Mobile Ad hoc Networks Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 9, 2009

I. Chakeres
CenGen
C. Perkins
WiChorus
March 8, 2009

Dynamic MANET On-demand (DYMO) Routing
draft-ietf-manet-dymo-17

Status of this Memo

Copyright Notice

Abstract

The Dynamic MANET On-demand (DYMO) routing protocol is intended for use by mobile routers in wireless, multihop networks. DYMO

determines unicast routes among DYMO routers within the network in an on-demand fashion, offering improved convergence in dynamic topologies.

Table of Contents

1. Overview

The Dynamic MANET On-demand (DYMO) routing protocol enables reactive, multihop unicast routing among participating DYMO routers. The basic operations of the DYMO protocol are route discovery and route maintenance.

During route discovery, the originator's DYMO router initiates dissemination of a Route Request (RREQ) throughout the network to find a route to the target's DYMO router. During this hop-by-hop dissemination process, each intermediate DYMO router records a route to the originator. When the target's DYMO router receives the RREQ, it responds with a Route Reply (RREP) sent hop-by-hop toward the originator. Each intermediate DYMO router that receives the RREP creates a route to the target, and then the RREP is unicast hop-by-hop toward the originator. When the originator's DYMO router receives the RREP, routes have then been established between the originating DYMO router and the target DYMO router in both directions.

Route maintenance consists of two operations. In order to preserve routes in use, DYMO routers extend route lifetimes upon successfully forwarding a packet. In order to react to changes in the network topology, DYMO routers monitor routers over which traffic is flowing. When a data packet is received for forwarding and a route for the destination is not known or the route is broken, then the DYMO router of source of the packet is notified. A Route Error (RERR) is sent toward the packet source to indicate the route to that particular destination is invalid or missing. When the source's DYMO router

receives the RERR, it deletes the route. If the source's DYMO router later receives a packet for forwarding to the same destination, it will need to perform route discovery again for that destination.

DYMO uses sequence numbers to ensure loop freedom [Perkins99]. Sequence numbers enable DYMO routers to determine the temporal order of DYMO route discovery messages, thereby avoiding use of stale routing information.

2. Applicability Statement

The DYMO routing protocol is designed for stub or disconnected mobile ad hoc networks (MANETs). DYMO handles a wide variety of mobility patterns by dynamically determining routes on-demand. DYMO also handles a wide variety of traffic patterns. In networks with a large number of routers, DYMO is best suited for sparse traffic scenarios where routers forward packets to with only a small portion of the other DYMO routers, due to the reactive nature of route discovery and

route maintenance.

DYMO is applicable to memory constrained devices, since very little routing state is maintained in each DYMO router. Only routing information related to active sources and destinations is maintained, in contrast to most other more proactive routing protocols that require routing information to all routers within the routing region be maintained.

DYMO supports routers with multiple interfaces participating in the MANET. DYMO routers can also perform routing on behalf of other nodes, attached via participating or non-participating interfaces.

DYMO routers perform route discovery to find a route to a particular destination. Therefore, DYMO routers MUST be configured to initiate route discovery on behalf of certain sources and find routes to certain destinations. When DYMO is the only protocol interacting with the forwarding table, DYMO MAY be configured to perform route discovery for all unknown unicast destinations.

DYMO MUST only utilizes bidirectional links. In the case of possible unidirectional links, either blacklists (see Section 7.2) or other

means (e.g. adjacency establishment with only neighboring routers that have bidirectional communication as indicated by NHDP [I-D.ietf-manet-nhdp]) of ensuring bi-directionality should be used. Otherwise, persistent packet loss may occur.

The routing algorithm in DYMO may be operated at layers other than the network layer, using layer-appropriate addresses. For operation at other layers DYMO's routing algorithm likely will not need to change. Although, modification of the packet/message format may be required.

3. 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 [RFC2119].

Additionally, this document uses some terminology from [I-D.ietf-manet-packetbb].

This document defines the following terminology:

Adjacency
: A relationship formed between selected bi-directional neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers become adjacent. Neighboring routers may form an adjacency based several different pieces of information or protocols; for example, exchange of DYMO routing messages, other protocols (e.g. NDP [RFC4861] or NHDP [I-D.ietf-manet-nhdp]), or manual configuration.

Distance (Dist)
: A metric of the distance a message or piece of information has traversed. The minimum value of distance is the number of IP hops traversed. The maximum value is 65,535.

DYMO Identifier (DID)

A DID is maintained by each DYMO routing protocol instance (ThisNode.DID), and the default value is zero (0). Each routing message is tagged with its associated DID (MsgTLV.DID), unless zero (0). Upon receipt of DYMO protocol message a DYMO routing protocol instance SHOULD only process messages with a matching DID value.

DYMO Sequence Number (SeqNum)
A DYMO Sequence Number is maintained by each DYMO router. This sequence number is used by other DYMO routers to identify the temporal order of routing information generated and ensure loop-free routes.

Forwarding Route
A route that is used to forward data packets. Forwarding routes are generally maintained in a forwarding information base (FIB) or the kernel forwarding/routing table.

Multihop-capable Unicast IP Address
A multihop-capable unicast IP address is a unicast IP address that when put into the IP.SoureAddress or IP.DestinationAddress field is scoped sufficiently to be forwarded by a router. For example, site-scoped or globally-scoped unicast IP addresses.

Originating Node (OrigNode)
The originating node is the source, its DYMO router creates a DYMO control message on its behalf in an effort to disseminate some routing information. The originating node is also referred to as a particular message's originator.

Route Error (RERR)
A RERR message is used indicate that a DYMO router does not have forwarding route to one or more particular addresses.

Route Reply (RREP)
A RREP message is used to disseminate routing information about the RREP OrigNode, to the RREP TargetNode and the DYMO routers between them.

Route Request (RREQ)
: A RREQ message is issued to discover a valid route to a particular destination address, called the RREQ TargetNode. When a DYMO router processes a RREQ, it learns routing information on how to reach the RREQ OrigNode.

Target Node (TargetNode)
: The TargetNode is the ultimate destination of a message.

This Node (ThisNode)
: ThisNode corresponds to the DYMO router currently performing a calculation or processing a message.

Type-Length-Value structure (TLV)
: A generic way to represent information, please see [I-D.ietf-manet-packetbb] for additional information.

Unreachable Node (UnreachableNode)
: An UnreachableNode is a node for which a forwarding route does not exist.

4. Data Structures

4.1. Route Table Entry

The route table entry is a conceptual data structure. Implementations may use any internal representation that conforms to the semantics of a route as specified in this document.

Conceptually, a route table entry has the following fields:

Route.Address
: The IP (host or network) destination address of the node(s) associated with the routing table entry.

Route.Prefix

Indicates that the associated address is a network address, rather than a host address. The value is the length of the netmask/ prefix.

Route.SeqNum
The DYMO SeqNum associated with this routing information.

Route.NextHopAddress
The IP address of the adjacent DYMO router on the path toward the Route.Address.

Route.NextHopInterface
The interface used to send packets toward the Route.Address.

Route.Forwarding
A flag indicating whether this Route can be used for forwarding data packets. This flag MAY be provided for management and monitoring.

Route.Broken
A flag indicating whether this Route is broken. This flag is set if the next-hop becomes unreachable or in response to processing a RERR (see Section 5.5.4).

The following field is optional:

Route.Dist
A metric indicating the distance traversed before reaching the Route.Address node.

Not including optional information may cause performance degradation, but it will not cause the protocol to operate incorrectly.

In addition to a route table data structure, each route table entry may have several timers associated with the information. These timers/timeouts are discussed in Section 5.2.3.

4.2. DYMO Messages

When describing DYMO protocol messages, it is necessary to refer to fields in several distinct parts of the overall packet. These locations include the IP or IPv6 header, the UDP header, and fields from [I-D.ietf-manet-packetbb]. This document uses the following notation conventions. Information found in the table.

Information Location	Notational Prefix
IP header	IP.
UDP header	UDP.
packetbb message header	MsgHdr.
packetbb message TLV	MsgTLV.
packetbb address blocks	AddBlk.
packetbb address block TLV	AddTLV.

Table 1

4.2.1. Generalized Packet and Message Structure

DYMO messages conform to the generalized packet and message format as described in [I-D.ietf-manet-packetbb]. Here is a brief description of the format. A packet is made up of messages. A message is made up of a message header, message TLV block, and zero or more address blocks. Each of the address blocks may also have an associated address TLV block.

