Ryuji Wakikawa
Keio University
Jari T. Malinen
Charles E. Perkins
Nokia Research Center
Anders Nilsson
University of Lund
Antti J. Tuominen
Helsinki University of Technology

Global connectivity for IPv6 Mobile Ad Hoc Networks
draft-wakikawa-manet-globalv6-05.txt

Status of This Memo

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 August 30, 2006.

Copyright Notice

Abstract

This document describes how to provide Internet connectivity with mobile ad-hoc networks. It describes how to obtain a globally routable address and internet gateway operation. Once a manet node obtains a global address from an internet gateway, it may exchange data with nodes on the Internet. This Internet access method is not dependent on a particular manet protocol. Further, use of global connectivity with Mobile IPv6 is specified.

Contents

1. Introduction

A mobile ad-hoc network (manet) is built dynamically when a set of manet routers creates routing state for their connectivity management, typically over a wireless network. Manet routing protocols aim to maintain a route to a destination despite movement of intermediate nodes that causes the route path to change. There are routing protocols standardized at IETF such as DYMO [1], OLSRv2 [2], AODV [11], OLSR [3], DSR [7], and TBRPF [10].

Global connectivity is often required for manet routers desiring communication with the fixed Internet. However, routing protocols for manets only maintain routes locally within the reach of a manet running the given protocol. This document specifies the method by which a node in the manet acquires a global address from a gateway, as well as how this node will communicate over the gateway.

The following assumptions are made for simplicity and definiteness:

- Address Family
  This document assumes IPv6 address family support. The manet routing protocol discussed in this document MUST be capable of routing for IPv6 addresses.

- Topological assumption
  There is at least one internet gateway somewhere in the manet.

- Address assumption
  All nodes in the manet must have or acquire a routable address, perhaps usable as a Mobile IPv6 [8] home address. The routable address is used for initial configuration when a node boots up and joins the manet

2. Terminology

manet node
: A node located inside a manet

internet node
: A node located within the Internet (outside manet)

internet gateway
: A router which provides Internet connectivity for nodes in the manet. This router is located somewhere in a manet and has a connection to both the Internet and the manet.

manet local address
: A manet node's identity address in manet. The address is used for ad-hoc routing.

global address
: A node's IPv6 address in the Internet, typically resolvable from a DNS name. The address identifies the mobile node, and is used for communication to the Internet

internet route
: A route to the Internet (i.e. internet gateway). It can be treated as a default route or a network route.

manet route
: A route to other manet nodes. It is typically host route in a manet.

internet gateway information
: The gateway's IP routing prefix, prefix length, and lifetime.

internet gateway advertisement
: A message to disseminate internet gateway information to a manet.

    IGWADV-M
    : Extends the manet protocol; a control message is specified for each particular protocol to advertise internet gateway information

    IGWADV-N
    : Extends NDP to indicate that the advertisement contains information about the internet gateway

internet gateway solicitation
: A message to solicit an internet gateway advertisement.

IGWSOL-M
: Extends the manet protocol; a control message is specified for each particular protocol to solicit internet gateway information

IGWSOL-N
: Extends NDP to solicit an internet gateway Advertisement.

internet gateway confirmation
: A message to confirm an IPv6 global address of a manet node. This can be an IGWCON or a signaling of each manet routing protocol (ex. RREP).

IGWCON-M
: Extends the manet protocol; a control message is specified for each particular protocol for the internet gateway confirmation.

IGWCON-N
: Extends NDP for the internet gateway confirmation.

internet gateways multicast address (IGW_MCAST)
: Specifically, ALL_MANET_GW_MULTICAST, the IPv6 global multicast address for all internet gateways in a manet.

3. Overview

The global connectivity for manet is defined for any global address configured to any manet network interface of a manet node, and it defines a method for configuring a globally routable address for such an interface. Once such global address is available, global mobile-initiated sessions, such as web browsing or DNS queries, can be used. A topologically correct address in the IP header's source field is sufficient for packets sent from the manet node in such sessions.

A manet node discovers an internet gateway by receiving an internet gateway advertisement. Each internet gateway MAY disseminate internet gateway advertisement proactively. Periodic advertisements, however, are not typically used with reactive manet protocols such as DYMO [1], AODV [11] and DSR[7]. Thus, a manet node can solicit internet gateway advertisement when it needs a route to the Internet, and will receive internet gateway advertisements back in response. This solicitation is optional when an internet gateway periodically floods a internet gateway advertisement. In this way, the reactive and proactive route discovery features of each manet routing protocol are not disturbed.

For these internet gateway solicitation and advertisement, we introduce modifications to the Neighbor Discovery Protocol (NDP) [9] and each manet routing protocol. Operators can use the preferred one to implement global connectivity. The proposed method targets all manet protocols regardless of whether they are reactive or proactive. An advertisement from the internet gateway provides prefix information, and advertisement processing possibly resolves a route to the gateway, inserted as a route toward the Internet (i.e. Internet Route). A prefix which is distributed by internet gateways can be used for configuring a (typically globally) routable IPv6 [5] address for each manet node.

After accepting an advertisement from the internet gateway, the manet node configures a global address from the prefix of the internet gateway and inserts the internet gateway address as an internet route. Each internet gateway monitors packets received from the manet, to avoid unnecessarily forwarding the packet to the Internet when the destination is already present within the manet. The destination of a packet passing through the internet gateway is checked on the internet gateway. If the manet is operating reactively, the internet gateway in this case may also supply an updated route to the sending node. The sending node then receives a notification and sends a route request to discover the direct route to the destination. To do so, each intenet-gateway MAY manage a roster of IP addresses of all the associated manet nodes. The

management is explained in Section 7.4.

