Internet Engineering Task Force (IETF)
Request for Comments: 5845
Category: Standards Track
ISSN: 2070-1721

A. Muhanna
M. Khalil
Ericsson
S. Gundavelli
K. Leung
Cisco

June 2010

Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6

Abstract

This specification defines a new mobility option for allowing the mobile access gateway and the local mobility anchor to negotiate Generic Routing Encapsulation (GRE) encapsulation mode and exchange the downlink and uplink GRE keys that are used for marking the downlink and uplink traffic that belong to a specific mobility session. In addition, the same mobility option can be used to negotiate the GRE encapsulation mode without exchanging the GRE keys.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5845.

Table of Contents

1. Introduction

The Proxy Mobile IPv6 specification [RFC5213] and IPv4 Support for Proxy Mobile IPv6 [RFC5844] allow the use of IPv6 and IPv4 encapsulation modes as specified in [RFC2473] and [RFC2003] for the tunneled traffic between the local mobility anchor (LMA) and the mobile access gateway (MAG). There are scenarios where these encapsulation modes are not sufficient to uniquely identify the destination of packets of a specific mobility session. Thus, there is a need for an encapsulation mode with richer semantics. The Generic Routing Encapsulation (GRE) [RFC2784], and the Key extension as defined in [RFC2890], has the required semantics to allow such a distinction for use in Proxy Mobile IPv6.

This specification defines the GRE Key option to be used for the negotiation of GRE encapsulation mode and exchange of the uplink and downlink GRE keys. The negotiated downlink and uplink GRE keys can be used for marking the downlink and uplink traffic for a specific mobility session. In addition, this specification enables the mobile access gateway and the local mobility anchor to negotiate the use of GRE encapsulation mode without exchanging the GRE keys.

This specification has no impact on IPv4 or IPv6 mobile nodes.

2. Conventions and Terminology

2.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Terminology

All the general mobility-related terminology and abbreviations are to be interpreted as defined in the Mobile IPv6 [RFC3775], Proxy Mobile IPv6 [RFC5213], and IPv4 Support for Proxy Mobile IPv6 [RFC5844] specifications. The following terms are used in this specification.

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 called 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 called 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 that belongs to a specific mobility session as described in this specification.

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 that belongs to a specific mobility session as described in this specification.

A Policy Check

When a local mobility anchor receives an initial, handoff-triggered Binding Lifetime Extension, or Binding Lifetime Extension Proxy Binding Update for a mobility session, the local mobility anchor determines if the GRE encapsulation mode only or GRE encapsulation and GRE keys are required based on a policy check. This policy could be a per-MAG-LMA pair, a per-LMA local policy, a per-MN policy, or the combination of any of them.

3. GRE Encapsulation and Key Exchange

This section describes how GRE encapsulation mode is negotiated and the GRE keys are dynamically exchanged using Proxy Mobile IPv6 protocol [RFC5213] signaling.

3.1. GRE Encapsulation Overview

Using the GRE Key option defined in this specification, the mobile access gateway and the local mobility anchor can negotiate GRE encapsulation mode only or GRE encapsulation mode and exchange the GRE keys for marking the downlink and uplink traffic. In the case when GRE encapsulation mode only is negotiated between the mobile access gateway and the local mobility anchor, then no GRE keys are used.

However, once the GRE keys have been exchanged between the mobile access gateway and the local mobility anchor as per this specification, the mobile access gateway will use the uplink GRE key that is assigned by the local mobility anchor in the GRE 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 header of the downlink payload packet.

