

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 24, 2016

L. Zheng, Ed.
Huawei Technologies
C. Pignataro
R. Penno
Cisco Systems, Inc.
Z. Wang
Huawei Technologies
January 21, 2016

**Yang Data Model for Generic Routing Encapsulation (GRE)
draft-zheng-intarea-gre-yang-01.txt**

Abstract

This document defines a YANG data model that can be used to configure and manage Generic Routing Encapsulation (GRE).

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 [RFC 2119](#) [[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 July 24, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Scope	2
3.	Design of the Data Model	3
4.	Data Hierarchy	3
5.	GRE Yang Module	3
6.	Examples	5
7.	Security Considerations	5
8.	IANA Considerations	6
9.	Acknowledgements	6
10.	References	6
10.1.	Normative References	6
10.2.	Informative References	6
	Authors' Addresses	7

1. Introduction

Generic Routing Encapsulation (GRE) [[RFC2784](#)] specifies a protocol for encapsulation of an arbitrary network layer protocol over another arbitrary network layer protocol. YANG [[RFC6020](#)] is a data definition language that was introduced to define the contents of a conceptual data store that allows networked devices to be managed using NETCONF [[RFC6241](#)]. This document defines a YANG data model that can be used to configure and manage GRE.

The rest of this document is organized as follows. [Section 2](#) presents the scope of this document. [Section 3](#) provides the design of the GRE configuration data model in details. [Section 4](#) presents the complete data hierarchy of GRE YANG model. [Section 5](#) specifies the YANG module and [section 6](#) lists examples which conform to the YANG module specified in this document. Finally, security considerations are discussed in [Section 7](#).

2. Scope

The fundemantel protocol of GRE is defined in [[RFC2784](#)]. [[RFC2890](#)] describes extensions by which two fields, Key and Sequence Number, can be optionally carried in the GRE Header. [[I-D.ietf-intarea-gre-ipv6](#)] specifies GRE procedures for IPv6, used

as either the payload or delivery protocol.

[[I-D.ietf-intarea-gre-mtu](#)] describes how vendors have solved the GRE fragmentation problem. These RFCs and documents are considered in this Yang Module.

3. Design of the Data Model

This YANG data model is defined to be used to configure and manage Generic Routing Encapsulation (GRE) . Under the top level container is the list gre-tunnel, the leaf tunnel-name is used as the key for the list. Under the list, nodes are defined to enable the tunnel encapsulation configuration when either IPv4 or IPv6 is used as the delivery protocol. Nodes are also defined to enable the checksum bit set, tunnel fragmentation, Path MTU Discovery, Key and Key value set, and Sequence Number configuration respectively, based on various GRE RFCs and documents which are summarized in [Section 2](#).

4. Data Hierarchy

The complete data hierarchy of GRE YANG model is presented below.

```
module: ietf-gre
  +--rw gre-tunnel
    +--rw gre-tunnel* [tunnel-name]
      +--rw tunnel-name                string
      +--rw (delivery-protocol)?
        | +--:(ipv4)
        | | +--rw source-ipv4-address?    inet:ipv4-address
        | | +--rw dest-ipv4-address?      inet:ipv4-address
        | +--:(ipv6)
        |   +--rw source-ipv6-address?    inet:ipv6-address
        |   +--rw dest-ipv6-address?      inet:ipv6-address
      +--rw pmtud-enable?                boolean
      +--rw fragmentation-enable?        boolean
      +--rw checksum-enable?             boolean
      +--rw key-enable?                  boolean
      +--rw key?                         uint32
      +--rw sequence-number-enable?      boolean
```

