Internet Engineering Task Force (IETF)
Request for Comments: 8502
Category: Standards Track
ISSN: 2070-1721
December 2018

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

L2L3 VPN Multicast MIB

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 that 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8502.

Copyright Notice

Table of Contents

1. Introduction

In BGP/MPLS Virtual Private Networks (VPNs), the Border Gateway Protocol (BGP) is used for distributing routes and Multiprotocol Label Switching (MPLS) is used for forwarding packets across service provider networks.

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

L2L3VpnMCast networks use various transport mechanisms for forwarding a packet to all or a subset of Provider Edge (PE) routers across service provider networks. These transport mechanisms are abstracted as provider tunnels (P-tunnels). The type of P-tunnel indicates the type of tunneling technology used to establish the P-tunnel. The syntax and semantics of a Tunnel Identifier are determined by the corresponding P-tunnel type [RFC6514]. The P-tunnel type and P-tunnel identifier together identify a P-tunnel.

A BGP attribute that specifies information of a P-tunnel is called a 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. The P-tunnel type and the P-tunnel identifier are included in the corresponding PMSI Tunnel attribute.

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

This document defines two TCs to represent

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

The document also defines MOs that will provide the information contained in a PMSI Tunnel attribute and corresponding P-tunnel.

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, and Multicast VPN concepts and/or mechanisms is assumed. Some terms specifically related to this document are explained below.

PMSI [RFC6513] is a conceptual interface instantiated by a P-tunnel, which is 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 to both "I-PMSI" and "S-PMSI".

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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-MULTICAST-TC-MIB and L2L3-VPN-MULTICAST-MIB.

- L2L3-VPN-MULTICAST-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-MULTICAST-MIB defines the following table: l2L3VpnMcastPmsiTunnelAttributeTable. An entry in this table corresponds to the attribute information of a specific P-tunnel on a PE router. Entries in this table will be used by other MIB modules for monitoring and/or configuring an L2L3VpnMCast network. The table index uniquely identifies a P-tunnel. It is composed of a type and identifier of a P-tunnel. The table may also be used in conjunction with other MIBs, such as the MPLS Traffic Engineering MIB (MPLS-TE-STD-MIB) [RFC3812], to obtain further information about a P-tunnel. It may also be used in conjunction with the Interfaces Group MIB (IF-MIB) [RFC2863] to obtain further information about the interface corresponding to a P-tunnel.

4. Definitions

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

This MIB module makes reference to the following documents: [RFC4875], [RFC5015], [RFC6388], [RFC7524], and [RFC7761].

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

   IMPORTS
     MODULE-IDENTITY, mib-2
        FROM SNMPv2-SMI                            -- RFC 2578

     TEXTUAL-CONVENTION
        FROM SNMPv2-TC;                            -- RFC 2579

   l2L3VpnMcastTCMIB MODULE-IDENTITY
     LAST-UPDATED "201812140000Z"  -- 14 December 2018
     ORGANIZATION "IETF BESS Working Group"
     CONTACT-INFO
                  "Zhaohui Zhang
                   Juniper Networks, Inc.
                   10 Technology Park Drive
                   Westford, MA 01886
                   United States of America
                   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"

     DESCRIPTION
         "This MIB module specifies textual conventions for
          Border Gateway Protocol/Multiprotocol Label
          Switching Layer 2 and Layer 3 Virtual Private Networks
          that support multicast (L2L3VpnMCast networks).

          Copyright (c) 2018 IETF Trust and the persons identified
          as authors of the code.  All rights reserved.

          Redistribution and use in source and binary forms, with or
          without modification, is permitted pursuant to, and subject
          to the license terms contained in, the Simplified BSD
          License set forth in Section 4.c of the IETF Trust's Legal
          Provisions Relating to IETF Documents
          (http://trustee.ietf.org/license-info).
         "
```

```
      -- Revision History

      REVISION "201812140000Z"  -- 14 December 2018
      DESCRIPTION
          "Initial version, published as RFC 8502."