All DYMO messages specified in this document are sent using UDP to the destination port MANET [I-D.ietf-manet-iana].

Most DYMO messages are sent with the IP destination address set to the link-local multicast address LL-MANET-ROUTERS [I-D.ietf-manet-iana] unless otherwise stated. Therefore, all DYMO routers SHOULD subscribe to LL-MANET-ROUTERS [I-D.ietf-manet-iana] for receiving control packets. Note that multicast packets may be sent via unicast. For example, this may occur for certain link-types (non broadcast mediums), improved robustness, or manually configured router adjacency.

Unicast DYMO messages (e.g. RREP) unless otherwise specified in this document are sent with the IP destination set to the Route.NextHopAddress of the route to the TargetNode.

The IPv4 TTL (IPv6 Hop Limit) field for all packets containing DYMO messages is set to 255. If a packet is received with a value other than 255, it is discarded. This mechanism helps to ensures packets have not passed through any intermediate routers, and it is known as GTSM [RFC5082].

The length of an IP address (32 bits for IPv4 and 128 bits for IPv6) inside a DYMO message depends on the IP packet header containing the

DYMO message/packet. For example, if the IP header uses IPv6 addresses then all addresses contained in the payload use IPv6

addresses of the same length. In the case of mixed IPv6 and IPv4 addresses, please use the methods specified in [I-D.ietf-manet-packetbb].

If a packet contains only a single DYMO message and no packet TLVs, it need not include a packet-header [I-D.ietf-manet-packetbb].

The aggregation of multiple messages into a packet is not specified in this document, but if aggregation does occur the IP.SourceAddress and IP.DestinationAddress of all contained messages MUST be the same.

Implementations MAY choose to temporarily delay transmission of messages for the purpose of aggregation (into a single packet) or to improve performance by using jitter [RFC5148].

DYMO control packets SHOULD be given priority queue and channel access.

4.2.2. Routing Messages (RM) - RREQ & RREP

Routing Messages (RMs) are used to disseminate routing information. There are two DYMO message types that are considered to be routing messages (RMs): RREQ and RREP. They contain very similar information and function, but have slightly different processing rules. The main difference between the two messages is that RREQ messages generally solicit a RREP, whereas a RREP is the response to RREQ.

RM creation and processing are described in Section 5.3.

A RM requires the following information:

IP.SourceAddress
: The IP address of the node currently sending this packet. This field is generally filled automatically by the operating system and should not require special handling.

IP.DestinationAddress
: The IP address of the packet destination. For multicast RREQ the IP.DestinationAddress is set to LL-MANET ROUTERS

[I-D.ietf-manet-iana]. For unicast RREQ and RREP the IP.DestinationAddress is set to the NextHopAddress toward the RREP TargetNode.

UDP.DestinationPort
By default, the UDP destination port is set to MANET [I-D.ietf-manet-iana].

MsgHdr.HopLimit
The remaining number of hops this message is allowed to traverse.

AddBlk.TargetNode.Address
The IP address of the message TargetNode. In a RREQ the TargetNode is the destination address for which route discovery is being performed. In a RREP the TargetNode is the RREQ OrigNode address. The TargetNode address is the first address in a routing message.

AddBlk.OrigNode.Address
The IP address of the originator and its associated prefix length. In a RREQ the OrigNode is the source's address and prefix. In a RREP the OrigNode is the RREQ TargetNode's address and prefix for which a RREP is being generated. This address is the second address in the message for RREQ.

OrigNode.AddTLV.SeqNum
The DYMO sequence number of the originator's DYMO router.

A RM may optionally include the following information:

TargetNode.AddTLV.SeqNum
The last known DYMO sequence number of the TargetNode.

TargetNode.AddTLV.Dist
The last known Distance to the TargetNode.

AddBlk.AdditionalNode.Address
The IP address of an additional node that can be reached via the DYMO router adding this information. Each AdditionalNode.Address MUST include its prefix. Each AdditionalNode.Address MUST also

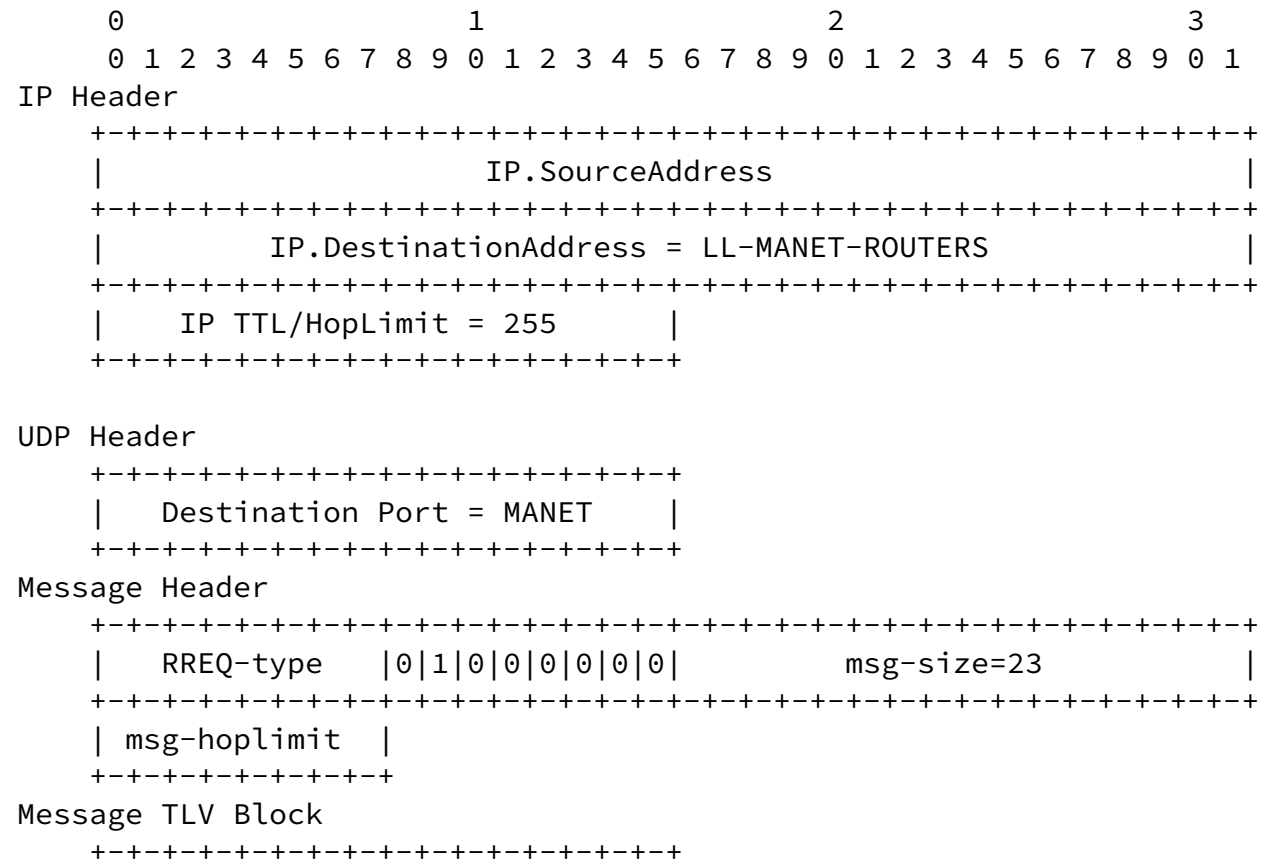
have an associated Node.SeqNum in the address TLV block.

AdditionalNode.AddTLV.SeqNum
The DYMO sequence number associated with this routing information.

OrigNode.AddTLV.Dist
A metric of the distance to reach the associated OrigNode.Address. This field is incremented by at least one at each intermediate DYMO router.

AdditionalNode.AddTLV.Dist
A metric of the distance to reach the associated AdditionalNode.Address. This field is incremented by at least one at each intermediate DYMO router.