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

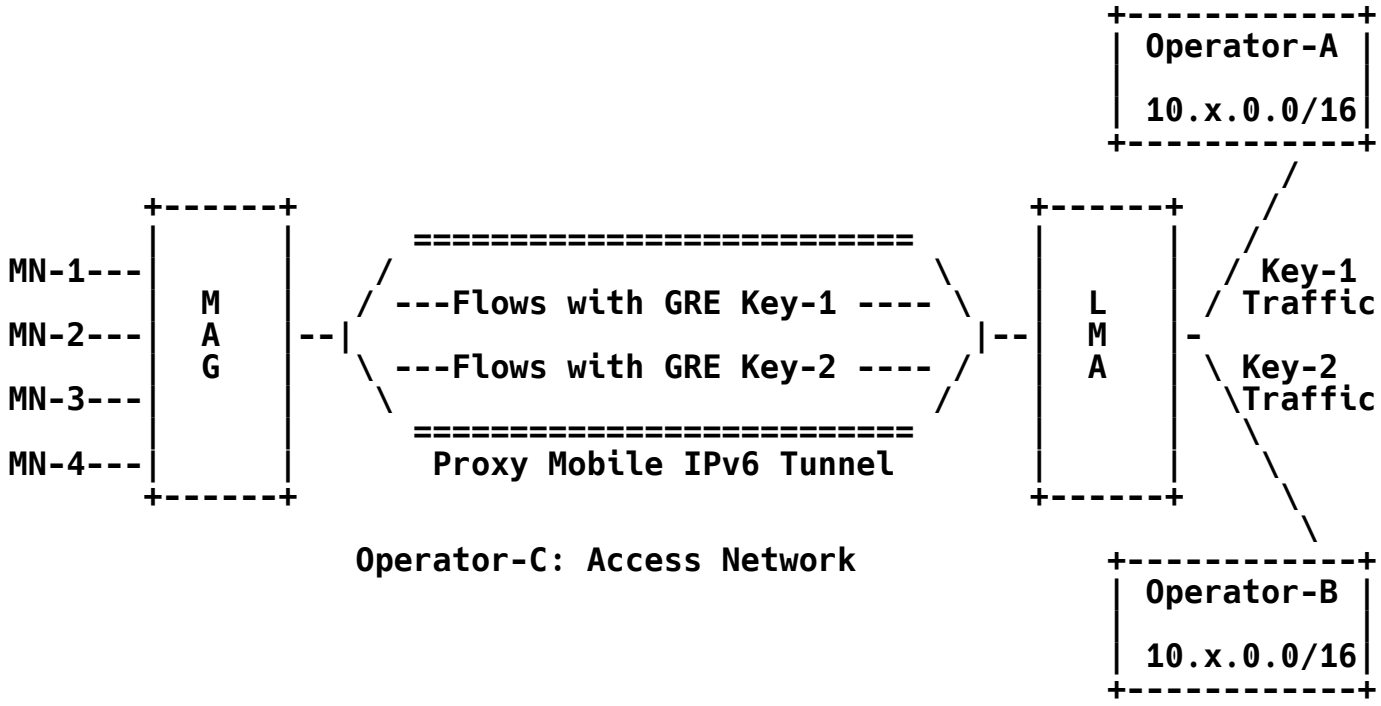

Figure 1: GRE Tunneling for IPv4 Private Address Space Overlapping

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 to distinguish flows belonging to different operators.

The mobile nodes MN-1 and MN-2 are visiting from Operator-A, and the 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's binding to be used for identifying the flows belonging to each mobile node.

The LMA and the MAG will be able to distinguish each mobile node flow(s) based on the GRE key present in the GRE header of the tunneled payload packet, and route them accordingly. However, the GRE keys, as in this specification, apply to the individual mobility binding updated by the Proxy Binding Update but not to all bindings that the mobile may have registered following procedures described in [RFC5648].

3.2. GRE Encapsulation Mode Only

In order for the mobile access gateway to request GRE encapsulation mode only without exchanging the GRE keys, the mobile access gateway MUST include the GRE Key option but omit the GRE Key Identifier field in the Proxy Binding Update.

If the local mobility anchor supports GRE encapsulation and the received Proxy Binding Update contains the GRE Key option but the GRE Key Identifier field is omitted, the mobile access gateway is requesting GRE encapsulation without exchanging the GRE keys dynamically. If the Proxy Binding Update processing is successful, the local mobility anchor sends a successful Proxy Binding Acknowledgement message with the GRE Key option but the GRE Key Identifier field is omitted.

When the mobile access gateway and the local mobility anchor successfully negotiate the GRE encapsulation mode only, then no GRE keys are used.

3.3. GRE Encapsulation and Key Exchange

The following subsections describe how the mobile access gateway and the local mobility anchor negotiate GRE encapsulation and exchange downlink and uplink GRE keys using the Proxy Mobile IPv6 registration procedure.

3.3.1. Initial GRE Key Exchange

When the mobile access gateway determines, based on, e.g., private IPv4 address support [RFC1918], the mobile access gateway local policy, or the MAG-LMA peer agreement, that GRE encapsulation is needed and GRE keys are required, the mobile access gateway MUST include the GRE Key option in the initial 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 of the GRE Key option.

After the local mobility anchor successfully processes the initial Proxy Binding Update and accepts the GRE encapsulation request and the downlink GRE key based on a policy check, the local mobility anchor MUST include the GRE Key option with the uplink GRE key in the GRE Key Identifier field in a successful Proxy Binding Acknowledgement and send it to the mobile access gateway.

3.3.2. GRE Key Exchange during Binding Re-Registration

If the local mobility anchor has successfully negotiated and exchanged the initial GRE keys with the mobile access gateway for a specific mobile node's mobility session, the local mobility anchor MUST maintain the same negotiated uplink GRE key for the lifetime of that mobility session. However, for administrative reasons, e.g., local mobility anchor reboot, the local mobility anchor MAY change the uplink GRE key for the mobility session. In that case, some packet loss may be experienced.

If the mobile access gateway has successfully negotiated and exchanged the initial GRE keys with the local mobility anchor for a specific mobile node's mobility session, the mobile access gateway MUST include the GRE Key option with the downlink GRE key in the Proxy Binding Update that is used to request a Binding Lifetime Extension. In this case, if the local mobility anchor successfully processes the Proxy Binding Update message, the local mobility anchor MUST return the same uplink GRE key that was exchanged with the mobile access gateway in the last successful Proxy Binding Update for the same mobility session in the GRE Key option in a successful Proxy Binding Acknowledgement message.

