MBONED WG
Internet-Draft
Intended status: Standards Track
Expires: 15 October 2026

Z. Zhang
ZTE Corporation
C. Wang
Individual
Y. Cheng
China Unicom
X. Liu
Alef Edge
M. Sivakumar
Juniper networks
13 April 2026

A YANG Data Model for Multicast Services
draft-ietf-mboned-multicast-yang-model-16

Abstract

This document provides a generic multicast YANG data model that shows the relevant technologies or protocols used by multicast flows. It provides a management view for network administrators to obtain information about multicast services.

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 https://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 15 October 2026.

Copyright Notice

Table of Contents

1. Introduction

Currently, there are many multicast protocol YANG models, such as PIM (Protocol Independent Multicast), MLD (Multicast Listener Discovery), and BIER (Bit Index Explicit Replication) and so on. But all these models are distributed in different working groups as separate files and focus on the protocol itself. Furthermore, they cannot describe a high-level multicast service required by network operators.

This document provides a general and all-round multicast model, which shows the relevant technologies or protocols used by multicast flows. It provides a management view for network administrators to obtain information about multicast services.

This document does not define any specific protocol model, instead, it depends on many existing multicast protocol models and relates several multicast information together to fulfill multicast service.

This document defines one YANG 1.1 [RFC7950] data model for the management of multicast service. This model can be used along with other multicast YANG models such as PIM [RFC9128], which are not covered in this document.

1.1. Terminology

The terminology for describing YANG data models is found in [RFC6020] and [RFC7950], including:

* data model
* data node
* identity
* module

The following abbreviations are used in this document and the defined model:

BIER: Bit Index Explicit Replication [RFC8279].

BIER-TE: Traffic Engineering for Bit Index Explicit Replication [RFC9262].

MLD: Multicast Listener Discovery [I-D.ietf-bier-mld].

MLDP: Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths [RFC6388].

MVPN: Multicast in MPLS/BGP IP VPNs [RFC6513].

P2MP-TE: Point-to-Multipoint Traffic Engineering [RFC4875].

PIM: Protocol Independent Multicast [RFC7761].

SR-P2MP: Segment Routing Point-to-Multipoint [I-D.ietf-pim-sr-p2mp-policy].

1.2. Conventions Used in This Document

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.

1.3. Tree Diagrams

Tree diagrams used in this document follow the notation defined in [RFC8340].

1.4. Prefixes in Data Node Names

In this document, names of data nodes, actions, and other data model objects are often used without a prefix, as long as it is clear from the context in which YANG module each name is defined. Otherwise, names are prefixed using the standard prefix associated with the corresponding YANG module, as shown in Table 1.

Prefix	YANG module	Reference
inet	ietf-inet-types	[RFC9911]
rt-types	ietf-routing-types	[RFC8294]

Table 1

2. Design of the Data Model

2.1. Scope of Model

This model can be used to configure and manage the multicast service. The operational state data can be retrieved by this model. The subscription and push mechanism defined in [RFC8639] and [RFC8641] can be implemented by the user to subscribe to notifications on the data nodes in this model.

The model contains all the basic configuration parameters to configure the multicast service. Depending on the implementation choices, some systems may not allow some of the advanced parameters to be configurable. The occasionally implemented parameters are modeled as optional features in this model. This model can be extended, and it has been structured in a way that such extensions can be conveniently made.

2.1.1. Usage of Multicast Model

This multicast YANG data model is mainly used by the management tools run by the network operators, in order to manage, monitor and debug the network resources that are used to deliver multicast service. This model is used for gathering data from the network as well.