Example IPv4 RREQ



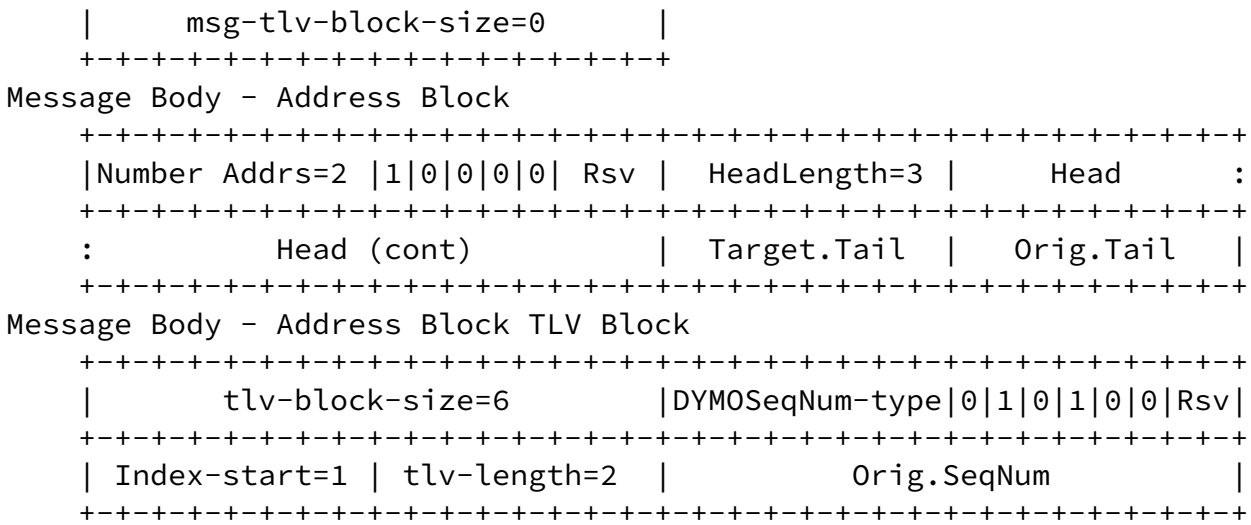


Figure 1

4.2.3. Route Error (RERR)

A RERR message is used to disseminate the information that a route is not available for one or more particular IP addresses.

RERR creation and processing are described in Section 5.5.

A RERR requires the following information:

IP.SourceAddress
: The IP address of the node currently sending this packet. This field is generally filled automatically by the operating system and should not require special handling.

IP.DestinationAddress
: For multicast RERR messages, The IP address is set to LL-MANET-ROUTERS [I-D.ietf-manet-iana]. For unicast RERR messages, The IP address is set to the NextHopAddress.

UDP.DestinationPort
: By default, the UDP destination port is set to MANET [I-D.ietf-manet-iana].

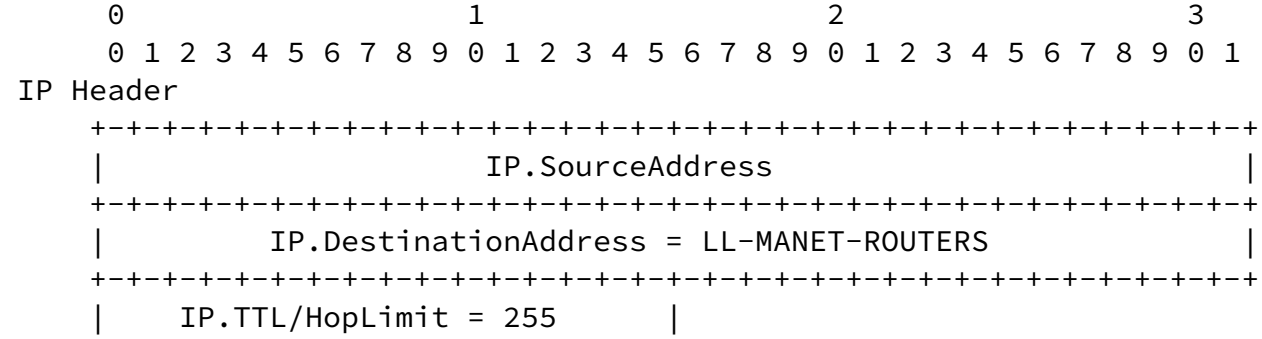
MsgHdr.HopLimit
: The remaining number of hops this message is allowed to traverse.

AddBlk.UnreachableNode.Address
   The IP address of an UnreachableNode and its associated prefix
   length. Multiple unreachable addresses may be included in a RERR.

A Route Error may optionally include the following information:

UnreachableNode.AddTLV.SeqNum
   The last known DYMO sequence number of the unreachable node. If a
   SeqNum for an address is not included, it is assumed to be
   unknown. This case occurs when a node receives a message to
   forward to a destination for which it does not have any
   information in its routing table.

Example IPv4 RERR



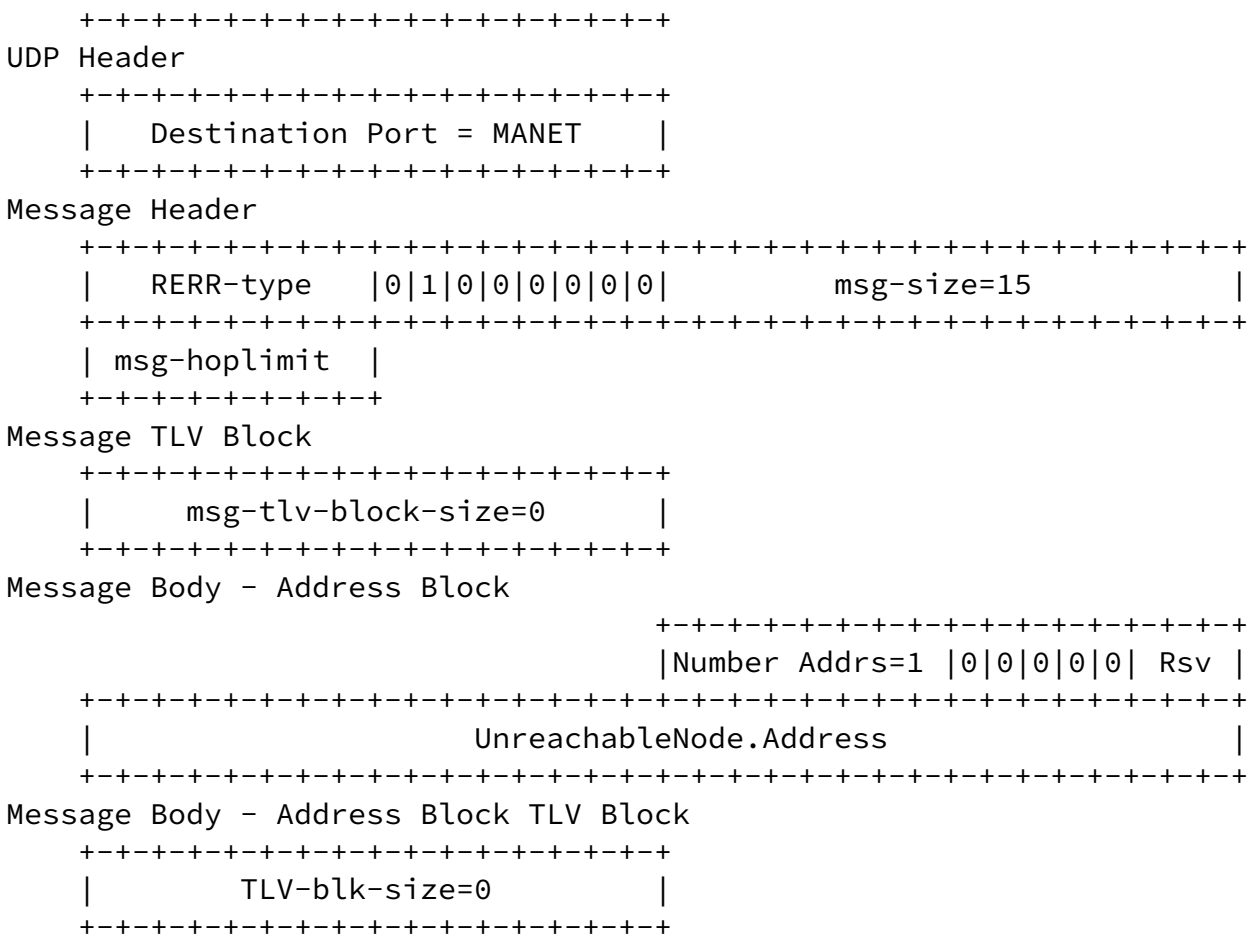


Figure 2

5. Detailed Operation

5.1. DYMO Sequence Numbers

DYMO sequence numbers allow nodes to judge the freshness of routing information and ensure loop freedom.

