Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 23, 2017

Z. Zhang
Juniper Networks, Inc.
H. Tsunoda
Tohoku Institute of Technology
June 21, 2017

L2L3 VPN Multicast MIB
draft-ietf-bess-l2l3-vpn-mcast-mib-09

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes two MIB modules which will be used by other MIB modules for monitoring and/or configuring Layer 2 and Layer 3 Virtual Private Networks that support multicast.

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 December 23, 2017.

Table of Contents

1. Introduction

In BGP/MPLS Virtual Private Networks (VPN), Border Gateway Protocol (BGP) is used for distributing routes and MultiProtocol Label Switching (MPLS) is used for forwarding packets accross service provider networks.

The procedures for supporting multicast in BGP/MPLS Layer 3 (L3) VPN are specified in [RFC6513]. The procedures for supporting multicast in BGP/MPLS Layer 2 (L2) VPN are specified in [RFC7117]. Throughout this document, we will use the term "L2L3VpnMCast" to mean BGP/MPLS L2 and L3 VPN that support multicast.

This document describes textual conventions (TCs) and common managed objects (MOs) which will be used by other Management Information Base (MIB) modules for monitoring and/or configuring L2L3VpnMCast.

L2L3VpnMCast can be achieved by using various kinds of transport mechanisms for forwarding a packet to all or a subset of Provider Edge routers (PEs) across service provider networks. Such transport mechanisms are referred to as provider tunnels (P-tunnels). TCs and MOs defined in this document will be used by other MIB modules for monitoring and/or configuring both L2 and L3 VPNs that support multicast.

There are two types of signaling mechanisms of P-tunnel choice: BGP-based and UDP-based [RFC6513]. BGP-based mechanisms for Virtual Private LAN Service and Multicast VPN are described in [RFC7117] and

[RFC6513], respectively. In [RFC6513], a UDP-based signaling mechanism is also specified.

A BGP attribute that specifies information of a P-tunnel is called Provider Multicast Service Interface (PMSI) tunnel attribute. The PMSI tunnel attribute is advertised/received by PEs in BGP auto-discovery (A-D) routes. [RFC6514] defines the format of a PMSI tunnel attribute.

This document defines two TCs to represent

(a) the tunnel type of a P-tunnel and
(b) the identifier of a P-tunnel

respectively.

This document also describes common MOs that provide the information in a PMSI tunnel attribute and corresponding tunnel information to other MIB modules.

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].

1.1. Terminology

This document adopts the definitions, acronyms and mechanisms described in [RFC6513] [RFC6514] [RFC7117] and other documents that they refer to. Familiarity with Multicast, MPLS, Layer 3 VPN, Multicast VPN concepts and/or mechanisms is assumed. Some terms specifically related to this document are explained below.

"Provider Multicast Service Interface (PMSI)" [RFC6513] is a conceptual interface instantiated by a P-tunnel, a transport mechanism used to deliver multicast traffic. A PE uses it to send customer multicast traffic to all or some PEs in the same VPN.

There are two kinds of PMSIs: "Inclusive PMSI (I-PMSI)" and "Selective PMSI (S-PMSI)" [RFC6513]. An I-PMSI is a PMSI that enables a PE attached to a particular Multicast VPN to transmit a message to all PEs in the same VPN. An S-PMSI is a PMSI that enables a PE attached to a particular Multicast VPN to transmit a message to some of the PEs in the same VPN.

Throughout this document, we will use the term "PMSI" to refer both "I-PMSI" and "S-PMSI."

2. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

3. Summary of MIB Modules

This document defines two MIB modules: L2L3-VPN-MCAST-TC-MIB and L2L3-VPN-MCAST-MIB.

- L2L3-VPN-MCAST-TC-MIB contains two Textual Conventions: L2L3VpnMcastProviderTunnelType and L2L3VpnMcastProviderTunnelId. L2L3VpnMcastProviderTunnelType provides an enumeration of the P-tunnel types. L2L3VpnMcastProviderTunnelId represents an identifier of a P-tunnel.

