NETLMM WG A. Muhanna
Internet-Draft M. Khalil
Intended status: Standards Track Nortel
Expires: January 9, 2009 S. Gundavelli
K. Leung
Cisco Systems
July 08, 2008

GRE Key Option for Proxy Mobile IPv6
draft-muhanna-netlmm-grekey-option-04.txt

Status of this Memo

Copyright Notice

Abstract

The Proxy Mobile IPv6 base specification and Proxy Mobile IPv6 support for IPv4 allow the mobile node's IPv4 and IPv6 traffic between the local mobility anchor and the mobile access gateway to be tunneled using IPv6 or IPv4 encapsulation headers. These encapsulation modes do not offer the tunnel end-points the required semantics to expose a service identifier that can be used to identify traffic for a certain classification, such as for supporting mobile nodes that are using overlapping private IPv4 addressing. The extension defined in this document allow the mobile access gateway and the local mobility anchor to negotiate GRE encapsulation mode and exchange the GRE keys for marking the flows, so that differential processing can be applied by the tunnel peers over those flows.

Table of Contents

1. Introduction

The base Proxy Mobile IPv6 specification [ID-PMIP6] and Proxy Mobile IPv6 support for IPv4 [ID-PMIP6-IPv4] allow the use of IPv6 and IPv4 encapsulation modes [RFC2473] , [RFC2003] for the tunneled traffic between the local mobility anchor and the mobile access gateway. There are scenarios where these encapsulation modes are not sufficient to uniquely identify the destination of packets of a specific flow. Thus, there is a need for an encapsulation mode with richer semantics. The Generic Routing Encapsulation [RFC2784] and the Key extension as defined in [RFC2890], has the required semantics to allow such distinction for use in Proxy Mobile IPv6.

This document defines an extension to the base Proxy Mobile IPv6 specification, for allowing the mobile access gateway and the local mobility anchor to negotiate GRE encapsulation mode and exchange the downlink and uplink GRE keys that can be used for marking the downlink and uplink traffic which belong to a specific mobile node session or a specific flow.

2. Conventions & Terminology

2.1. Conventions

The keywords "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 Mobile IPv6 specification [RFC3775] and Proxy Mobile IPv6 specification [ID-PMIP6]. The following terms are used in this document.

Downlink Traffic

The traffic in the tunnel between the local mobility anchor and the mobile access gateway, heading towards the mobile access gateway and tunneled at the local mobility anchor. This traffic is also referenced as forward direction traffic.

Uplink Traffic

The traffic in the tunnel between the mobile access gateway and the local mobility anchor, heading towards the local mobility anchor and tunneled at the mobile access gateway. This traffic is

also referenced as reverse direction traffic.

Downlink GRE Key

The GRE key is assigned by the mobile access gateway and used by the local mobility anchor to mark the downlink traffic which belongs to a specific mobile node session or flow as described in this document.

Uplink GRE Key

The GRE key is assigned by the local mobility anchor and used by the mobile access gateway to mark the uplink traffic which belongs to a specific mobile node session or flow as described in this document.

3. GRE Encapsulation and Keys Exchange

3.1. GRE Encapsulation Overview

Using the extension defined in this specification, the mobile access gateway and the local mobility anchor can negotiate GRE encapsulation mode and the exchange of GRE keys for marking the downlink and uplink traffic.

Once the GRE keys have been exchanged between the mobile access gateway and the local mobility anchor, the mobile access gateway will use the uplink GRE key that is assigned by the local mobility anchor in the GRE encapsulation header of the uplink payload packet. Similarly, the local mobility anchor will use the downlink GRE key as negotiated with the mobile access gateway in the GRE encapsulation header of the downlink payload packet.