5.1.1. Maintaining A Node's Own Sequence Number

DYMO requires that each DYMO router in the network to maintain its own DYMO sequence number (OwnSeqNum), a 16-bit unsigned integer. The

circumstances for ThisNode to incrementing its OwnSeqNum are described in Section 5.3.

5.1.2. Numerical Operations on OwnSeqNum

When ThisNode increments its OwnSeqNum (as described in Section 5.3) it MUST do so by treating the sequence number value as an unsigned number.

5.1.3. OwnSeqNum Rollover

If the sequence number has been assigned to be the largest possible number representable as a 16-bit unsigned integer (i.e., 65,535), then the sequence number SHOULD be set to one (1) incremented.

5.1.4. Actions After OwnSeqNum Loss

A DYMO router SHOULD maintain its sequence number in persistent storage.

If a DYMO router's OwnSeqNum is lost, it MUST take certain actions to avoid creating routing loops. To prevent this possibility after OwnSeqNum loss a DYMO router MUST wait for at least ROUTE_DELETE_TIMEOUT before fully participating in the DYMO routing protocol. If a DYMO control message is received during this waiting period, the DYMO router SHOULD process it normally but MUST NOT transmit or retransmit any DYMO messages. If a data packet is received for forwarding to another destination during this waiting period, the DYMO router MUST generate a RERR message indicating that this route is not available and reset its waiting timeout. At the end of the waiting period the DYMO router sets its OwnSeqNum to one (1) and begins participating.

The longest a node need wait is ROUTE_SEQNUM_AGE_MAX_TIMEOUT. At the end of the maximum waiting period a node SHOULD set its OwnSeqNum to one (1) and begins participating.

5.2. DYMO Routing Table Operations

5.2.1. Judging Routing Information's Usefulness

Given a route table entry (Route.SeqNum, Route.Dist, and Route.Broken) and new incoming routing information for a particular node in a RM (Node.SeqNum, Node.Dist, and RM message type - RREQ/

RREP), the quality of the new routing information is evaluated to determine its usefulness. Incoming routing information is classified as follows:

1. Stale
   If Node.SeqNum - Route.SeqNum < 0 (using signed 16-bit arithmetic) the incoming information is stale. Using stale routing information is not allowed, since doing so might result in routing loops.

   ```
   (Node.SeqNum - Route.SeqNum < 0)
       using signed 16-bit arithmetic
   ```

2. Loop-possible
   If Node.SeqNum == Route.SeqNum the incoming information may cause loops if used; in this case additional information MUST be examined. If Route.Dist or Node.Dist is unknown or zero (0), then the routing information is loop-possible. If Node.Dist > Route.Dist + 1, then the routing information is loop-possible. Using loop-possible routing information is not allowed, otherwise routing loops may be formed.

   ```
   (Node.SeqNum == Route.SeqNum) AND
   ((Node.Dist is unknown) OR
    (Route.Dist is unknown) OR
    (Node.Dist > Route.Dist + 1))
   ```

3. Inferior
   In case of known equal SeqNum, the information is inferior in multiple cases: (case i) if Node.Dist == Route.Dist + 1 (it is a greater distance route) AND Route.Broken == false; (case ii) if Node.Dist == Route.Dist (equal distance route) AND Route.Broken == false AND this RM is a RREQ. The inferior condition stops forwarding of RREQ with equivalent distance.

   ```
   ((Node.SeqNum == Route.SeqNum) AND
    (((Node.Dist == Route.Dist + 1) AND (Route.Broken == false)) OR
     ((Node.Dist == Route.Dist) AND
      (RM is RREQ) AND (Route.Broken == false))))
   ```

4. Superior
   Incoming routing information that does not match any of the above criteria is loop-free and better than the information existing in the routing table. Information is always superior if Node.SeqNum - Route.SeqNum > 0 (using signed 16-bit arithmetic). In the case of equal sequence numbers, the information is superior in multiple cases: (case i) if Node.Dist < Route.Dist; (case ii) if Node.Dist

== Route.Dist + 1 AND Route.Broken == true (a broken route is

being repaired); (case iii) if Node.Dist == Route.Dist AND it is a RREP (RREP with equal distance are forwarded) OR Route.Broken == true (a broken route is being repaired). For completeness, we provide the following (optimized) pseudo-code.

```
(Node.SeqNum - Route.SeqNum > 0) OR
    using signed 16-bit arithmetic
((Node.SeqNum == Route.SeqNum) AND
 ((Node.Dist < Route.Dist) OR
  ((Node.Dist == Route.Dist + 1) AND (Route.Broken == true)) OR
  ((Node.Dist == Route.Dist) AND
   ((RM is RREP) OR (Route.Broken == true)))))
```

5.2.2. Creating or Updating a Route Table Entry with Received Superior Routing Information

The route table entry is populated with the following information:

1. the Route.Address is set to Node.Address,

2. the Route.Prefix is set to the Node.Prefix.

3. the Route.SeqNum is set to the Node.SeqNum,

4. the Route.NextHopAddress is set to the node that transmitted this DYMO RM packet (i.e., the IP.SourceAddress),

5. the Route.NextHopInterface is set to the interface that this DYMO packet was received on,

6. if known, the Route.Dist is set to the Node.Dist,

Fields without known values are not populated with any value.

Previous timers for this route table entry are removed. A timer for the minimum delete timeout (ROUTE_AGE_MIN) is set to ROUTE_AGE_MIN_TIMEOUT. A timer for the maximum delete timeout (ROUTE_SEQNUM_AGE_MAX). ROUTE_SEQNUM_AGE_MAX is set to Node.AddTLV.VALIDITY_TIME [I-D.ietf-manet-timetlv] if included; otherwise, ROUTE_SEQNUM_AGE_MAX is set to

ROUTE_SEQNUM_AGE_MAX_TIMEOUT. The usage of these timers and others are described in Section 5.2.3.

At this point, a forwarding route should be created and the Route.Forwarding flag set. Afterward, the route can be used to send any queued data packets and forward any incoming data packets for Route.Address. This route also fulfills any outstanding route discovery attempts for Node.Address.

5.2.3. Route Table Entry Timeouts

5.2.3.1. Minimum Delete Timeout (ROUTE_AGE_MIN)

When a DYMO router transmits a RM, other DYMO routers expect the transmitting DYMO router to have a forwarding route to the RM originator. After updating a route table entry, it should be maintained for at least ROUTE_AGE_MIN. Failure to maintain the information might result in lost messages/packets, or in the worst case scenario several duplicate messages.

After the ROUTE_AGE_MIN timeout a route can safely be deleted.

5.2.3.2. Maximum Sequence Number Delete Timeout (ROUTE_SEQNUM_AGE_MAX)

Sequence number information is time sensitive, and MUST be deleted after a time in order to ensure loop-free routing.

After the ROUTE_AGE_MAX timeout a route's sequence number information MUST be discarded.

5.2.3.3. Recently Used Timeout (ROUTE_USED)

When a route is used to forward data packets, this timer is set to expire after ROUTE_USED_TIMEOUT. This operation is also discussed in Section 5.5.2.

If a route has not been used recently, then a timer for ROUTE_DELETE is set to ROUTE_DELETE_TIMEOUT.

5.2.3.4. Delete Information Timeout (ROUTE_DELETE)

As time progresses the likelihood that old routing information is

useful decreases, especially if the network nodes are mobile. Therefore, old information should be deleted.

After the ROUTE_DELETE timeout, the routing table entry should be deleted. If a forwarding route exists, it should be removed and the Route.Forwarding flag unset.

5.3. Routing Messages

5.3.1. RREQ Creation

Before a DYMO router creates a RREQ it SHOULD increment its OwnSeqNum by one (1) according to the rules specified in Section 5.1.2. Incrementing OwnSeqNum will ensure that all nodes with existing routing information will consider this new information superior to

existing routing table information. If the sequence number is not incremented, certain DYMO routers might not consider this information superior, if they have existing better routing information already.

First, ThisNode adds the AddBlk.TargetNode.Address to the RREQ; the unicast IP Destination Address for which a forwarding route does not exist.

