GRE Key Option for Proxy Mobile IPv6
draft-muhanna-netlmm-grekey-option-02.txt

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 October 16, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

The Proxy Mobile IPv6 base specification defined in [PMIP6-ID] allows the mobile node’s IPv4 and IPv6 traffic between the local mobility anchor and the mobile access gateway to be tunneled using IPv6, IPv4 or IPv4-UDP encapsulation headers. These encapsulation modes do not offer semantics for the tunnel end-points 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 extensions defined in this document allow the mobile access gateway and the local mobility anchor to negotiate GRE encapsulation mode and along with the GRE symmetric key or asymmetric keys for marking the flows, so that differential processing can be applied by the tunnel peers over those flows.

Table of Contents

1. Introduction ..................................................... 3
2. Conventions used in this document .............................. 3
3. Protocol Overview ............................................... 3
4. Local Mobility Anchor Considerations .......................... 5
   4.1. GRE Tunneling and Encapsulation Procedures ............... 5
   4.2. Operational Summary ..................................... 6
5. Mobility Access Gateway Considerations ....................... 6
   5.1. Extensions to the Conceptual Data Structure .............. 7
   5.2. Operational Summary .................................. 8
6. Message Formats .................................................. 9
   6.1. GRE Key Identifier Option ................................ 9
   6.2. Status Codes ........................................... 10
7. IANA Considerations ............................................. 11
8. Security Considerations ....................................... 11
9. Acknowledgements ............................................. 11
10. References ..................................................... 11
   10.1. Normative References .................................. 12
   10.2. Informative References ................................. 12
Authors’ Addresses .................................................. 12
Intellectual Property and Copyright Statements .................. 14
1. Introduction

The base Proxy Mobile IPv6 specification allows the use of IPv6, IPv4 or IPv4-UDP encapsulation modes for the tunneled traffic between the local mobility anchor and the mobile access gateway. There are scenarios where these encapsulation modes are not sufficient and there is a need for an encapsulation mode with richer semantics. The Generic Routing Encapsulation [RFC-2784] and coupled with the Key and Sequence Number extension [RFC-2890], has the required semantics for use in Proxy Mobile IPv6.

This document defines extensions to the base Proxy Mobile IPv6 specification, for allowing the mobile access gateway and the local mobility anchor to negotiate GRE encapsulation mode and for exchanging the GRE symmetric or asymmetric key(s) that can be used for marking the forward and reverse traffics.

2. Conventions used in this document

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 RFC 2119 [4].

All the general mobility related terminology and abbreviations are to be interpreted as defined in Mobile IPv6 specification [RFC-3775] and Proxy Mobile IPv6 specification [PMIP6-SPEC].

Forward Direction 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.

Reverse Direction 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.

3. Protocol Overview

Using the extension defined in this specification, the mobile access gateway and the local mobility anchor can negotiate GRE encapsulation mode along with the GRE keys for marking the forward and reverse
traffics.

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

![Figure 1: Overlapping IPv4 Private Address Space](image-url)
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 agree upon a key(s) for identifying the flows belonging to each mobile node.

The local mobility anchor and the mobile access gateway will be able to distinguish these flows based on the key present in the GRE header of the tunneled packet, and can route them accordingly.

4. Local Mobility Anchor Considerations

4.1. GRE Tunneling and Encapsulation Procedures

As per the base Proxy Mobile IPv6 specification, the tunnel transport between the mobile access gateway and the local mobility anchor can be IPv6, IPv4 or IPv4-UDP. When GRE tunneling is negotiated as per this specification, the semantics related to the tunnel transport is not impacted, but an additional GRE header is added above the payload packet as indicated below.

```
+---------------------------+                      +---------------------------+
|     Delivery Header       |                      |                           |
| IPv4, IPv4-UDP or IPv6   |                      |       Payload Packet      |
|                           |                      |  (IPv4 or IPv6)           |
+---------------------------+                      +---------------------------+
                     ===>                             ===>
+---------------------------+                      +---------------------------+
| GRE Header with Key,      |                      | Payload Packet            |
| Sequence Number Ext       |                      |                           |
+---------------------------+                      +---------------------------+
                                     | Payload Packet
```

4.2. Operational Summary

- Upon receiving a Proxy Binding Update message with the GRE Key Identifier 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 148, (GRE Encapsulation not supported).

- If the received Proxy Binding Update message does not contain the GRE Key Identifier Option, and if the local mobility anchor determines that overlapping IPv4 private addressing is in use, 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 149, indicating that GRE encapsulation is required.

- Upon receiving a Proxy Binding Update message with the GRE Key Identifier Option, the local mobility anchor, if it determines that overlapping private IPv4 addressing is not in use, MUST send the Proxy Binding Acknowledgement message to the mobile access gateway with the status code success without including the GRE Key Identifier option.

- If the GRE tunneling is negotiated between the local mobility anchor and the mobile access gateway, every packet that is originating from the mobile node’s home gateway, MUST be encapsulated with a GRE header, and MUST use the negotiated forward direction GRE key and with the chosen transport header such as IPv4, IPv4-UDP or IPv6, just as per the base Proxy Mobile IPv6 specification.

- 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 lookup the mobile node’s home gateway address for forwarding the packet after removing the encapsulation headers.