4. Conceptual Data Structures and Messages

4.1. Conceptual Data Structures

This specification assumes that all manet nodes support the following data structures. These structures are similar to the data structures defined in Neighbor Discovery Protocol (NDP)[9]. These structures can be implemented in several ways. An example is extending the structures implemented for NDP.

- Internet Gateway List (IGW List)
  A list of available internet gateways to which packets may be sent. In this list, the internet gateway information described later must be stored. Each entry also has an associated invalidation timer value (extracted from internet gateway Advertisements) used to delete entries that are no longer advertised. The entries are listed below:

  1. internet gateway global address

  2. internet gateway lifetime

  3. internet gateway manet-local address (optional)

- Internet Gateway Prefix List (Prefix List)
  A list of prefixes that are advertised by internet gateways. This Internet Gateway Prefix List entries are created from information received as internet gateway advertisements. Each entry has an associated invalidation timer value (extracted from the internet gateway advertisement) used to expire prefixes when they become invalid. The entries are listed below:

  1. internet gateway prefix address

  2. internet gateway prefix address length

  3. internet gateway prefix preferred lifetime

  4. the number of advertised internet gateways

- Associated MANET nodes list
  Each internet gateway manages an associated manet node list for all the manet nodes to which it supplies a global connectivity. The following information must be managed on each internet gateway.

  1. A global address of a manet node

4.2. Internet Gateway Information

A manet node needs a globally routable address in order to be globally reachable, so that it can receive packets from the Internet. The manet node needs to learn its topological location and an address of the internet gateway that provided the node with this access to the Internet. The node therefore needs to obtain a global prefix owned and distributed by internet gateways. The information which a manet node needs to know for internet connectivity is listed below. An internet gateway advertises these items as its internet gateway information. This internet gateway information is introduced to keep compatibility with NDP [9].

- internet gateway global address
  The internet gateway's global address, which can be used as a route to the Internet on manet nodes.

- Internet Gateway Prefix address
  The network prefix address which internet gateway is serving. The prefix MUST be valid address and topologically correct address on the Internet.

- Internet Gateway Prefix length
  Prefix length of the network prefix address of an internet gateway.

- Internet Gateway Prefix Preferred Lifetime
  The addresses generated from the prefix via stateless address autoconfiguration remain preferred [13]. A value of all one bits (0xffffffff) represents infinity. See [13]. After expiration of the lifetime, the manet node MUST delete its autoconfigured IPv6 global address.

- Internet Gateway Lifetime
  The lifetime of an internet gateway. After expiration of the lifetime, a manet node MUST NOT use the internet gateway as an internet route. It SHOULD get fresh internet gateway information.

- internet gateway's manet address (option)
  A manet address which can be used for internal communication with an internet gateway.

4.3. Messages

This specification defines three messages such as internet gateway solicitation, internet gateway advertisement and internet gateway

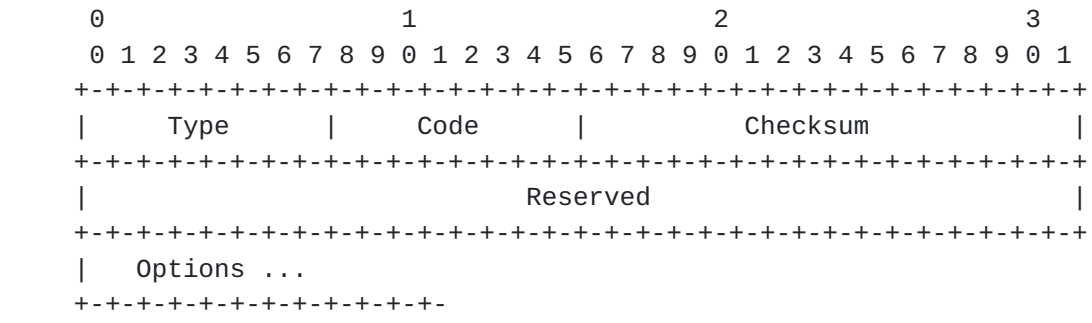
confirmation. Those messages are implemented in two ways: extension of NDP and extension of manet routing protocol's messages.

As we explained in [14], NDP messages such as a router solicitation, a router advertisement and a neighbor advertisement are not originally designed to route over multi-hop, because NDP [9] is operated between on-link nodes and routers. NDP assumes to use link-local scoped addresses as the IPv6 destination and source address fields for router advertisement and router solicitation messages. Link-local address is not an appropriate address scope for multi-hop networks since IPv6 prohibits to forward packets sent to an address of link-local scope. For doing so, new NDP packets must be defined.

In this section, we introduce three new NDP messages named IGWSOL-N, IGWADV-N, IGWCON-N and examples of routing signaling modifications (IGWSOL-M, IGWADV-M, IGWCON-M).

4.3.1. IGWSOL-N

The IGWSOL-N is same as the Route Solicitation message of NDP except for the Type value.



