IPv4 Mobility extension for Multicast and Broadcast Packets
draft-chakrabarti-mip4-mcbc-00

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 January 3, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Intended Status <To Be Removed Upon Publication>

Intended status: Informational
Abstract

The IP Mobility Protocol [RFC3344] describes the multicast and broadcast packet transmission between the mobile node and the home-network or visited network. The Reverse Tunneling for Mobile IP, Revised [RFC3024] describes reverse tunneling the multicast and broadcast packets to the home network using encapsulating delivery style between mobile nodes and the foreign agent. However, [RFC3024] says that all packets must be encapsulated in the IP-in-IP tunnel once the encapsulated delivery style is negotiated. This restriction causes over-the-air tunnel overhead in the wireless medium between the mobile and the foreign agent. This document provides a generic solution to ease the restriction of unicast packet to be encapsulated in encapsulating delivery mode. It also provides alternatives of direct delivery of multicast/broadcast packets between a foreign agent and a mobile node in point-to-point link such as Wimax network.
Table of Contents

1. Introduction .................................................. 5
2. Definition Of Terms ............................................. 6
3. Existing Multicast/broadcast routing in Mobile IP .............. 7
4. Exclusive Encapsulating Delivery Style for Multicast and Broadcast only ................................................. 8
   4.1. Packet header formats for visited network traffic ......... 9
   4.2. Packet header formats for homebound traffic .............. 9
5. Exclusive Encapsulating delivery Style Vs RFC3024 Encapsulating delivery ............................................... 11
6. Link Direct Delivery Style for multicast and broadcast packets ................................................................. 12
7. Implementation Notes ............................................. 13
8. Security Considerations ........................................ 14
9. IANA Considerations ............................................ 15
10. Acknowledgments ............................................... 16
11. References ..................................................... 17
   11.1. Normative references ..................................... 17
   11.2. Informative references ................................... 17
Appendix A. Intellectual Property Statement ....................... 18
Authors’ Addresses ................................................ 19
Intellectual Property and Copyright Statements .................... 20
1. Introduction

[RFC3344] section 4.3 and 4.4 discusses multicast and broadcast routing from and to mobile node in the triangular routing and co-located Care-of-address mode. Reverse tunneling for Mobile IP [RFC3024] introduces encapsulating delivery style for reverse tunneling multicast and broadcast packets from mobile node through a foreign agent. However, [RFC3344] also mandates that all multicast and broadcast packets should be delivered encapsulated from foreign agent to mobile-node. This again imposes tunnel overhead for the multicast broadcast packets. While tunneling overhead on the wired link may be acceptable in terms of network performance, it has a much higher cost and throughput impact in the wireless link. So far, Mobile IP has been deployed for 3G data services and there has been not much usage of multicast or broadcast data transfer to or from the mobile node. Wimax Network Architecture [NWG] uses Mobile IP services as one of the mobility services which could be used for both Voice-over-IP and data. In future, PTT (Push-To-Talk) service may be popular and thus demands efficient usage of multicast delivery from the mobile to the network access provider network. Similarly, IPTV may use multicast to distribute streaming media across high bandwidth wireless network such as Wimax [NWG].

Moreover, neither RFC3344 or RFC3024 clearly specifies multicast/broadcast packet delivery for FA-Care-of-address; for example, for encapsulated delivery, the source address of the outer and inner IP header is home-address of the mobile (RFC3024, section 5.2.2), but it is not clear about local delivery of multicast/broadcast packets in the visited network. Multicast messages from the mobile node to the visited network may be needed for retrieving service information. Currently different organizations [3GPP2] define their own mechanism to obtain such information through AAA during link establishment. All Mobility-agent multicast is used for router solicitation by the mobile and the implementation can treat this address specially at the foreign-agent, but the implementation gets very complex if the mobile client uses home-address as source address for other multicast messages destined to the home and visited network, in the reverse tunnel mode.

This document aims to clarify multicast messages for reverse tunnel mode, adds an delivery encapsulation for only multicast/broadcast delivery from mobile to foreign agent and explores direct delivery options of multicast messages between the mobile and the foreign agent by using link-layer information.

(TBD: Describe which section does what)
2. Definition Of Terms

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.

FA-COA
Foreign Agent as care-of-address.

Other
XXX

OTHER2
YYY
3. Existing Multicast/broadcast routing in Mobile IP

Some text [RFC3344] and [RFC3024]
4. Exclusive Encapsulating Delivery Style for Multicast and Broadcast only

The Mobile IP reverse tunneling [RFC3024] defines Encapsulating delivery style for delivering multicast and broadcast packets from the mobile to the foreign agent in the FA-CoA mode. It also mandates Encapsulating delivery mode for sending multicast/broadcast packets to reverse-tunnel to home agent via the foreign agent. But RFC3024 section 2 says that all traffic is encapsulated when Encapsulating Delivery is negotiated. This extension is added such that only multicast and broadcast packets are encapsulated to the foreign agent, but all unicast packets are delivered directly. The main motivation for adding this extension is to save the overhead of additional IP header for unicast packets. This procedure works for both shared media like ethernet, IEEE 802.11 and point-to-point links such as IEEE 802.16e.