However, during inter-MAG handoff and if the new mobile access gateway determines, based on, e.g., private IPv4 address support, the mobile access gateway local policy, the MAG-LMA peer agreement, or an indication during the handoff process, that GRE encapsulation and GRE keys exchange are required, the new mobile access gateway MUST include the GRE Key option with the downlink GRE key in the Proxy Binding Update that is used to request an after-handoff Binding Lifetime Extension. In this case, the new mobile access gateway may either pick a new downlink GRE key or use the downlink GRE key that was used by the previous mobile access gateway for the same binding. For the new mobile access gateway to know the downlink GRE key used by the previous mobile access gateway, it may require transfer of

context from the previous mobile access gateway to the new mobile access gateway during a handoff. Such mechanisms are out of scope for this specification.

If the local mobility anchor successfully processes a handoff-triggered Binding Lifetime Extension Proxy Binding Update message that contains a GRE Key option with a downlink GRE key included, the local mobility anchor MUST return the same uplink GRE key that was exchanged with the previous mobile access gateway for the same mobility session in the GRE Key option in a successful Proxy Binding Acknowledgement.

If the local mobility anchor receives a handoff-triggered Binding Lifetime Extension Proxy Binding Update message without the GRE Key option for a Binding Cache entry (BCE) that is using GRE keys and GRE encapsulation, the local mobility anchor makes a policy check regarding GRE encapsulation and GRE key exchange. If, according to the policy check, GRE encapsulation and GRE key exchange are required, the local mobility anchor MUST reject the Proxy Binding Update by sending a Proxy Binding Acknowledgement message with the Status field set to GRE_KEY_OPTION_REQUIRED as defined in Section 6.4. Otherwise, the local mobility anchor SHOULD accept the Proxy Binding Update, and if it is processed successfully, the local mobility anchor MUST return a successful Proxy Binding Acknowledgement without including the GRE Key option.

4. Mobile Access Gateway Considerations

4.1. Extensions to the Conceptual Data Structure

Every mobile access gateway maintains a Binding Update List (BUL) entry for each currently attached mobile node, as explained in Section 6.1 of the Proxy Mobile IPv6 specification [RFC5213]. To support this specification, the conceptual Binding Update List entry data structure must be extended with the following four new additional fields.

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

- The downlink GRE key used in the GRE encapsulation header of the tunneled payload 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 mobile access gateway and communicated to the local mobility anchor in the GRE Key option in the Proxy Binding Update message.

- The uplink GRE key used in the GRE encapsulation header of the tunneled payload 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 Key option present in the received Proxy Binding Acknowledgement message sent by the local mobility anchor as specified in this document.

- A flag indicating whether UDP-based TLV-header format (Section 7.2) is enabled for the mobile node's traffic. This flag is TRUE only when UDP tunneling as in [RFC5844] and GRE encapsulation as in this specification are both enabled for this mobility session.

4.2. Operational Summary

- If the mobile access gateway determines that GRE encapsulation mode only is required, the mobile access gateway MUST include the GRE Key option but omit the GRE Key Identifier field in the Proxy Binding Update message that is sent to the local mobility anchor.

- If the mobile access gateway determines that GRE encapsulation and GRE keys are required, the mobile access gateway MUST include the GRE Key option with the downlink GRE key in the GRE Key Identifier field in the Proxy Binding Update message that is sent to the local mobility anchor.

- After receiving a successful Proxy Binding Acknowledgement message with the GRE Key option with the GRE Key Identifier field omitted, the mobile access gateway MUST update the mobile node's Binding Update List entry described in Section 4.1 by only setting the GRE-encapsulation-enabled flag.

- After receiving a successful Proxy Binding Acknowledgement message with the GRE Key option and the uplink GRE key included in the GRE Key Identifier field, the mobile access gateway MUST update the related fields in the mobile node's Binding Update List entry described in Section 4.1. Additionally, the mobile access gateway MUST use the assigned uplink GRE Key for tunneling all the traffic that belongs to this mobile node BUL entry and that originated from the mobile node before forwarding the tunneled traffic to the local mobility anchor.

- If the mobile access gateway includes the GRE Key option in the Proxy Binding Update for a specific mobile node and the local mobility anchor accepts the Proxy Binding Update by sending a Proxy Binding Acknowledgement with a success status code (less than 128) other than GRE_KEY_OPTION_NOT_REQUIRED, but without the

GRE Key option, then the mobile access gateway MUST consider that the local mobility anchor does not support the GRE Key option as per this specification. The mobile access gateway SHOULD NOT include the GRE Key option in any subsequent Proxy Binding Update message that is sent to that local mobility anchor.