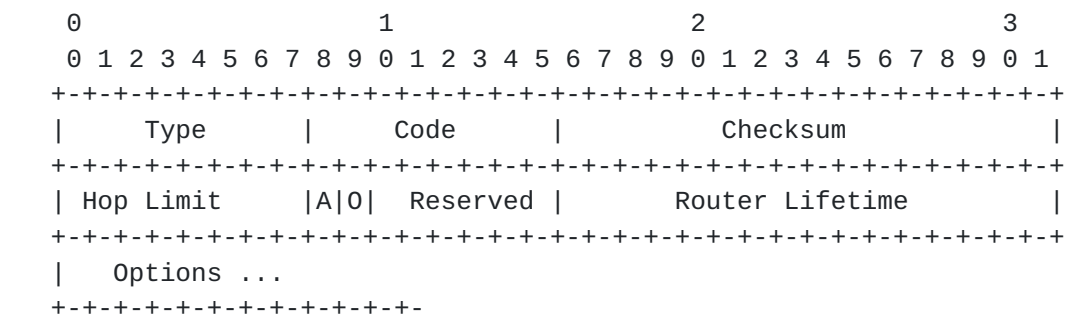
TYPE

TBA.

4.3.2. IGWADV-N

The IGWADV-N is similar to the Route Advertisement message of NDP. However, the internet gateways MUST NOT forward this message to internet nodes. The sender MUST include a Prefix Information option [9] with a globally routable prefix. The prefix information option is not modified for manet global connectivity. However, L flag must be unset and the Valid Lifetime field MUST be set to zero for the IGWADV-N, since on-link determination can not be used for manet. A Source Manet Address option may be required in order to

store a manet local address of the internet gateway, depending on the manet protocol.



TYPE
: TBA.

Code
: zero

Checksum
: The ICMP checksum.

Hop Limit
: The hop count between an Internet Gateway and a manet node.

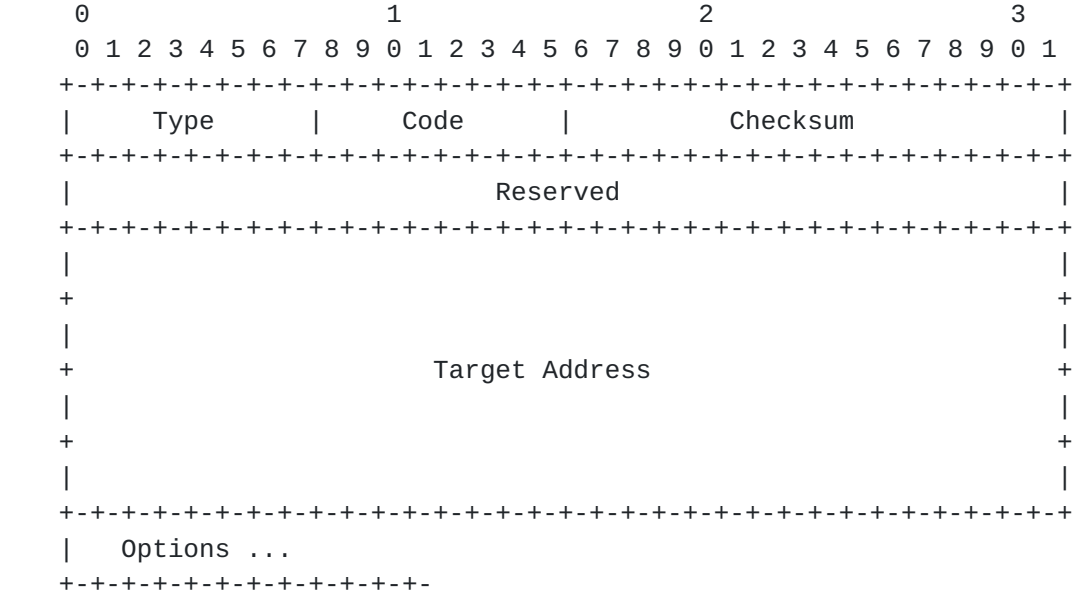
A
: 1-bit ``Acknowledgment'' flag. It requests Internet Gateway Confirmation to a manet node

O
: 1-bit ``Other stateful configuration'' flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information.

Router Lifetime
: 16-bit unsigned integer. The lifetime associated with the default router in units of seconds. The maximum value corresponds to 18.2 hours. A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the internet gateway list. The Router Lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options.

4.3.3. IGWCON-N

The IGWCON-N is sent only when an internet gateway requests acknowledgment (ex. Set A flag in IGWADV-N). This message is used to manage an associated manet node list on the internet gateway.



TYPE
: TBA

Code
: zero

Checksum
: The ICMP checksum.

