IPv6 Support for Generic Routing Encapsulation (GRE)
draft-ietf-intarea-gre-ipv6-05

Abstract

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

   This document specifies GRE procedures for IPv6, used as either the
   payload or delivery protocol. It updates the GRE specification, 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

Copyright Notice

Table of Contents

[1](#). Introduction

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

   This document specifies GRE procedures for IPv6, used as either the
   payload or delivery protocol. Like [RFC 2784](#), this document describes
   GRE how has been implemented by several vendors. It updates [RFC 2784](#)
   .

1.1. Terminology

The following terms are used in this document:

o 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.

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

o GRE payload - a network layer packet that is encapsulated by the
   GRE header.

o GRE overhead - the combined size of the GRE delivery header and
   the GRE header, measured in bytes

o 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 equal cost multipath
   (ECMP), the PMTU is equal to the minimum link MTU of all links
   contributing to the multipath.

o 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].

o GRE MTU (GMTU) - the maximum transmission unit, i.e., maximum
   packet size in bytes, that can be conveyed over a GRE tunnel
   without fragmentation of any kind. The GMTU is equal to the PMTU
   associated with the path between the GRE ingress and the GRE
   egress, minus the GRE overhead

2. GRE Header Fields

This document does not change the GRE header format or any behaviors
specified by RFC 2784 or RFC 2890.

2.1. Checksum Present

When the delivery protocol is IPv6, the GRE ingress node SHOULD set
the Checksum Present field to zero. GRE egress nodes MUST accept
either a value of zero or one in this field. If the GRE egress node
receives a value of one, it MUST use that information to calculate
the GRE header length. It MUST also use the checksum to verify
packet integrity.

[3](#). IPv6 As GRE Payload

   The following considerations apply to GRE tunnels that carry IPv6
   payload.

[3.1](#). GRE Protocol Type Considerations

   The Protocol Type field in the GRE header MUST be set to Ether Type
   [ETYPES] 0x86DD.

[3.2](#). MTU Considerations

   A GRE tunnel MUST be able to carry a 1280-byte IPv6 packet from
   ingress to egress, without fragmenting the payload packet. All GRE
   tunnels with a GMTU of 1280 bytes or greater satisfy this
   requirement. GRE tunnels that can fragment and reassemble delivery
   packets also satisfy this requirement, regardless of their GMTU.
   However, the ability to fragment and reassemble delivery packets is
   not a requirement of this specification. This specification requires
   only that GRE ingress nodes refrain from activating GRE tunnels that
   do not satisfy the above-mentioned requirement.

   Before activating a GRE tunnel and periodically thereafter, the GRE
   ingress node MUST execute procedures that verify the tunnel's ability
   to carry a 1280-byte IPv6 payload packet from ingress to egress,
   without fragmenting the payload. Having executed those procedures,
   the GRE ingress node MUST activate or deactivate the tunnel
   accordingly.

   Implementation details regarding the above-mentioned verification
   procedures are beyond the scope of this document. However, a GRE
   ingress node can verify tunnel capabilities by sending a 1280-byte
   IPv6 packet addressed to itself through the tunnel under test.

[3.3](#). Fragmentation Considerations

   When the GRE ingress receives an IPv6 payload packet whose length is
   less than or equal to the GMTU, it can encapsulate and forward the
   packet without fragmentation of any kind. In this case, the GRE
   ingress router MUST NOT fragment the payload or delivery packets.

   When the GRE ingress receives an IPv6 payload packet whose length is
   greater than the GMTU, and the GMTU is greater than or equal to 1280
   bytes, the GRE ingress router MUST:

   o discard the IPv6 payload packet

o send an ICMPv6 Packet Too Big (PTB) [RFC4443] message to the IPv6
   payload packet source. The MTU field in the ICMPv6 PTB message is
   set to the GMTU.

When the GRE ingress receives an IPv6 payload packet whose length is
greater than the GMTU, and the GMTU is less than 1280 bytes, the GRE
ingress router MUST:

o encapsulate the entire IPv6 packet in a single GRE header and IP
   delivery header

o fragment the delivery header, so that it can be reassembled by the
   GRE egress

4. IPv6 As GRE Delivery Protocol

The following considerations apply when the delivery protocol is
IPv6.

4.1. Next Header Considerations

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.

If the GRE header immediately follows the GRE delivery header, the
Next Header field in the IPv6 header of the GRE delivery packet MUST
be set 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 set to 47.

4.2. Checksum Considerations

As stated in [RFC2784], the GRE header can contain a checksum. If
present, the GRE header checksum can be used to detect corruption of
the GRE header and GRE payload.

The GRE header checksum cannot be used to detect corruption of the
IPv6 delivery header. Furthermore, the IPv6 delivery header does not
contain a checksum of its own. Therefore, no available checksum can
be used to detect corruption of the IPv6 delivery header.

In one failure scenario, the destination address in the IPv6 delivery
header is corrupted. As a result, the IPv6 delivery packet is
delivered to a node other than the intended GRE egress node.
Depending upon the state and configuration of that node, it will
either:

a. Drop the packet

b. De-encapsulate the payload and forward it to its intended
    destination

c. De-encapsulate the payload and forward it to a node other than
    its intended destination. For example, the payload might be
    intended for a node on one VPN, but delivered to an identically
    numbered node in another VPN.

Behaviors a) and b) are acceptable. Behavior c) is not acceptable.

Before deploying GRE over IPv6, network operators should consider the
likelihood of behavior c) in their network. GRE over IPv6 is
deployable only in environments where the network operator deems the
risk associated with behavior c) to be acceptable.

The risk associated with behavior c) could be mitigated with end-to-
end authentication of the payload.

4.3. MTU Considerations

By default, the GRE ingress node cannot fragment the IPv6 delivery
header. However, implementations MAY support an optional
configuration in which the GRE ingress node can fragment the IPv6
delivery header.

Also by default, the GRE egress node cannot reassemble the IPv6
delivery header. However, implementations MAY support an optional
configuration in which the GRE egress node can reassemble the IPv6
delivery header.

5. IANA Considerations

This document makes no request of IANA.

6. Security Considerations

The Security Considerations section of [RFC4023] addresses MPLS in
GRE. However, it applies equally to the current specification.
Beyond that, the current specification introduces no security
considerations beyond those mentioned in RFC 2784.

7. Acknowledgements

The authors would like to thank Fred Baker, Stewart Bryant, Dino
Farinacci, Tom Herbert, Fred Templin, Joe Touch, Andrew Yourtchenko
and Lucy Yong for their thorough review and useful comments.

8. Normative References

   [ETYPES]   IANA, "ETHER TYPES", 2014,
               <http://www.iana.org/assignments/ieee-802-numbers/
               ieee-802-numbers.xhtml#ieee-802-numbers-1>.

   [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.

   [RFC4023]   Worster, T., Rekhter, Y., and E. Rosen, "Encapsulating
               MPLS in IP or Generic Routing Encapsulation (GRE)", RFC
               4023, March 2005.

   [RFC4443]   Conta, A., Deering, S., and M. Gupta, "Internet Control
               Message Protocol (ICMPv6) for the Internet Protocol
               Version 6 (IPv6) Specification", RFC 4443, March 2006.

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

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com