      ::= { mib-2 244 }

    -- 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 networks.
           These labeled numbers are aligned with the definition
           of Tunnel Types in Section 5 of RFC 6514 and
           Section 14.1 of RFC 7524.

           The enumerated values and the corresponding P-tunnel types
           are as follows:

            noTunnelInfo       (0) : No tunnel information RFC 6514
            rsvpP2mp           (1) : RSVP-TE P2MP LSP      RFC 4875
            ldpP2mp            (2) : mLDP P2MP LSP         RFC 6388
            pimSsm             (3) : PIM-SSM Tree          RFC 7761
            pimAsm             (4) : PIM-SM Tree           RFC 7761
            pimBidir           (5) : BIDIR-PIM Tree        RFC 5015
            ingressReplication (6) : Ingress Replication   RFC 6513
            ldpMp2mp           (7) : mLDP MP2MP LSP        RFC 6388
            transportTunnel    (8) : Transport Tunnel      RFC 7524

           These numbers are registered at IANA.
           A current list of assignments can be found at
           <https://www.iana.org/assignments/bgp-parameters/>.
          "
      REFERENCE
          "RFC 4875
           RFC 5015
           RFC 6388
           RFC 6513
           RFC 6514, Section 5
           RFC 7524, Section 14.1
           RFC 7761
          "
      SYNTAX       INTEGER
           {
             noTunnelInfo       (0),
             rsvpP2mp           (1),
             ldpP2mp            (2),
             pimSsm             (3),
             pimAsm             (4),
             pimBidir           (5),
             ingressReplication (6),
             ldpMp2mp           (7),
             transportTunnel    (8)
           }

    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 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

           The Tunnel Type is set to 'No tunnel information'
           when the PMSI Tunnel attribute carries no tunnel
           information (there is no Tunnel Identifier).
           The value of the corresponding L2L3VpnMcastProviderTunnelId
           object will be a string of length zero.
           For Tunnel Type rsvpP2mp(1), the corresponding Tunnel
           Identifier is composed of an Extended Tunnel ID (4 octets in
           IPv4, 16 octets in IPv6), 2 unused (Reserved) octets that of
           value zero, a Tunnel ID (2 octets), and a Point-to-Multipoint
           (P2MP) ID (4 octets).  The size of the corresponding
           L2L3VpnMcastProviderTunnelId object will be 12 octets in IPv4
           and 24 octets in IPv6.

           For Tunnel Type ldpP2mp(2), the corresponding Tunnel
           Identifier is the P2MP Forwarding Equivalence Class (FEC)
           Element (RFC 6388).  The size of the corresponding
           L2L3VpnMcastProviderTunnelId object will be 17 octets
           in IPv4 and 29 octets in IPv6.

           For Tunnel Types pimSsm(3), PimAsm(4), and 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.

           For Tunnel Type 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.

           For Tunnel Type ldpMp2mp(7), the Tunnel Identifier is
           a Multipoint-to-Multipoint (MP2MP) FEC Element (RFC 6388).
           The size of the corresponding L2L3VpnMcastProviderTunnelId
           object will be 17 octets in IPv4 and 29 octets in IPv6.

           For Tunnel Type transportTunnel(8), the Tunnel Identifier
           is a tuple of Source PE Address and Local Number,
           which is a number that is unique to the Source PE (RFC 7524).
           Both Source PE Address and Local Number are 4 octets in IPv4
           and 16 octets in IPv6.
           The size of the corresponding L2L3VpnMcastProviderTunnelId
           object will be 8 octets in IPv4 and 32 octets in IPv6.
          "
      REFERENCE
          "RFC 6514, Section 5
           RFC 4875, Section 19.1
           RFC 6388, Sections 2.2 and 3.2
           RFC 7524, Section 14.1
          "
      SYNTAX       OCTET STRING ( SIZE (0|4|8|12|16|17|24|29|32) )