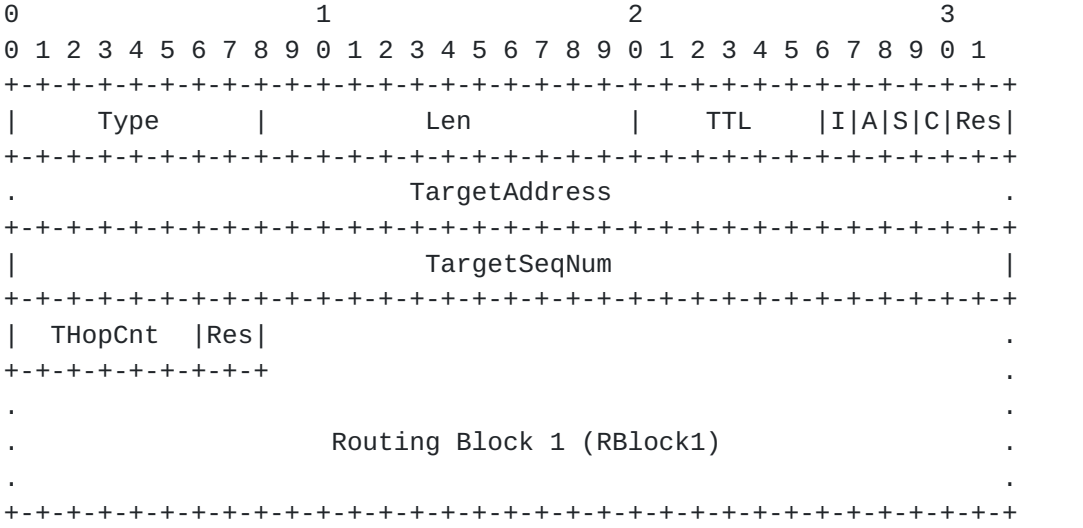
Reserved
: zero

Target Address
: The global address of the manet node. This target address will be stored in a associated manet node list of an internet gateway.

4.3.4. DYMO Modifications

DYMO has already specified a gateway concept in the specification [1]. The internet gateway lifetime can be retrieved from the route entry's lifetime for the internet gateway. We defined a new global connectivity block as shown in below. This global connectivity block is carried by RREP. We also introduces

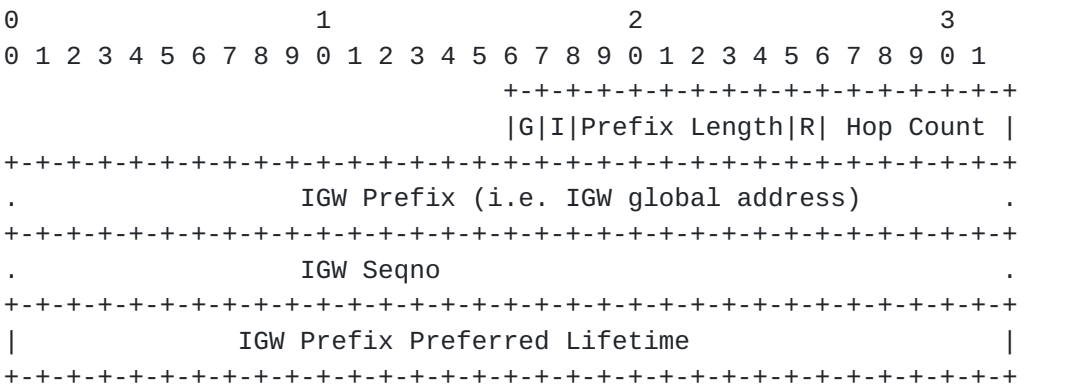
a new C flag in the ``Reserved'' field of Routing Element (RE) to indicate an internet gateway confirmation message. RREP can be recognized as the Internet Gateway Advertisement message, and RREQ is as the Internet Gateway Solicitation message. The Internet Gateway Confirmation message can be RREP with C flag set.



C

The C flag indicates requesting Internet Gateway Confirmation message. A manet node must include its new global address in a routing block and unicasts it to the particular internet gateway.

We also define a new DYMO Internet Gateway Prefix Block (IGWBlock) as follows.



I

The I flag indicates Internet Gateway Prefix Block (IGW block) for RE.

Prefix Length
: The length of IGW global Prefix

R
: 1 bit Reserved field

Hop Count
: Same as the Hop Count of Routing Block (RBlock)

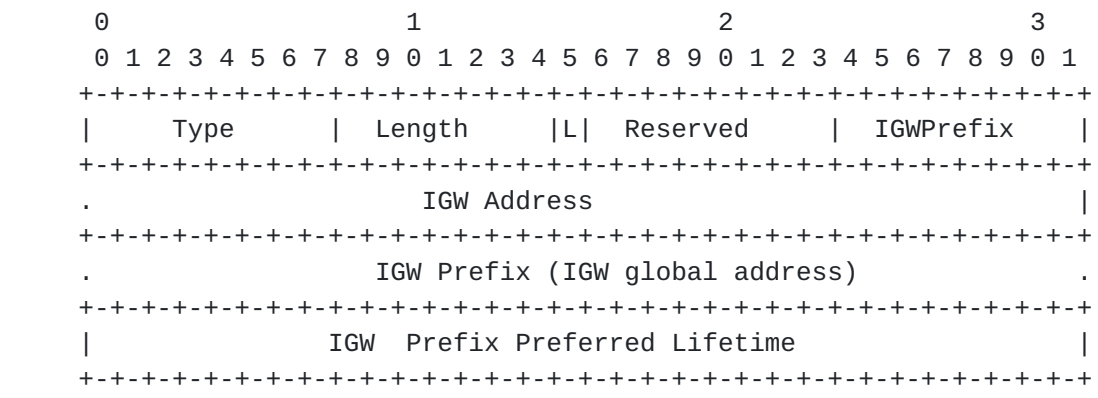
IGW Prefix
: The global address of the internet gateway

IGW Seqno
: The sequence number of the internet gateway

IGW Prefix Preferred Lifetime
: The preferred lifetime of the IGW Prefix.

4.3.5. OLSRv2 Modifications

For OLSRv2, we define a new message TLV for global connectivity as illustrated in below. The internet gateway lifetime is also retrieved from the route entry's lifetime for the internet gateway.