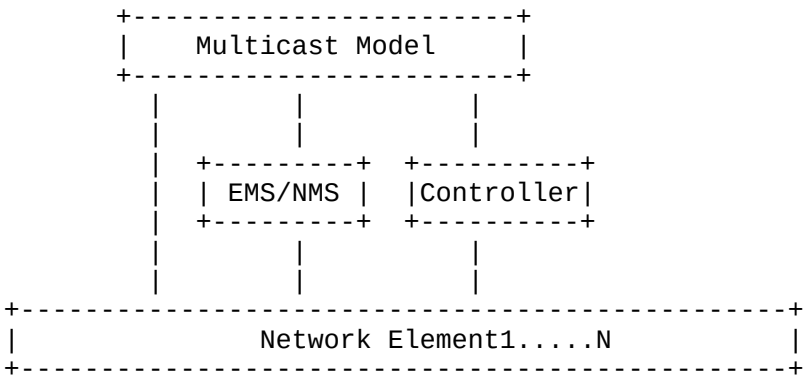

Figure 1: Usage of Multicast Model

Figure 1 illustrates example use cases for this multicast model. Network operators can use this model in a controller which is responsible to implement specific multicast flows with specific protocols and work with the corresponding protocols' model to configure the network elements through NETCONF/RESTCONF/CLI. Or network operators can use this model to the EMS (Element Management System)/ NMS (Network Management System) to manage or configure the network elements directly.

On the other hand, when the network elements detect failure or some other changes, the network devices can send the affected multicast flows and the associated signaling/ transport information to the controller. Then the controller/ EMS/NMS can respond immediately due to the failure. Such as the changing of the failure signaling protocol to another one, as well as transport protocol. Network nodes can enable appropriate signaling and transport technologies for multicast flows based on the YANG model configuration obtained from the controller. For example, the network ingress node of a multicast flow can specify its signaling protocol as MVPN and its network transport technology as BIER based on the obtained YANG model configuration. If the network ingress node does not support BIER technology, it will send a notification to the controller so that the controller can respond and adjust accordingly. Different multicast flow can use the same or different signaling and transport protocols. For the same multicast traffic, different signaling and transport technologies can also be used due to different management needs.

The Route Distinguisher, source-address and group-address of L3 multicast flow are the multicast flow keys. For example, when the group-address is set, and the source-address is set to * or a specific value, this is (*,G) or (S,G) analogous. In addition to the source-address and group-address, when vpn-rd is also set, this is MVPN use case. For non-VPN multicast, according to the definition in section 2.1 of RFC7716, when all RDs are set to zero, it indicates non-VPN multicast, i.e., Global Table Multicast.

* When the ingress node of a multicast flow receives the configured YANG model, it can announce the multicast flow using the signaling protocol specified, such as MVPN. Egress nodes with receiving needs will initiate a join signaling message to the ingress node.

* When a multicast flow’s egress node receives a configured YANG model, if a signaling protocol is specified, it can initiate joining using the specified signaling protocol based on its calculated upstream multicast next hop.

* When a transport protocol type is configured, the specified transport protocol type may be added to the signaling. For protocols that can use virtual topology for forwarding via IGP routing, such as BIER, MLDP, and PIM, when topology and flex algo number are configured, traffic will be forwarded according to the corresponding logical topology.

* More than one ingress node for a multicast flow can be set in the model. In this situation, two or more ingress nodes are used for a multicast flow forwarding, the ingress routers can be backup for each other. More information can be found in [I-D.ietf-mboned-redundant-ingress-failover].

* Network ingress or egress nodes can feed back the YANG model to the controller so that network administrators can check the consistency of configuration and effectiveness. When the received information is inconsistent with expectations, for example, a multicast flow should be forwarded through BIER transmission, but the received information shows that the multicast flow is forwarded by PIM, there may be some management inconsistencies.

2.2. Specification

This model imports and augments ietf-routing YANG model defined in [RFC8349]. The container "multicast-service" is the top-level container in this data model. The container is expected to enable multicast service functionality.

The YANG data model defined in this document conforms to the Network Management Datastore Architecture (NMDA) [RFC8342]. The operational state data is combined with the associated configuration data in the same hierarchy [RFC9907].

2.3. Overview

Tree diagrams used in this document follow the notation defined in [RFC8340].

