Mobile Ad Hoc Networking Working Group K. Weniger
INTERNET DRAFT M. Zitterbart
22 February 2002 Universitaet Karlsruhe (TH)

IPv6 Stateless Address Autoconfiguration for Hierarchical Mobile Ad Hoc Networks

<draft-weniger-manet-addressautoconf-ipv6-00.txt>

Status of this Memo

Abstract

This document describes, how the IPv6 Stateless Address Autoconfiguration [1] can be applied to hierarchical mobile ad hoc networks. A hierarchical address space is build up to limit the protocol overhead needed for the Duplicate Address Detection (DAD) and to enable route aggregation for hierarchical routing protocols. Unique addresses are guaranteed, even if the network splits up and merges later on.

Contents

1. Introduction

Routing protocols assume network-wide unique node identifiers. Because mobile ad hoc networks are infrastructure-free, highly dynamic wireless networks, central administration or manual configuration of the IP stack is impractical. The Internet Protocol IPv6 defines mechanisms to autoconfigure interfaces of nodes in wired networks in a distributed manner. This document specifies a method, how the IPv6 Stateless Address Autoconfiguration (SAA) and the Neighbor Discovery Protocol (NDP) can be applied to mobile ad hoc networks. The protocol overhead is limited due to a hierarchical approach. The resulting hierarchical address space can be used by routing protocols for route aggregation. Most notably, this approach guarantees to detect all duplicate addresses within a limited time, even if the network splits up and merges later on.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC 2119].

A leader node is the center of a subnet and sends Router Announcement (RA) messages. The scope of a node is an area of r hops around this node. Furthermore, the terminology of [1], [2] and [3] are used.

3. Limitations and Assumptions

The assignment of global routable addresses is outside the scope of this document. The hierarchical addresses can only be used for

communication within the ad hoc network. Due to the hierarchy, the address changes if a node changes the subnet. This situation can lead to the interruption of TCP-sessions and has to be handled by routing or mobility protocols. This is outside the scope of this document. Furthermore, it is assumed that the nodes do not necessarily have any kind of guaranteed unique interface identifier. This assumption is especially true for networks with devices, which do not own IEEE 802.x MAC-addresses (even they are not guaranteed to be unique). It is assumed, that an interface knows that it is in MANET operation and, subsequently, when to use this modified version of IPv6 SAA.

4. Protocol Overview

First, a node generates a link-local address as described in [1]. After that, the Duplicate Address Detection (DAD) is performed. The node broadcasts a modified Neighbor Solicitation (NS) message [2] extended by the so-called MANET-option. This message will be flooded within a limited area, the so-called scope. A node, which has the same address replies with a Neighbor Advertisement (NA) message. Subsequently, the sender of the NS message chooses a new address and repeats the process. This guarantees the uniqueness of the addresses within each node's scope.

An hierarchy is build by periodically sending these NS messages. Therefore, the MANET-option contains a weight that implies how well a node qualifies to be a leader node. This SHOULD include the number of neighbors, the degree of association with neighboring nodes and the remaining battery power of the node. The node with the highest weight within a scope becomes the leader node. This node sends Router Announcement (RA) containing a randomly chosen subnet ID. All nodes within the scope of the leader node construct a site-local address based on the subnet ID. In order to guarantee the uniqueness of subnet IDs, a Duplicate Subnet ID Detection (DSD) is performed between all leader nodes. Subsequently, the site-local addresses are guaranteed to be unique within the entire ad hoc network and can be

used for communication within the ad hoc network.

5. Address Generation

The generation of a link-local address is performed as described in [1]. This address MAY only be used for the communication within the scope of the node. Based on the subnet ID contained in the Router Announcements (RAs) sent by the leader node, nodes construct a site-local address. This address can be used for communication within the entire ad hoc network. The lifetime of the prefixes contained in the RAs SHALL be set to two times the period which the RAs are issued.

Router Solicitation messages MUST NOT be send as described in [2].

6. Duplicate Address Detection

The DAD is only performed within the scope of a node and guarantees the uniqueness of the link-local address within the scope. A node performing the DAD sends a modified NS message to the all-nodes multicast address [3] with the link-local address as solicitation target address. This message will be flooded within a limited area, the so-called scope. A node with the same address replies with a NA message. Subsequently, the sender of the NS message chooses a new address and repeats the process. Unsolicited NA messages SHALL NOT be send. Further differences to [1] are, that addresses can already be used before the DAD is completed (it is repeated anyway) and that the autoconfiguration process is started even if no RAs are received.

6.1. Random Source ID

In order to distinguish NS messages of different senders, which potentially have the same IP address, a Random Source ID (RS-ID) is introduced. Every NS message includes a new, randomly chosen ID. This ID is not changed if the message is forwarded only. First, this prevents nodes from forwarding the same message more than one time. Second, this allows nodes to detect address conflicts: Nodes remember the last RS-IDs used for sending NS messages. If a node receives an NS message with an RS-ID that it did not use recently and a target address, which is equal to its own address, an address conflict is

detected and the node replies with an NA message. Subsequently, the corresponding node chooses a new address and the conflict is resolved. If the RS-ID were not be changed continuously, an address conflict of two nodes with the same IP and the same RS-ID would never be detectable.