4.4. Changing the ICMPv6 Redirect

For global connectivity, an ICMPv6 Redirect message [9] is used by the internet gateway to notify a sending node that a destination is located on this manet and instead should send packets to it using ordinary manet routing. According to [9], a gateway MUST send an ICMPv6 Redirect messages from only link-local address. However, in manet situation, an internet gateway needs to send it from non link-local address due to multihop routing. Thus, we relax this limitation in this specification. An internet gateway can send the redirect message from either a manet local address or a global

address. In the target address field, the internet gateway SHOULD insert the wildcard IPv6 address (i.e. ::).

5. Manet Node Operation

For internet connectivity, each manet node needs to generate a global address and configure a route to the Internet.

5.1. Receiving Internet Gateway Advertisement

Two different messages are possible for internet gateway advertisement: IGWADV-N and IGWADV-M. When a manet node receives an internet gateway advertisement, it first verifies the message according to either the NDP specification [9] or each routing protocol specification. In addition to the verification, the manet node MUST conduct additional check as follows:

- The source address MUST be non link-local address. If the message is sent from a link-local address, the message MUST be silently discarded.

- The message MUST have a correct prefix information option. Otherwise, the message MUST silently be discarded. Each node MUST verify following items for the prefix information option.

  * The prefix address must be global routable prefix address

  * The prefix length must be valid length. (i.e. shorter than 128 and greater than 0).

  * Prefix Preferred Lifetime must be greater than zero.

  For the NDP based Intenet Gateway advertisement message (IGWADV-N), the following checks is required.

  * The Valid Lifetime MUST be set to zero

  * L flag MUST be unset and A flag MUST be set

After successful verifications, the manet node keeps the internet gateway information into the Internet Gateway List and Internet Gateway Prefix List as described in Section 4.1.

5.2. Address Autoconfiguration

After an internet gateway advertisement has been received from the internet gateway(s), a manet node SHOULD generate a global address by using the internet gateway information. The node SHOULD use its EUI-64 in order to construct a valid address with the

acquired prefix. The address generation is same as NDP Address Autoconfiguration [13] except for DAD. DAD operation is out of scope.

5.3. Default Route Setup

The manet node SHOULD set a route toward the Internet in the routing table. An ``example'' of a routing table is as follows:

```
     Destination/prefix length    Next-Hop
     -------------------------   ----------------------------
 Internet Route *
     default (::) **               <internet gateway address-A>
     default (::)                  <internet gateway address-B>
        :                                  :

 Host Route/128 ***
    <internet gateway address>    <next-hop address>
```

How to implement to hold a default route is up to manet routing protocols, implementations and operating systems. Some operating system (ex. Linux) are capable to keep multiple default routes and some (ex. BSD) are not supporting multiple routes for the same destination. It is possible to extend the BSD to hold multiple entries for a same destination.

Even if a node does not hold multiple internet gateways in a routing table, it can still keep these information in the internet gateway list. Thus it can refer the internet gateway list whenever it loses reachability to the default route which is set in a routing table.

These routing entries MUST be held until expiration of the prefix lifetime. The router lifetime of the default route entry and the global prefix information is the same with the prefix lifetime. During active lifetime, the receiving node can use the global prefix and the internet gateway as the default route entry. The default route does not function as the general default route for reactive route protocols, because the default route MUST be used with the mechanism described in Section 7.5 in addition to the general route lookup mechanism.

During active use of the internet gateway as a route path for communications, the manet node SHOULD update internet gateway information by receiving internet gateway advertisements. If necessary, the manet node can unicast an internet gateway solicitation to the respective internet gateway, or alternatively it can broadcast an internet gateway solicitation to all over the manet again. The former method can allow the manet node to update the current internet gateway status, while the latter method enables the

manet node to quickly discover all possible internet gateways in the manet.

5.4. Source Address Selection

Each manet node carefully selects a source address for outgoing communication. For communication, the manet node MUST NOT use its link-local address. The following decision MUST be made before sending packets.

- If a destination is an internet node, it MUST use its global address. The global address can be home address.

- If a destination is a manet node located within the manet, it SHOULD use it manet-local address. However the manet node MAY use its global address.

5.5. Receiving ICMPv6 Error Messages

If a manet node receives an ICMPv6 Destination Unreachable message after sending data packets along a manet route, the node MUST delete the manet route from the routing table. On the other hand, if the manet node uses an internet route, it SHOULD NOT delete the internet route. But it SHOULD stop sending packets to the destination. The node, then, MAY re-discover the destination by routing requests if necessary. Unless the node finds the destination node, it must give up communicating with the destination for a while.

If the manet node receives an ICMPv6 Redirect message from an internet gateway, the manet node SHOULD use the host route instead of the default route. Getting the host route, the manet node uses its method of learning a manet destination, e.g., by sending a route requests for the destination.

5.6. Interaction with Mobility Protocols

If a global address is more permanent one on a manet node, it can be used as a Mobile IPv6 [8] home address, to provide an always-on reachability from the fixed Internet with a statically known address. In such a case, reachability can be provided even when the node moves between manets and different points of the fixed network. A mobile node should use Mobile IPv6 when it is not on its home link. When arriving at a visited link in the fixed network, it will receive router advertisements to detect movement. If it is not at home, it registers with its home agent using a globally routable address from the visited network. In manet, Mobile IPv6 uses the internet gateway

advertisement to detect node's movement and to generate a globally routable address (i.e. Care-of address). The same mechanism can be applied to the NEMO Basic Support protocol [6].

