Mobile Ad Hoc Networking Working Group
INTERNET DRAFT
**14 November 2001**

Charles E. Perkins
Nokia Research Center
Elizabeth M. Belding-Royer
University of California, Santa Barbara
Samir R. Das
University of Cincinnati

# IP Flooding in Ad hoc Mobile Networks

draft-ietf-manet-bcast-00.txt

## Status of This Memo



## Abstract

An ad hoc mobile network is a collection of nodes, each of which communicates over wireless channels and is capable of movement. Nodes participating in such an ad hoc network communicate on a peer-to-peer basis. Flooding is often a desired form of communication in these networks, as it can enable both the dissemination of control information and the delivery of data packets. This document describes a method for sending packets to every node in an d hoc networks.

## 1. Introduction

This document makes a particular specification for a classical flooding algorithm, as it can be used to disseminate IP packets across ad hoc networks. Flooding is needed in many circumstances; in particular, it is useful for the kind of route discovery operations that are required for on-demand route acquisition in several candidate manet protocols.

This protocol specification works when the nodes flooding packets ensure that each distinct such packet that they send is tagged with a distinct value in the ident field of the IP header.

In IPv4, there are two kinds of broadcast address, and it seems that neither one of them is likely to present a good choice for the IP address to be used for flooding. The IPv4 address for "limited broadcast" is 255.255.255.255, and is not supposed to be forwarded. Since the nodes in an ad hoc network are asked to forward the flooded packets, the limited broadcast address is a poor choice. The other available choice, the "directed broadcast" address, would presume a choice of routing prefix for the ad hoc network and thus is not a reasonable choice.

Thus, in this specification, new multicast groups for flooding to all nodes of an ad hoc network are specified. These multicast groups are specified to contain all nodes of a contiguous ad hoc network, so that packets transmitted to the multicast address associated with the group will be delivered to all nodes as desired. For IPv6, the multicast address is specified to be "site-local". The names of the multicast groups are given as "ALL_IPv4_MANET_NODES" and "ALL_IPv6_MANET_NODES".

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 RFC 2119 [1].

## 2. Flooding

For the purposes of this document, the IPv4 flooding address is "ALL_IPv4_MANET_NODES" (TBD). The analogous address for transmissions to all IPv6 ad hoc network nodes is "ALL_IPv6_MANET_NODES" (TBD). This document does not specify transmissions to any directed broadcast address. Transmissions to the IPv4 "limited broadcast" address, that is 255.255.255.255, are not forwarded by nodes obeying this specification.

Every node maintains a list to keep track of which flooded packets have already been received and retransmitted. The list contains, for

each distinct flooded packet received, a value called the Flooded Packet Identifier (FPI). For IPv4, this FPI is composed of the source IP address, the IP ident value, and the fragment offset values obtained from the IP header of the flooded packet. For IPv6, the FPI is calculated as specified in section 3.

When a node receives a flooded packet, it checks its list for the FPI of the flooded packet's IP header [2]. If there is such a list entry with matching FPI, the node silently discards the flooded packet since it has already been received and forwarded. The node then checks to see whether it is enabled for retransmitting flooded packets. By default, all nodes in the ad hoc network are so enabled; however, this is not required (see section 5) and may be changed by configuration. If the node is not enabled for retransmitting flooded packets, it takes no further action. If there is no existing list entry containing the same FPI, and if the node has been enabled to forward flooded packets, the node retransmits the packet.

List entries SHOULD be kept for at least BROADCAST_RECORD_TIME before the node expunges the record. BROADCAST_RECORD_TIME is a configurable parameter, but it MUST be at least equal to NET_TRAVERSAL_TIME.

## 3. FPI computation for IPv6

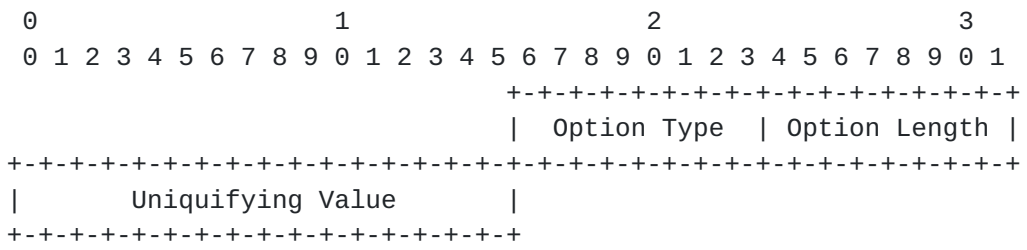
To obtain the FPI for IPv6 packets, a node uses MD5 [3] to perform the following calculation for the incoming flooded packet:

FPI = MD5 (IPv6 packet data).

