Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 18, 2011

P. Yegani
Juniper Networks
K. Leung
Cisco Systems
A. Lior
Bridgewater Systems
K. Chowdhury
J. Navali
Cisco Systems

Oct 15, 2010

GRE Key Extension for Mobile IPv4
draft-ietf-mip4-gre-key-extension-03.txt

Abstract

The GRE specification contains a Key field, which MAY contain a value that is used to identify a particular GRE data stream. This specification defines a new Mobile IP extension that is used to exchange the value to be used in the GRE Key field. This extension further allows the Mobility Agents to set up the necessary protocol interfaces prior to receiving the mobile's traffic. The new extension allows a foreign agent to request GRE tunneling without disturbing the Home Agent behavior specified for Mobile IPv4. GRE tunneling with the Key field allows the operators to have home networks that consist of multiple Virtual Private Networks (VPNs), which may have overlapping home addresses. When the tuple < Care of Address, Home Address and Home Agent Address > is the same across multiple subscriber sessions, GRE tunneling will provide a means for the FA and HA to identify data streams for the individual sessions based on the GRE key. In the absence of this key identifier, the data streams cannot be distinguished from each other, a significant drawback when using IP-in-IP tunneling.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 18, 2011.

Table of Contents

1. Introduction

This document specifies a new extension for use by Foreign Agents operating Mobile IP for IPv4. The new extension allows a foreign agent to request GRE tunneling without disturbing the Home Agent behavior specified for Mobile IPv4 [RFC3344]. This extension contains the GRE key [RFC2890] required for establishing a GRE tunnel between the FA and the HA.

GRE tunneling with the Key field allows the operators to have home networks that consist of multiple Virtual Private Networks (VPNs), which may have overlapping home addresses. When the tuple < Care of Address, Home Address and Home Agent Address > is the same across multiple subscriber sessions, GRE tunneling will provide a means for the FA and the HA to identify data streams for the individual sessions based on the GRE key. In the absence of this key identifier, the data streams cannot be distinguished from each other, a significant drawback when using IP-in-IP tunneling.

2. Terminology

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]. Other terminology is used as already defined in [RFC3344].

3. GRE-Key Extension

The format of the GRE-Key Extension conforms to the Extension format specified for Mobile IPv4 [RFC3344]. This extension option is used by the Foreign Agent to supply GRE key and other necessary information to the Home Agent to establish a GRE tunnel between the FA and the HA.

4. Operation and Use of the GRE-Key Extension

4.1. Foreign Agent Requirements for GRE Tunneling Support

The FA MUST support IP-in-IP tunneling of datagrams for Mobile IPv4 [RFC3344]. The FA may support GRE tunneling that can be used, for example, to allow for overlapping private home IP addresses [X.S0011-D]. If the FA is capable of supporting GRE encapsulation, it should set the ’G’ bit in the Flags field in the Agent Advertisement message sent to the MN during the Mobile IP session establishment.

If the MN does not set the 'G' bit, the FA MAY fall back to using IP-in-IP encapsulation for the session per [RFC3344].

If the MN does not set both the 'G' bit and the 'D' bit (i.e., the mobile node is not using a co-located care-of address), and the local policy allows the FA to override the 'G' bit setting received from the MS, the FA MUST include the GRE-Key Extension as defined in this memo in the Registration Request that it propogates to the HA. The presence of this extension is a request for GRE encapsulation that takes precedence over the setting of the 'G' bit in the Registration Request. The FA MUST NOT modify the 'G' bit in the Registration Request because it is protected by the Mobile-Home Authentication Extension.

If the FA does not support GRE encapsulation, the FA MUST reset the 'G' bit in the Agent Advertisement message. In this case, if the MN sets the 'G' bit in the Registration Request message, the FA returns a Registration Reply message to the MN with code 'Requested Encapsulation Unavailable' (72) per [RFC3344].

If the FA allows GRE encapsulation, and either the MN requested GRE encapsulation or local policy dictates using GRE encapsulation for the session and the 'D' bit is not set (i.e., the mobile node is not using a co-located care-of address, the FA MUST include the GRE Key in the GRE Key Extension in all Mobile IP Registration Requests (including initial, renewal and de-registration requests) before forwarding the request to the HA. The FA may include a GRE key of value zero in the GRE Key Extension to signal that the HA assign GRE keys in both directions. The GRE key assignment in the FA and the HA is outside the scope of this memo.

The GRE Key Extension SHALL follow the format defined in [RFC3344]. This extension SHALL be added after the MN-HA and MN-FA Challenge and MN-AAA extensions (if any) and before the FA-HA Auth extension (if any).

4.2. Home Agent Requirements for GRE Tunneling Support [RFC3344]

The HA MUST follow the procedures specified in RFC 3344 in processing this extension in Registration Request messages. If the HA receives the GRE Key Extension in a Registration Request and does not recognize this non-skippable extension, it MUST silently discard the message. The HA MUST use other alternative forms of encapsulation (e.g., IP-in-IP tunneling), when requested by the mobile node per [RFC3344].