- L2L3-VPN-MCAST-MIB defines a table l2L3VpnMcastPmsiTunnelAttributeTable. An entry in this table corresponds to a PMSI Tunnel Attribute (PTA) advertised/received by a PE router. Entries in this table will be used by other MIB modules for monitoring and/or configuring L2L3VpnMCast. The table index uniquely identifies a tunnel. It is composed of a set of attributes which depend on the tunnel type. The table may also be used in conjunction with other MIBs, such as MPLS Traffic Engineering MIB (MPLS-TE-STD-MIB) [RFC3812], to obtain further information of a tunnel by following the row pointer of the corresponding tunnel's row in this table. It may also be used in conjunction with Interfaces Group MIB (IF-MIB) [RFC2863] to obtain further information of the interface corresponding to the tunnel by following the row pointer of the corresponding tunnel's row in this table.

4. Definitions

4.1. L2L3-VPN-MCAST-TC-MIB Object Definitions

```
  L2L3-VPN-MCAST-TC-MIB DEFINITIONS ::= BEGIN

  IMPORTS
    MODULE-IDENTITY, mib-2
       FROM SNMPv2-SMI                              -- [RFC2578]

    TEXTUAL-CONVENTION
       FROM SNMPv2-TC;                              -- [RFC2579]

  l2L3VpnMcastTCMIB MODULE-IDENTITY
    LAST-UPDATED "201706211200Z"  -- 21th June, 2017
    ORGANIZATION "IETF BESS Working Group."
    CONTACT-INFO
          "        Zhaohui Zhang
                   Juniper Networks, Inc.
                   10 Technology Park Drive
                   Westford, MA 01886
                   USA
                   Email: zzhang@juniper.net

                   Hiroshi Tsunoda
                   Tohoku Institute of Technology
                   35-1, Yagiyama Kasumi-cho
                   Taihaku-ku, Sendai, 982-8577
                   Japan
                   Email: tsuno@m.ieice.org

                   Comments and discussion to bess@ietf.org
          "
    DESCRIPTION
        "This MIB module specifies textual conventions for
         Border Gateway Protocol/MultiProtocol Label
         Switching Layer 2 and Layer 3 Virtual Private Network
         that support multicast (L2L3VpnMCast).

         Copyright (C) The Internet Society (2017).
        "


    -- Revision history.

    REVISION "201706211200Z"  -- 21th June, 2017
    DESCRIPTION
        "Initial version, published as RFC XXXX."

    -- RFC Ed.: replace XXXX with actual RFC number and remove this note
```

```
    ::= { mib-2 AAAA }

    -- IANA Reg.: Please assign a value for "AAAA" under the
    -- 'mib-2' subtree and record the assignment in the SMI
    -- Numbers registry.

    -- RFC Ed.: When the above assignment has been made, please
    -- remove the above note
    -- replace "AAAA" here with the assigned value and
    -- remove this note.

  -- Textual convention

  L2L3VpnMcastProviderTunnelType ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "This textual convention enumerates values
         representing the type of a provider tunnel (P-tunnel)
         used for L2L3VpnMCast.
         These labeled numbers are aligned with the definition
         of Tunnel types in Section 5 of [RFC6514] and
         Section 14.1 of [RFC7524].

         The enumerated values and the corresponding tunnel type
         are as follows:

           noTunnelInfo       (0) : no tunnel information present
           rsvpP2mp           (1) : RSVP-TE P2MP LSP
           ldpP2mp            (2) : mLDP P2MP LSP
           pimSsm             (3) : PIM-SSM Tree
           pimAsm             (4) : PIM-SM Tree
           pimBidir           (5) : BIDIR-PIM Tree
           ingressReplication (6) : Ingress Replication
           ldpMp2mp           (7) : mLDP MP2MP LSP
           transportTunnel    (8) : Transport Tunnel

         These numbers are registered at IANA.
         A current list of assignments can be found at
          <https://www.iana.org/assignments/bgp-parameters/
           bgp-parameters.xhtml#pmsi-tunnel-types>.
        "
    REFERENCE
        "RFC6514, Section 5
         RFC7385
         RFC7524, Section 14.1
        "
    SYNTAX       INTEGER
         {
```

```
          noTunnelInfo       (0), -- no tunnel information present
          rsvpP2mp           (1), -- RSVP-TE P2MP LSP
          ldpP2mp            (2), -- mLDP P2MP LSP
          pimSsm             (3), -- PIM-SSM Tree
          pimAsm             (4), -- PIM-SM Tree
          pimBidir           (5), -- BIDIR-PIM Tree
          ingressReplication (6), -- Ingress Replication
          ldpMp2mp           (7), -- mLDP MP2MP LSP
          transportTunnel    (8)  -- Transport Tunnel
        }

  L2L3VpnMcastProviderTunnelId ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "This textual convention represents the tunnel identifier
         of a P-tunnel.

         The size of the identifier depends on the address family
         (IPv4 or IPv6) and the value of the corresponding
         L2L3VpnMcastProviderTunnelType object.

         The corresponding L2L3VpnMcastProviderTunnelType object
         represents the type of the tunneling technology used
         to establish the P-tunnel.

         The size of the identifier for each tunneling technology
         is summarized below.

          L2L3VpnMcastProviderTunnelType            Size (in octets)
           (tunneling technology)                      IPv4  IPv6
         ------------------------------------------------------------
           noTunnelInfo       (No tunnel information)    0     0
           rsvpP2mp           (RSVP-TE P2MP LSP)        12    24
           ldpP2mp            (mLDP P2MP LSP)           17    29
           pimSsm             (PIM-SSM Tree)             8    32
           pimAsm             (PIM-SM Tree)              8    32
           pimBidir           (BIDIR-PIM Tree)           8    32
           ingressReplication (Ingress Replication)      4    16
           ldpMp2mp           (mLDP MP2MP LSP)          17    29
           transportTunnel    (Transport Tunnel)         8    32

         A L2L3VpnMcastProviderTunnelType object of value
         noTunnelInfo(0) indicates that the corresponding
         Provider Multicast Service Interface (PMSI) Tunnel
         attribute does not have tunnel information.
         The value of the corresponding L2L3VpnMcastProviderTunnelId
         object will be a string of length zero.
```