The mobile node uses the globally routable address acquired from the internet gateway as its care-of-address when possibly performing a home registration. If no home registration is needed, the mobile node is at home in the manet and the prefix of its home address belongs to its internet gateway. If the mobile node starts Return Routability procedure for route optimization, HoTI and CoTI are sent through its internet gateway and HoT and CoT are returned to the mobile node via the internet gateway. There is no special operation for Return Routability on manet.

All manet nodes SHOULD support Mobile IPv6 Correspondent Node (CN) requirements describe in [8], so that they understand the home address option. Manet nodes using Mobile IPv6 with global connectivity support whatever Mobile IPv6 functionality they wish to use. Manet mobile nodes SHOULD NOT use home address options and CN binding updates when exchanging routing information with other nodes in the manet. This keeps control packets smaller and does not require manet nodes to support full CN functionality. A manet mobile node MAY insert a routing header to an outgoing data packet for explicit gateway routing in addition to the possible home address option. If the node is a CN, the possible routing header injected by Mobile IPv6 is modified by inserting the entry for gateway prior to the entry for home address, and setting the segments left to two.

6. Reactive Manet Node Operation

This section introduces additional operations for manet nodes running reactive manet routing protocols.

6.1. Soliciting Internet Gateway Advertisement (Optional)

A manet node sends an internet gateway solicitation in order to prompt an internet gateway(s) to generate internet gateway advertisements.

The following steps are required for sending the internet gateway solicitation.

- The source address of the message MUST NOT be a link local address. The IPv6 address used during any of these operations could be any routable address, for example a Mobile IPv6 home address. If no such address is available, the node SHOULD allocate a temporary global-scope address, generated from the well-known MANET_INITIAL_PREFIX [12]. This temporary address (MANET_TEMPORARY_ADDRESS) should be deallocated after obtaining the globally routable IPv6 address from an internet gateway.

- The manet node unicasts the router solicitation to an internet gateway if it has already known the address of the internet gateway. Otherwise, it floods the message to a new all internet gateway multicast address (i.e. ALL_MANET_GW_MULTICAST).

- The Hop Limit field in the IPv6 header SHOULD be set to an appropriate value. This can be the default constant usually inserted when unicasting packets, or chosen e.g., according to broadcasting/flooding scheme such as an expanding ring search technique.

6.2. Route Selection for Reactive Protocols

In reactive manets, a manet node and an internet gateways do not know the complete topology of the manet which they belong to. They MUST discover a host route for a destination as soon as they start to communicate. Therefore, whenever a node needs to send a packet it uses the following routing algorithm:

- The node looks up its routing table for the destination node. If it found the discovered route, it sends the packet towards the destination. The internet route SHOULD NOT be selected as a route for the destination at this point.

- If not, the node MAY request a route for the destination node.

    1. If an internet route exists, the node MAY wait for the above route request.

    2. If an internet route does not exist, the manet node obtains a default route.

    3. If the manet node does not get any route, the node sets an route entry into the routing table with the destination node pointing towards the internet route. Then the manet node uses the route to transmit the packet through the internet route.

- If the manet node gets a route for the destination, it sets a host route for the destination, and sends packets according to this route (not the internet route).

The node SHOULD know whether a route request was earlier sent for a destination whose route lookup found the default route. To prevent repeated route requests for packets destined to the destination, the node MUST put a route entry for the destination with the internet route as a next hop of the destination node . An ``example'' routing table of the node SHOULD be configured for the destination as shown below. As explained in Section 5.2, how to implement to hold these routes is up to manet routing protocols, implementations and operating systems.

Destination/prefix length	Next-Hop
Internet Route	
:: (default)	<internet gateway address>
Host Route/128	
<internet gateway address>	<next-hop address>
<Destination address>	<internet gateway address>

If the protocol allows, the node SHOULD send at least one request for a route of such a destination before sending data packets, even if it has already had a default route in its routing table. If the routing protocol is using an expanding ring search, care should be taken so as not to let this affect the delay too much. If the ring is expanded too far, unnecessary delay is introduced. Simulations have shown that one route request is optimal in most cases.

If the node gets a route for such a destination, the node assumes the destination node is located within manet, sets a host route for the destination, and sends packets normally according to this host route.

6.3. Use of Routing Header

A manet node sends data along an internet route when a destination is an internet node. The node has different way to transmit packets through an internet gateway.

- Without IPv6 routing extension header
  The manet node sends the packet to an IP address of an internet node and relies upon next hop routing in the other nodes.

- With IPv6 routing extension header
  The manet node uses the internet gateway address in the destination address of the IPv6 header and the real destination address in the routing header.

When a reactive manet routing protocol is used, each node may know only partial topology or link. In such case, if a packet meant for an internet node is sent without a routing header, each intermediate node will try to discover a manet route due to absence of the routing entry for the destination address. For example, table driven routing protocol such as AODV may have this problem. Intermediate nodes of a manet route only knows information of manet nodes on its routing table. Intermediate nodes do not know that whether the destination address is located on the Internet until route discovery for the destination address is completed. In addition, we can not assume that all manet nodes inside a manet acquire an internet route. If an intermediate node who does not have an internet route receives a packet meant for an internet node, it will not be able to route the packets. Therefore, if the packet is sent with a routing header, the destination address of the packet is the internet gateway while it is routed within the manet. Therefore, the intermediate node can route the packet to the internet gateway without generating additional route discovery and even without an internet route.