    END
```

4.2. L2L3-VPN-MULTICAST-MIB Object Definitions

This MIB module makes reference to the following documents: [RFC3811].

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

  IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, mib-2, zeroDotZero
       FROM SNMPv2-SMI                                -- RFC 2578

    MODULE-COMPLIANCE, OBJECT-GROUP
       FROM SNMPv2-CONF                               -- RFC 2580

    RowPointer
       FROM SNMPv2-TC                                 -- RFC 2579

    MplsLabel
       FROM MPLS-TC-STD-MIB                           -- RFC 3811

    L2L3VpnMcastProviderTunnelType,
    L2L3VpnMcastProviderTunnelId
       FROM L2L3-VPN-MULTICAST-TC-MIB;                -- RFC 8502

  l2L3VpnMcastMIB MODULE-IDENTITY
    LAST-UPDATED "201812140000Z"  -- 14 December 2018
    ORGANIZATION "IETF BESS Working Group"
    CONTACT-INFO
                  "Zhaohui Zhang
                   Juniper Networks, Inc.
                   10 Technology Park Drive
                   Westford, MA 01886
                   United States of America
                   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"

    DESCRIPTION
        "This MIB module defines a table representing the attribute
         information of the provider tunnels (P-tunnels) on a PE router.
         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 network).

         Copyright (c) 2018 IETF Trust and the persons identified
         as authors of the code.  All rights reserved.

         Redistribution and use in source and binary forms, with or
         without modification, is permitted pursuant to, and subject
         to the license terms contained in, the Simplified BSD License
         set forth in Section 4.c of the IETF Trust's Legal Provisions
         Relating to IETF Documents
         (http://trustee.ietf.org/license-info).
        "

    -- Revision History

    REVISION "201812140000Z"  -- 14 December 2018
    DESCRIPTION
        "Initial version, published as RFC 8502."

    ::= { mib-2 245 }

  -- 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
          the attribute information of a specific
          P-tunnel on a PE router.
          A part of the attributes corresponds to fields in
          a Provider Multicast Service Interface (PMSI) Tunnel
          attribute advertised and received by a PE router.
          The entries will be referred to by other MIB modules
          for monitoring and/or configuring L2L3VpnMCast networks.
         "
     REFERENCE
         "RFC 6514, Section 5"
     ::= { l2L3VpnMcastStates 1 }

  l2L3VpnMcastPmsiTunnelAttributeEntry OBJECT-TYPE
     SYNTAX        L2L3VpnMcastPmsiTunnelAttributeEntry
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
         "A conceptual row corresponding to a specific
          P-tunnel on this router.
         "
     REFERENCE
         "RFC 6514, Section 5"
     INDEX {
             l2L3VpnMcastPmsiTunnelAttributeType,
             l2L3VpnMcastPmsiTunnelAttributeId
           }
     ::= { l2L3VpnMcastPmsiTunnelAttributeTable 1 }

  L2L3VpnMcastPmsiTunnelAttributeEntry ::=
      SEQUENCE {
          l2L3VpnMcastPmsiTunnelAttributeType
              L2L3VpnMcastProviderTunnelType,
          l2L3VpnMcastPmsiTunnelAttributeId
              L2L3VpnMcastProviderTunnelId,
          l2L3VpnMCastPmsiTunnelLeafInfoRequired
              INTEGER,
          l2L3VpnMcastPmsiTunnelAttributeMplsLabel
              MplsLabel,
          l2L3VpnMcastPmsiTunnelPointer
              RowPointer,
          l2L3VpnMcastPmsiTunnelIf
              RowPointer
      }

  l2L3VpnMcastPmsiTunnelAttributeType OBJECT-TYPE
     SYNTAX        L2L3VpnMcastProviderTunnelType
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
         "This object indicates the type of tunneling technology
          used to establish the P-tunnel corresponding to this entry.

          When BGP-based PMSI signaling is used, the value of
          this object corresponds to the Tunnel Type field
          in the PMSI Tunnel attribute advertised/received
          in a PMSI auto-discovery (A-D) route.
         "
     REFERENCE
         "RFC 6514, Section 5"
     ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 1 }

  l2L3VpnMcastPmsiTunnelAttributeId OBJECT-TYPE