When the L2L3VpnMcastProviderTunnelType object is of value
rsvpP2mp(1), the corresponding Tunnel Identifier is composed of
Extended Tunnel ID (4 octets in IPv4, 16 octets in IPv6),
Reserved (2 octets), Tunnel ID (2 octets), and
P2MP ID (4 octets).
The size of the corresponding L2L3VpnMcastProviderTunnelId
object will be 12 octets in IPv4 and 24 octets in IPv6.

When the L2L3VpnMcastProviderTunnelType object is of value
ldpP2mp(2), the corresponding Tunnel Identifier is P2MP
Forwarding Equivalence Class (FEC) Element [RFC6388].
The size of the corresponding L2L3VpnMcastProviderTunnelId
object will be 17 octets in IPv4 and 29 octets in IPv6

When the L2L3VpnMcastProviderTunnelType object is of value
pimSsm(3), PimAsm(4), or PimBidir(5), the corresponding
Tunnel Identifier is composed of the source IP address
and the group IP address.
The size of the corresponding L2L3VpnMcastProviderTunnelId
object will be 8 octets in IPv4 and 32 octets in IPv6.

When the L2L3VpnMcastProviderTunnelType object is of value
ingressReplication(6), the Tunnel Identifier is
the unicast tunnel endpoint IP address of the local PE.
The size of the corresponding L2L3VpnMcastProviderTunnelId
object will be 4 octets in IPv4 and 16 octets in IPv6.

When the L2L3VpnMcastProviderTunnelType object is of value
ldpMp2mp(7), the Tunnel Identifier is MP2MP FEC Element
[RFC6388].
The size of the corresponding L2L3VpnMcastProviderTunnelId
object will be 17 octets in IPv4 and 29 octets in IPv6.

When the L2L3VpnMcastProviderTunnelType object is of value
transportTunnel(8), the Tunnel Identifier is a tuple of
Source PE Address (4 octets in IPv4, 16 octets in IPv6) and
Local Number (the same length as the Source PE Address)
[RFC7524].
The size of the corresponding L2L3VpnMcastProviderTunnelId
object will be 8 octets in IPv4 and 32 octets in IPv6.
"

REFERENCE
"RFC6514, Section 5
RFC4875, Section 19.1
RFC6388, Section 2.2 and 3.2
RFC7524, Section 14.1
"