The IP packet data includes all non-mutable IPv6 headers and extensions, as well as any higher-level protocol data. The source node for each flooded packet MUST ensure that this FPI is distinct from the FPI from every other flooded packet which the node has transmitted during the last BROADCAST_RECORD_TIME. In the unlikely event that the FPI value is identical to some such recently transmitted packet, the source node MUST add a Unique Identifier Destination Option to the flooded packet (see section 4).

## 4. Unique Identifier Destination Option

The Unique Identifier option is encoded in type-length-value (TLV) format as follows:




Option Type

TBD

Option Length

2

Uniquifying Value

The 16-bit Uniquifying Value is chosen to make the flooded packet FPI computation different than that for any other flooded packet from the same source node.

The Unique Identifier MUST be placed in the Destination Options before the Routing Header (and, thus, before the fragment header). This allows proper handling by all intermediate forwarding nodes

## 5. Selective Retransmission for Flooded Packets

By default, each node in the ad hoc network is enabled to retransmit each distinct flooded packet that it receives. However, in some cases, there may be additional control signaling in place that is used to reduce the number of nodes that perform this retransmission, in order to reduce the overall bandwidth consumption and congestion which can be caused by excessive flooding. This document does not specify any such control protocol to disable or enable such node selection. However, an ad hoc network which employs such a node selection protocol can still be considered to be compliant with the flooding protocol specified in this document.

## 6. Configuration Parameters

This section gives default values for some important values associated with flooding operations. Mobile nodes in particular ad hoc networks may wish to change certain of the parameters, in particular the NET_DIAMETER and NODE_TRAVERSAL values. Choice of these parameters may affect the robustness of the flooding operation.

| Parameter Name | Value |
|---|---|
| BROADCAST_RECORD_TIME | 2 * NET_TRAVERSAL_TIME |
| NET_DIAMETER | 35 |
| NODE_TRAVERSAL_TIME | 40 milliseconds |
| NET_TRAVERSAL_TIME | 3 * NODE_TRAVERSAL_TIME * NET_DIAMETER / 2 |

NET_DIAMETER measures the maximum possible number of hops between two nodes in the network. NODE_TRAVERSAL_TIME is a conservative estimate of the average one hop traversal time for packets and should include queuing delays, interrupt processing times and transfer times. NET_TRAVERSAL_TIME is a conservative estimate of how long it should take for a message to traverse the entire ad hoc network.

## 7. Security Considerations

This draft specifies a general mechanism for flooding packets in an ad hoc network. It does not make any provision for securing the contents of the flooded data, either to protect against tampering or to protect against unauthorized inspection of the data.

## 8. Acknowledgments

This flooding method is a codification of a well known algorithm which has been assumed for general use in various ad hoc protocols. Thus, the protocol specification in this draft should be considered the joint work of many engineers who have worked on producing ad hoc network protocols. The authors of this draft hope that we have been able to faithfully and usefully represent the work of these many engineers.

## References

[1] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. Request for Comments (Best Current Practice) 2119, Internet Engineering Task Force, March 1997.

[2] J. Postel. Internet Protocol. Request for Comments (Standard) 791, Internet Engineering Task Force, September 1981.

[3] R. Rivest. The MD5 Message-Digest Algorithm. Request for Comments (Informational) 1321, Internet Engineering Task Force, April 1992.

## A. Changes since the last revision

- Changed terminology from "broadcast" to "flood", to avoid ambiguity with the various flavors of IPv4 broadcast.

- Specified a new IPv4 multicast address and a new IPv6 multicast address.

## Author's Addresses

Questions about this memo can be directed to:

Charles E. Perkins
Communications Systems Laboratory / Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94303
+1 650 625 2986
+1 650 625-2502 (fax)
charliep@iprg.nokia.com

Elizabeth M. Royer
Dept. of Electrical and Computer Engineering
University of California, Santa Barbara
Santa Barbara, CA 93106
+1 805 893 7788
+1 805 893 3262 (fax)
eroyer@alpha.ece.ucsb.edu

Samir R. Das
Dept. of Electrical and Computer Engineering & Computer Science
University of Cincinnati
Cincinnati, OH 45221-0030
+1 513 556 2594
+1 513 556 7326 (fax)
sdas@ececs.uc.edu