6.2. Hop Limit

The hop limit field in the IPv6 header has to be set to the radius of the scope. Subsequently, NDP packets with a hop limit field other than 255 MUST NOT be discarded as it is specified in [2].

6.3. Relay of DAD messages

Because all nodes within the scope of a leader node form one subnet and have the same subnet ID, they must have a unique interface identifier part. This can only be guaranteed, if the link-local

addresses are unique within a subnet, which is equal to the scope of the leader node. Therefore, the leader node has to relay NS and NA messages received from nodes of its subnet with a hop limit set to the radius of the subnet. Before the leader node changes the hop limit field, it stores its value in the so-called pre-relay hop limit field of the MANET-option. Subsequently, each node knows the distance to the sender, even after the modification of the hop limit field, by adding the value of the pre-relay hop limit field. This is required for a fair leader election, where each node only competes with the nodes within its scope. The default value for this field is 0.

7. Leader Election

The algorithm for the leader election is not specified in this document. It SHOULD consider the number of neighbors, the degree of association with neighboring nodes and the remaining battery power of the node. A weight, that has to be defined more detailed, implies how well a node qualifies to be a leader node. Each node includes its weight in the NS messages sent. Because these messages are sent periodically, each node knows about the current weight of all nodes within its scope and can decide, who the current leader node is. The

election results in a minimum distance between two leader nodes equal to the radius of the scope. After entering the Leader State (LS), the node subscribes to the all-leadernodes multicast group. Nodes, that are not in LS are in Host State (HS).

8. Duplicate Subnet ID Detection

In order to guarantee unique subnet IDs, the leader nodes need to perform a Duplicate Subnet ID Detection (DSD). Therefore, they send NS messages to the all-nodes multicast address containing a site-local address constructed by the subnet ID and an interface identifier of 0 as solicitation target address. A so-called D-flag indicates, that the message is used for the detection of duplicate subnet IDs. Only nodes in HS forward this message. In case of an conflict, an NA messages is issued and a new subnet ID is chosen. The hop limit field SHOULD be set to the diameter of the ad hoc network. This can be estimated by the number of leader nodes, which is equal to the number of NS messages received during the DSD, and the scope radius.

9. Network Partitioning

The leader node election is done periodically along with the DAD and the DSD in order to maintain the hierarchical address space and to

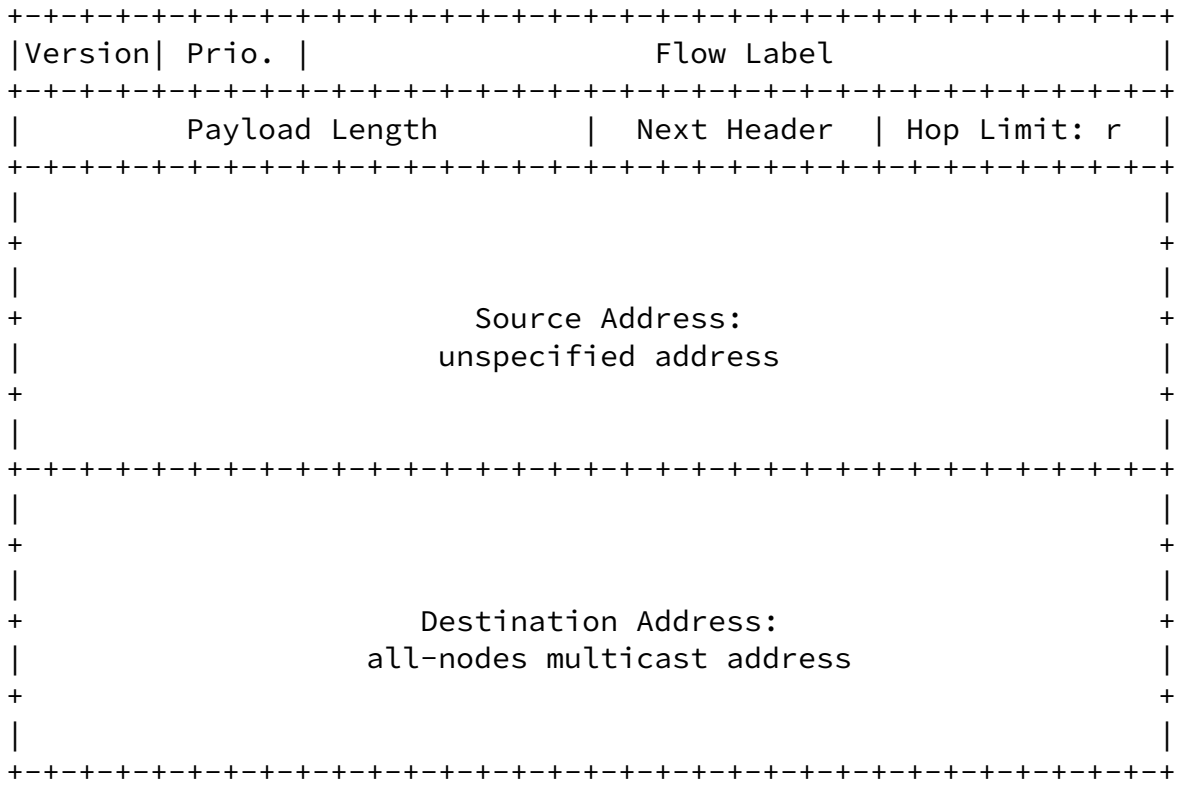
cope with the network dynamics. Therefore, network partitioning and merging is supported.