SYNTAX OCTET STRING (SIZE (0|4|8|12|16|17|24|29|32))

```
END
```

4.2. L2L3-VPN-MCAST-MIB Object Definitions

```
L2L3-VPN-MCAST-MIB DEFINITIONS ::= BEGIN

IMPORTS
  MODULE-IDENTITY, OBJECT-TYPE, mib-2, zeroDotZero
     FROM SNMPv2-SMI                              -- [RFC2578]

  MODULE-COMPLIANCE, OBJECT-GROUP
     FROM SNMPv2-CONF                             -- [RFC2580]

  RowPointer
     FROM SNMPv2-TC                               -- [RFC2579]

  MplsLabel
     FROM MPLS-TC-STD-MIB                         -- [RFC3811]

  L2L3VpnMcastProviderTunnelType,
  L2L3VpnMcastProviderTunnelId
     FROM L2L3-VPN-MCAST-TC-MIB;                  -- [RFCXXXX]

  -- RFC Ed.: replace XXXX with actual RFC number and remove this note

l2L3VpnMcastMIB MODULE-IDENTITY
  LAST-UPDATED "201706211200Z"  -- 21th June, 2017
  ORGANIZATION "IETF BESS Working Group."
  CONTACT-INFO
        "        Zhaohui Zhang
                 Juniper Networks, Inc.
                 10 Technology Park Drive
                 Westford, MA 01886
                 USA
                 Email: zzhang@juniper.net

                 Hiroshi Tsunoda
                 Tohoku Institute of Technology
                 35-1, Yagiyama Kasumi-cho
                 Taihaku-ku, Sendai, 982-8577
                 Japan
                 Email: tsuno@m.ieice.org

                 Comments and discussion to bess@ietf.org
        "
  DESCRIPTION
      "This MIB module will be used by other MIB modules designed for
       monitoring and/or configuring Border Gateway
```

```
         Protocol/MultiProtocol Label Switching
         Layer 2 and Layer 3 Virtual Private
         Network that support multicast (L2L3VpnMCast).
         Copyright (C) The Internet Society (2017).
        "
    -- Revision history.

    REVISION "201706211200Z"  -- 21th June, 2017
    DESCRIPTION
        "Initial version, published as RFC XXXX."

    -- RFC Ed.: replace XXXX with actual RFC number and remove this note

    ::= { mib-2 BBBB }

    -- IANA Reg.: Please assign a value for "BBBB" under the
    -- 'mib-2' subtree and record the assignment in the SMI
    -- Numbers registry.

    -- RFC Ed.: When the above assignment has been made, please
    -- remove the above note
    -- replace "BBBB" here with the assigned value and
    -- remove this note.

  -- Top level components of this MIB.
  l2L3VpnMcastStates      OBJECT IDENTIFIER
                          ::= { l2L3VpnMcastMIB 1 }
  l2L3VpnMcastConformance OBJECT IDENTIFIER
                          ::= { l2L3VpnMcastMIB 2 }

  -- tables, scalars, conformance information
  -- Table of PMSI Tunnel Attributes

  l2L3VpnMcastPmsiTunnelAttributeTable OBJECT-TYPE
     SYNTAX        SEQUENCE OF L2L3VpnMcastPmsiTunnelAttributeEntry
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
         "An entry in this table corresponds to a
          (Provider Multicast Service Interface) PMSI Tunnel
          attribute and is maintained by a PE router
          that advertises and receives the attribute.
          The entries will be referred to by other MIB modules
          for monitoring and/or configuring L2L3VpnMCast.
         "
     REFERENCE
         "RFC6514, Section 5"
     ::= { l2L3VpnMcastStates 1 }
```

```
  l2L3VpnMcastPmsiTunnelAttributeEntry OBJECT-TYPE
     SYNTAX        L2L3VpnMcastPmsiTunnelAttributeEntry
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
         "A conceptual row corresponding to a PTA
          that is advertised/received on this router.
         "
     REFERENCE
         "RFC6514, Section 5"
     INDEX {
             l2L3VpnMcastPmsiTunnelAttributeFlags,
             l2L3VpnMcastPmsiTunnelAttributeType,
             l2L3VpnMcastPmsiTunnelAttributeLabel,
             l2L3VpnMcastPmsiTunnelAttributeId
           }
     ::= { l2L3VpnMcastPmsiTunnelAttributeTable 1 }

  L2L3VpnMcastPmsiTunnelAttributeEntry ::=
      SEQUENCE {
          l2L3VpnMcastPmsiTunnelAttributeFlags
              OCTET STRING,
          l2L3VpnMcastPmsiTunnelAttributeAddlFlags
              OCTET STRING,
          l2L3VpnMcastPmsiTunnelAttributeType
              L2L3VpnMcastProviderTunnelType,
          l2L3VpnMcastPmsiTunnelAttributeLabel
              MplsLabel,
          l2L3VpnMcastPmsiTunnelAttributeId
              L2L3VpnMcastProviderTunnelId,
          l2L3VpnMcastPmsiTunnelPointer
              RowPointer,
          l2L3VpnMcastPmsiTunnelIf
              RowPointer
      }

  l2L3VpnMcastPmsiTunnelAttributeFlags OBJECT-TYPE
     SYNTAX        OCTET STRING (SIZE (1))
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
         "This object represents the Flags field in the PMSI Tunnel
          attribute. The Flags field has the following format.

             0 1 2 3 4 5 6 7
            +-+-+-+-+-+-+-+-+
            |U|E|    U    |L|
            +-+-+-+-+-+-+-+-+
```

