Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2010

A. Muhanna (Ed.)
Nortel
S. Chakrabarti
IP Infusion
G. Montenegro
Microsoft Corporation
Y. Wu
ZTE USA
B. Patil
Nokia

July 08, 2009

IPv4 Mobility Extension for Multicast and Broadcast Packets
draft-chakrabarti-mip4-mcbc-04.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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 9, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights

and restrictions with respect to this document.

Abstract

This specification defines a new Mobile IPv4 extension which is used to negotiate the Multicast-Broadcast Encapsulation Delivery style in the case of Mobile IPv4 Foreign Agent Care-of Address mode registration. This mechanism allows the mobile node to negotiate which type of traffic to be delivered encapsulated to the foreign agent while delivering other types of IP packets using direct delivery style. In particular, this mechanism gives the flexibility to eliminate tunnel overhead in the (typically) wireless medium between the mobile node and the foreign agent. In addition to the reduced overhead, the new mechanism makes many multicast and broadcast services available to the mobile node in a much more deterministic and efficient way.

Table of Contents

1. Introduction

The IP Mobility Protocol [RFC3344] describes multicast and broadcast packet transmission between the mobile node and the home network or visited network. Reverse Tunneling for Mobile IP [RFC3024] includes support for reverse tunneling of multicast and broadcast packets to the home network using the encapsulating delivery style between the mobile nodes and the foreign agent. However, [RFC3024] says that once the encapsulated delivery style is negotiated, all packets exchanged between the mobile node and the foreign agent must be delivered encapsulated. In particular, this imposition prevents direct delivery of unicast packets from the mobile node to the foreign agent. This causes a huge tunnel overhead in the (typically) wireless medium between the mobile node and the foreign agent and indirectly makes it impossible for the mobile node to use any of the multicast and broadcast services.

Additionally, [RFC3344] sections 4.3 and 4.4 discusses multicast and broadcast routing to and from the mobile node in the presence of triangular routing and with a co-located Care-of address. Reverse tunneling for Mobile IP [RFC3024] uses the optimal direct delivery style from the mobile node via the foreign agent if only unicast traffic is being reverse tunneled. If, however, multicast or broadcast packets are also meant to be reverse tunneled, it introduces the Encapsulating Delivery Style. Unfortunately, once the encapsulating delivery style is negotiated, it applies to all reverse tunneling traffics, including unicast. [RFC3344] also mandates, in the case of FA Care-of Address mode, that all multicast and broadcast packets be delivered encapsulated to mobile node. This also imposes tunnel overhead for multicast and broadcast packets. While tunneling overhead on wired links may be acceptable, it has a higher cost and throughput impact in wireless links. Even though, Mobile IP has been deployed for 3G data services, there has not been much usage of multicast or broadcast data transfer to or from the mobile node. The 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 the future, PTT (Push-To-Talk) service may be popular and thus demands efficient usage of multicast delivery from the mobile node to the access network. Similarly, IPTV may use multicast to distribute streaming media across high bandwidth wireless network such as Wimax [NWG].

Moreover, neither [RFC3344] nor [RFC3024] clearly specify multicast/ broadcast packet delivery for FA Care-of address; for example, for encapsulating delivery style, the source address of the outer and inner IP header is the home address of the mobile node as described in section 5.2.2 of [RFC3024]. In addition, section 5.4 talks about local delivery of multicast/broadcast packets in the visited network

but some boarder cases are not completely specified. In particular, multicast messages from the mobile node to the visited network may be needed for retrieving service information. The all Mobility-agents multicast address is used for router solicitation by the mobile node, so foreign agent implementations must use it as a special address. This leads to complexity if in the reverse tunnel the mobile node uses its home address as the source address for other multicast messages destined to the home and visited network.

Currently different organizations [3GPP2] define their own mechanism to obtain local information such as DNS server IP address through AAA. All Mobility-agent multicast is used for router solicitation by the mobile node and the implementation can treat this address specially at the foreign agent. However, the implementation of foreign agent needs to apply multicast-address filtering and gets very complex if the mobile client uses the home address as source address for other multicast messages destined to the home and visited network, in the reverse tunnel mode. Even if multicast packets are delivered locally, the return packet which has the destination address as the home address will be routed back all the way to the home agent of the mobile node to be tunneled back to the foreign agent and then to the mobile node. [RFC3024] recommends selective reverse tunneling by delivering packets directly to the foreign agent, while encapsulating them for reverse tunnel delivery. But the specification is not clear about the source addresses of the packets from the mobile node in case of selective direct delivery. Although it clearly states that for the mobile node which uses co-located care-of address mode.

This specification aims to clarify the delivery of multicast messages when reverse tunneling is used, adds the capability to selectively negotiates which type of traffic to be delivered using encapsulating delivery, e.g., only for multicast and broadcast packets from mobile node to foreign agent, while allowing direct delivery for other type of traffic, e.g., unicast, and explores direct delivery options of multicast messages between the mobile node and the foreign agent by using link-layer capabilities.

Section 3 describes the new delivery extension for multicast-broadcast packets in reverse tunnel mode.