- If the mobile access gateway sent a Proxy Binding Update message without the GRE Key option, but the received Proxy Binding Acknowledgement has the status code GRE_KEY_OPTION_REQUIRED, indicating that GRE encapsulation and GRE keys are required, the mobile access gateway SHOULD resend the Proxy Binding Update message with the GRE Key option. If the mobile access gateway does not support the GRE Key option, it MAY log the event and possibly raise an alarm to indicate a possible misconfiguration.

- If the mobile access gateway sent a Proxy Binding Update message with the GRE Key option and the downlink GRE key included and received a successful Proxy Binding Acknowledgement message with the status code GRE_KEY_OPTION_NOT_REQUIRED, the mobile access gateway MUST consider that GRE encapsulation and GRE keys are not required for this specific mobility session. The mobile access gateway follows procedures in the Proxy Mobile IPv6 specification [RFC5213] for the handling of uplink and downlink traffic and MUST NOT include the GRE Key option in any subsequent Proxy Binding Update message that is sent to the local mobility anchor for this mobility session.

- If the mobile access gateway has successfully negotiated GRE encapsulation and exchanged the GRE keys with the local mobility anchor for a specific mobility session, the mobile access gateway SHOULD NOT include the GRE Key option in the de-registration Proxy Binding Update.

- On receiving a packet from the tunnel with the GRE header, the mobile access gateway MUST use the GRE key present in the GRE extension header as an additional identifier to determine to which mobility session this packet belongs. The GRE header is removed before further processing takes place.

5. Local Mobility Anchor Considerations

5.1. Extensions to the Binding Cache Entry

When the local mobility anchor and the mobile access gateway successfully negotiate 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's BCE. This requires the BCE described in Section 5.1 of the Proxy Mobile IPv6

specification [RFC5213] to be extended. To support this specification, the BCE must be extended with the following four additional fields.

- A flag indicating whether GRE encapsulation is enabled for the mobile node's traffic flows.
- The downlink GRE key, assigned by the mobile access gateway and used in the GRE encapsulation header of the tunneled payload packet from the local mobility anchor to the mobile access gateway.
- The uplink GRE key, assigned by the local mobility anchor and used in the GRE encapsulation header of the tunneled payload packet from the mobile access gateway to the local mobility anchor.
- A flag indicating whether UDP-based TLV-header format (Section 7.2) is enabled for the mobile node's traffic. This flag is TRUE only when UDP tunneling as in [RFC5844] and GRE encapsulation as in this specification are both enabled for this mobility session.

5.2. Operational Summary

- If the local mobility anchor successfully processes a Proxy Binding Update message with the GRE Key option, but the GRE Key Identifier field is omitted for initial GRE key exchange, the local mobility anchor MUST include the GRE Key option but omit the GRE Key Identifier field when responding with a successful Proxy Binding Acknowledgement message.
- If the local mobility anchor successfully processes a Proxy Binding Update message with the GRE Key option and the downlink GRE key included in the GRE Key Identifier field for initial GRE key exchange as in Section 3.3.1, the local mobility anchor MUST include the GRE Key option with the uplink GRE key included in the GRE Key Identifier field when responding with a successful Proxy Binding Acknowledgement message.
- If the GRE tunneling is negotiated and the downlink and uplink GRE keys have been exchanged between the mobile access gateway and the local mobility anchor for a specific mobility session, the local mobility anchor MUST use the negotiated downlink GRE key in the GRE header of every packet that is destined to the mobile node of this specific mobility session over the GRE tunnel to the mobile access gateway.

- If the received Proxy Binding Update message does not contain the GRE Key option, and if the local mobility anchor based on a policy check determines that GRE encapsulation and GRE keys are required, e.g., overlapping IPv4 private addressing is in use, a local mobility anchor local policy, or LMA-MAG peer agreement, the local mobility anchor MUST reject the request and send a Proxy Binding Acknowledgement message to the mobile access gateway with the status code GRE_KEY_OPTION_REQUIRED as defined in Section 6.4. This indicates that GRE encapsulation and GRE keys are required.

- If, after receiving and successfully processing a Proxy Binding Update message with the GRE Key option, the local mobility anchor determines, based on a policy check, that GRE encapsulation and GRE keys are not required for this specific binding, e.g., private IPv4 addressing is not in use, the local mobility anchor SHOULD send a successful Proxy Binding Acknowledgement message to the mobile access gateway with the status code GRE_KEY_OPTION_NOT_REQUIRED. In this case, the local mobility anchor MUST NOT include the GRE Key option in the Proxy Binding Acknowledgement.

- If the local mobility anchor successfully processes a de-registration Proxy Binding Update message, the local mobility anchor follows the same de-registration process as described in the Proxy Mobile IPv6 specification [RFC5213] to clean the Binding Cache entry and all associated resources including the downlink and uplink GRE keys.

- On receiving a packet from the tunnel with the GRE header, the local mobility anchor MUST use the GRE key in the GRE extension header as an additional identifier to determine to which mobility session this packet belongs. The GRE header is removed before further processing takes place.

6. Message Formats

This section defines an extension to the Mobile IPv6 protocol [RFC3775] messages. The use of the GRE Key option for supporting GRE tunneling and GRE key exchange for Proxy Mobile IPv6 is defined in this specification.

