based universal IPv6 interface IDs", draft-dupont-ipv6-imei-08 (work in progress), October 2004.

[I-D.ruffino-conn-scenarios]
Ruffino, S., "Connectivity Scenarios for MANET", draft-ruffino-conn-scenarios-00 (work in progress), February 2005.

[I-D.singh-autoconf-adp]
Singh, S., "Ad hoc network autoconfiguration: definition and problem statement", draft-singh-autoconf-adp-00 (work in progress), February 2005.

[I-D.wakikawa-manet-ipv6-support]
Wakikawa, R., "IPv6 Support on Mobile Ad-hoc Network", draft-wakikawa-manet-ipv6-support-00 (work in progress), February 2005.

[JELGER] Jelger, C., Noel, T., and A. Frey, "Gateway and address autoconfiguration for IPv6 adhoc networks", I-D draft-jelger-manet-gateway-autoconf-v6-02.txt, April 2004.

[JEONG] Jeong, J., Park, J., Kim, H., and D. Kim, "Ad Hoc IP Address Autoconfiguration", I-D draft-jeong-adhoc-ip-addr-autoconf-02.txt, February 2004.

[PAAKKONEN]
Paakkonen, P., Rantonen, M., and J. Latvakoski, "IPv6 addressing in a heterogeneous MANET-network", I-D draft-paakkonen-addressing-htr-manet-00.txt, December 2003.

[PERKINS] Perkins, C., Malinen, J., Wakikawa, R., and E. Belding-Royer, "IP Address Autoconfiguration for Ad Hoc Networks", I-D draft-perkins-manet-autoconf-01.txt, November 2001.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC2501] Corson, S. and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations", RFC 2501, January 1999.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[RFC3684] Ogier, R., Templin, F., and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, February 2004.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[SINGH] Singh, S., Kim, JH., Choi, YG., Kang, KL., and YS. Roh, "Mobile multi-gateway support for IPv6 mobile ad hoc networks", I-D draft-singh-manet-mmg-00.txt, June 2004.

[WAKI-GLOBAL6] Wakikawa, R., Malinen, J., Perkins, C., Nilsson, A., and A. Tuominen, "Global connectivity for IPv6 Mobile Ad Hoc Networks", I-D draft-wakikawa-manet-globalv6-03.txt, October 2003.

[WWRF] "World Wireless Research Forum", http://www.wireless-world-research.org .

[ZEROCONF] Aboba, B., "Dynamic Configuration of Link-Local IPv4 Addresses", draft-ietf-zeroconf-ipv4-linklocal-17 (work in progress), July 2004.

Authors' Addresses

Simone Ruffino
Telecom Italia LAB
Via G.Reiss Romoli 274
Torino 10148
Italy

Phone: +39 011 228 7566
Email: simone.ruffino@telecomitalia.it

Patrick Stupar
Telecom Italia LAB
Via G.Reiss Romoli 274
Torino 10148
Italy

Phone: +39 011 228 5727
Email: patrick.stupar@telecomitalia.it

Appendix A. Acknowledgments

The authors would like to thank Ivano Guardini for his valuable comments.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.