If a previous value of the TargetNode.SeqNum is known (from a routing table entry using longest-prefix matching), it SHOULD be placed in TargetNode.AddTLV.SeqNum in all but the last RREQ attempt. If a TargetNode.SeqNum is not included, it is assumed to be unknown by processing nodes. This operation ensures that no intermediate DYMO routers reply, and ensures that the TargetNode's DYMO router increments its sequence number.

Next, the node adds AddBlk.OrigNode.Address, its prefix, and the OrigNode.AddTLV.SeqNum (OwnSeqNum) to the RM.

The OrigNode.Address is the address of the source for which this DYMO router is initiating this route discovery. The OrigNode.Address MUST be a unicast IP address. This information will be used by nodes to create a route toward the OrigNode, enabling delivery of a RREP, and eventually used for proper forwarding of data packets.

If OrigNode.Dist is included it is set to a number greater than zero

(0).

The MsgHdr.HopLimit SHOULD be set to MSG_HOPLIMIT.

For RREQ, the MsgHdr.HopLimit MAY be set in accordance with an expanding ring search as described in [RFC3561] to limit the RREQ propagation to a subset of the local network and possibly reduce route discovery overhead.

The IP.DestinationAddress for multicast RREQ is set to LL-MANET-ROUTERS. The IP.DestinationAddress for unicast RREQ is set to the NextHopAddress.

Each DYMO routing protocol message SHOULD contain ThisNode.DID's value in a message TLV (MsgTLV.DID). If ThisNode.DID value is zero (0) it MAY be omitted.

5.3.2. RREP Creation

First, the AddBlk.TargetNode.Address is added to the RREP. The TargetNode is the ultimate destination of this RREP; the RREQ OrigNode.Address.

Next, AddBlk.OrigNode.Address and prefix are added to the RREP. The AddBlk.OrigNode.Address is the RREQ TargetNode.Address. The AddBlk.OrigNode.Address MUST be a unicast IP address. ThisNode SHOULD advertise the largest known prefix containing AddBlk.OrigNode.Address.

When the TargetNode's DYMO router creates a RREP, if the TargetNode.SeqNum was not included in the RREQ, ThisNode MUST increment its OwnSeqNum by one (1) according to the rules specified in Section 5.1.2.

If TargetNode.SeqNum is included in the RM and TargetNode.SeqNum - OwnSeqNum < 0 (using signed 16-bit arithmetic), OwnSeqNum SHOULD be incremented by one (1) according to the rules specified in Section 5.1.2.

If TargetNode.SeqNum is included in the RM and TargetNode.SeqNum == OwnSeqNum (using signed 16-bit arithmetic) and Dist will not be included in the RREP being generated, OwnSeqNum SHOULD be incremented

by one (1) according to the rules specified in Section 5.1.2.

If OwnSeqNum is not incremented the routing information might be considered stale. In this case, the RREP might not reach the RREP Target.

After any of the sequence number operations above, the RREP OrigNode.AddTLV.SeqNum (OwnSeqNum) MUST also added to the RREP.

Other AddTLVs in the RREP for the OrigNode and TargetNode SHOULD be included and set accordingly. If OrigNode.Dist is included it is set to a number greater than zero (0) and less than 65,535. The Distance value will influence judgment of the routing information (Section 5.2.1) against known information at other DYMO routers that process this RM.

The MsgHdr.HopLimit is set to MSG_HOPLIMIT.

The IP.DestinationAddress for RREP is set to the IP address of the Route.NextHopAddress for the route to the RREP TargetNode.

Each DYMO routing protocol message SHOULD contain ThisNode.DID's value in a message TLV (MsgTLV.DID). If ThisNode.DID value is zero (0) it MAY be omitted.

5.3.3. Intermediate DYMO Router RREP Creation

Sometimes a DYMO router other than the TargetNode's DYMO router (call it an "intermediate DYMO router") has routing information that can

satisfy an incoming RREQ. An intermediate DYMO router can issue a intermediate DYMO router RREP on behalf of the TargetNode's DYMO router.

Before creating a intermediate DYMO router RREP, OwnSeqNum SHOULD be incremented by one (1) according to the rules specified in Section 5.1.2.

If OwnSeqNum is not incremented the routing information about ThisNode might be considered stale by a processing DYMO router. In this case, the RREP would not reach the RREP TargetNode.

When an intermediate DYMO router originates a RREP in response to a RREQ on behalf of the TargetNode's DYMO router, it sends the RREP to the RREQ OrigNode with additional routing information (Address, Prefix, SeqNum, Dist, etc.) about the RREQ TargetNode. Appending additional routing information is described in Section 5.3.5.

The Intermediate DYMO router SHOULD also issue a RREP to the RREQ TargetNode, so that the RREQ TargetNode receives routing information on how to reach the RREQ OrigNode.

When an intermediate DYMO router creates this RREP, it sends a RREP to the RREQ TargetNode with additional routing information (Address, Prefix, SeqNum, Dist, etc.) about the RREQ OrigNode.

5.3.4. RM Processing

First, ThisNode decides whether to process this message. If the message contains a MsgTLV.DID it SHOULD match ThisNode.DID's value. If the message does not contain a MsgTLV.DID it is assumed to be zero (0) and SHOULD be discarded if ThisNode.DID's value is not zero (0).

Next, ThisNode MAY selectively process messages based upon information in the message. ThisNode SHOULD only process messages from adjacent DYMO routers. If ThisNode chooses not to process this message, the message is discarded and further processing stopped.

ThisNode checks if the AddBlk.OrigNode.Address is a valid multihop-capable (e.g. site or global scope) unicast IP address. If the address is not a valid unicast IP address, the messages is discarded and further processing stopped.

ThisNode also checks whether AddBlk.OrigNode.Address is an address handled by this DYMO router. If this node is the originating DYMO router, the RM is dropped.

ThisNode checks if the AddBlk.TargetNode.Address is a valid multihop-

capable unicast IP address. If the address is not a valid unicast IP address, the messages is discarded and further processing stopped.

Next, ThisNode checks whether its routing table has an entry to the AddBlk.OrigNode.Address using longest-prefix matching [RFC1812]. If

a route with a valid Route.SeqNum does not exist, then the new routing information is considered fresh and a new route table entry is created and updated as described in Section 5.2.2. If a route table entry does exists and it has a valid Route.SeqNum, the incoming routing information is compared with the route table entry following the procedure described in Section 5.2.1. If the incoming routing information is considered superior, the route table entry is updated as described in Section 5.2.2.

For each address (except the TargetNode) in the RM that includes AddTLV.Dist information, the AddTLV.Dist information MAY be incremented. The updated Distance value will influence judgment of the routing information (Section 5.2.1).

If the resulting Distance value for the OrigNode is greater than 65,535, the message is discarded. If the resulting Distance value for another node is greater than 65,535, the associated address and its information are removed from the RM.

After processing the OrigNode's routing information, then each address that is not the TargetNode should be considered for creating and updating routes. Creating and updating routes to other nodes can eliminate RREQ for those IP destinations, in the event that data needs to be forwarded to the IP destination(s) now or in the near future.

For each of the additional addresses considered, ThisNode first checks the that the address is a multihop-capable unicast IP address. If the address is not a unicast IP address, the address and all related information MUST be removed.

If the routing table does not have a matching route with a valid Route.SeqNum for this additional address using longest-prefix matching exists, then a route is created and updated as described in Section 5.2.2. If a route table entry exists with a valid Route.SeqNum, the incoming routing information is compared with the route table entry following the procedure described in Section 5.2.1. If the incoming routing information is considered superior, the route table entry is updated as described in Section 5.2.2.

If the routing information for an AdditionalNode.Address is not considered superior, then it is removed from the RM. Removing this information ensures that the information is not propagated.

At this point, if the routing information for the OrigNode was not superior then this RM SHOULD be discarded and no further processing of this message SHOULD be performed.

If the ThisNode is the DYMO router responsible for the TargetNode and this RM is a RREQ, then ThisNode responds with a RREP to the RREQ OrigNode (the new RREP's TargetNode). The procedure for issuing a new RREP is described in Section 5.3.2. At this point, ThisNode need not perform any more operations for this RM.