The following illustration explains the use of GRE encapsulation mode and the use of GRE keys for supporting the scenario where overlapping IPv4 private address [RFC1918] allocation is in use.

```
                                                          +------------+
                                                          | Operator-A |
                                                          |            |
                                                          | 10.x.0.0/16|
                                                          +------------+
                                                                   /
        +------+                                      +------+    /
        |      |      ==========================      |      |   /
 MN-1---|      |    /                            \    |      |  / Key-1
        |  M   |   / ---Flows with GRE Key-1 ---- \   |  L   | / Traffic
 MN-2---|  A   |--|                                |--|  M   |-
        |  G   |   \ ---Flows with GRE Key-2 ---- /   |  A   | \ Key-2
 MN-3---|      |    \                            /    |      |  \Traffic
        |      |      ==========================      |      |   \
 MN-4---|      |       Proxy Mobile IPv6 Tunnel       |      |    \
        +------+                                      +------+     \
                                                                    \
                   Operator-C: Access Network             +------------+
                                                          | Operator-B |
                                                          |            |
                                                          | 10.x.0.0/16|
                                                          +------------+
```

Figure 1: Overlapping IPv4 Private Address Space

Figure 1 illustrates a local mobility anchor providing mobility service to mobile nodes that are from different operators and are assigned IPv4 addresses from overlapping private address space. In this scenario, the mobile access gateway and the local mobility anchor must be able distinguish the flows belonging to a given operator from the flows belonging to some other operator.

The mobile nodes, MN-1 and MN-2 are visiting from Operator-A, and mobile nodes, MN-3 and MN-4 are visiting from Operator-B. The mobile access gateway and the local mobility anchor exchange a specific pair of downlink and uplink GRE keys and save them as part of the mobile node binding to be used for identifying the flows belonging to each mobile node.

The local mobility anchor and the mobile access gateway will be able to distinguish each mobile node flow(s) based on the GRE key present in the GRE header of the tunneled packet, and route them accordingly.

3.2. GRE Encapsulation Support

To request GRE encapsulation support without exchanging the GRE keys, the mobile access gateway MUST include the GRE Encapsulation Option in the Proxy Binding Update message sent to the local mobility anchor. The mobile access gateway MUST set the length field of the GRE encapsulation option to 2.

If the local mobility anchor supports GRE encapsulation and upon the successful process of the Proxy Binding Update, the LMA sends a Proxy Binding Acknowledgement and MUST include the GRE Encapsulation option with the length field set to 2.

However, If the local mobility anchor does not support GRE encapsulation, the LMA MUST reject the Proxy Binding Update by sending a Proxy Binding Acknowledgement message with the status field is set to TBA1 as defined in Section 6.2.

3.3. GRE Keys Exchange Mechanism

The following subsections describe how the mobile access gateway and the local mobility anchor exchange downlink and uplink GRE keys using proxy mobile IPv6 registration procedure. The mechanism for de-registering the GRE keys pair(s) is also described.

3.3.1. Initial GRE Keys Exchange

When the mobile access gateway determines based on, e.g., private IPv4 address overlapping [RFC1918] support, the MAG local policy, or MAG-LMA peer agreement that GRE encapsulation is needed and a new pair of GRE keys is required, the mobile access gateway MUST include the GRE Encapsulation Option in the Proxy Binding Update message sent to the local mobility anchor. The mobile access gateway MUST include the downlink GRE key in the GRE Key Identifier field.

Upon the successful process of the PBU and accepting the downlink GRE key, the LMA MUST include the uplink GRE key and echo the downlink included in the GRE Key Identifier field of the option. In this case, the first key is the downlink key while the second is the uplink key.

3.3.2. GRE Keys De-registration

If the GRE key option is present in the initial PBU, it MUST always be present in the re-registration or de-registration messages and with the same GRE key value.

If the local mobility anchor successfully process a deregistration

PBU message which contains a GRE Encapsulation option with a downlink GRE key included, the LMA follows the same session deregistration process as per the base Proxy Mobile IPv6 specification [ID-PMIP6] to clean the binding cache entry and the associated resources including the uplink GRE key. In the case that the deregistration PBU does not include the GRE encapsulation option and the corresponding mobile node session has been assigned downlink and uplink GRE keys, the LMA will follow the same process in cleaning the associated resources including the GRE keys. The mechanism that the LMA uses for reassigning the uplink GRE keys for other sessions is implementation specific and out of scope.

4. Mobile Access Gateway Considerations

4.1. Extensions to the Conceptual Data Structure

Every mobile access gateway maintains a Binding Update List entry for each currently attached mobile node, as explained in Section 6.1 of the base Proxy Mobile IPv6 specification [ID-PMIP6]. To support this specification, the conceptual Binding Update List entry data structure must be extended with the following three new additional fields.

- A flag indicating whether GRE encapsulation is enabled for the mobile node's traffic flows.

