Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 14, 2017

Z. Zhang
Juniper Networks, Inc.
H. Tsunoda
Tohoku Institute of Technology
April 12, 2017

L2L3 VPN Multicast MIB
draft-ietf-bess-l2l3-vpn-mcast-mib-07

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 common managed objects used by other MIB modules which are designed for monitoring and/or configuring both Layer 2 and Layer 3 Virtual Private Networks (VPN) that support multicast.

Table of Contents

1. Introduction

[RFC7117] and [RFC6513] specify procedures for supporting multicast in Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Layer 2 (L2) and Layer 3 (L3) VPN (Virtual Private Network), respectively.

Multicast service in BGP/MPLS L2 and L3 VPN 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).

The signaling of P-tunnel choice is very similar for multicast in both L2 and L3 VPNs. [RFC7117] and [RFC6513] describe BGP-based mechanisms for Virtual Private LAN Service (VPLS) and Multicast VPN (MVPN), respectively. [RFC6514] defines the Provider Multicast Service Interface (PMSI) tunnel attribute, a BGP attribute that specifies information of a P-tunnel. The PMSI tunnel attribute is advertised/received by PEs in BGP auto-discovery (A-D) routes. [RFC6513] also proposes a UDP-based signaling mechanism.

This document defines a textual convention (TC) that can be used to represent types of P-tunnels used for multicast in BGP/MPLS L2 or L3 VPN within MIB module specifications.

This document also describes common managed objects used by other MIB modules which are designed for monitoring and/or configuring both L2 and L3 VPN that support multicast.

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, L3 VPN, MVPN (Multicast VPN) concepts and/or mechanisms is assumed. Some terms specifically related to this document are explained below.

The term "Multicast VPN (MVPN)" [RFC6513] refers to a BGP/MPLS L3 (IP) VPN service that supports multicast.

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

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

[RFC6513] describes the following tunnel setup techniques that can be used to create the P-tunnels that instantiate the PMSIs.

- Protocol Independent Multicast tree
  - Sparse Mode (PIM-SM) tree [RFC4601]
  - Source Specific Multicast (PIM-SSM) tree [RFC4601]
  - Bidirectional Protocol Independent Multicast (BIDIR-PIM) tree [RFC5015]
- Label Distribution Protocol Extension for Multipoint Label Switched Paths (mLDP) [RFC6388]
  - Point-to-MultiPoint (mLDP P2MP)
  - Point-to-MultiPoint (mLDP MP2MP)

- Resource Reservation Protocol - Traffic Engineering Point-to-Multipoint (RSVP-TE P2MP) Label Switched Path [RFC4875]

- Ingress Replication through Unicast Tunnels [RFC6513]

A created tunnel will be identified by Tunnel Identifier. The length of the identifier differs depending on the setup technique that is used to create the tunnel.

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 Module

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

- L2L3-VPN-MCAST-TC-MIB contains three Textual Conventions: L2L3VpnMcastProviderTunnelType, L2L3VpnMcastPmsiTunnelPointerType, and L2L3VpnMcastPmsiTunnelPointer.
  L2L3VpnMcastProviderTunnelType provides an enumeration of the provider tunnel types. L2L3VpnMcastPmsiTunnelPointerType indicates a type of pointer to the row pertaining to a table entry that represents a provider tunnel. L2L3VpnMcastPmsiTunnelPointer denotes a pointer to the row pertaining to a table entry that represents a provider tunnel.

- L2L3-VPN-MCAST-MIB defines a table l2L3VpnMcastPmsiTunnelAttributeTable. An entry in this table corresponds to a PMSI Tunnel Attribute (PTA) advertised/received by PE routers. The entry of the table will be used by other MIB modules which are designed for monitoring and/or configuring both L2 and L3 VPN that support multicast.
  The table index is composed of multiple attributes that depend on the tunnel type and uniquely identify a tunnel.

The table may also be used in conjunction with other MIBs, such as MPLS Traffic Engineering MIB (MPLS-TE-STD-MIB) [RFC3812], to obtain the other details 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 the other details of a corresponding interface that tunnel uses 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 "201702211200Z"  -- 21th February, 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 contains a textual convention for
       Border Gateway Protocol/MultiProtocol Label
       Switching (BGP/MPLS) Layer 2 (L2) and Layer 3
       (L3) Virtual Private Network (VPN).
       Copyright (C) The Internet Society (2017)."
```

```
    -- Revision history.

    REVISION "201702211200Z"  -- 21th February, 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 the values
         representing a type of a provider tunnel
         used for multicast in BGP/MPLS L2 or L3 VPN.
         These labelled numbers are aligned based on the definition
         of Tunnel types in Section 5 of [RFC6514].
         "
    REFERENCE
        "RFC6514, Section 5"
    SYNTAX       INTEGER
         { noTunnelId         (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
         }

  L2L3VpnMcastProviderTunnelPointer ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "Denotes a pointer to the row pertaining
         to a table entry that represents a
```

```
        provider tunnel used for multicast in BGP/MPLS L2 or L3 VPN.