Assume the destination is located inside the manet but the sender can not reach the destination via a host route. Such the case can be occurred when reactive manet routing protocol is used. If the manet node sends packets to the destination via the internet gateway without a routing header, an intermediate node who has a host route for the destination will route packets to it directly, but the sender node is not aware of this. The sender is never notified that packets is not passing through the internet gateway. If the sender always uses a routing header, every packet is explicitly routed through the internet gateway. If the internet gateway detects that the destination is located within the manet, the internet gateway can send an ICMPv6 Redirect error message to the sender. After receiving the ICMPv6 Redirect messages, the manet node can re-discover a manet route for the destination.

Using a routing header is preferable when there are more than two internet gateways, because the node then have the ability to decide which internet gateway is the best, by distance in hops, or by some other priority. By assign a priority number for each internet gateway, the route reply message and the manet router advertisement messages could be extended to support a candidate internet gateway option in it.

7. Internet Gateway Operation

This section describes required operation for internet gateways.

7.1. Joining a Mobile Ad-hoc Routing Domain

An internet gateway joins a mobile ad-hoc network with a manet interface while it maintains the Internet connectivity with other interfaces.

The internet gateway requires to listen routing messages in order to collect routing information. However, it should not involve local manet routing with its manet interface so that route examination becomes much easier as described in Section 7.5.

The internet gateway SHOULD NOT become an intermediate node of a manet route. To achieve this, the internet gateway SHOULD NOT forward the flooded packets to its neighbors of the manet interface. For example, in AODV, the internet gateway SHOULD NOT propagate a RREQ message even if it receives the RREQ from neighbors. In OLSR, the internet gateway SHOULD NOT generate TC message. It can be done with the Willingness configuration set to NEVER.

7.2. Sending Internet Gateway Advertisement

An internet gateway sends out an internet gateway advertisement either periodically or response to an internet gateway solicitation. The internet gateway allows to send unsolicited internet gateway advertisements, although sending them periodically would generate unnecessary packets in the Manet.

When an IGWADV-N is used, it MUST carry a Prefix Information Option [9, 8]. The internet gateway contains its global prefix in the prefix information option. The source address of the IGWADV-N must be a global address of the internet gateway and MUST NOT use its link-local address.

Although the NDP specification requires to set 255 to a hop limit field, the Hop Limit field in the IPv6 header SHOULD be set to an appropriate value in a MANET. The internet gateway can either flood or unicast the internet gateway advertisement. An internet gateway SHOULD use optimized flooding mechanism such as the expanding ring search and multipoint relay flooding.

When the internet gateway uses IGWADV-M, it must follow the specifications of each manet protocols.

7.3. Receiving Internet Gateway Solicitation

When an internet gateway receives an internet gateway solicitation, it MUST unicast an internet gateway advertisement back to the originator of the solicitation.

When it receives an IGWSOL-N, the internet gateway must operate following verifications in addition to the verification specified in [9].

- If the source address is link local address, it SHOULD drop the IGWSOL-N.

- If the hop limit field of the IGWSOL-N is equal to zero, the message MUST silently be discarded.

After successful verification, the internet gateway keeps the originator's global address in its global manet node lists with INITIAL_GLOBAL_LIFE_TIME. It also unicasts back a IGWADV-N as described in Section 7.2.

When a IGWSOL-M is received, the internet gateway must verify the packet and returns IGWADV-M if necessary.

7.4. Management of Manet Nodes on Internet Gateway

An internet gateway SHOULD manage an associated manet node list for all the manet nodes which acquire a global address from the internet gateway. This knowledge is used when internet gateway determines a route for incoming packets described in section 7.5. It is recommended that the internet gateway supports this feature specially when reactive manet protocol is used.

When using proactive manet protocols, an internet gateway can see entire topology of all the manet nodes. Therefore, the internet gateway can know whether a node locates inside manet or not, as soon as it checks its topology map. On the other hand, most of reactive manet protocols only maintain partial topology of manet nodes. Each manet node MUST contact to the internet gateway at least once it establishes an internet route with the internet gateway. During this operation, the internet gateway records the manet node's addresses into a routing table and SHOULD mark as a manet node who has global address. This approach can be applied to most of reactive manet protocol, but any mechanism can be selected to know all manet nodes information.

To acquire a global address of each manet node, an internet gateway confirmation message can be used. After address autoconfiguration

on each manet node, the manet node notifies its global address by sending the internet gateway confirmation message. The internet gateway ask a manet node to send a internet gateway confirmation message by setting a flag in an internet gateway advertisement message. The internet gateway confirmation message will be unicasted to an internet gateway which a manet node receives the internet gateway information.

When there are multiple internet gateways, the associated manet node list SHOULD be exchanged among internet gateways. This exchange can be done in several way (ex. running routing protocol between internet gateways, if internet gateways are connected each other by wired link)

7.5. Route Examination

When an internet gateway forwards a packet from a manet to the Internet , it must examine the packet's source address. This examination prevents leaking unnecessary packets to the Internet.

This examination is based on the following steps.

1. The internet gateway first checks the destination address with its global prefix. If the prefix of the destination address is matched with the global prefix, the internet gateway MUST NOT forward the packet to the Internet. It returns the packet back to the manet if it has a manet route for the destination. If the internet gateway does not have a manet route, it just discards the packet and returns an ICMP Unreachable message to the sender.

