IPv6 Support on Mobile Ad-hoc Network
draft-wakikawa-manet-ipv6-support-01.txt

Status of This Memo

This document is a submission to the MANET Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the manet@ietf.org mailing list.

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 18, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).
Abstract

This draft defines the IPv6 addressing architecture for Mobile Ad-hoc Network. This document includes problem statements when manet using IPv6, IPv6 addressing model, IPv6 manet node’s required addresses. Note that this document does not discuss how an IPv6 address is allocated to each manet node.

Contents

Status of This Memo 1
Copyright Notice 1
Abstract 1
1. Introduction 3
2. IPv6 Addressing for MANET 3
   2.1 Link Local Unicast Address 3
   2.2 Unique Local Unicast Address 4
   2.3 Global Unicast Address 5
3. Manet node requirements 5
   3.1 General node’s required Address 5
   3.2 Optional required address for global communication 6
4. Source Address Selection 6
5. Neighbor Discovery Protocol for MANET 6
   5.1 Neighbor Cache Resolution 7
   5.2 Address Auto-configuration 7
   5.3 Duplicate Address Detection 7
6. MANET Routing Protocols 8
   6.1 Message Flooding 8
   6.2 Neighbor Sensing 9
   6.3 Consideration of Longer IPv6 Address 9
7. Running Mobility Protocols 9
   7.1 Mobile IPv6 9
   7.2 Network Mobility 10
8. Changes 11
Acknowledgments 11
References 11

R. Wakikawa et.al. Expires 20 Dec 2005 [Page 1]
1. Introduction

This document investigates issues when IPv6 [3] is operated with mobile ad hoc networks. In general, routing protocols disregard differences between IPv4 and IPv6, and suggest both can be supported if routing messages for both protocols are defined. However, there are some differences which may well affect how the routing protocols should work with IPv6.

In addition there are several issues that may or may not be covered in other documents. This document tries to provide information about implementing and deploying IPv6 mobile ad hoc networks. Addressing in mobile ad hoc networks is a problem for both IPv4 and IPv6. When manet connects to the global Internet, IPv4 might do NAT, but in IPv6 we want to have a more integrated solution. This means potentially acquiring an address with global scope. In an effort to alleviate problems related to address scopes [2], we first study applicability of each scope of addresses to mobile ad hoc networks and give guidelines for IPv6 address assignment. After defining address assignment, we briefly discuss the Neighbor Discovery Protocol [10] operations and manet operations on IPv6 mobile ad hoc networks.

2. IPv6 Addressing for MANET

IPv6 has a notion of ‘‘scope’’ to control validity of each IPv6 address. In a manet, a link-local scope is used to identify a physical link and an edge of a manet is identified by a unique-local scope. A global scope is used for global communication to the Internet.

2.1. Link Local Unicast Address

A link local unicast address is designed to use with on-link neighbors, but not over multi-hop. The IPv6 specification prohibits forwarding packets sent to/from a link local address over a link.

A manet does not have a clear link definition in terms of multi-hop routing. Indeed, there are two interpretations of ‘‘on-link’’ in manet observation.

- physical medium [9]
  The link local address is valid only with one-hop neighbors.

- manet wide (till an edge of a manet)
  The link local address is valid over multi-hop. However it breaks the original definition of link local address.
Considering fact that many IPv6 related protocol including the Neighbor Discovery Protocol have already been operated with the legacy link local address definition, it is reasonable to inherit the original interpretation of "link" for manets. Otherwise, it could break interoperability between a manet node and a node on the Internet. It is possible that a node visits both an IPv6 network and a manet.

The link local address is used only for communication with 1-hop neighbors. This address is also used for the Neighbor Discovery Protocol. The link-local all-manet-node multicast address (ff02::TBD) is used for application flooding described in Section 6.1.

Routes for link local addresses MUST NOT be exchanged over multi-hop neighbors by manet routing protocols. A node may exchange routes for link local address with 1-hop neighbors, but this should be done carefully. This is because whenever a manet node moves and a set of 1-hop neighbors is changed, the route becomes invalid. Thus, each manet node must carefully maintain routes for link local address.