Alternatively, ThisNode MAY choose to distribute routing information about ThisNode (the RREQ TargetNode) more widely, ThisNode MAY optionally perform a route discovery; by issuing a RREQ with ThisNode listed as the TargetNode, using the procedure in Section 5.3.1. At this point, ThisNode need not perform any more operations for the original RM.

If ThisNode is not the TargetNode, this RM is a RREQ, the RREQ contains the TargetNode.AddTLV.SeqNum, and ThisNode has a forwarding route to the TargetNode with a SeqNum where Route.TargetNode.SeqNum - RREQ.TargetNode.AddTLV.SeqNum >= 0 (using signed 16-bit arithmetic); then this node MAY respond with an intermediate DYMO router RREP. The procedure for performing intermediate DYMO router RREP is described in Section 5.3.3. If an intermediate DYMO router RREP is sent, ThisNode need not perform any more operations for the original RM.

After processing a RM or creating a new RM, a node can append additional routing information to the RM, according to the procedure described in Section 5.3.5. The additional routing information can help reduce route discoveries at the expense of increased message size.

For each address (except the TargetNode) in the RM that includes AddTLV.Dist information, the AddTLV.Dist information is incremented by at least one (1). The updated Distance value will influence judgment of the routing information (Section 5.2.1) against known information at other DYMO routers that process this RM.

If the resulting Distance value for the OrigNode is greater than 65,535, the message is discarded. If the resulting Distance value for another node is greater than 65,535, the associated address and its information are removed from the RM.

Next, the MsgHdr.HopLimit is decremented by one (1). If this RM's MsgHdr.HopLimit is greater than or equal to one (1), ThisNode is not the TargetNode, AND this RM is a RREQ, then the current RM (altered by the procedure defined above) SHOULD be sent to the

IP.DestinationAddress LL-MANET-ROUTERS [I-D.ietf-manet-iana]. If the RREQ is unicast, the IP.DestinationAddress is set to the NextHopAddress.

If this RM's MsgHdr.HopLimit is greater than or equal to one (1), ThisNode is not the TargetNode, AND this RM is a RREP, then the current RM is sent to the Route.NextHopAddress for the RREP's TargetNode.Address. If no forwarding route exists to Target.Address, then a RERR SHOULD be issued to the OrigNode of the RREP.

By sending the updated RM ThisNode is advertising that it will provide routing for IP addresses contained in the outgoing RM based on the information enclosed. ThisNode MAY choose not to send the RM, though not resending this RM could decrease connectivity in the network or result in a non-shortest distance path.

Some examples of why ThisNode might choose to not re-issue a RM are: if ThisNode does not want to advertise routing for the contained IP addresses because it is already heavily loaded; if ThisNode has already issued nearly identical routing information (e.g. ThisNode had recently issued a RM with nearly the same distance); or if ThisNode is low on energy and does not want to expend energy for control message sending or packet forwarding. This type of advanced behavior is not defined in this specification.

5.3.5. Adding Additional Routing Information to a RM

Appending routing information can alleviate route discovery attempts to the nodes whose information is included, if other DYMO routers use this information to update their routing tables.

DYMO routers can append routing information to a RM. This option should be administratively configurable or intelligently controlled.o

Prior to appending an address controlled by this DYMO router to a RM, ThisNode MAY increment its OwnSeqNum as defined in Section 5.1.2. If OwnSeqNum is not incremented the appended routing information might not be considered superior, when received by nodes with existing routing information. Incrementation of the sequence number when appending information to an RM in transit should be administratively configurable or intelligently controlled.

If an address controlled by this DYMO router includes ThisNode.Dist, it is set to a number greater than zero (0).

For added addresses (and their prefixes) not controlled by this DYMO router, Route.Dist can be included if known. If Route.Dist is not known, it MUST NOT be included.

MaxAge information about the appended address(es) MUST be included.

Additional information (e.g. SeqNum and Dist) about any appended address(es) SHOULD be included.

Note that, the routing information about the TargetNode MUST NOT be added. Also, duplicate address entries SHOULD NOT be added. Instead, only the best routing information (Section 5.2.1) for a particular address SHOULD be included.

5.4. Route Discovery

When a source's DYMO router needs to forward a data packet on behalf of an attached node and it does not have a forwarding route to the data packet's unicast IP destination address, ThisNode sends a RREQ (described in Section 5.3.1) to discover a route to the particular destination (TargetNode).

After issuing a RREQ, the OrigNode DYMO router waits for a route to be created to the TargetNode. If a route is not created within RREQ_WAIT_TIME, ThisNode may again try to discover a route by issuing another RREQ using the procedure defined in Section 5.3.1 again.

To reduce congestion in a network, repeated attempts at route discovery for a particular TargetNode SHOULD utilize an exponential backoff.

For example, the first time a DYMO router issues a RREQ, it waits RREQ_WAIT_TIME for a route to the TargetNode. If a route is not found within that time, the DYMO router MAY send another RREQ. If a route is not found within two (2) times the current waiting time, another RREQ may be sent, up to a total of RREQ_TRIES. For each additional attempt, the waiting time for the previous RREQ is multiplied by two (2) so that the waiting time conforms to a binary exponential backoff.

Data packets awaiting a route SHOULD be buffered by the source's DYMO router. This buffer SHOULD have a fixed limited size (BUFFER_SIZE_PACKETS or BUFFER_SIZE_BYTES) and older data packets SHOULD be discarded first.

Buffering of data packets can have both positive and negative effects, and therefore buffer settings SHOULD be administratively configurable or intelligently controlled.

If a route discovery has been attempted RREQ_TRIES times without receiving a route to the TargetNode, all data packets destined for the corresponding TargetNode are dropped from the buffer and a

Destination Unreachable ICMP message should be delivered to the source.

5.5. Route Maintenance

A RERR SHOULD be issued if a data packet is to be forwarded and it cannot be delivered to the next-hop because no forwarding route for the IP.DestinationAddress exists; RERR generation is described in Section 5.5.3.

Upon this condition, an ICMP Destination Unreachable message SHOULD NOT be generated unless this router is responsible for the IP.DestinationAddress and that IP.DestinationAddress is known to be unreachable.

In addition to inability to forward a data packet, a RERR SHOULD be issued immediately after detecting a broken link of an forwarding route to quickly notify DYMO routers that a link break occurred and that certain routes are no longer available. If the route with the broken link has not been used recently (indicated by ROUTE_USED), the RERR SHOULD NOT be generated.

5.5.1. Active Link Monitoring

Nodes MUST monitor next-hop links on forwarding routes. This monitoring can be accomplished by one or several mechanisms, including:

- Link layer feedback
- Neighborhood discovery [I-D.ietf-manet-nhdp]
- Route timeout
- Other monitoring mechanisms or heuristics

Upon determining that a link is broken or the next-hop is unreachable, ThisNode MUST remove the affected forwarding routes (those with an unreachable next-hop) and unset the Route.Forwarding flag. ThisNode also flags the associated routes in DYMO's routing table as Broken. For each broken route a timer for ROUTE_DELETE is set to ROUTE_DELETE_TIMEOUT.

5.5.2. Updating Route Lifetimes During Packet Forwarding

To avoid removing the forwarding route to reach the IP.SourceAddress, ThisNode SHOULD set a timeout (ROUTE_USED) to ROUTE_USED_TIMEOUT for the route to the IP.SourceAddress upon receiving a data packet. If a

timer for ROUTE_DELETE is set, it is removed.

To avoid removing the forwarding route to the IP.DestinationAddress that is being used, ThisNode SHOULD set a timeout (ROUTE_USED) to ROUTE_USED_TIMEOUT for the route to the IP.DestinationAddress upon sending a data packet. If a timer for ROUTE_DELETE is set, it is removed.

5.5.3. RERR Generation

A RERR informs DYMO routers that a route to certain destinations is not available through ThisNode.

When creating a new RERR, the address of first UnreachableNode (IP.DestinationAddress from a data packet or RREP.TargetNode.Address) is inserted into an Address Block AddBlk.UnreachableNode.Address. If a prefix is known for the UnreachableNode.Address, it SHOULD be included. Otherwise, the UnreachableNode.Address assumed to be a host address with a full length prefix. If a value for the UnreachableNode's SeqNum (UnreachableNode.AddTLV.SeqNum) is known, it SHOULD be placed in the RERR. The MsgHdr.HopLimit is set to

MSG_HOPLIMIT.