The model as a whole consists of multicast flow key-value pairs, upstream and downstream information. Upstream information includes the multicast flow’s ingress node in the multicast domain and the dynamic signaling protocols it may use; downstream information includes the multicast flow’s egress node in the multicast domain, the dynamic signaling protocols it may use, and the transport protocols it may use. Here, the multicast domain refers to a management domain, which includes all edge nodes (ingress and egress nodes) and corresponding intermediate nodes.

```
module: ietf-multicast
  +--rw multicast-service
     +--rw multicast-flow* [vpn-rd source-address group-address]
        +--rw vpn-rd            rt-types:route-distinguisher
        +--rw source-address    ip-multicast-source-address
        +--rw group-address     rt-types:ip-multicast-group-address
        +--rw upstream
```

```
|  +--rw neighbor* [neighbor-address]
|     +--rw neighbor-address    inet:ip-address
|     +--rw vni-type?           identityref
|     +--rw signaling?          identityref
|     +--rw (protocol-type)?
|        +--:(evpn)
|        +--:(mld)
|        +--:(mld-snooping)
|        +--:(mvpn)
|        +--:(pim)
+--rw downstream* [signaling transport]
   +--rw neighbor* [neighbor-address]
   |  +--rw neighbor-address    inet:ip-address
   +--rw signaling               identityref
   +--rw (protocol-type)?
   |  +--:(evpn)
   |  +--:(mld)
   |  +--:(mld-snooping)
   |  +--:(mvpn)
   |  +--:(pim)
   +--rw transport               identityref
   +--rw (transport-tech-type)?
      +--:(bier) {bier}?
      |  +--rw bier* [sub-domain]
      |     +--rw sub-domain         uint16
      |     +--rw tad* [mt-id fa-number data-plane]
      |     |  +--rw mt-id          uint16
      |     |  +--rw fa-number      uint8
      |     |  +--rw data-plane     uint8
      |     +--rw bitstringlength?   uint16
      |     +--rw bier-encap-type?   identityref
      +--:(bier-te) {bier-te}?
      |  +--rw bitstring* [name]
      |     +--rw name           string
      |     +--rw bier-te-adj* [adj-id]
      |        +--rw adj-id    uint16
      +--:(mldp) {mldp}?
      |  +--rw mt-id?            uint16
      |  +--rw fa-number?        uint8
      +--:(rsvp-te-p2mp) {p2mp-te}?
      |  +--rw tunnel-name?      string
      +--:(pim) {pim}?
      |  +--rw source-address?   ip-multicast-source-address
      |  +--rw group-address
      |  |       rt-types:ip-multicast-group-address
      |  +--rw bidir?            boolean {bidir}?
      |  +--rw tad* [mt-id fa-number data-plane]
      |     +--rw mt-id          uint16
```

```
                |     +--rw fa-number     uint8
                |     +--rw data-plane    uint8
               +--:(ir-tunnel) {ir-tunnel}?
               |  +--rw ir-tunnel-type?   uint8
               +--:(sr-p2mp) {sr-p2mp}?
               +--:(native)

     notifications:
       +---n ingress-egress-event
          +--ro event-type?       identityref
          +--ro multicast-flow* [vpn-rd source-address group-address]
             +--ro vpn-rd            rt-types:route-distinguisher
             +--ro source-address    ip-multicast-source-address
             +--ro group-address     rt-types:ip-multicast-group-address
             +--ro upstream
             |  +--ro neighbor-address?   inet:ip-address
             |  +--ro signaling?          identityref
             +--ro downstream* [signaling transport]
                +--ro neighbor-address?   inet:ip-address
                +--ro signaling           identityref
                +--ro transport           identityref
```

2.4. Multicast YANG data model Configuration

This model can work with other protocol data models to provide multicast service.