6.1. GRE Key Option

A new mobility option, the GRE Key option, is defined for use in the Proxy Binding Update and Proxy Binding Acknowledgement messages exchanged between the mobile access gateway and the local mobility anchor. This option can be used for negotiating GRE encapsulation mode only or GRE encapsulation and exchanging the downlink and uplink

GRE keys. These GRE keys can be used by the peers in all GRE encapsulated payload packets for marking that specific mobile node's data traffic.

The alignment requirement for this option is 4n.

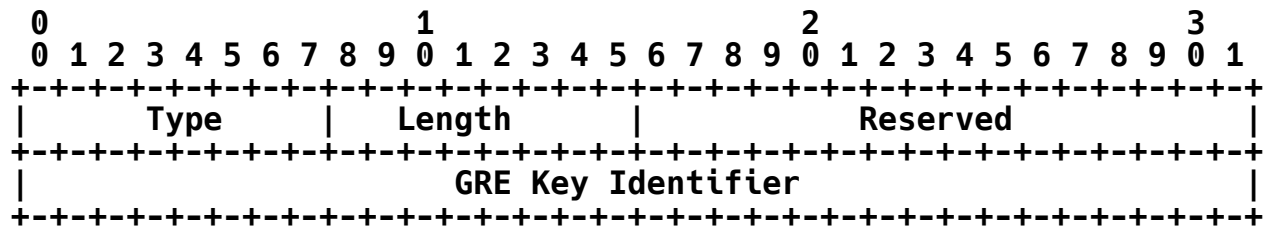

Figure 2: GRE Key Option

Type

33

Length

An 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 Key Identifier field is not being carried in the option. If the Length field is set to a value of 6, it means that either the downlink or the uplink GRE key is carried.

Reserved

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

GRE Key Identifier

A 32-bit field containing the downlink or the uplink GRE key. This field is present in the GRE Key option only if the GRE keys are being exchanged using the Proxy Binding Update and Proxy Binding Acknowledgement messages.

6.2. Proxy Binding Update Message Extension

This specification extends the Proxy Binding Update message as defined in [RFC5213] with the new TLV-header format (T) flag. The new (T) flag is described below and shown as part of the Proxy Binding Update message as in Figure 3.

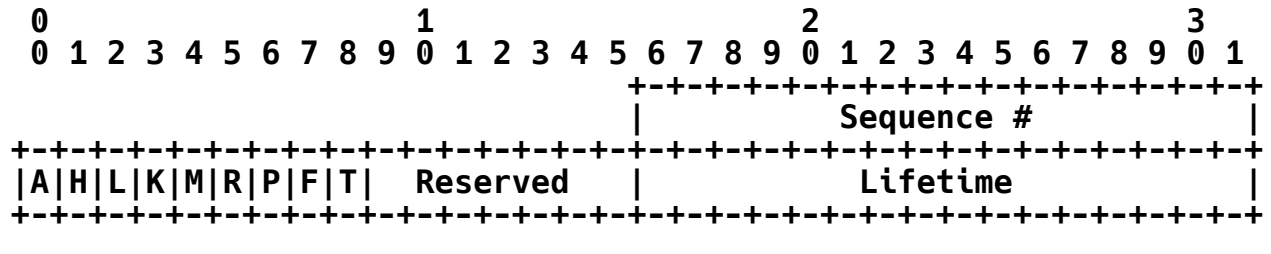

Figure 3: Proxy Binding Update Message

TLV-header format (T)

When set, this flag indicates that the mobile access gateway requests the use of the TLV header for encapsulating IPv6 or IPv4 packets in IPv4. The TLV-header format is described in Section 7.2. None of the other fields or flags in the Proxy Binding Update are modified by this specification.

6.3. Proxy Binding Acknowledgement Message Extension

This specification extends the Proxy Binding Acknowledgement message as defined in [RFC5213] with the new TLV-header format (T) flag. The new (T) flag is described below and shown as part of the Proxy Binding Acknowledgement message as in Figure 4.

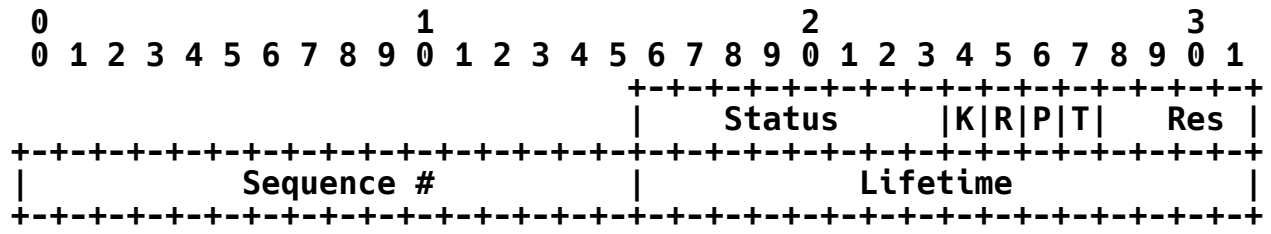

Figure 4: Proxy Binding Acknowledgement Message

TLV-header format (T)

When set, this flag indicates that the sender of the Proxy Binding Acknowledgement, the LMA, supports tunneling IPv6-or-IPv4 in IPv4 using TLV-header format. None of the other fields or flags in the Proxy Binding Acknowledgement are modified by this specification.