        An L2L3VpnMcastProviderTunnelPointer value is always
        interpreted within the context of an
        L2L3VpnMcastProviderTunnelPointerType value.
        Every usage of the L2L3VpnMcastProviderTunnelPointer
        textual convention MUST specify the
        L2L3VpnMcastProviderTunnelPointerType object which
        provides the context.

        Furthermore, MIB authors SHOULD define a separate
        L2L3VpnMcastProviderTunnelPointerType object for each
        L2L3VpnMcastProviderTunnelPointer object.
        The L2L3VpnMcastProviderTunnelPointerType object which
        defines the context must be registered immediately before
        the object which uses the L2L3VpnMcastProviderTunnelPointer
        textual convention.

        The value of an L2L3VpnMcastProviderTunnelPointer object
        must always be consistent with the value of the associated
        L2L3VpnMcastProviderTunnelPointerType object. Attempts
        to set a L2L3VpnMcastProviderTunnelPointer object to a value
        which is inconsistent with the associated
        L2L3VpnMcastProviderTunnelPointerType must fail with
        an inconsistentValue error.
        "
    SYNTAX       OBJECT IDENTIFIER


  L2L3VpnMcastProviderTunnelPointerType ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "This textual convention enumerates the types of
         tables having the row that an L2L3VpnMcastProviderTunnelPointer
         object points to.
         The row pertains to the entry that represents a
         provider tunnel used for multicast in BGP/MPLS
         L2 or L3 VPN.

         The enumerated values have the following meaning:

           null(0)
             A pointer is null.

           pointerToMplsTunnelTable(1)
             A pointer points to the row in mplsTunnelTable defined in
             [RFC3812].
```

```
          pointerToTunnelIfTableForGRE(2)
            A pointer points to the row in tunnelIfTable defined in
            [RFC4087] for GRE tunnel.
        "
    REFERENCE
        "RFC3812, RFC4087"

    SYNTAX       INTEGER
         { null                          (0), -- A pointer is null.
           pointerToMplsTunnelTable      (1), -- A pointer to the row
                                              -- in mplsTunnelTable
           pointerToTunnelIfTableForGRE (2)  -- A pointer to the row
                                              -- in tunnelIfTable
                                              -- for GRE tunnel
         }