Additional UnreachableNodes that require the same unavailable link (routes with the same Route.NextHopAddress and Route.NextHopInterface) SHOULD be added to the RERR, as additional AddBlk.UnreachableNode.Address entries with their associated prefix. The SeqNum if known SHOULD also be included. Appending UnreachableNode information notifies each processing node of additional routes that are no longer available. This option SHOULD be administratively configurable or intelligently controlled.

If SeqNum information is not known or not included in the RERR, all nodes processing the RERR will assume their routing information associated with the UnreachableNode is no longer valid and flag those routes as broken.

Each DYMO routing protocol message SHOULD contain ThisNode.DID's value in a message TLV (MsgTLV.DID). If ThisNode.DID value is zero (0) it MAY be omitted.

A multicast RERR is sent to the IP.DestinationAddress LL-MANET-ROUTERS [I-D.ietf-manet-iana]. Sending the RERR to the LL-MANET-ROUTERS address notifies all nearby DYMO routers that might depend on the now broken link. If the RERR is unicast, the IP.DestinationAddress is set to the NextHopAddress.

At this point, the packet or message that forced generation of this

RERR SHOULD be discarded.

5.5.4. RERR Processing

First, ThisNode decides whether to process this message. If the message contains a MsgTLV.DID it SHOULD match ThisNode.DID's value. If the message does not contain a MsgTLV.DID it is assumed to be zero (0) and SHOULD be discarded if ThisNode.DID's value is not zero (0).

Next, ThisNode MAY selectively process messages based upon information in the message. ThisNode MAY choose to only process messages from adjacent DYMO routers. If ThisNode chooses not to process this message, the message is discarded and further processing stopped.

When a DYMO router processes a RERR, it processes each UnreachableNode's information. The processing DYMO router removes the forwarding route, unsets the Route.Forwarding flag, sets the Route.Broken flag, and a timer for ROUTE_DELETE is set to ROUTE_DELETE_TIMEOUT for each UnreachableNode.Address found using longest prefix matching that meet all of the following conditions:

1. The UnreachableNode.Address is a multihop-capable unicast IP address.

2. The Route.NextHopAddress is the same as the RERR IP.SourceAddress.

3. The Route.NextHopInterface is the same as the interface on which the RERR was received.

4. The Route.SeqNum is zero (0), unknown, OR the UnreachableNode.SeqNum is zero (0), unknown, OR Route.SeqNum - UnreachableNode.SeqNum <= 0 (using signed 16-bit arithmetic).

During processing if Route.SeqNum is zero (0) or unknown and UnreachableNode.SeqNum exists in the RERR, then Route.SeqNum MAY be set to UnreachableNode.SeqNum. Setting Route.SeqNum can reduce future RRER processing and forwarding.

Each UnreachableNode that did not result in a broken route is removed from the RERR, since propagation of this information will not result in any benefit.

Each UnreachableNode that did result in a broken route SHOULD remain in the RERR.

If any UnreachableNode was removed, all other information (AddTLVs)

associated with the removed address(es) MUST also removed.

After processing if Route.SeqNum is known and an UnreachableNode.SeqNum is not included in the RERR, then Route.SeqNum (i.e. UnreachableNode.SeqNum) MAY be added to the RERR. Including UnreachableNode.SeqNum can reduce future RRER processing and forwarding.

If no UnreachableNode addresses remain in the RERR, no other processing is required and the RERR is discarded.

If processing continues, the MsgHdr.HopLimit is decremented by one (1). Further, if this RERR's new MsgHdr.HopLimit is greater than one (1) and at least one unreachable node address remains in the RERR, then the updated RERR SHOULD be sent.

A multicast RERR is sent to the IP.DestinationAddress LL-MANET-ROUTERS [I-D.ietf-manet-iana]. If the RERR is unicast, the IP.DestinationAddress is set to the NextHopAddress.

5.6. DYMO Identifier (DID)

Each DYMO routing protocol instance MUST have an associated DYMO Identifier (DID). The default value is zero (0). The DID value should be administratively configured.

Each DYMO routing protocol message sent SHOULD contain its associated DID in a message TLV. If the DID value is zero (0) it MAY be omitted.

Upon receipt of DYMO protocol message a DYMO routing protocol instance SHOULD only process messages with a DID (MsgTLV.DID) value matching its own DID (ThisNode.DID).

The DID allows multiple DYMO routing protocol instances to operate over the same links and same node independently.

The DID fulfills a function similar to OSPF Instance ID [RFC2740] [I-D.ietf-ospf-multi-instance], OSPF Area ID [RFC2328] [RFC2740], and/or the MANET_ID TLV [I-D.chakeres-manet-manetid].

5.7. Unknown Message & TLV Types

If a message with an unknown type is received, the message is discarded.

For processing of messages that contain unknown TLV types, operation should be administratively controlled.

5.8. Advertising Network Addresses

DYMO routers advertise specify the prefix length for each advertised address. Any nodes (other than the advertising DYMO router) within the advertised prefix MUST NOT participate in the DYMO protocol directly. For example, A.B.C.1 with a prefix length of 24 indicates all nodes with the matching A.B.C.X are reachable through the DYMO router with address A.B.C.1.

5.9. Simple Internet Attachment

Simple Internet attachment consists of a stub network of MANET routers connected to the Internet via a single Internet DYMO router (IDR). The Internet may be connected via multiple DYMO routers, but such behavior is not specified in this document.

The IDR is responsible for responding to RREQs for DYMO routers on behalf of TargetNodes on the Internet, as well as delivering packets to destinations on the Internet.

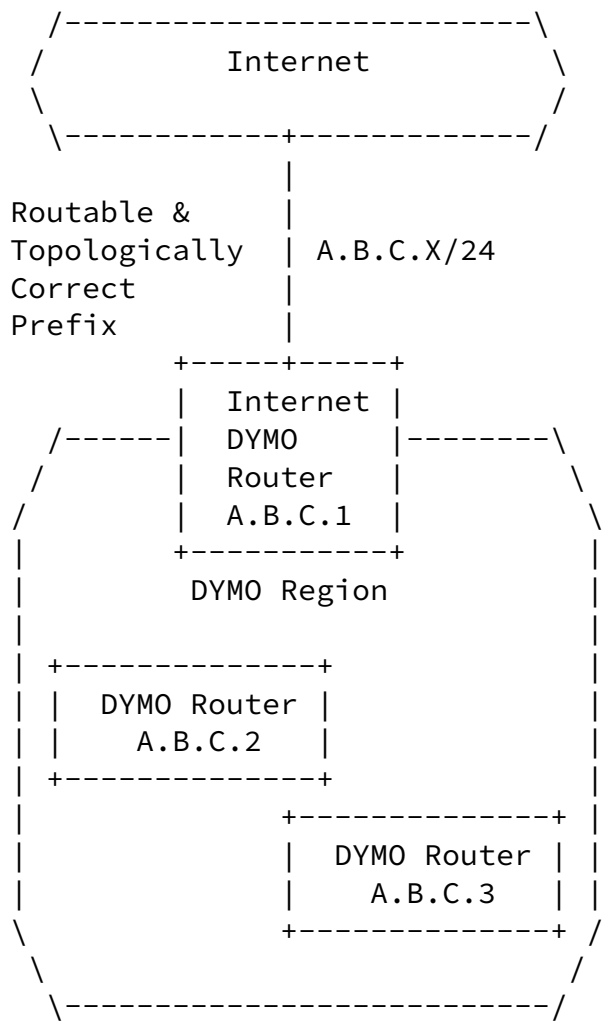


Figure 3: Simple Internet Attachment Example

DYMO routers wishing to be reachable from nodes in the Internet MUST have IP addresses within the IDR's routable and topologically correct prefix. Given a node with a routeable address or care-of address handled by the IDR, the IDR is responsible for routing and forwarding packets received from the Internet destined for nodes inside its MANET.

When DYMO router within the MANET want to send packets to a node on the Internet, they simply issue RREQ for those IP Destination Addresses; using normal DYMO route discovery. The IDR is responsible for properly responding to RREQ on behalf of the Internet destinations, and maintaining their associated sequence number(s).

For an IDR and other DYMO routers that maintain the sequence number on behalf of other nodes, these routers MUST know the IP addresses for which they MUST generate DYMO messages and maintain OwnSeqNum. Likewise, they MUST be capable of advertising an address within the same prefix as these IP addresses. Alternatively, they may behave as a proxy on behalf of Internet destinations.

