Intarea Working Group
Internet-Draft
Updates: 2784 (if approved)
Intended status: Standards Track
Expires: April 3, 2015

C. Pignataro
Cisco Systems
R. Bonica
Juniper Networks
September 30, 2014

IPv6 Support for Generic Routing Encapsulation (GRE)
draft-pignataro-intarea-gre-ipv6-00

Abstract

Generic Routing Encapsulation (GRE) can be used to carry any network layer protocol over any network layer protocol. GRE procedures are specified for IPv4, used as either the payload or delivery protocol. However, GRE procedures are not specified for IPv6, used as either the payload or delivery protocol.

This document specifies GRE procedures for IPv6, used as either the payload or delivery protocol, and updates RFC 2784.

Requirements Language

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

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 3, 2015.

Table of Contents

1. Introduction

Generic Routing Encapsulation (GRE) [RFC2784] [RFC2890] can be used to encapsulate and carry any network layer protocol (payload) over any network layer protocol (delivery). GRE procedures are specified for IPv4 [RFC0791], used as either the payload or delivery protocol. However, GRE procedures are not specified for IPv6 [RFC2460], used as either the payload or delivery protocol.

This document specifies GRE procedures for IPv6, used as either the payload or delivery protocol, and updates RFC 2784 [RFC2784].

1.1. Terminology

The following terms are specific to GRE and are modeled from [RFC2784]:

- GRE delivery header - an IPv4 or IPv6 header whose source address represents the GRE ingress node and whose destination address represents the GRE egress node. The GRE delivery header encapsulates a GRE header.

- GRE header - the GRE protocol header. The GRE header is encapsulated by the GRE delivery header and encapsulates GRE payload.

- GRE payload packet - a network layer packet that needs to be encapsulated and delivered to some destination, and is encapsulated by the GRE header.

The following terms are specific MTU discovery:

- path MTU (PMTU) - the minimum MTU of all the links in a path between a source node and a destination node. If the source and destination node are connected through an equal cost multipath (ECMP), the PMTU is equal to the minimum LMTU of all links contributing to the multipath.

- Path MTU Discovery (PMTUD) - A procedure for dynamically discovering the PMTU between two nodes on the Internet. PMTUD procedures for IPv6 are defined in [RFC1981].

2. IPv6 as a GRE Payload

When the GRE payload is IPv6, the Protocol Type field in the GRE header MUST be equal to 0x86DD.

3. IPv6 as a GRE Delivery Protocol

When the GRE delivery protocol is IPv6, the GRE header MAY immediately follow the GRE delivery header. Alternatively, IPv6 extension headers MAY be inserted between the GRE delivery header and the GRE header. However, the IPv6 Destination Options Header MUST NOT be inserted between the GRE delivery header and the GRE header.

If the GRE header immediately follows the GRE delivery header, the IPv6 Next Header field in GRE delivery packet MUST be equal to 47. If extension headers are inserted between the GRE delivery header and the GRE header, the Next Header field in the last IPv6 extension header MUST be equal to 47.

Following guidance provided in Section 5 of [RFC2460], GRE ingress nodes SHOULD implement PMTUD, in order to discover and take advantage of PMTUs greater than the IPv6 required minimum (1280 octets). However, a GRE ingress node MAY simply restrict itself to sending packets no larger than 1280 octets, and omit implementation of PMTUD.

4. IANA Considerations

This document makes no request of IANA.

5. Security Considerations

This document adds no additional security risks to GRE, beyond what is specified in [RFC2784]. It also does not provide any additional security for GRE.

6. Acknowledgements

The authors would like to thank Fred Baker and Andrew Yourtchenko for there thorough review and useful comments.

7. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, 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.

Authors' Addresses

Carlos Pignataro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, North Carolina 27709
USA

Email: cpignata@cisco.com

Ron Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, Virginia
USA

Email: rbonica@juniper.net