E: Extension flag [RFC7902]
U: Unassigned
L: Leaf Information Required flag [RFC6514]

When BGP-based PMSI signaling is used, the value of
this object corresponds to the Flags field in
an advertised/received PMSI auto-discovery (A-D) route.

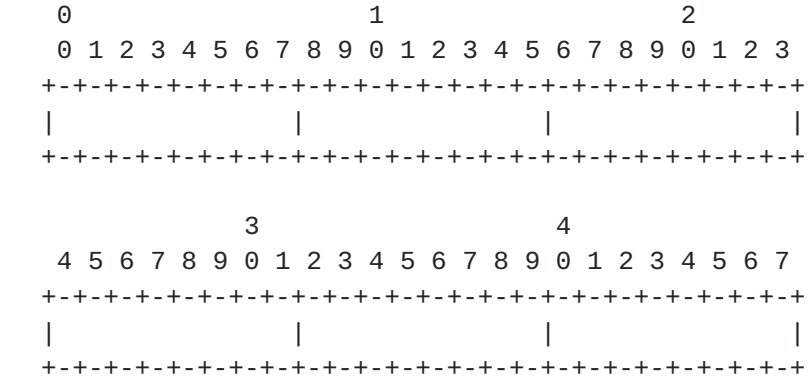
When UDP-based S-PMSI signaling is used, the value of
this object is zero.

These flags are registered at IANA.
A current list of assignments can be found at
<https://www.iana.org/assignments/bgp-parameters/
bgp-parameters.xhtml#pmsi-tunnel-attributes>.
"

REFERENCE
"RFC6514, Section 5
RFC7902
"
::= { l2L3VpnMcastPmsiTunnelAttributeEntry 1 }

l2L3VpnMcastPmsiTunnelAttributeAddlFlags OBJECT-TYPE
SYNTAX OCTET STRING (SIZE (6))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"This object represents BGP Additional PMSI
Tunnel Attribute Flags Extended Community
defined in [RFC7902].

Additional PMSI Tunnel Attribute Flags is
48 one-bit Flags and has the following format.