10. Message Formats

10.1 IPv6 Header

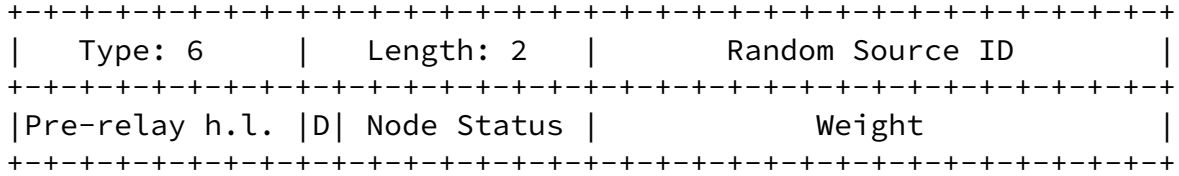
Changed fields in the IPv6 Header include the hop limit field and the destination address. The solicited-node multicast address can not be used, because all nodes must be able to receive and forward a message.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```



10.2 MANET-option

NDP messages as specified in [2] are extended by the MANET-option



Random Source ID
: Random number to distinguish between different senders of messages with the same IP address

Pre-relay hop limit
: Contains the value of the hop limit field prior to modification by the leader node

Node Status
: Can be either Host State (0) or Leader State (1)

D-Flag
: Can be either Duplicate Address Detection (0) or Duplicate Subnet ID Detection (1)

Weight
: Indicates, how well a node qualifies to be a leader node

11. Security Considerations

TBD.

References

[1] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", Request for Comments 2462, Internet Engineering Task Force, Dec. 1998

[2] T. Narten, El. Nordmark and W. Simpson , "Neighbor Discovery for IP version 6", Request for Comments 2461, Internet Engineering Task Force, Dec. 1998

[3] R. Hinden and S. Deering , "IP version 6 Addressing Architecture", Request for Comments 2373, Internet Engineering Task Force, July 1998

Author's Address

Questions about this memo can be directed to:

Kilian Weniger, Martina Zitterbart
Zirkel 2
Institute of Telematics
Universitaet Karlsruhe (TH)

76128 Karlsruhe

Germany
Phone: +49 721 608 {6415,6400}
Fax: +49 721 388097
Email: {weniger,zit}@tm.uka.de

Appendix A: Estimation of Protocol Overhead

In this section, the overhead of this protocol is estimated. First, we assume 1000 nodes and a period of 5 seconds for the DAD and the DSD.

Number of nodes	N_NODES	1000
Size of NS msg (bytes)	S_NS	72
Network density	DEN	3
Period of DAD (sec)	PERIOD	5

The network density is defined as the average number of nodes within the range of a node competing for access to the shared medium. We assume that power control algorithms are used in dense networks. Therefore, a number of 3 seems to be reasonable.

The number of leader nodes can be estimated giving the number of nodes and the scope radius (assumed that each node is a member of only one subnet). The optimal value of leader nodes is estimated by minimizing the number of messages that a node has to forward (N_MSG).

```
Optimal number of leader nodes
N_LEADER = N_NODES^(1/2) =~ 32

Scope radius (hops)
R_SCOPE  = (N_NODES/(N_LEADER*pi))^(1/2) =~ 3

N_MSG = pi*R_SCOPE^2 + N_LEADER =~ 64
```

This results in the following utilization of an 802.11b link (brutto data rate: 11MBit/s, netto data rate: 600 kbyte/s):

```
Bandwidth of link (bytes)
BANDWIDTH  600 000

Link utilization
UTIL = N_MSG * S_NS * DEN / (PERIOD * BANDWIDTH)
     = 64 * 72 * 3 / (5 * 600 000) =~ 0.0046 or 0.46 %
```

The utilization increases proportional to N_MSG, which is in turn proportional to N_NODES^(1/2):

$$UTIL \sim N\_MSG = N\_NODES/N\_NODES^{(1/2)} + N\_NODES^{(1/2)} = 2*N\_NODES^{(1/2)}$$

If the number of nodes doubles, the utilization increases only by 2^(1/2) =~ 1.4. Subsequently, the utilization is as follows for our system and a system without a hierarchy, respectively:

# of nodes	with hierarchy	without hierarchy
1 000	0.5 %	7.2 %
10 000	1.4 %	72.0 %
100 000	4.6 %	>100.0 %