6.4. Status Codes

The following status code values are defined for use in the Binding Acknowledgement message when using Proxy Mobile IPv6.

GRE_KEY_OPTION_NOT_REQUIRED (2)

When the local mobility anchor receives a Proxy Binding Update with the GRE Key option, and based on a policy check it determines that GRE encapsulation is not required for this specific mobility session, it uses this code to indicate to the mobile access gateway that the Proxy Binding Update has been processed successfully but GRE encapsulation and GRE keys are not required.

GRE_TUNNELING_BUT_TLV_HEADER_NOT_SUPPORTED (3)

If the local mobility anchor receives a Proxy Binding Update with the GRE Key option and TLV-header format (T) flag set, the local mobility anchor uses this code to indicate to the mobile access gateway that GRE encapsulation has been successfully negotiated but TLV-header format is NOT supported.

GRE_KEY_OPTION_REQUIRED (163)

When the local mobility anchor receives a Proxy Binding Update without the GRE Key option while based on a policy check, the local mobility anchor determines that GRE encapsulation is required for this specific mobility session and uses this code to reject the Proxy Binding Update and indicate to the mobile access gateway that GRE encapsulation and GRE keys are required.

7. Data Packets Processing Considerations

This section describes how the local mobility anchor and mobile access gateway encapsulate and decapsulate data packets when GRE encapsulation and GRE keys are used for tunneling the mobile node's data traffic between these two mobile nodes.

7.1. Tunneling Format

When GRE encapsulation is used, the mobile access gateway is allowed to use various tunneling formats depending on the mobile access gateway location and the network capabilities between the mobile access gateway and the local mobility anchor. Using GRE encapsulation, as described in [RFC2784] and [RFC2890], the mobile access gateway can tunnel the IPv6-or-IPv4 payload packet in IPv6 or in IPv4 following the rules in [RFC5213] and [RFC5844].

If UDP-based tunneling is used in conjunction with GRE encapsulation between the mobile access gateway and the local mobility anchor, the TLV-header UDP tunneling format as shown in Figure 5 MUST be used.

[IPv4 Header]

[UDP Header]

[TLV Header]

[GRE Header]

[Payload - IPv6 or IPv4 Header]

Upper Layer protocols

Figure 5: TLV-Header UDP-Based Encapsulation Header Order

When a UDP-based tunneling format is used between the mobile access gateway and the local mobility anchor, the use of the TLV header is negotiated during the Proxy Binding Update/Acknowledgement exchange as described in Sections 7.3 and 7.4. If the TLV-header format is agreed upon between the mobile access gateway and local mobility anchor, the local mobility anchor expects the TLV header to follow the UDP header as shown in Figure 5. The TLV header contains the Type field, the following payload packet header type, and its length. The Type field in the TLV header is always set to a value of 0 to enhance the processing of the received packet by ensuring that the receiver can differentiate whether what came after the UDP header is a TLV-header Type field or an IP version field of an IP header. Hence, the TLV header can carry traffic other than IP as indicated in the Next Header field. The distinction between IP and TLV encapsulation is needed, because the Proxy Binding Update (IP packet) and the data packets (GRE packets) can be sent over the same UDP tunnel.

When processing a UDP packet with the TLV-header format, if the receiving node found that the payload packet length as calculated from the UDP header length field is different than its length as calculated from the TLV-header length field, the receiving node MUST discard the received IP packet.

7.2. TLV-Header Tunneling Negotiation

The mobile access gateway negotiates the format for tunneling payload traffic during the Proxy Mobile IPv6 registration procedure. If the mobile access gateway is required to use the TLV-header UDP encapsulation format, the mobile access gateway MUST set the TLV-header format (T) flag in the Proxy Binding Update message sent to the local mobility anchor. If the local mobility anchor supports the TLV-header UDP tunneling format, the local mobility anchor SHOULD set the TLV-header format (T) flag in the Proxy Binding Acknowledgement.

Otherwise, the TLV-header format (T) flag is cleared. The setting of the TLV-header Format (T) flag in the Proxy Binding Acknowledgement indicates to the mobile access gateway that it MUST use the TLV-header UDP encapsulation format for all packets tunneled to the local mobility anchor for the entire duration the mobile node is attached to the mobile access gateway. The TLV-header UDP tunneling format SHOULD NOT change during a Binding Lifetime Extension Proxy Binding Update (re-registration) from the same mobile access gateway.