     SYNTAX        L2L3VpnMcastProviderTunnelId
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
         "This object represents the Tunnel Identifier field, which
          uniquely identifies a P-tunnel, in the PMSI Tunnel attribute
          of the P-tunnel corresponding to this entry.

          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
          tunneling technology used to establish the P-tunnel.
         "
     REFERENCE
         "RFC 6514, Section 5"
     ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 2 }


  l2L3VpnMCastPmsiTunnelLeafInfoRequired OBJECT-TYPE
     SYNTAX        INTEGER {
                       false       (0),
                       true        (1),
                       notAvailable (2)
                   }
     MAX-ACCESS    read-only
     STATUS        current
     DESCRIPTION
         "When the value of this object is set to 1 (true),
          it indicates that the PE that originated the
          PMSI Tunnel attribute of the P-tunnel corresponding
          to this entry requests receivers to originate
          a new Leaf A-D route.

          A value of zero (false) indicates that there is no such
          request.

          When the P-tunnel does not have a corresponding PMSI
          Tunnel attribute, the value of this object will be
          2 (notAvailable).
          In the case of multicast in MPLS/BGP IP VPNs,
          this object represents the 'Leaf Information Required flag'
          (RFC 6514) in the Flags field in the PMSI Tunnel attribute
          of the P-tunnel corresponding to this entry.
         "
     REFERENCE
         "RFC 6514, Section 5
         "
     ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 3 }

  l2L3VpnMcastPmsiTunnelAttributeMplsLabel OBJECT-TYPE
     SYNTAX        MplsLabel
     MAX-ACCESS    read-only
     STATUS        current
     DESCRIPTION
         "This object represents the MPLS Label in the PMSI Tunnel
          attribute of the P-tunnel corresponding to this entry.

          When BGP-based PMSI signaling is used, the PMSI Tunnel
          attribute of the P-tunnel will be advertised/received
          in a PMSI A-D route.  The value of
          this object corresponds to the MPLS Label in the attribute.

          When the P-tunnel does not have a PMSI tunnel
          attribute, the value of this object will be zero.
         "
     REFERENCE
         "RFC 6514, Section 5"
     ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 4 }

  l2L3VpnMcastPmsiTunnelPointer OBJECT-TYPE
     SYNTAX        RowPointer
     MAX-ACCESS    read-only
     STATUS        current
     DESCRIPTION
         "Details of a P-tunnel identified by
          l2L3VpnMcastPmsiTunnelAttributeId may be present
          in some other table, e.g.,
          mplsTunnelTable (RFC 3812).  This object specifies
          the pointer to the row that pertains to the entry
          in the table.

          If no such entry exists, the value of this object
          will be zeroDotZero.
         "
     REFERENCE
         "RFC 3812, Sections 6.1 and 11"
     DEFVAL        { zeroDotZero }
```

```
        ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 5 }

     l2L3VpnMcastPmsiTunnelIf OBJECT-TYPE
        SYNTAX        RowPointer
        MAX-ACCESS    read-only
        STATUS        current
        DESCRIPTION
            "If the P-tunnel identified by
             l2L3VpnMcastPmsiTunnelAttributeId has a corresponding
             entry in ifXTable (RFC 2863), this object will
             point to the row in ifXTable that pertains to the entry.
             Otherwise, the value of this object will be zeroDotZero.
            "
        REFERENCE
            "RFC 2863, Section 6"
        DEFVAL        { zeroDotZero }
        ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 6 }

     -- Conformance Information

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

     -- Compliance Statements

     l2L3VpnMcastCoreCompliance MODULE-COMPLIANCE
         STATUS  current
         DESCRIPTION
            "The core compliance statement for SNMP entities
             that implement the L2L3-VPN-MULTICAST-MIB module.
            "
         MODULE  -- this module

         MANDATORY-GROUPS {
              l2L3VpnMcastCoreGroup
         }
         ::= { l2L3VpnMcastCompliances 1 }