When BGP-based PMSI signaling is used, and the
Extension flag of l2L3VpnMcastPmsiTunnelAttributeFlags

```
          object is set, the value of this object corresponds to
          the value of Additional PMSI Tunnel Attribute Flags
          Extended Community in an advertised/received PMSI
          auto-discovery (A-D) route.

          When UDP-based S-PMSI signaling is used, the value of
          this object is zero.

          These flags are registered at IANA.
          A current list of assignments can be found at
          <https://www.iana.org/assignments/bgp-extended-communities/
           bgp-extended-communities.xhtml
           #additional-pmsi-tunnel-attribute-flags>.
         "
    REFERENCE
        "RFC6514, Section 5
         RFC7902
        "
    ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 2 }

  l2L3VpnMcastPmsiTunnelAttributeType OBJECT-TYPE
    SYNTAX        L2L3VpnMcastProviderTunnelType
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION
        "The Tunnel Type field that identifies
         the type of the tunneling technology used to
         establish the provider tunnel (P-tunnel), in a
         PMSI Tunnel attribute.

         When BGP-based PMSI signaling is used, the value of
         this object corresponds to the Tunnel Type field in
         an advertised/received PMSI auto-discovery (A-D) route.

         When UDP-based S-PMSI signaling is used, the value of
         this object will be one of pimAsm (3), pimSsm (4), or
         pimBidir (5).
        "
    REFERENCE
        "RFC6514, Section 5"
    ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 3 }

  l2L3VpnMcastPmsiTunnelAttributeLabel OBJECT-TYPE
    SYNTAX        MplsLabel
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION
        "The MPLS Label field in a PMSI Tunnel attribute.
```

```
          When BGP-based PMSI signaling is used, the value of
          this object corresponds to the MPLS Label field in
          an advertised/received PMSI A-D route.

          When UDP-based S-PMSI signaling is used, the value of
          this object is zero that indicates the absence of MPLS
          Label.
         "
      REFERENCE
          "RFC6514, Section 5"
      ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 4 }

   l2L3VpnMcastPmsiTunnelAttributeId OBJECT-TYPE
      SYNTAX        L2L3VpnMcastProviderTunnelId
      MAX-ACCESS    not-accessible
      STATUS        current
      DESCRIPTION
          "The Tunnel Identifier field that uniquely
          identifies a tunnel, in a PMSI Tunnel attribute.
          The size of the identifier depends on the address family
          (IPv4 or IPv6) and the value of the corresponding
          l2L3VpnMcastPmsiTunnelAttributeType object i.e., the type of
          the tunneling technology used to establish the provider
          tunnel.
         "
      REFERENCE
          "RFC6514, Section 5"
      ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 5 }

   l2L3VpnMcastPmsiTunnelPointer OBJECT-TYPE
      SYNTAX        RowPointer
      MAX-ACCESS    read-only
      STATUS        current
      DESCRIPTION
          "The tunnel identified by l2L3VpnMcastPmsiTunnelAttributeId
          may be represented as an entry in some other table, e.g.,
          mplsTunnelTable [RFC3812]. This object specifies
          the pointer to the row pertaining to the entry.

          If such an entry does not exist, the value of this object
          MUST be zeroDotZero.
         "
      DEFVAL        { zeroDotZero }
      ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 6 }

   l2L3VpnMcastPmsiTunnelIf OBJECT-TYPE
      SYNTAX        RowPointer
      MAX-ACCESS    read-only
```

```
    STATUS       current
    DESCRIPTION
        "If the tunnel identified by l2L3VpnMcastPmsiTunnelAttributeId
         has a corresponding entry in the ifXTable [RFC2863],
         this object will point to the row pertaining to the entry
         in the ifXTable. Otherwise, this object MUST be set to
         zeroDotZero."
    DEFVAL       { zeroDotZero }
    ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 7 }

-- Conformance Information

l2L3VpnMcastGroups      OBJECT IDENTIFIER
                        ::= { l2L3VpnMcastConformance 1 }
l2L3VpnMcastCompliances OBJECT IDENTIFIER
                        ::= { l2L3VpnMcastConformance 2 }

-- Compliance Statements

l2L3VpnMcastCompliance MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
       "The compliance statement: no mandatory groups "
    MODULE  -- this module

    GROUP l2L3VpnMcastOptionalGroup
         DESCRIPTION
             "This group is optional."
    ::= { l2L3VpnMcastCompliances 1 }

-- units of conformance

l2L3VpnMcastOptionalGroup    OBJECT-GROUP
    OBJECTS {
        l2L3VpnMcastPmsiTunnelPointer,
        l2L3VpnMcastPmsiTunnelIf
    }
    STATUS      current
    DESCRIPTION
        "Support of these objects is not required."
    ::= { l2L3VpnMcastGroups 1 }

END
```

5. Security Considerations

There are no management objects defined in these MIB modules that have a MAX-ACCESS clause of read-write and/or read-create. So, if this MIB module is implemented correctly, then there is no risk that an intruder can alter or create any management objects of this MIB module via direct SNMP SET operations.