2.2. Unique Local Unicast Address

A unique local unicast address is not routable on the global Internet, however it can be used for local communication within limited area such as site and manet. More characteristics are described in [7]. A unique local unicast address is not automatically generated, but it is assigned through address auto-configuration [12], DHCPv6 [6], static, etc in an IPv6 network. The locally assigned unique local prefix is generated randomly by each network and assigned it without any verification of its uniqueness. Even when a unique local prefix is duplicated, the damage of this duplication is kept in minimum, because the duplicated prefix is valid within each limited area and is not used for global communication. Unless two networks are merged, they cannot know of duplication of the unique local prefix.

IPv6 enabled mobile ad-hoc networks can be treated as a limited area due to its different routing approaches from the Internet (IGP, BGP, etc). A unique Local Unicast address is expected to be assigned to all manet nodes. The unique local unicast address is used only for local communication within manets.

Routes for unique local address should be advertised and exchanged within a manet. These routes MUST NOT be leaked out to the Internet. Even if some routes for unique local addresses are leaked out, the backbone routers located to the Internet would often reject and ignored these routes. It is easier to exclude routes for unique
local addresses from the global Internet in terms of different address scope.

2.3. Global Unicast Address

A global unicast address is routable on the global Internet and used for communications on the Internet. A global unicast address must be unique on the Internet. Having a global unicast address is not mandated to all manet nodes, but only to manet nodes which need global Internet connectivity. The notion of global unicast address is applied without any changes to manets. Only manet nodes which want global connectivity acquires a global unicast address through some mechanism. A global unicast address can be used for both local communication within a manet and global communication to the Internet.

Routes for topologically correct global address can be advertised to the Internet. However, these routes MUST be aggregated. Un-aggregated routes, like host routes often used within a manet, SHOULD NOT be re-distributed to outside the manet without aggregation.

On the other hand, some manet nodes may have a home address of Mobile IPv6 [8] and a mobile network prefix of the NEMO basic support protocol [4]. The routes for a home address and a mobile network prefix SHOULD NOT be leaked to the Internet because of topologically incorrectness. Otherwise, it will disrupt the IPv6 routing architecture. Detailed operations can be found in Section 7

3. Manet node requirements

This section describes required address(es) for each manet node. There are two classification, General required address and extra-required address for Connected manet ( [11])

3.1. General node’s required Address

An isolated manet is a network formed dynamically with wireless manet nodes, but which is disconnected from the global Internet. This is defined in [11].

Each manet node MUST generate a link local address according to the IPv6 specification [3] and MUST also obtain a unique local address. A unique local prefix, used for the generation of the unique local address, is identical to all nodes within each mobile ad-hoc network. The unique local address is generated from locally assigned unique
global ID [7]. How to auto-configure an unique local address is out of scope for this specification.

Even if two manets are merged, or if a manet is partitioned, the nodes should keep the originally assigned unique local prefix. When two manets are merged, they can exchange routes of two unique local prefixes within the merged manet, and can communicate between different unique local prefixes. This can avoid address conflicts and prevents storm of duplicate address detection when manets are merged. When a manet is partitioned, two networks now share the same unique local prefix. However, these prefixes are not routed in the global Internet. Thus, this is not problematic unless the two manets re-merge. Each manet may re-assign a new unique local prefix for merged/separated scenarios. However, this completely depends on address configuration mechanism and its operation.

3.2. Optional required address for global communication

A connected mobile ad-hoc network is a wireless multi-hop network that has global connectivity to the Internet by using Internet Gateway [13] or OSPF extensions.

Each manet node acquires a global unicast address for global communication. The assignment of global unicast address is needed for connected mobile ad-hoc network. Whenever a manet node detects that the global address is not topologically correct in a foreign network, it MUST release the invalid global address and obtain topologically correct address.

Note that manet routes for global addresses should not be leaked to the Internet without aggregation.

4. Source Address Selection

RFC3484 [5] specifies the source/destination address selection algorithm. There is no special treatment for manets and each manet node uses the proposed default algorithm defined in [5].

5. Neighbor Discovery Protocol for MANET

Neighbor Discovery Protocol (NDP) assumes to be run on a link. However a manet does not have clear definition of ‘‘link’’ as described in Section 2. A manet is wireless multi-hop network and all manet nodes inside a manet is expected to be a router. Thus, this section discuss how NDP can be made fit for manets.
Similar to the current NDP protocol, the IPv6 Hop Limit field of both Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA), and Redirect message must be set to ‘255’ all the time. The IP Hop Limit field set to 255 indicates that the packet should not be forwarded by a router.