Based on the concept of multicast, the model includes upstream and downstream information. The content of this model includes multicast service keys, the multicast service signaling, the transport protocol information. Multicast keys include the features of multicast flow, such as (vpn-rd, multicast source and multicast group) information.

Multicast flows can be advertised via dynamic protocol signaling. Both ingress and egress nodes can be configured and obtain the dynamic signaling protocol types they use through the model. In certain scenarios, multicast flows can also perform tunnel encapsulation (GRE, VXLAN, etc.) before transport protocol encapsulation; the tunnel encapsulation type is included in the upstream information. Multicast flows can specify transport protocols and can further specify their associated logical topology based on topology and flex algo number; transport protocol information is included in the downstream information.

When a multicast flow does not need to be advertised via a dynamic signaling protocol, the addresses of all ingress and egress nodes can be directly specified in the model. When a multicast flow is

advertised between ingress and egress nodes via a dynamic signaling protocol, it is not necessary to include the addresses of all ingress and egress nodes in the model; only the address of the ingress or egress node needs to be included. When a multicast flow needs to be transmitted via a specified protocol, the downstream information in the model needs to include the transmission protocol information.

2.4.1. Example

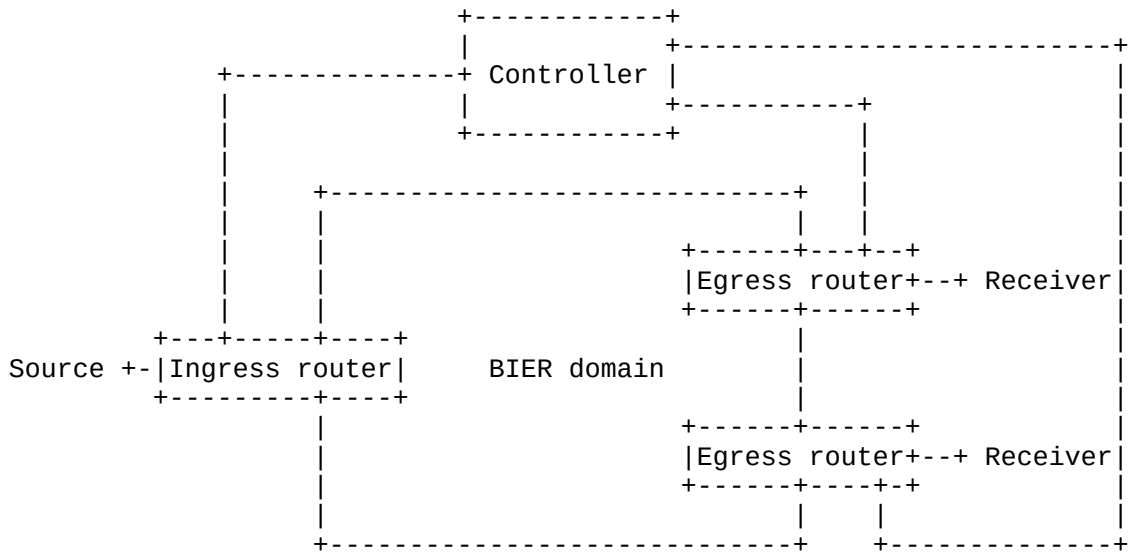

Figure 2: Example

In this example, a multicast flow using MVPN with a group address of 233.252.0.10 will be sent from one ingress node to two egress nodes within this multicast domain via BIER technology.

The models sent to both the ingress (upstream) and egress nodes (downstream) will contain key-value information about the flow, such as the RD and group address. The source address can be set to "*". The ingress node address is 198.51.100.10. When the ingress node receives the model, it can identify itself as upstream based on the address and configure its signaling as MVPN. The ingress node with address 198.51.100.10 will then use MVPN signaling to announce the multicast flow information.