2. Conventions & Terminology

2.1. Conventions used in this document

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].

2.2. Terminology

All the general mobility related terminology and abbreviations are to be interpreted as defined in IP Mobility Protocol [RFC3344] and Reverse tunneling for Mobile IP [RFC3024]. The following terms are used in this document.

MN

Mobile Node.

FA

Foreign Agent.

FA-CoA

Foreign Agent as the Mobile Node Care-of Address.

3. Multicast-Broadcast Encapsulating Delivery Style

The Mobile IP reverse tunneling [RFC3024] defines the Encapsulating delivery style for delivering multicast and broadcast packets from the mobile node 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 reverse-tunneled traffic is encapsulated when Encapsulating Delivery is negotiated. The "Multicast-Broadcast Encapsulating Delivery Style" (MBEDS) extension defined in this specification applies encapsulation only to the reverse-tunneled multicast and broadcast packets, leaving direct delivery for reverse-tunneled unicast packets. The main motivation for adding this extension is to save the overhead of additional IP header for unicast packets which consequently will enable the use of Multicast and Broadcast packets when Mobile IPv4 is in use. This procedure works for both shared media like ethernet, IEEE 802.11 and links of a point-to-point nature such as those defined by 3GPP, 3GPP2 and IEEE 802.16.

3.1. Multicast-Broadcast Encapsulating Delivery Extension

The proposed extension is used in Mobile IPv4 signaling to negotiate the Multicast-Broadcast Encapsulation Delivery Style. Foreign agents SHOULD support the Multicast-Broadcast Encapsulating Delivery Style Extension. A registration request MAY include either a regular

encapsulating delivery extension (see section 3.3 in [RFC3024]) or a Multicast-Broadcast Encapsulating Delivery extension, but not both. If both extensions are present, the foreign agent will consider that an error scenario and the FA MUST reject the registration request by sending a registration reply with the code field set to "Poorly Formed Request".

If a foreign agent supports MBEDS, then the foreign agent SHOULD advertise the MBEDS extension in its router advertisement to inform the mobile node about the type of delivery style it supports. This will avoid the possibility of multiple registration requests to figure out which encapsulating mode the foreign agent supports.

If the MN includes an MBEDS extension, if MUST do so 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 no delivery style extension is present, Direct Delivery per RFC 3024 is assumed.

The Multicast-Broadcast Encapsulation Extension format is as in Figure 1 below.

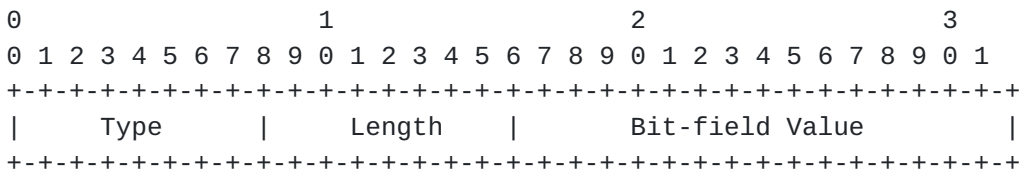

Figure 1: Multicast-Broadcast Encapsulating Extension

Type

<IANA>

Length

8-bit unsigned integer indicating the length in octets of the Bit-Field . It is set to 2.

Bit-Field Value

A 16-bit bit-field. Value specifies what type of packets are encapsulated. The following bits are defined (0 being the right-most bit, 15 the left-most bit):

0:

All packets are encapsulated between a mobile node and a foreign agent. It is same as the Encapsulating Delivery Style in RFC3024. NOTE: obsolete EDS in 3024?.

1:

Only multicast and broadcast packets are encapsulated (MBEDS).

2:

Link-layer Assisted Delivery Style (LLAS) for local network.

All other bits values are reserved.

NOTE: Only MBEDS packets are reverse tunneled after being decapsulated at the foreign agent, not those directly destined to the foreign-agent address or all mobility agent address. These are processed locally by the foreign agent.

3.2. Packet Header Formats for Visited Network Traffic

Other than Mobile IP agent solicitation packets, there might be some multicast or broadcast packets meant for consumption at 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 the reverse tunnel after being decapsulated at the foreign agent; only exceptions are the multicast solicitation messages for the mobility agent.

In some cases, the mobile node may want to send multicast or broadcast packets to 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-layer Assisted Delivery Style' below for details.

3.3. 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 Reverse Tunneling for Mobile IP [RFC3024]. Additionally, the packet format and processing for unicast traffic is the same as defined in section 5.1 of the same specification.

4. Multicast-Broadcast Encapsulating delivery Style Vs RFC3024 Encapsulating delivery

RFC3024 encapsulating delivery style does not require the foreign-agent to advertise an extension as well for the mobile node efficiency. MBEDS provides an option for foreign agent to advertise the extension with supported extension types, so that a mobile node can request a delivery style that the foreign agent supports.

RFC3024 encapsulating delivery style requires all multicast, broadcast and unicast traffic to be encapsulated in order to be reverse tunneled. In MBEDS unicast packets are always direct delivered to the foreign agent. Most of the the cases a node sends unicast packets for communication with a correspondent node and occasionally it may send broadcast or multicast packets to the home network. Thus this new style of delivery relieves the overhead of encapsulation for most traffic.