Any Proxy Binding Update message triggered by a handoff (Section 5.3.4 of [RFC5213]) may renegotiate the tunneling format. Therefore, in order to avoid interoperability issues, the local mobility anchor MUST NOT set the TLV-header format (T) flag unless it was set in the Proxy Binding Update received from the mobile access gateway.

The TLV-header format is as shown below in Figure 6.

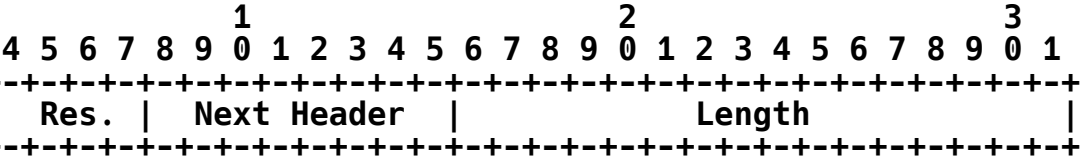

Figure 6: TLV-Header Format

Type

This field is always 0 (zero) and distinguishes the TLV header from the IPv4 and IPv6 headers.

Res.

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

Next Header

An 8-bit unsigned integer that indicates the protocol number of the payload header following this TLV header. It is set to the protocol number as assigned by IANA in the "Assigned Internet Protocol Numbers" registry. For example, if an IPv6 header follows, it should be '41'; if a GRE header follows, it should be '47'.

Length

A 16-bit unsigned integer indicating the length in octets of the payload following this header, excluding the TLV header itself.

7.3. Mobile Access Gateway Operation

When sending a Proxy Binding Update message over an IPv4 transport network, the mobile access gateway follows the procedures specified in [RFC5844] for using IPv4-UDP encapsulation mode. However, when using GRE header in conjunction with IPv4-UDP encapsulation mode is required, the mobile access gateway MUST set the TLV-header format (T) flag in the Proxy Binding Update and follow this specification for GRE encapsulation negotiation. If the received Proxy Binding Acknowledgement is successful and the TLV-header format (T) flag is set and the GRE Key option included, the mobile access gateway MUST update the mobile node's Binding Update List entry described in Section 4.1 by setting the UDP-based TLV-header format (T) flag. In this case, the mobile access gateway MUST use the TLV-header UDP-based encapsulation format as shown in Figure 5.

If the mobile access gateway receives a Proxy Binding Acknowledgement with the status GRE_TUNNELING_BUT_TLV_HEADER_NOT_SUPPORTED in response to a Proxy Binding Update with the GRE Key option and the (T) flag set, the mobile access gateway MUST use GRE encapsulation without UDP encapsulation. If the mobile access gateway is allowed to use GRE encapsulation without UDP tunneling, the mobile access gateway MUST update the mobile node's Binding Update List entry described in Section 4.1 by setting the GRE-encapsulation-enabled flag and the uplink and downlink GRE key fields. In this case, the mobile access gateway MUST set the UDP-based TLV-header format (T) flag to FALSE. A Proxy Binding Acknowledgement message with the status code GRE_TUNNELING_BUT_TLV_HEADER_NOT_SUPPORTED has the (T) flag cleared. Alternatively, the mobile access gateway may resend the Proxy Binding Update to negotiate different tunneling options, e.g., using UDP-based tunneling without GRE encapsulation if possible or de-register the mobile node mobility session.

7.3.1. Sending and Receiving Data Packets

When the mobile access gateway is located in an IPv6-enabled or IPv4-enabled network, it may be required to use GRE encapsulation for tunneling IPv6 or IPv4 data packets to the local mobility anchor. In this case, and if the mobile access gateway has successfully negotiated GRE encapsulation mode only or GRE encapsulation and GRE keys as described in this specification, the mobile access gateway encapsulates or decapsulates IPv6-or-IPv4 payload packets following the rules described in [RFC5213] and [RFC5844] while ensuring that the GRE header is present as shown in Figure 7.

[IPv6 or IPv4 Header]

[GRE Header]

[Payload - IPv6 or IPv4 Header]

Upper Layer protocols

Figure 7: IPv6-or-IPv4 over IPv4 Using GRE Encapsulation

On the other hand, if the mobile access gateway is located in an IPv4-only network where NAT has been detected on the path between the mobile access gateway and the local mobility anchor and successfully negotiated GRE encapsulation and the TLV-header format, the mobile access gateway MUST use UDP TLV-header tunneling format when sending an IPv6-or-IPv4 payload packet to the local mobility anchor according to the format described in Figure 5. The source and the destination of the IPv4 outer header are mobile node IPv4 Proxy Care-of Address, IPv4-Proxy-CoA, and the IPv4 local mobility anchor address, IPv4-LMAA, respectively. In addition, the source and the destination IP addresses of the IPv6-or-IPv4 payload data packet are the mobile node's IPv6-or-IPv4 home address, IPv6/IPv4-MN-HoA, and the IPv6-or-IPv4 corresponding node's address, IPv6/IPv4-CN-Addr, respectively.