- The Downlink GRE Key used in the GRE encapsulation header of the tunneled packet from the local mobility anchor to the mobile access gateway that is destined to the mobile node. This GRE Key is generated by the MAG and communicated to the LMA in the GRE Encapsulation option in the PBU message.

- The Uplink GRE Key used in the GRE encapsulation header of the tunneled packet from the mobile access gateway to the local mobility anchor that is originating from the mobile node. This GRE Key is obtained from the GRE Key Identifier field of the GRE Encapsulation option present in the received PBA message sent by the LMA as specified in this document.

4.2. Operational Summary

- If IPv4 Home Address support is enabled for the mobile node and if the IPv4 Home Address Option is included in the Proxy Binding Update message that is sent by the mobile access gateway to the mobile node's local mobility anchor, the GRE Encapsulation Option MAY be included in the Proxy Binding Update message. In order to exchange GRE keys, the MAG MUST include the downlink GRE key in

the GRE Key Identifier field.

- After receiving a Proxy Binding Acknowledgment message with the status code indicating the acceptance of the Proxy Binding Update message and with the GRE Encapsulation Option with both the downlink and uplink GRE keys, the mobile access gateway MUST update the related three fields in the mobile node Binding Update List entry described in Section 4.1. Additionally, the MAG MUST use the assigned uplink GRE Key for tunneling all the traffic originating from the mobile node.

- For a given mobile node, if the local mobility anchor rejects the Proxy Binding Update by sending the Proxy Binding Acknowledgement with the status code TBA1 (GRE Encapsulation not supported), the mobile access gateway MUST NOT include the GRE Encapsulation Option in the subsequent Proxy Binding Update messages that are sent to that LMA.

- If the mobile access gateway has sent a Proxy Binding Update message without the GRE Encapsulation Option, but the received Proxy Binding Acknowledgement has the Status Code TBA2, indicating that the GRE encapsulation is required, the mobile access gateway SHOULD resend the Proxy Binding Update message with the GRE Encapsulation Option.

- On receiving a packet from the tunnel with the GRE encapsulation header, the mobile access gateway MUST use the GRE Key to determine the necessary special processing for the data packet, e.g., lookup the mobile node's layer-2 address, determine any special processing or treatment for the data packet flow, before forwarding the packet after removing the encapsulation headers.

5. Local Mobility Anchor Considerations

5.1. Extensions to the Binding Cache Entry

When the local mobility anchor and the mobile access gateway successfully negotiates GRE encapsulation and exchange downlink and uplink GRE keys, the local mobility anchor MUST maintain the downlink and uplink GRE keys as part of the mobile node BCE. This requires that the BCE described in section 5.1 of the Proxy Mobile IPv6 base specification [ID-PMIP6] is extended. To support this specification, the BCE must be extended with the following three additional fields.

- A flag indicating whether GRE encapsulation is enabled for the mobile node's traffic flows.

- The Downlink GRE Key, assigned by the MAG and used in the GRE encapsulation header of the tunneled packet from the local mobility anchor to the mobile access gateway.

- The Uplink GRE Key, assigned by the LMA and used in the GRE encapsulation header of the tunneled packet from the mobile access gateway to the local mobility anchor.

5.2. Operational Summary

- Upon receiving a Proxy Binding Update message with the GRE Encapsulation Option, the local mobility anchor, if it does not support GRE encapsulation mode, MUST send the Proxy Binding Acknowledgement message to the mobile access gateway with the status code TBA1 as defined in Section 6.2.

- Upon the successful process of a Proxy Binding Update message with the GRE Encapsulation Option with the downlink GRE key included in the GRE Key Identifier field, the local mobility anchor MUST include the GRE Encapsulation option with the downlink and uplink GRE keys in the GRE Key Identifier field when responding with a successful PBA message. When GRE Key Identifier field carries the downlink and uplink GRE keys, the first key is always set to the downlink GRE key.

- If the GRE tunneling is negotiated and the downlink and uplink GRE keys have been exchanged between the local mobility anchor and the mobile access gateway, every packet that is destined to the mobile node through the local mobility anchor MUST be encapsulated with a GRE header using the negotiated downlink GRE key.

- If the received Proxy Binding Update message does not contain the GRE Encapsulation Option, and if the local mobility anchor determines that GRE encapsulation is required, e.g., overlapping IPv4 private addressing is in use, LMA local policy, the local mobility anchor MUST reject the request, and MUST send the Proxy Binding Acknowledgement message to the mobile access gateway with the status code TBA2, indicating that GRE encapsulation is required.