The model sent to the egress nodes (198.51.100.20, 198.51.100.30) will, in addition to containing the multicast flow key, specify its downstream neighbors address. The egress nodes will recognize themselves as the egress node based on the downstream neighbor

address and can then notify the upstream node of its joining information for the multicast group via MVPN signaling, specifying that traffic transmission should be via BIERin6. Furthermore, traffic transmission can be performed using a specific virtual topology, such as a virtual topology built based on the Flex Algo number 200 soft-dataplane.

The JSON example in the appendix can be considered a configuration example of this model. In practical applications, it is not necessary to specify both upstream and downstream information simultaneously; specifying only upstream or downstream is sufficient for it to function.

When there is no dynamic signaling protocol between the ingress and egress nodes, the configuration YANG model includes all ingress and egress nodes and specifies the use of the BIER transport protocol in the downstream information. Referring to the JSON example in the appendix, the signaling parameter can be removed from the upstream and downstream information.

2.5. Multicast YANG data model State

Multicast model states are the same with the configuration. In most cases, network administrators can use this model to obtain multicast flows and related protocol information such as signaling protocols and transport technologies.

2.6. Multicast YANG data model Notification

The defined Notifications include the events of ingress or egress nodes. Like ingress node failure, signaling/ transport module loading/ unloading. And the potential failure about some multicast flows and associated signaling/ transport technologies.