If the HA receives the GRE Key Extension in a Registration Request

and recognizes the GRE Key Extension but is not configured to support GRE encapsulation, it MUST send an RRP with code 'Requested Encapsulati on Unavailable (139)' [RFC3024] .

If the HA receives a Registration Request with a GRE Key Extension but without the 'G' bit set, the HA SHOULD treat this as if 'G' bit is set in the Registration Request i.e., the presence of GRE Key Extension indicates a request for GRE encapsulation.

If the HA receives the GRE Key Extension in a Registration Request and recognizes the GRE Key Extension as well as supports GRE encapsulation, the following procedures should apply:

The HA SHOULD accept the RRQ and send a RRP with code 'Accepted (0)'. The HA MUST assign a GRE key and include the GRE Key Extension in the RRP before sending it to the FA. The HA MUST include the GRE Key Extension in all RRPs in response to any RRQ that included GRE Key Extension, when a GRE key is available for the registration.

If the HA receives the GRE Key Extension in the initial Registration Request and recognizes the GRE Key Extension carrying a GRE key value of zero, it SHOULD accept the RRQ and send a RRP with code 'Accepted (0)'. The HA MUST assign GRE keys for both directions and include these keys in the GRE Key Extension in the RRP before sending it to the FA. The HA MUST include the GRE Key Extension in the RRP in response to the initial RRQ that included GRE Key Extension, when a GRE key is available for the registration.

4.3. Mobile Node Requirements for GRE Tunneling Support

If the MN is capable of supporting GRE encapsulation, it SHOULD set the 'G' bit in the Flags field in the Registration Request per [RFC3344].

5. GRE Key Extension and Tunneling Procedures

GRE tunneling support for Mobile IP will permit asymmetric GRE keying i.e., the FA assigns a GRE key for use in encapsulated traffic and the HA can assign its own GRE key. Once the GRE keys have been exchanged, the FA uses the HA-assigned key in the encapsulating GRE header for reverse tunneling and the HA uses the FA-assigned key in the encapsulating GRE header.

The format of the GRE Key Extension is as shown below.

The GRE Key extension MAY be included in Registration Requests [RFC3344]. The GRE Key extension is used to inform the recipient of

the Mobile IP request of the value to be used in GRE's Key field.

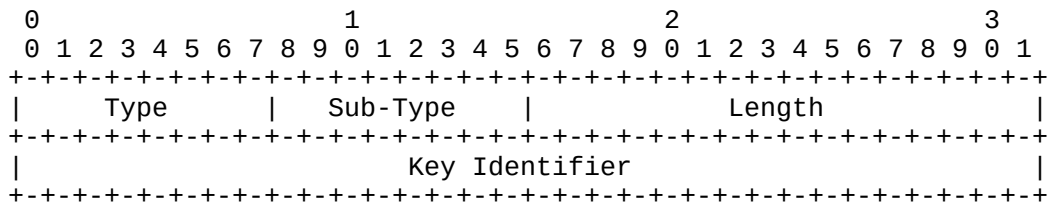

Figure 1: GRE Key Extension

Type
To be assigned by IANA. An 8-bit identifier of the GRE Key Extension type (non-skippable)

Sub-Type
0

Length
4

Key Identifier
This is a four octet value assigned during registration and inserted in every GRE packet of the user traffic.

6. IANA Considerations

The GRE Key extension defined in this memo is a Mobile IP extension as defined in [RFC3344]. IANA should assign a Type value for this Extension from the non-skippable range (0-127).

7. Security Considerations

This specification does not introduce any new security considerations, beyond those described in [RFC3344]

Despite its name, the GRE Key extension has little to do with security. The word "Key" here is not used in the cryptographic sense of a shared secret that must be protected, but rather is used in the sense of an "index" or demultiplexing value that can be used to distinguish packets belonging to a given flow within a GRE tunnel.

8. Acknowledgements

Thanks to Jun Wang, Gopal Dommety and Sri Gundavelli for their helpful comments, offline discussions and reviewing the initial draft. Also, Pete McCann and Simon Mizikovsky provided valuable review comments.

9. Normative references

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

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

[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.

Authors' Addresses

Parviz Yegani
Juniper Netowrks
1194 North Mathilda Ave.
Sunnyvale, California 94089
U.S.A

Phone: +1 408-759-1973
Email: pyegani@juniper.net

Kent Leung
Cisco Systems Incorporated
170 West Tasman Drive
San Jose, California 95134
U.S.A

Phone: +1 408 526 5030
Email: kleung@cisco.com

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
Canada

Phone: +1 613-591-6655
Email: avi@bridgewatersystems.com

Kuntal Chowdhury
Cisco Systems Incorporated
170 West Tasman Drive
San Jose, California 95134
U.S.A

Email: kchowdhu@cisco.com

Jay Navali
Cisco Systems Incorporated
170 West Tasman Drive
San Jose, California 95134
U.S.A

Email: jnavali@cisco.com