MBEDS introduces TLV style extension for delivery style. Therefore, this extension can be used to negotiate different delivery styles in the future. Currently, it can be backward compatible with RFC3024 encapsulating delivery style when the value field is zero. NOTE: We should make this a bit field to allow for easier advertisement and other extensions.

A mobile node SHOULD use either RFC3024 style encapsulating delivery extension or the MBEDS extension (defined in this document), but not both at the same time. If both extensions are received at the foreign-agent, the foreign agent MUST reject the registration request by sending a registration reply with error (70) "Poorly Formed Request".

5. Link-layer Assisted Delivery Style (LLADS)

This section discusses direct-delivery of multicast and broadcast packets between the mobile node and the foreign agent by taking advantage of link-layer mechanisms. Certain link-layers allow for direct delivery from the MN to the FA (and vice-versa) without the

need for encapsulation. In effect, this is assumed by RFC 3024 for Direct Delivery Style. In this mode, a unicast packet at the IP layer is carried over a unicast link-layer delivery mechanism. For example, the FA's MAC address is the link-layer destination address, or the packet is sent on a link of a point-to-point nature as in 3G or WiMAX networks. Broadcast and multicast packets, however are typically sent using a link-layer broadcast or multicast mechanism: a broadcast or multicast MAC address for IEEE 802.11 networks. If, however, these packets had the FA unicast MAC address while carrying an IP layer broadcast or multicast destination, then there would be no need for encapsulation to remove the ambiguity. The packet would be unequivocally directed at, and consumed by the FA. Notice that in links of a point-to-point nature, there is no ambiguity even for multicast and broadcast packets: these are unequivocally delivered to the FA. The Link-layer Assisted Delivery Style allows for direct delivery of unicast, multicast and broadcast packets over link-layers that can support it. In particular, it requires that regardless of whether the IP layer packet is unicast, broadcast or multicast, (1) when sending from MN to FA, the FA unicast address always be used, and (2) when sending from FA to MN, the MN unicast address always be used. The FA advertises such capability per the extension defined above, and the MN requests it in its registration request.

The LLADS imposes the least amount of tunneling overhead of the delivery styles as it effectively uses the equivalent of direct delivery for unicast, broadcast and multicast. It enables the MN to deliver packets to the FA for the foreign agent to reverse tunnel them back to the MN's home network.

However LLADS does not by itself allow the MN to deliver packets such that the FA know whether or not it should reverse tunnel them, or process them as local packets (e.g., perhaps forwarding them to local services). Certain networks have the capability of enabling additional context at the link-layer to effect different classification and treatment of packets otherwise indistinguishable at the IP layer, e.g., by establishing additional PDP contexts in 3GPP or additional service flows (and the corresponding CIDs) in WiMAX networks. In such networks, it is possible for the MN and the FA to establish additional context such that packets sent by the MN to the FA are classified correctly upon arrival into either packets meant for local consumption, or packets meant to be reverse tunneled. In the absence of any IP layer differentiation (i.e., by sending packets meant for local consumption with the MN's local care-of address as source address), such link-layer mechanisms can provide the necessary means for the FA to select the correct processing for packets received from the MN. Such link-layer mechanisms, however, are out of scope of this document.

6. Security Considerations

This draft does not introduce any security threats on the top of what is defined in IP Mobility Protocol [RFC3344]. If included, the Multicast-Broadcast Encapsulating Delivery Style extension MUST be added after the MN-HA authentication extension and before the MN-FA authentication extension, if present.

7. IANA Considerations

This document defines a new IP Mobility extension, as described in Section 3.1 and uses a type <IANA-TBD>. The Multicast-Broadcast Encapsulation Delivery Extension type is assigned from the range of values associated with the skippable IP Mobility extensions.

8. Acknowledgments

The authors like to thank Charlie Perkins, Alex Bachmutsky, De Juan Huarte Federico, Parviz Yegani, 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 intial discussion of the problem. Thanks to Prakash Iyer for approving this work for Wimax forum.

9. References

9.1. Normative references

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

[RFC3024] Montenegro, G., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

9.2. Informative references

[3GPP2] "3GPP2 - Third Generation Partnership Project 2: X.P0028-200", Online web site http://www.3gpp2.org.

[NWG] "NWG - Wimax Network Architecture Group", Online web site http://www.wimaxforum.org.

Appendix A. Appendix-A

TBD.

Authors' Addresses

Ahmad Muhanna (Editor)
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
USA

Email: amuhanna@nortel.com

Samita Chakrabarti
IP Infusion
1188 Arquest Street
Sunnyvale, CA
USA

Email: samitac@ipinfusion.com

Gabriel Montenegro
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

Email: gabriel.montenegro@microsoft.com

Yingzhe Wu
ZTE USA
10105 Pacific Heights Blvd, Suite 250
San Diego, CA 92121
USA

Email: yingzhe.wu@zteusa.com

Basavaraj Patil
Nokia
6021 Connection Drive
Irving, TX 75039
USA

Email: basavaraj.patil@nokia.com