7.4. Local Mobility Anchor Operation

When the local mobility anchor receives a Proxy Binding Update encapsulated in UDP and containing the IPv4 Home Address Request option ([RFC5844]), it needs to follow all the steps in [RFC5213] and [RFC5844]. In addition, if the TLV-header format (T) flag is set in the Proxy Binding Update, the local mobility anchor needs to determine whether it can accept the TLV-header UDP-based encapsulation format. If it does, it SHOULD set the TLV-header format (T) flag in the Proxy Binding Acknowledgement. Otherwise, the local mobility anchor MUST NOT set the TLV-header format (T) flag in the Proxy Binding Acknowledgement.

If the local mobility anchor (LMA) receives a Proxy Binding Update with the GRE Key option and TLV-header format (T) flag set and, based on a policy check, the LMA determines that GRE encapsulation is required and the LMA supports TLV-header tunneling and the LMA sent a successful Proxy Binding Acknowledgement with the TLV-header format (T) flag set, the LMA MUST update the mobile node's Binding Cache entry described in Section 5.1 by setting the GRE-encapsulation-enabled flag and update the uplink and downlink GRE key fields. In addition, the LMA MUST set the UDP-based TLV-header format flag.

If the LMA receives a Proxy Binding Update with the GRE Key option and TLV-header format (T) flag set and, based on a policy check, the LMA determines that GRE encapsulation is required BUT the LMA does NOT support TLV-header tunneling and if the Proxy Binding Update has been successfully processed, the LMA MUST send a successful Proxy Binding Acknowledgement with the status code GRE_TUNNELING_BUT_TLV_HEADER_NOT_SUPPORTED. This way, the LMA indicates to the mobile access gateway that GRE encapsulation has been successfully negotiated BUT TLV-header UDP-based tunneling format is not supported. In this case, the LMA MUST update the mobile node's BCE described in Section 5.1 by setting the GRE encapsulation enabled flag and update the uplink and downlink GRE key fields. In this case, the LMA MUST set the UDP-based TLV-header format flag to FALSE.

If the local mobility anchor and the mobile access gateway have successfully negotiated the TLV-header UDP-based tunneling format and GRE encapsulation for a specific mobility session, the local mobility anchor processes data packets as described in the following subsection.

7.4.1. Sending and Receiving Data Packets

The local mobility anchor may use GRE encapsulation for tunneling an IPv6 or IPv4 data packet to the mobile access gateway. If the local mobility anchor has successfully negotiated GRE encapsulation with the mobile access gateway for a specific mobility session, the local mobility anchor encapsulates and decapsulates IPv6-or-IPv4 payload data packets following the rules described in [RFC5213] and [RFC5844] while ensuring that the GRE header is present as shown in Figure 7.

In the case when TLV-tunneling format and GRE encapsulation for a specific mobility session have been successfully negotiated between the local mobility anchor and the mobile access gateway, the local mobility anchor follows the TLV-header UDP-based tunneling format and header order as shown in Figure 5 to encapsulate IPv4 or IPv6 payload packets in IPv4 before sending the IPv4 packet to the mobile access gateway. In this case, the source and the destination of the IPv4 outer header are IPv4-LMAA and IPv4-Proxy-CoA, respectively. In addition, the source and the destination IP addresses of the IPv6-or-IPv4 payload data packet are IPv6/IPv4-CN-Addr and IPv6/IPv4-MN-HoA, respectively. On the other hand, the local mobility anchor ensures the same TLV-header UDP-based tunneling format and header order when it decapsulates received IPv4 packets from the mobile access gateway for the same mobility session.

8. IANA Considerations

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

This specification also defines three new Binding Acknowledgement status codes as described in Section 6.4 and IANA has allocated the numeric values as specified in Section 6.4 from the "Status Codes" registry of the Mobility IPv6 Parameters.

9. Security Considerations

The GRE Key option, defined in this specification, when carried in Proxy Binding Update and Proxy Binding Acknowledgement messages, reveals the group affiliation of a mobile node identified by its Network Access Identifier (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 Proxy Binding 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.

In Proxy Mobile IPv6 [RFC5213], the use of IPsec [RFC4301] for protecting a mobile node's data traffic is optional. Additionally, Proxy Mobile IPv6 recommends the use of Encapsulating Security Payload (ESP) [RFC4303] in tunnel mode when using ESP for protecting the mobile node's data traffic. However, when GRE encapsulation is used, both IPsec tunnel mode and transport mode can be used to protect the GRE header. The IPsec traffic selectors will contain the protocol number for GRE, and there is currently no mechanism to use the GRE key as a traffic selector.

10. Acknowledgements

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

11. References

11.1. Normative References

[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.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

11.2. Informative References

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.

Authors' Addresses

Ahmad Muhanna
Ericsson, Inc.
2201 Lakeside Blvd.
Richardson, TX 75082
USA

EMail: ahmad.muhanna@ericsson.com

Mohamed Khalil
Ericsson, Inc.
6300 Legacy Dr.
Plano, TX 75024
USA

EMail: Mohamed.khalil@ericsson.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