- On receiving a packet from the tunnel with the GRE encapsulation header, the local mobility anchor MUST use the GRE Key present in the GRE extension header to determine the necessary special processing for the data packet, e.g., lookup the mobile node's home gateway address, determine any special processing or treatment for the data packet flow, before forwarding the packet after removing the encapsulation headers.

6. Message Formats

This section defines an extension to the Mobile IPv6 [RFC3775] protocol messages for supporting the GRE tunneling and GRE Keys exchange for Proxy Mobile IPv6.

6.1. GRE Encapsulation Option

A new option, the GRE Encapsulation Option, is defined for use in the Proxy Binding Update and Proxy Binding Acknowledgment messages exchanged between the mobile access gateway and the local mobility anchor. This option can be used for negotiating GRE encapsulation and exchanging the GRE keys to be applied by the peer on all GRE encapsulated packets for the specified mobile node session or flow.

The alignment requirement for this option is 4n.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |      Type     |   Length      |           Reserved            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                      GRE Key Identifier                       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: GRE Encapsulation Option

Type

<IANA>

Length

8-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. If the Length field is set to 2, it indicates that the GRE keys are not being carried in the option. If the length field is set to a value of 6 or 10, it means that down link GRE key or downlink and uplink GRE keys are carried, respectively.

Reserved

These fields are unused. They MUST be initialized to zero by the sender and MUST be ignored by the receiver.

GRE Key Identifier

32-bit field containing the Downlink GRE Key, or 64-bit field containing the Downlink and Uplink GRE keys. This field is present in the mobility option only if the GRE keys are being exchanged using the PBU and PBA messages.

6.2. Status Codes

The following status code values are defined for using them in the Binding Acknowledgment message when using Proxy Mobile IPv6 protocol. The value allocation for this usage needs to be approved by the IANA and must be updated in the IANA registry.

TBA1: GRE Encapsulation not required.

TBA2: GRE Encapsulation and GRE Key Identifier option required.

7. IANA Considerations

This document defines a new Option, the GRE Encapsulation Option, described in Section 6.1. This option is carried in the Mobility Header. The type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options defined in the Mobile IPv6 specification [RFC3775].

This document also defines two new Binding Acknowledgement status codes TBA1 and TBA2 as described in Section 6.2. This document requests that these two codes be allocated from the "Status Codes" registry of the Mobility IPv6 Parameters located at http://www.iana.org/assignments/mobility-parameters and that the numeric value of these codes be greater than 128.

8. Security Considerations

The GRE Encapsulation Option, defined in this document, that can be carried in Proxy Binding Update and Proxy Binding Acknowledgement messages, reveals the group affiliation of a mobile node identified by its NAI or an IP address. It may help an attacker in targeting flows belonging to a specific group. This vulnerability can be prevented, by enabling confidentiality protection on the Proxy Binding Update and Acknowledgement messages where the presence of the NAI and GRE Encapsulation Options establish a mobile node's relation to a specific group. This vulnerability can also be avoided by enabling confidentiality protection on all the tunneled data packets

between the mobile access gateway and the local mobility anchor, for hiding all the markings.

9. Acknowledgements

The authors would like to thank Allesio Casati, Barney Barnowski, Mark Grayson and Parviz Yegani for their input on the need for this option. The authors would like to thank Curtis Provost, Irfan Ali, Julien Langanier, Jouni Korhonen, Suresh Krishnan, Kuntal Chowdhury, and Vijay Devarapalli for their review and comments.

10. Normative References

[ID-PMIP6]
Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-18 (work in progress), May 2008.

[ID-PMIP6-IPv4]
Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", draft-ietf-netlmm-pmip6-ipv4-support-03 (work in progress), May 2008.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

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

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, September 2000.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

Authors' Addresses

Ahmad Muhanna
Nortel
2221 Lakeside Blvd.
Richardson, TX 75082
USA

Email: amuhanna@nortel.com

Mohamed Khalil
Nortel
2221 Lakeside Blvd.
Richardson, TX 75082
USA

Email: mkhalil@nortel.com

Sri Gundavelli
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Kent Leung
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
USA

Email: kleung@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).