5.10. Multiple Interfaces

DYMO may be used with multiple interfaces; therefore, the particular interface over which packets arrive MUST be known whenever a packet is received. Whenever a new route is created, the interface through which the Route.Address can be reached is also recorded in the route table entry.

When multiple interfaces are available, a node transmitting a multicast packet with IP.DestinationAddress set to LL-MANET-ROUTERS SHOULD send the packet on all interfaces that have been configured for DYMO operation.

Similarly, DYMO routers should subscribe to LL-MANET-ROUTERS on all their DYMO interfaces.

5.11. DYMO Control Packet/Message Generation Limits

To ensure predictable control overhead, DYMO router's rate of packet/message generation SHOULD be limited. The rate and algorithm for limiting messages is left to the implementor and should be

administratively configurable or intelligently controlled. DYMO control messages SHOULD be discarded in the following order of preferences RREQ, RREP, and finally RERR.

6. Configuration Parameters and Other Administrative Options

Suggested Parameter Values

Name	Value
MSG_HOPLIMIT	10 hops
ROUTE_TIMEOUT	5 seconds
ROUTE_AGE_MIN_TIMEOUT	1 second
ROUTE_SEQNUM_AGE_MAX_TIMEOUT	60 seconds
ROUTE_USED_TIMEOUT	ROUTE_TIMEOUT
ROUTE_DELETE_TIMEOUT	2 * ROUTE_TIMEOUT
ROUTE_RREQ_WAIT_TIME	2 seconds
RREQ_TRIES	3 tries
UNICAST_MESSAGE_SENT_TIMEOUT	1 second

Table 2

These suggested values work well for small and medium well connected networks with moderate topology changes. These parameters SHOULD be administratively configurable for the network where DYMO is used. Ideally, for networks with frequent topology changes the DYMO parameters should be adjusted using either experimentally determined values or dynamic adaptation. For example, in networks with infrequent topology changes ROUTE_USED_TIMEOUT may be set to a much larger value.

In addition to the parameters above several administrative options exist. Many of these options can be administratively controlled, but they may be better served by intelligent control. The following table enumerates several of the options.

Important Settings

Name	Description
RESPONSIBLE_ADDRESSES	List of addresses, and their associated prefix, for which this DYMO router is responsible.
DYMO_INTERFACES	List of the interfaces participating in DYMO routing protocol.

Table 3

Note: several fields have limited size (bits or bytes) these sizes and their encoding may place specific limitations on the values that can be set. For example, MsgHdr.HopLimit is a 8-bit field and therefore MSG_HOPLIMIT cannot be larger than 255.

7. IANA Considerations

In its default mode of operation, DYMO uses the UDP port MANET [I-D.ietf-manet-iana] to carry protocol packets. DYMO also uses the link-local multicast address LL-MANET-ROUTERS [I-D.ietf-manet-iana].

This section specifies several messages types, message tlv-types, and address tlv-types.

7.1. DYMO Message Type Specification

DYMO Message Types

Name	Type
Route Request (RREQ)	10 - TBD
Route Reply (RREP)	11 - TBD
Route Error (RERR)	12 - TBD

Table 4

7.2. Packet and Message TLV Type Specification

Packet TLV Types

Name	Type	Length	Value
Unicast Response Request	10 - TBD	0 octets	Indicates to the processing node that the previous hop (IP.SourceAddress) expects a unicast message within UNICAST_MESSAGE_SENT_TIMEOUT. Any unicast packet will serve this purpose, and it MAY be an ICMP REPLY message. If a message is not sent, then the previous hop can assume that the link is unidirectional and MAY blacklist the link to this node.

Table 5

7.3. Address Block TLV Specification

Address Block TLV Types

Name	Type	Length	Value
DYMO Identifier (DID)	9 - TBD	DID length	ThisNode.DID's value. More information can be found in Section 5.6
DYMO Sequence Number (DYMOSeqNum)	10 - TBD	up to 2 octets	The DYMO sequence num associated with this address. The sequence number may be the last known sequence number.
Distance	11 - TBD	up to 2 octets	A metric of the distance traversed by the information associated with this address.
VALIDITY_TIME - AKA MaxAge	TBD [I-D.ietf-man et-timetlv]		The maximum amount of time that information can be maintained before being deleted. The VALIDITY_TIME TLV is defined in [I-D.ietf-manet-timetlv].

Table 6

8. Security Considerations

This document does not mandate any specific security measures. Instead, this section describes various security considerations and potential avenues to secure DYMO routing.

The most important security mechanisms for DYMO routing are integrity/authentication and confidentiality.

In situations where routing information or router identity are suspect, integrity and authentication techniques SHOULD be applied to DYMO messages. In these situations, routing information that is

distributed over multiple hops SHOULD also verify the integrity and identity of information based on originator of the routing information.

A digital signature could be used to identify the source of DYMO messages and information, along with its authenticity. A nonce or timestamp SHOULD also be used to protect against replay attacks. S/MIME and OpenPGP are two authentication/integrity protocols that could be adapted for this purpose.

In situations where confidentiality of DYMO messages is important, cryptographic techniques SHOULD be applied.

In certain situations, like sending a RREP or RERR, a DYMO router could include proof that it has previously received valid routing information to reach the destination, at one point of time in the past. In situations where routers are suspected of transmitting maliciously erroneous information, the original routing information along with its security credentials SHOULD be included.

Note that if multicast is used, any confidentiality and integrity algorithms used must permit multiple receivers to process the message.

9. Acknowledgments

DYMO is a descendant of the design of previous MANET reactive protocols, especially AODV [RFC3561] and DSR [RFC4728]. Changes to previous MANET reactive protocols stem from research and implementation experiences. Thanks to Elizabeth Belding-Royer for her long time authorship of DYMO. Additional thanks to Luke Klein-Berndt, Pedro Ruiz, Fransisco Ros, Koojana Kuladinithi, Ramon

Caceres, Thomas Clausen, Christopher Dearlove, Seung Yi, Romain Thouvenin, Tronje Krop, Henner Jakob, Alexandru Petrescu, Christoph Sommer, Cong Yuan, Lars Kristensen, and Derek Atkins for reviewing of DYMO, as well as several specification suggestions.

10. References

10.1. Normative References

[I-D.ietf-manet-iana]
Chakeres, I., "IANA Allocations for MANET Protocols", draft-ietf-manet-iana-07 (work in progress), November 2007.

[I-D.ietf-manet-packetbb]
Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized MANET Packet/Message Format", draft-ietf-manet-packetbb-17 (work in progress), November 2008.

[I-D.ietf-manet-timetlv]
Clausen, T. and C. Dearlove, "Representing multi-value time in MANETs", draft-ietf-manet-timetlv-08 (work in progress), September 2008.

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007.

10.2. Informative References

[I-D.chakeres-manet-manetid]
Chakeres, I., "MANET_ID TLV", draft-chakeres-manet-manetid-03 (work in progress), February 2008.

[I-D.ietf-manet-nhdp]
Clausen, T., Dearlove, C., and J. Dean, "MANET Neighborhood Discovery Protocol (NHDP)", draft-ietf-manet-nhdp-07 (work in progress), July 2008.

[I-D.ietf-ospf-multi-instance]

Lindem, A., Roy, A., and S. Mirtorabi, "OSPF Multi-Instance Extensions", draft-ietf-ospf-multi-instance-00 (work in progress), February 2009.

[Perkins99] Perkins, C. and E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, February 1999.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC2740] Coltun, R., Ferguson, D., and J. Moy, "OSPF for IPv6", RFC 2740, December 1999.

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

[RFC4728] Johnson, D., Hu, Y., and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, February 2007.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC5148] Clausen, T., Dearlove, C., and B. Adamson, "Jitter Considerations in Mobile Ad Hoc Networks (MANETs)", RFC 5148, February 2008.

Authors' Addresses

Ian D Chakeres
CenGen
9250 Bendix Road North
Columbia, Maryland 21045
USA

Email: ian.chakeres@gmail.com
URI: http://www.ianchak.com/

Charles E. Perkins
WiChorus Inc.
3590 North First Street, Suite 300
San Jose, CA 95134
USA

Phone: +1-408-421-1172
Email: charliep@computer.org