5.1. Neighbor Cache Resolution

Although a manet does not have the clear definition of link, a manet node can resolve a neighbor cache (i.e. MAC address) of one-hop neighbors by using NS and NA messages sent to and from link-local addressed. It is enough for manet nodes to resolve neighbor caches of one-hop neighbors, because manet nodes do not share the physical link with two-hop neighbors.

Even if a manet node can resolve a neighbor cache of two-hop neighbors, it can not send packets directly to the two-hop neighbors due to lack of L2 routing mechanisms. Each manet node manages neighbor caches for one-hop neighbors and confirms manet node’s reachability for one-hop neighbors by using NS and NA (i.e. NDP). Neighbor nodes, located more than one-hop away, are confirmed by the manet routing protocol governing the network.

It is important to inherit original interpretation of link for NDP. A manet node is not always connected to a manet, but it can be attached to an IPv6 link. In such case, a manet node does not need to change the operation of NDP, while there is no mechanism to detect whether attached network is a manet or a normal IPv6 network.

5.2. Address Auto-configuration

IPv6 has an address auto-configuration scheme based on exchange of RS and RA. However, the address auto-configuration is not designed for wireless multi-hop networks (i.e. manets). A manet needs to extend or re-invent address auto-configuration schemes for global addresses and unique local addresses. For global addresses, it is required that the addresses must be topologically correct and routable. [13].

5.3. Duplicate Address Detection

Duplicate Address Detection (DAD) can guarantee the uniqueness of any scope of addresses by sending a NS for a target address. If a NA is detected in response to the NS, the address is duplicated. DAD only defends addresses on a physical link due to link-local scope limitation of NS and NA. Thus, DAD can be conducted to guarantee
only the uniqueness of addresses within one-hop neighbors. (Note
that even if there is no duplication within on-hop neighbors, it
is possible that two-hop neighbors may have a duplicated address.)
This is not useful because one-hop neighbors are often changed due
to node mobility. Once neighbors are changed, the uniqueness is not
guaranteed. Each manet node SHOULD stop using DAD and use another
duplication address detection mechanism specially tuned for manet.

6. MANET Routing Protocols

6.1. Message Flooding

There are two different forwarding engines for message flooding for
manet routing protocols such as ‘application forwarding’ and ‘IP
forwarding’.

- Application Forwarding:
  For application forwarding, it is required that each application
  (ex. routing daemon) must send a flooded packet with single
  hop-limit to all neighbors. The recipient processes the
  flooded packet and will re-send it to all its neighbors if
  necessary. The flooded packets are thus repeatedly forwarded
  by an application until it has reached all nodes inside mobile
  ad-hoc network. Most of manet routing protocol use application
  flooding for protocol message exchanges.

- IP Forwarding
  Flooded packets can be forwarded by IP layer. The forwarding is
totally blind from applications. If a destination is multicast
address, an application on each manet node receive the flooded
packet, but the flooded packet is forwarded to next neighbors at
IP layer at the same time. The application should not need to
re-send the flooded packet.

For application flooding, each manet node sends a flooded packet to
the link-local all-manet-node multicast address (ff02::TBD). If the
flooded packet is used to setup a route for the sender node (i.e.
reverse route), it should use the address except for link-local
address as a source address. This is because routes for link local
addresses are garbage on multihop networks. Otherwise, the source
address should be set to a link-local address due to one hop limit
packets.

For IP forwarding, each manet node needs to send a flooded
packet from either global address or unique local address to an
all-manet-multicast address that is currently undefined. The
all-manet-multicast address can be defined for global scope, but must
be defined for unique local scope, too. This is because all manet
nodes do not always have global address.

6.2. Neighbor Sensing

Most manet routing protocols uses hello message to sense 1-hop
neighbors. IPv6 permits allocating multiple addresses to a single
interface. For example, a manet node may have 3 addresses (such as
a link-local address, a unique local address, and a global address).
In that case, each manet node SHOULD contain addresses except for
link local addresses (i.e. the unique local and global address).
Even if the link local address is included in hello messages, the
route for the link local address SHOULD not be maintained on each
manet node. The link local address SHOULD be used to send NS and NA
for Neighbor Cache resolution.