     l2L3VpnMcastFullCompliance MODULE-COMPLIANCE
         STATUS  current
         DESCRIPTION
            "The full compliance statement for SNMP entities
             that implement the L2L3-VPN-MULTICAST-MIB module.
            "
         MODULE  -- this module
```

```
      MANDATORY-GROUPS {
           l2L3VpnMcastCoreGroup,
           l2L3VpnMcastOptionalGroup
      }
      ::= { l2L3VpnMcastCompliances 2 }

  -- Units of Conformance

  l2L3VpnMcastCoreGroup    OBJECT-GROUP
      OBJECTS {
          l2L3VpnMCastPmsiTunnelLeafInfoRequired,
          l2L3VpnMcastPmsiTunnelAttributeMplsLabel
      }
      STATUS      current
      DESCRIPTION
          "Support of these objects is required.
          "
      ::= { l2L3VpnMcastGroups 1 }

  l2L3VpnMcastOptionalGroup    OBJECT-GROUP
      OBJECTS {
          l2L3VpnMcastPmsiTunnelPointer,
          l2L3VpnMcastPmsiTunnelIf
      }
      STATUS      current
      DESCRIPTION
          "Support of these objects is optional.
          "
      ::= { l2L3VpnMcastGroups 2 }

  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 objects in these MIB modules may be considered sensitive or vulnerable in some network environments. This includes INDEX objects with a MAX-ACCESS of not-accessible, and any indices from other modules exposed via AUGMENTS. 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:

- o 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 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 P-tunnel and its 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

The MIB module in this document uses the following IANA-assigned OBJECT IDENTIFIER values recorded in the "SMI Network Management MGMT Codes Internet-standard MIB" registry:

Name	Description	OBJECT-IDENTIFIER value
l2L3VpnMcastTCMIB	L2L3-VPN-MULTICAST-TC-MIB	{ mib-2 244 }
l2L3VpnMcastMIB	L2L3-VPN-MULTICAST-MIB	{ mib-2 245 }

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, <https://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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc2580>.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000, <https://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, <https://www.rfc-editor.org/info/rfc3414>.

[RFC3811] Nadeau, T., Ed. and J. Cucchiara, Ed., "Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management", RFC 3811, DOI 10.17487/RFC3811, June 2004, <https://www.rfc-editor.org/info/rfc3811>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc3826>.

[RFC4875] Aggarwal, R., Ed., Papadimitriou, D., Ed., and S. Yasukawa, Ed., "Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)", RFC 4875, DOI 10.17487/RFC4875, May 2007, <https://www.rfc-editor.org/info/rfc4875>.

[RFC5015] Handley, M., Kouvelas, I., Speakman, T., and L. Vicisano, "Bidirectional Protocol Independent Multicast (BIDIR-PIM)", RFC 5015, DOI 10.17487/RFC5015, October 2007, <https://www.rfc-editor.org/info/rfc5015>.

[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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc6353>.

[RFC6388] Wijnands, IJ., Ed., Minei, I., Ed., Kompella, K., and B. Thomas, "Label Distribution Protocol Extensions for Point- to-Multipoint and Multipoint-to-Multipoint Label Switched Paths", RFC 6388, DOI 10.17487/RFC6388, November 2011, <https://www.rfc-editor.org/info/rfc6388>.

[RFC6513] Rosen, E., Ed. and R. Aggarwal, Ed., "Multicast in MPLS/BGP IP VPNs", RFC 6513, DOI 10.17487/RFC6513, February 2012, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7117>.

[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, <https://www.rfc-editor.org/info/rfc7524>.

[RFC7761] Fenner, B., Handley, M., Holbrook, H., Kouvelas, I., Parekh, R., Zhang, Z., and L. Zheng, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", STD 83, RFC 7761, DOI 10.17487/RFC7761, March 2016, <https://www.rfc-editor.org/info/rfc7761>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

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, <https://www.rfc-editor.org/info/rfc3410>.

Acknowledgements

Glenn Mansfield Keeni did the MIB Doctor review and provided valuable comments.

Authors' Addresses

Zhaohui (Jeffrey) Zhang
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886
United States of America

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