Some of the readable objects in these MIB modules (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

- the l2L3VpnMcastPmsiTunnelAttributeTable collectively shows the P-tunnel network topology and its performance characteristics. For instance, l2L3VpnMcastPmsiTunnelAttributeId in this table will contain the identifier that uniquely identifies a created P-tunnel. This identifier may be composed of source and multicast group IP addresses. l2L3VpnMcastPmsiTunnelPointer and l2L3VpnMcastPmsiTunnelIf will point to the corresponding entries in other tables containing configuration and/or performance information of a tunnel and an interface. If an Administrator does not want to reveal this information, then these objects should be considered sensitive/vulnerable.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

Implementations SHOULD provide the security features described by the SNMPv3 framework (see [RFC3410]), and implementations claiming compliance to the SNMPv3 standard MUST include full support for authentication and privacy via the User-based Security Model (USM) [RFC3414] with the AES cipher algorithm [RFC3826]. Implementations MAY also provide support for the Transport Security Model (TSM) [RFC5591] in combination with a secure transport such as SSH [RFC5592] or TLS/DTLS [RFC6353].

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to

the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

6. IANA Considerations

IANA is requested to root MIB objects in the MIB module contained in this document under the mib-2 subtree.

7. References

7.1. 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>.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, DOI 10.17487/RFC2578, April 1999, <http://www.rfc-editor.org/info/rfc2578>.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, DOI 10.17487/RFC2579, April 1999, <http://www.rfc-editor.org/info/rfc2579>.

[RFC2580] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Conformance Statements for SMIv2", STD 58, RFC 2580, DOI 10.17487/RFC2580, April 1999, <http://www.rfc-editor.org/info/rfc2580>.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000, <http://www.rfc-editor.org/info/rfc2863>.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, DOI 10.17487/RFC3414, December 2002, <http://www.rfc-editor.org/info/rfc3414>.

[RFC3812] Srinivasan, C., Viswanathan, A., and T. Nadeau, "Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)", RFC 3812, DOI 10.17487/RFC3812, June 2004, <http://www.rfc-editor.org/info/rfc3812>.

[RFC3826] Blumenthal, U., Maino, F., and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", RFC 3826, DOI 10.17487/RFC3826, June 2004, <http://www.rfc-editor.org/info/rfc3826>.

[RFC4087] Thaler, D., "IP Tunnel MIB", RFC 4087, DOI 10.17487/RFC4087, June 2005, <http://www.rfc-editor.org/info/rfc4087>.

[RFC5591] Harrington, D. and W. Hardaker, "Transport Security Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 5591, DOI 10.17487/RFC5591, June 2009, <http://www.rfc-editor.org/info/rfc5591>.

[RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5592, DOI 10.17487/RFC5592, June 2009, <http://www.rfc-editor.org/info/rfc5592>.

[RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 6353, DOI 10.17487/RFC6353, July 2011, <http://www.rfc-editor.org/info/rfc6353>.

[RFC6513] Rosen, E., Ed. and R. Aggarwal, Ed., "Multicast in MPLS/BGP IP VPNs", RFC 6513, DOI 10.17487/RFC6513, February 2012, <http://www.rfc-editor.org/info/rfc6513>.

[RFC6514] Aggarwal, R., Rosen, E., Morin, T., and Y. Rekhter, "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs", RFC 6514, DOI 10.17487/RFC6514, February 2012, <http://www.rfc-editor.org/info/rfc6514>.

[RFC7117] Aggarwal, R., Ed., Kamite, Y., Fang, L., Rekhter, Y., and C. Kodeboniya, "Multicast in Virtual Private LAN Service (VPLS)", RFC 7117, DOI 10.17487/RFC7117, February 2014, <http://www.rfc-editor.org/info/rfc7117>.

[RFC7385] Andersson, L. and G. Swallow, "IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points", RFC 7385, DOI 10.17487/RFC7385, October 2014, <http://www.rfc-editor.org/info/rfc7385>.

[RFC7524] Rekhter, Y., Rosen, E., Aggarwal, R., Morin, T., Grosclaude, I., Leymann, N., and S. Saad, "Inter-Area Point-to-Multipoint (P2MP) Segmented Label Switched Paths (LSPs)", RFC 7524, DOI 10.17487/RFC7524, May 2015, <http://www.rfc-editor.org/info/rfc7524>.

7.2. Informative References

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, DOI 10.17487/RFC3410, December 2002, <http://www.rfc-editor.org/info/rfc3410>.

Authors' Addresses

Zhaohui (Jeffrey) Zhang
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886
USA

Email: zzhang@juniper.net

Hiroshi Tsunoda
Tohoku Institute of Technology
35-1, Yagiyama Kasumi-cho
Taihaku-ku, Sendai 982-8577
Japan

Phone: +81-22-305-3411
Email: tsuno@m.ieice.org