6.3. Consideration of Longer IPv6 Address

The length of IPv6 address is 128-bit which is 4 times longer than
IPv4 address. Therefore, protocol messages including IPv6 routes are
tend to be longer than the IPv4 counterparts. Specially in proactive
routing protocols, as a number of manet nodes are increased, routing
messages could be longer. If routing messages becomes larger than
the link MTU, the messages are fragmented by IP layer. This should
be avoided since one piece of fragmented packets can be dropped due
to unstable manet path (depending on topology change speed). Each
manet node SHOULD avoid IP fragmentation of each routing messages by
divided the routing messages into multiple messages at higher than IP
layer (i.e., applications). In alternative way, routing messages can
be shorten by any header or data compression mechanisms.

7. Running Mobility Protocols

7.1. Mobile IPv6

In Mobile IPv6 [8], a mobile host has a permanent global scope
address called its ‘‘home address’’. When a mobile host roams into a
manet, it can still use the home address as a source or destination
address of communications.

Although a mobile host can exchange routes for its home address
(global scope) within manet by using the appropriate manet routing
protocol, these routes should not be leaked to the Internet (i.e.
IGP) as described in Section 2.3. This is because a home address is
not topologically correct global address and leaking topologically
incorrect routes disturbs the IPv6 routing architecture.
When a manet is an isolated manet, a mobile host can not acquire a global address and can not form a care-of address so that it will give up sending a binding update to its home agent. Although Mobile IPv6 does not explicitly prohibit using unique-local address as a care-of address, but there is no specification for that. A mobile host can keep using its home address in a visiting manet by exchange a manet route of its home address. In such case, the mobile host does not use a bi-directional tunnel between it and home agent, but it sends packets along to manet routes.

On the other hand, when a manet is connected manet, a mobile host can acquire a global address and register the care-of address to its home agent. The mobile host can communicate with either a home address and a care-of address in a manet by route exchanges. When the mobile host communicates with a destination located in the same manet, it may have a host route toward the destination and can skip using bi-directional tunnel for the destination. If a destination is outside manet, the mobile host must encapsulate packets to its home agent as Mobile IPv6 does. The mobile host may use route optimization for a destination located in either manet or the Internet.

7.2. Network Mobility

In the NEMO Basic Support protocol (NEMO), a mobile router has a permanent global scope prefix called "mobile network prefix". A mobile router may also roam into manet with its mobile network prefix.

A mobile router can exchange a route of its home address (global scope) and its mobile network prefix within manet by using manet routing protocols. However these routes should not be leaked to the Internet (i.e. IGP) as described in Sectionglobal, too. It is because a home address and a mobile network prefix are not topologically correct global address at the visiting manet and leaking topologically incorrect routes disturbs the IPv6 routing architecture.

When a mobile router, which is NEMO mobile router but not manet node, roams into an isolated manet, it can not acquire a care-of address and will give up home registration to its home agent. However, the mobile router can exchange manet route for its mobile network prefix and use the manet route for communications from/to its mobile network. The mobile router should not try to use a bi-directional tunnel as NEMO does.

On the other hand, when a manet is connected manet, a mobile router can acquire a global address and register the care-of address to its
home agent. The mobile router also exchange manet route for its mobile network prefix. When the mobile route finds that a manet route of a destination is in its routing table (i.e. destination is located within the same manet), it can bypass all procedure of NEMO (i.e. tunneling to home agent, etc) and will forward packets along the manet route. If not, the mobile router process packets and tunnel them to its home agent according to binding information. NEMO does not specify any route optimization scheme.

Note that some issues related NEMO might be solved by using manet [1].

8. Changes

This is the initial version of this specification.

Acknowledgments

The authors would like to thank all the participants of OLSR workshop@San Diego.

References


Authors’ Addresses

Ryuji Wakikawa
Keio University
Dept. of Environmental Information
5322 Endo Fujisawa Kanagawa
252, JAPAN
Phone: +81-466 49-1394
EMail: ryuji@sfc.wide.ad.jp

Antti J. Tuominen
Helsinki University of Technology
Laboratory for Theoretical Computer Science
P.O. Box 9201
HUT FIN-02015, Finland
Phone: +358 9 451 5136
Fax: +358 9 451 5351
EMail: anttit@tcs.hut.fi

Thomas Heide Clausen
Project PCRI
Pole Commun de Recherche en Informatique du plateau de Saclay
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud
Ecole polytechnique
Laboratoire d’informatique
91128 Palaiseau Cedex, France
Email: T.Clausen@computer.org
Phone: +33 1 69 33 40 73

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the
use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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