5. Mobility Access Gateway Considerations

For requesting the GRE Tunneling support, the mobile access gateway MUST include the GRE Key Identifier Option in the Proxy Binding Update message sent to the local mobility anchor. In case the mobile
access gateway local policy requires the MAG to generate the forward direction GRE key, the MAG must include the forward key in the GRE key Identifier Option. Optionally, the MAG may set the GRE key Identifier field in the GRE key Identifier Option to zero to indicate that the MAG will accept either symmetric or asymmetric GRE keys as specified by the LMA. In the case the MAG requires the LMA to specify two asymmetric keys, the MAG will set the GRE Key Identifier field in the GRE Key Identifier option to all-ones. In the case of symmetric keys, the LMA must return one single key in the GRE Key Identifier option. However, in the case of asymmetric GRE keys, the LMA must send two GRE keys in the GRE Key Identifier option, with the first key being the forward direction key and the second is the reverse direction key. In the latter case, the GRE Key Identifier option length MUST be set to 10.

5.1. Extensions to the Conceptual Data Structure

Every mobile access gateway maintains a Binding Update List for each currently attached mobile node, as explained in Section 6.2 of the base Proxy Mobile IPv6 specification [PMIP6-SPEC]. The Binding Update List is a conceptual data structure, described in Section 11.1 of the Mobile IPv6 base specification [RFC-3775]. For supporting this specification, the conceptual Binding Update List data structure must be extended with the following two new additional fields related to bi-directional GRE Key identifiers used for tagging the mobile node’s tunneled traffic.

- A flag indicating whether GRE encapsulation is enabled for the mobile node’s traffic flows.
- The Reverse GRE Key Identifier used in the GRE encapsulation header of the tunneled packet from the mobile access gateway to the local mobility anchor and that is originating from the mobile node. This GRE Key identifier is obtained from the GRE Key Identifier Option present in the received Proxy Binding Acknowledgement message sent by the local mobility anchor as specified in this document.
- The Forward GRE Key Identifier used in the GRE encapsulation header of the tunneled packet from the local mobility anchor to the mobile access gateway and that is destined to the mobile node. This GRE Key identifier may be a locally configured key or as specified by the LMA as per this specification. This key identifier may be the same as the reverse direction key used for the outgoing flows from the mobile access gateway to the local mobility anchor.
5.2.  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 Key Identifier Option SHOULD be included in the Proxy Binding Update message. If the MAG includes the forward key in the GRE Key Identifier Option, the local mobility anchor must use this key to identify the mobile node’s traffic encapsulated in a GRE header as specified in the GRE specification [RFC-2784] and using the GRE Key and Sequence Number extension [RFC-2890] with the assigned GRE key.

- After receiving a Proxy Binding Acknowledgment message with the status code indicating the acceptance of the Proxy Binding Update message and with the GRE Key Identifier Option, the mobile access gateway MUST use GRE encapsulation and the assigned Reverse GRE Key for tunneling all the traffic originating from the mobile node.

- For a given mobile nodes, if the local mobility anchor rejects the Proxy Binding Update by sending the Proxy Binding Acknowledgement with the status code 148 (GRE Encapsulation not supported), the mobile access gateway MUST NOT include the GRE Key Identifier Option in the subsequent Proxy Binding Update messages that are sent to that Local Mobility Anchor.

- If the mobile access gateway has sent a Proxy Binding Update message with out the GRE Key Identifier Option, but the received Proxy Binding Acknowledgement has the Status Code 149, indicating that the GRE encapsulation is required, the mobile access gateway SHOULD resend the Proxy Binding Update message with the GRE Key Identifier Option.

- If the mobile access gateway has sent a Proxy Binding Update message with the GRE Key Identifier Option, but the received Proxy Binding Acknowledgement has the Status Code success without the GRE Key Identifier option, indicating that the GRE encapsulation is not required for this mobile node, the mobile access gateway must not use GRE encapsulation for this Mobile node.

- If the GRE tunneling is negotiated between the local mobility anchor and the mobile access gateway, every packet originating from the mobile node MUST be encapsulated with a GRE header using the Reverse GRE key and the chosen transport header such as IPv4, IPv4-UDP or IPv6, just as per the base Proxy Mobile IPv6 specification.
One receiving a packet from the tunnel with the GRE encapsulation header, the mobile access gateway MUST use the GRE Key to lookup the mobile node’s layer-2 address and use it for forwarding the packet after removing the encapsulation headers.

6. Message Formats

This section defines extensions to the Mobile IPv6 [RFC-3775] protocol messages for supporting this specification.

6.1. GRE Key Identifier Option

A new option, the GRE Key Identifier Option, is defined for use in the Proxy Binding Update and Acknowledgment messages exchanged between the mobile access gateway and the local mobility anchor. This option can be used for exchanging the GRE key to be applied by the peer on all GRE encapsulated packets over either IPv4 or IPv6 transport.

The alignment requirement for this option is 4n.
Type

<IANA>

Length

Eight-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. This is set to a value of 6 or 10.

Reserved

This field is reserved for future use. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

GRE Key Identifier

A four-byte field containing the Reverse GRE Key Identifier. or eight-byte containing the Forward and Reverse GRE keys respectively. The values of zero and all-ones are reserved.

Figure 3: GRE Key Identifier Option

6.2. Status Codes

Proxy Binding Acknowledgment Status Values

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.

148: GRE Encapsulation not required.

149: GRE Encapsulation is required. GRE Key Identifier option
required.

Status values less than 128 indicate that the Binding Update was processed successfully by the receiving nodes. Values greater than 128 indicate that the Binding Update was rejected by the Home Agent.

7. IANA Considerations

This document defines a new Option, the GRE Key Option, described in Section 3. 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 [RFC-3775].

8. Security Considerations

The GRE Key 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 Key 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 Barowsky, Mark Grayson and Parviz Yegnani for their input on the need for this option. The authors would like to thank Curtis Provost for his detailed review and comments.

10. References
10.1. Normative References


10.2. Informative References


Authors’ Addresses

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

Email: amuhanna@nortel.com

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

Email: mkhalil@nortel.com

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

Email: sgundave@cisco.com

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

Email: kleung@cisco.com