5. GRE Yang Module

```
<CODE BEGINS> file "ietf-gre@2015-07-02.yang"
module ietf-gre {
  namespace "urn:ietf:params:xml:ns:yang:ietf-gre";
  //namespace to be assigned by IANA
  prefix "gre";
  import ietf-inet-types {
```



```
    prefix "inet";
}
organization "IETF INTAREA Working Group";
contact "draft-zheng-intarea-gre-yang";
description "This module contains the YANG definition for GRE
            parameters as per RFC2784, RFC2890,
            draft-ietf-intarea-gre-ipv6 and
            draft-ietf-intarea-gre-mtu";
revision "2015-07-02" {
  description "Initial revision.";
  reference "draft-zheng-intarea-gre-yang";
}

container gre-tunnel {
  description "Top level container";
  list gre-tunnel {
    key "tunnel-name";
    description "GRE tunnel";
    leaf tunnel-name {
      type string {
        length "1..63";
      }
      description "GRE tunnel name";
    }
  }
  choice delivery-protocol {
    case ipv4 {
      leaf source-ipv4-address {
        type inet:ipv4-address;
        description "Source IP address";
      }
      leaf dest-ipv4-address {
        type inet:ipv4-address;
        description "Destination IP address";
      }
    }
    case ipv6 {
      leaf source-ipv6-address {
        type inet:ipv6-address;
        description "Source IP address";
      }
      leaf dest-ipv6-address {
        type inet:ipv6-address;
        description "Destination IP address";
      }
    }
  }
  description "Delivery protocol";
}
leaf pmtud-enable {
```



```
        type boolean;
        description "Enable tunnel PMTU discovery";
    }
    leaf fragmentation-enable {
        type boolean;
        description "Enable delivery packets fragmentation";
    }
    leaf checksum-enable {
        type boolean;
        description "Enable GRE tunnel checksum verification";
    }
    leaf key-enable {
        type boolean;
        description "Enable optional GRE tunnel Key";
    }
    leaf key {
        when "/gre-tunnel/gre-tunnel/key-enable == 'true'" {
            description "When key-enable is true";
        }
        type uint32;
        description "GRE tunnel key value";
    }
    leaf sequence-number-enable {
        type boolean;
        description "Enable optional GRE tunnel Sequence Number";
    }
}
}
}
<CODE ENDS>
```

6. Examples

Examples of using Yang module to configure and manage GRE will be given here in the update when the Yang module is stable.

7. Security Considerations

The configuration and state data defined in this document is designed to be accessed via the NETCONF protocol [[RFC6241](#)]. The lowest NETCONF layer is the secure transport layer and the mandatory-to-implement secure transport is SSH [[RFC6242](#)]. The authors recommend to implement the NETCONF access control model [[RFC6536](#)] to restrict access for particular NETCONF users to a pre-configured subset of all available NETCONF protocol operations and content.

There are a number of config true nodes defined in the YANG module which are writable/creatable/deletable. These data nodes may be

considered sensitive or vulnerable in some network environments. Write operations to these data nodes without proper protection can have a negative effect on network operations.

8. IANA Considerations

The IANA is requested to assign a new namespace URI from the IETF XML registry.

URI:TBA

9. Acknowledgements

We would also like to thank XXX.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", [RFC 2784](#), DOI 10.17487/RFC2784, March 2000, <<http://www.rfc-editor.org/info/rfc2784>>.
- [RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", [RFC 2890](#), DOI 10.17487/RFC2890, September 2000, <<http://www.rfc-editor.org/info/rfc2890>>.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", [RFC 6020](#), DOI 10.17487/RFC6020, October 2010, <<http://www.rfc-editor.org/info/rfc6020>>.

10.2. Informative References

- [I-D.ietf-intarea-gre-ipv6] Pignataro, C., Bonica, R., and S. Krishnan, "IPv6 Support for Generic Routing Encapsulation (GRE)", [draft-ietf-intarea-gre-ipv6-14](#) (work in progress), September 2015.

[I-D.ietf-intarea-gre-mtu]

Bonica, R., Pignataro, C., and J. Touch, "A Widely-Deployed Solution To The Generic Routing Encapsulation (GRE) Fragmentation Problem", [draft-ietf-intarea-gre-mtu-05](#) (work in progress), May 2015.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", [RFC 6241](#), DOI 10.17487/RFC6241, June 2011, <<http://www.rfc-editor.org/info/rfc6241>>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", [RFC 6242](#), DOI 10.17487/RFC6242, June 2011, <<http://www.rfc-editor.org/info/rfc6242>>.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", [RFC 6536](#), DOI 10.17487/RFC6536, March 2012, <<http://www.rfc-editor.org/info/rfc6536>>.

Authors' Addresses

Lianshu Zheng (editor)
Huawei Technologies
China

Email: vero.zheng@huawei.com

Carlos Pignataro
Cisco Systems, Inc.
USA

Email: cpignata@cisco.com

Reinaldo Penno
Cisco Systems, Inc.
USA

Email: repenno@cisco.com

Zishun Wang
Huawei Technologies
China

Email: wangzishun@huawei.com