  END
```

4.2. L2L3-VPN-MCAST-MIB Object Definitions

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

  IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, mib-2
       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,
    L2L3VpnMcastProviderTunnelPointerType,
    L2L3VpnMcastProviderTunnelPointer
       FROM L2L3-VPN-MCAST-TC-MIB;

  l2L3VpnMcastMIB MODULE-IDENTITY
    LAST-UPDATED "201702211200Z"  -- 21th February, 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 both Layer 2 (L2) and
         Layer 3 (L3) Virtual Private Networks (VPN) that support
         multicast.
         Copyright (C) The Internet Society (2017)."

    -- Revision history.

    REVISION "201702211200Z"  -- 21th February, 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 of this table corresponds to a
         PMSI Tunnel attribute and is created by a PE router
         that advertises and receives the attribute.
         The entry in the table will be referred by other MIB modules
         which are designed for monitoring and/or configuring
         both L2 and L3 VPN that support multicast."
    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,
          l2L3VpnMcastPmsiTunnelAttributeType
              L2L3VpnMcastProviderTunnelType,
          l2L3VpnMcastPmsiTunnelAttributeLabel
              MplsLabel,
          l2L3VpnMcastPmsiTunnelAttributeId
              OCTET STRING,
          l2L3VpnMcastPmsiTunnelPointerType
              L2L3VpnMcastProviderTunnelPointerType,
          l2L3VpnMcastPmsiTunnelPointer
              L2L3VpnMcastProviderTunnelPointer,
          l2L3VpnMcastPmsiTunnelIf
              RowPointer
      }
```

```
  l2L3VpnMcastPmsiTunnelAttributeFlags OBJECT-TYPE
     SYNTAX        OCTET STRING (SIZE (1))
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
         "Denotes the Flags field in a PMSI Tunnel attribute
          with the following format.

               0 1 2 3 4 5 6 7
              +-+-+-+-+-+-+-+-+
              |  reserved   |L|
              +-+-+-+-+-+-+-+-+

              L: Leaf Information Required

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

          When UDP-based S-PMSI signaling is used, the value of
          this object is zero."
     REFERENCE
         "RFC6514, Section 5"
     ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 1 }

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

          When BGP-based I/S-PMSI signaling is used, the value of
          this object corresponds to the Tunnel Type field in
          an advertised/received I/S-PMSI 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 2 }

  l2L3VpnMcastPmsiTunnelAttributeLabel OBJECT-TYPE
     SYNTAX        MplsLabel
```

```
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION
        "Denotes the MPLS Label field that contains
         an MPLS label, in a PMSI Tunnel attribute.

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

         When UDP-based S-PMSI signaling is used, the value of
         this object is zero that indicates absence of MPLS
         Label."
    REFERENCE
        "RFC6514, Section 5"
    ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 3 }

  l2L3VpnMcastPmsiTunnelAttributeId OBJECT-TYPE
    SYNTAX        OCTET STRING ( SIZE (0|4|8|12|16|17|24|29|32) )
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION
        "Denotes the Tunnel Identifier field that uniquely
         identifies a created tunnel, in a PMSI Tunnel
         attribute.
         The size of the identifier depends on the address family
         (IPv4 or IPv6) and the value of
         l2L3VpnMcastPmsiTunnelAttributeType, i.e., the type of
         the tunneling technology used to establish the provider
         tunnel.

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

          Size (in octets)   l2L3VpnMcastPmsiTunnelAttributeType
             IPv4  IPv6      (tunneling technology)
           ------------------------------------------------
              0     0       noTunnelId (No tunnel information present)
             12    24       rsvpP2mp   (RSVP-TE P2MP LSP)
             17    29       ldpP2mp    (mLDP P2MP LSP)
              8    32       pimSsm     (PIM-SSM Tree)
              8    32       pimAsm     (PIM-SM Tree)
              8    32       pimBidir   (BIDIR-PIM Tree)
              4    16       ingressReplication
                                       (Ingress Replication)
             17    29       ldpMp2mp   (mLDP MP2MP LSP)

         When l2L3VpnMcastPmsiTunnelAttributeType is set to
```

```
            noTunnelId(0), the PMSI Tunnel attribute does not have
            tunnel information. Thus, the size of this object is zero.

            When l2L3VpnMcastPmsiTunnelAttributeType is set to
            rsvpP2mp(1), the 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). Thus, the size of this object is
            12 octets in IPv4 and 24 octets in IPv6.

            When l2L3VpnMcastPmsiTunnelAttributeType is set to
            ldpP2mp(2), the Tunnel Identifier is 17 octets
            (in IPv4) or 29 octets (in IPv6) P2MP Forwarding
            Equivalence Class (FEC) Element.

            When l2L3VpnMcastPmsiTunnelAttributeType is set to
            pimSsm(3), PimAsm(4), or PimBidir(5), the Tunnel Identifier is
            a pair of source and group IP addresses.
            Thus, the size of this object is 16 octets in IPv4
            and 32 octets in IPv6.

            When l2L3VpnMcastPmsiTunnelAttributeType is set to
            ingressReplication(6), the Tunnel Identifier is
            the unicast tunnel endpoint IP address of the local
            PE. Thus, the size of this object is 4 octets in IPv4
            and 16 octets in IPv6.

            When l2L3VpnMcastPmsiTunnelAttributeType is set to
            ldpMp2mp(7), the Tunnel Identifier is 17 octets
            (in IPv4) or 29 octets (in IPv6) MP2MP FEC Element.

            When BGP-based I/S-PMSI signaling is used, the value of
            this object corresponds to the Tunnel
            Identifier field in an advertised/received I/S-PMSI
            A-D route. Thus, the size of this object is determined
            by the above table.

            When UDP-based S-PMSI signaling is used, the value of
            this object is a pair of source and group IP addresses.
            Thus, the size of this object is 16 octets in IPv4
            and 32 octets in IPv6."
        REFERENCE
            "RFC6514, Section 5
             RFC4875, Section 19.1
             RFC6388, Section 2.2 and 2.3"
        ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 4 }

    l2L3VpnMcastPmsiTunnelPointerType    OBJECT-TYPE
```

```
    SYNTAX        L2L3VpnMcastProviderTunnelPointerType
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION
        "The type of l2L3VpnMcastPmsiTunnelPointer.

         The tunnel identified by l2L3VpnMcastPmsiTunnelAttributeId
         may be represented as an entry in other table, e.g,
         mplsTunnelTable [RFC3812]. This object specifies
         the type of pointer to the row pertaining to the entry.

         If such an entry does not exist, the value of this object
         becomes null(0).
        "
    ::= { l2L3VpnMcastPmsiTunnelAttributeEntry 5 }

  l2L3VpnMcastPmsiTunnelPointer OBJECT-TYPE
    SYNTAX        L2L3VpnMcastProviderTunnelPointer
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION
        "The pointer to a table entry representing the tunnel
         identified by l2L3VpnMcastPmsiTunnelAttributeId.

         The type of this pointer is specified with
         the corresponding instance of the
         l2L3VpnMcastPmsiTunnelPointerType object.

         If the value of the corresponding instance of the
         l2L3VpnMcastPmsiTunnelPointerType is null(0),
         the value of this object MUST be null.
        "
    ::= { 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, the pointer is null."
    ::= { 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 {
          l2L3VpnMcastPmsiTunnelPointerType,
          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 this MIB module 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 this MIB module (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:

- o l2L3VpnMcastPmsiTunnelPointer and l2L3VpnMcastPmsiTunnelIf in l2L3VpnMcastPmsiTunnelAttributeTable 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>.

[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>.

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>.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, DOI 10.17487/RFC4601, August 2006, <http://www.rfc-editor.org/info/rfc4601>.

[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, <http://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, <http://www.rfc-editor.org/info/rfc5015>.

[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, <http://www.rfc-editor.org/info/rfc6388>.

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