2. If the prefix of the destination address is not matched with the global prefix, the internet gateway carefully examines the route for the destination.

   - If the internet gateway can not be an intermediate node of manet routes as shown in Section 7.4, goes to Step-3 below.

   - If the internet gateway can be an intermediate node and knows full topology of the manet , it searches its routing table for a manet route of the destination. If the route is found, it routes the packet back to the manet. The internet gateway SHOULD generate an ICMP6 Redirect Message to the source node.

   - On the other hand, if the internet gateway can be an intermediate node and does not have full topology, it compares the destination address with manet nodes' global addresses maintained in the associated manet node list. If there is a manet route, it SHOULD route the packet along the

manet route. The internet gateway SHOULD generate an ICMP6 Redirect Message to the source node.

3. The internet gateway compares the source address with its global prefix. If the prefix part is not matched, this packet is sent from non-routable address in this manet. Thus, the packet MUST NOT be routed to the Internet. If there is no manet route for the destination, the packet MUST be silently discarded. The internet gateway SHOULD return an ICMP6 Parameter Problem message to the source node.

4. Otherwise, it can forward the packet to the Internet.

Note that ICMP error messages are subject to rate limiting in the same manner as is done for ICMPv6 messages [4].

8. Protocol Constants

Parameter Name	Value
ALL_MANET_GW_MULTICAST	TBD (ff1e::xx/64 global-scope)

9. Security Considerations

This document does not define any method for secure operation of the protocol. There is no widely accepted model for securing state-altering protocols in manet. A reason for this is the lack of scalability in security association setup among manet nodes arriving from arbitrary domains. Before well accepted SA setup methods exist, any node can pretend to be an internet gateway and result in other nodes setting their routing state in a way denying proper operation of this service.

Acknowledgments

The authors would like to thank Elizabeth Royer for her comments on streamlining some aspects of the design. The authors thank Thierry Ernst and Fred Templin for his comments. The authors thank Thomas Clausen for his many improvements having to do with proactive routing protocols. The authors also thank Alex Hamidian for his contributions and improvements to section 7.2.

References

[1] I. Chakeres, E. Belding-Royer, and C. Perkins. Dynamic MANET On-demand (DYMO) Routing (work in progress). Internet Draft, Internet Engineering Task Force, October 2005.

[2] T. Clausen. The optimized link-state routing protocol version 2 (work in progress). Internet Draft, Internet Engineering Task Force, August 2005.

[3] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol OLSR. Request for Comments (Experimental) 3561, Internet Engineering Task Force, October 2003.

[4] A. Conta and S. Deering. Internet Control Message Protocol (ICMPv6) for the Internet protocol version 6 (ipv6) specification. Request for Comments (Draft Standard) 2463, Internet Engineering Task Force, December 1998.

[5] S. Deering and R. Hinden. Internet Protocol, Version 6 (ipv6) Specification. Request for Comments (Proposed Standard) 1883, Internet Engineering Task Force, December 1995.

[6] V. Devaraplli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol (proposed standard). Request for Comments 3963, Internet Engineering Task Force, January 2005.

[7] D. Johnson, D. Maltz, and Y. C. Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) (work in progress, draft-ietf-manet-dsr-09.txt). Internet Draft, Internet Engineering Task Force, April 2003.

[8] D. Johnson, C. Perkins, and J. Arkko. Mobility support in IPv6. Request for Comments (Proposed Standard) 3775, Internet Engineering Task Force, June 2004.

[9] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (ipv6). Request for Comments (Draft Standard) 2461, Internet Engineering Task Force, December 1998.

[10] R. Ogier, , F. Templin, and M. Lewis. Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). Request for Comments (Experimental) 3684, Internet Engineering Task Force, February 2004.

[11] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Request for Comments (Experimental) 3561, Internet Engineering Task Force, July 2003.

[12] C. Perkins, J. Malinen, R. Wakikawa, E. Royer, and Y. Sun. IP address Autoconfiguration for Ad hoc Networks (expired, draft-ietf-manet-autoconf-01.txt). Internet Draft, Internet Engineering Task Force, November 2001.

[13] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. Request for Comments (Draft Standard) 2462, Internet Engineering Task Force, December 1998.

[14] R. Wakikawa, A. Tuimonen, and T. Clausen. Ipv6 support on mobile ad-hoc network (work in progress, draft-wakikawa-manet-ipv6-00.txt). Internet Draft, Internet Engineering Task Force, February 2005.

Authors' Addresses

Ryuji Wakikawa
Dept. of
Environmental Information
Keio University
5322 Endo Fujisawa Kanagawa
252 JAPAN
EMail: ryuji@sfc.wide.ad.jp
Phone: +81-466 49-1394
Fax: +81 466 49-1395

Charles Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California
94043 USA
EMail: charliep@iprg.nokia.com
Phone: +1-650 625-2986
Fax: +1 650 625-2502

Jari T. Malinen
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California
94043 USA
EMail: Jari.T.Malinen@nokia.com
Phone: +1-650 625-2355
Fax: +1 650 625-2502

Anders Nilsson
Dept. of Communication Systems
Lund Institute of Technology
Box 118
SE-221 00 Lund
Sweden
E: andersn@telecom.lth.se
Phone: +46 46-39 72 92
Fax: +46 46-14 58 23

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgement

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