Foreign agents SHOULD support the Exclusive Encapsulating Delivery Style Extension. A registration request should contain either regular Encapsulating delivery extension (see section 3.3 in RFC3024) or Exclusive Encapsulating Delivery style, but not both. If both extensions are present, only the first extension will be taken into consideration and the second one will be skipped.

If a foreign agent supports Exclusive Encapsulating Delivery Style (EEDS), then the foreign agent SHOULD advertise the EEDS extension along with the router advertisement to inform the mobile about the type of delivery style it supports. This will avoid the possibility of multiple registration requests to figure out which encapsulating method the foreign agent supports.

mobile node MUST include the Exclusive Encapsulating Delivery Style Extension after the Mobile-Home Authentication Extension, and before the Mobile-Foreign Authentication Extension, if present. The Encapsulating Delivery Style Extension MUST NOT be included if the ‘T’ bit is not set in the Registration Request.

If this extension or RFC3024 compliant Encapsulating Delivery style extension is absent, Direct Delivery is assumed. Encapsulation is done according to what was negotiated for the forward tunnel (that is, IP in IP is assumed unless specified otherwise).
<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TBD</td>
</tr>
</tbody>
</table>

2

It is a 16bit unsigned integer. Value specifies what type of packets are encapsulated.

0: All packets are encapsulated between a mobile node and a foreign agent. It is same as encapsulated delivery style in RFC3024.
1: Only multicast and broadcast packets are encapsulated

NOTE: Exclusive encapsulated packets are reverse tunneled after being de-capsulated at the foreign agent except those are directly destined to the foreign-agent address or all mobility agent address.

### 4.1. Packet header formats for visited network traffic

There might be some multicast or broadcast packets other than Mobile IP agent solicitation packets towards the visited network. If the mobile node can acquire a local IP address, then it MUST direct deliver the multicast and broadcast traffic for local use. If the mobile-node can have only one IP address, (i.e. home address) then it MUST send all the multicast and broadcast packets encapsulated. These packets will be sent to the home-network through reverse-tunnel after the de-capsulation at the foreign agent; only exceptions are the multicast solicitation messages for the mobility agent.

In some cases, the mobile may want to send multicast or broadcast packets to the visited network entities other than the foreign agent. In those cases they should always be direct delivered by acquiring a local IP address or using link-layer mechanism if possible. Please see the section 'Link direct delivery style' below for details.

### 4.2. Packet header formats for homebound traffic

The packet format and processing for encapsulated multicast and broadcast traffic is the same as defined in section 5.2 of Mobile IP
Reverse tunnel document.
5. Exclusive Encapsulating delivery Style Vs RFC3024 Encapsulating delivery

TBD
6. Link Direct Delivery Style for multicast and broadcast packets

This section discusses direct-delivery of multicast and broadcast packets between mobile and the foreign agent by taking advantage of link-layer (such as point-to-point link in Wimax) mechanism. More ideas are being discussed by the authors of this draft. This section will have more information in the later version.
7. Implementation Notes

- A
- B
- C
8. Security Considerations
9. IANA Considerations
10. Acknowledgments

The authors like to thank Charlie Perkins, De Juan Huarte Federico, Parviz Yeghani, Jayshree Bharatia for their comments and contribution in shaping up this document. We also thank the WiMAX Forum NWG members for their valuable input and suggestions for the initial discussion of the problem. Thanks to Prakash Iyer for approving this work for WiMAX forum.
11. References

11.1. Normative references


11.2. Informative references


Appendix A. Intellectual Property Statement

This document only defines a source preference flag to choose Cryptographically Generated Address (CGA) as source address when applicable. CGA are obtained using public keys and hashes to prove address ownership. Several IPR claims have been made about such methods.
Authors’ Addresses

Samita Chakrabarti
Azaire Networks

Email: samita.chakrabarti@azairenet.com

Ahmad Muhanna
Nortel Networks

Email: amuhanna@nortel.com

Gabriel Montenegro
Microsoft

Email: gabriel.montenegro@microsoft.com

Alexander Bachmutsky
Nokia Siemens Network

Email: alexander.bachmutsky@nsn.com

Yingzhe Wu
Huawei

Email: ywu@huawei.com

Basavaraj Patil
Nokia Siemens Networks

Email: basavaraj.patil@nsn.com