3. Multicast YANG data Model

This module references [RFC4541], [RFC4875], [RFC4915], [RFC5015], [RFC5120], [RFC6388], [RFC6513], [RFC6514], [RFC7348], [RFC7432], [RFC7637], [RFC7716], [RFC7761], [RFC7988], [RFC8174], [RFC8279], [RFC8294], [RFC8296], [RFC8556], [RFC8926], [RFC9179], [RFC9262], [RFC9350], [RFC9502], [RFC9524], [RFC9572], [RFC9624], [RFC9658], [RFC9911], [I-D.ietf-bier-mld], [I-D.ietf-bier-bierin6], [I-D.ietf-bier-pim-signaling], [I-D.ietf-lsr-flex-soft-dataplane], [I-D.ietf-pim-sr-p2mp-policy], [I-D.ietf-pim-flex-algo].

```
<CODE BEGINS> file "ietf-multicast@2026-04-12.yang"
module ietf-multicast {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-multicast";
  prefix ietf-multicast;

  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 9911: Common YANG Data Types";
  }
  import ietf-routing-types {
    prefix rt-types;
    reference
      "RFC 8294: Common YANG Data Types for the Routing Area";
  }

  organization
    " IETF MBONED (MBONE Deployment) Working Group";
  contact
    "WG Web:   https://datatracker.ietf.org/wg/mboned/
     WG List:  <mailto:mboned@ietf.org>

     Editor:   Zheng Zhang
               <mailto:zhang.zheng@zte.com.cn>
     Editor:   Cui Wang
               <mailto:lindawangjoy@gmail.com>
     Editor:   Ying Cheng
               <mailto:chengying10@chinaunicom.cn>
     Editor:   Xufeng Liu
               <mailto:xufeng.liu.ietf@gmail.com>
     Editor:   Mahesh Sivakumar
               <mailto:sivakumar.mahesh@gmail.com>
    ";

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

  description
    "The module defines the YANG definitions for multicast service
     management. This model can be used to send multicast flow
     information to or retrieve multicast flow information from
     devices, including upstream and downstream node information,
     possible signaling protocols, and the multicast transmission
     protocol that actually carries the multicast flow.

     Copyright (c) 2026 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 Revised BSD License set
      forth in Section 4.c of the IETF Trust's Legal Provisions
      Relating to IETF Documents
      (https://trustee.ietf.org/license-info).

      This version of this YANG module is part of RFC XXXX
      (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
      for full legal notices.

      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 (RFC 2119) (RFC 8174) when, and only when,
      they appear in all capitals, as shown here.";

  revision 2026-04-12 {
    description
      "Initial revision.";
    reference
      "RFC XXXX: A YANG Data Model for multicast service management
       YANG.";
  }

  /*
   *feature
   */

  feature bier {
    description
      "Cooperation with BIER technology.";
    reference
      "RFC 8279: Multicast Using Bit Index Explicit Replication
         (BIER)";
  }

  feature bier-te {
    description
      "Cooperation with BIER-TE technology.";
    reference
      "RFC 9262: Tree Engineering for Bit Index Explicit Replication
         (BIER-TE)";
  }

  feature sr-p2mp {
    description
      "Cooperation with multipoint Segment Routing replication
```

```
          technology.";
      reference
        "RFC 9524: Segment Routing Replication for Multipoint
           Service Delivery";
    }

    feature ir-tunnel {
      description
        "Cooperation with Ingress Replication tunnel technology.";
      reference
        "RFC 7988: Ingress Replication Tunnels in Multicast VPN";
    }

    feature mldp {
      description
        "Cooperation with MLDP technology.";
      reference
        "RFC 6388: Label Distribution Protocol Extensions
           for Point-to-Multipoint and Multipoint-to-Multipoint
           Label Switched Paths";
    }

    feature p2mp-te {
      description
        "Cooperation with RSVP TE P2MP technology.";
      reference
        "RFC 4875: Extensions to Resource Reservation Protocol -
          Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE
          Label Switched Paths (LSPs)";
    }

    feature pim {
      description
        "Cooperation with PIM technology.";
      reference
        "RFC 7761: Protocol Independent Multicast - Sparse Mode
         (PIM-SM): Protocol Specification (Revised)";
    }

    feature bidir {
      description
        "Cooperation with BIDIR-PIM technology.";
      reference
        "RFC 5015: Bidirectional Protocol Independent Multicast
         (BIDIR-PIM)";
    }

    /*
```

```
     *typedef
     */

    typedef ip-multicast-source-address {
      type union {
        type enumeration {
          enum * {
            description
              "Any source address.";
          }
        }
        type inet:ipv4-address;
        type inet:ipv6-address;
      }
      description
        "Multicast source IP address type.";
    }

    /*
     * Identities
     */

    identity dynamic-signaling-type {
      description
        "Base identity for the dynamic signaling type of multicast
         service technology.";
    }

    identity transport-type {
      description
        "Identity for the multicast transport technology.";
    }

    identity tunnel-encap-type {
      description
        "Base identity for the type of multicast flow tunnel
         encapsulation.";
    }

    identity tunnel-encap-vxlan {
      base tunnel-encap-type;
      description
        "The VXLAN encapsulation is used for flow encapsulation.";
      reference
        "RFC 7348: Virtual eXtensible Local Area Network (VXLAN):
          A Framework for Overlaying Virtualized Layer 2 Networks
          over Layer 3 Networks";
    }
```

```
  identity tunnel-encap-nvgre {
    base tunnel-encap-type;
    description
      "The NVGRE encapsulation is used for flow encapsulation.";
    reference
      "RFC 7637: NVGRE: Network Virtualization Using Generic
        Routing Encapsulation";
  }

  identity tunnel-encap-geneve {
    base tunnel-encap-type;
    description
      "The GENEVE encapsulation is used for flow encapsulation.";
    reference
      "RFC 8926: Geneve: Generic Network Virtualization
        Encapsulation";
  }

  identity bier-encapsulation{
    description
      "Base identity for BIER encapsulation.";
  }
  identity bier-encap-mpls {
    base bier-encapsulation;
    description
      "This identity represents MPLS encapsulation for bier.";
  }
  identity bier-encap-ipv6 {
    base bier-encapsulation;
    description
      "This identity represents ipv6 encapsulation for bier.";
  }
  identity bier-encap-ethernet {
    base bier-encapsulation;
    description
      "This identity represents ethernet encapsulation for bier.";
  }

  identity signaling-pim {
    base dynamic-signaling-type;
    description
      "Using PIM as multicast service signaling technology.
       This signaling protocol needs to be used in conjunction
       with the transport protocol set to BIER.";
    reference
      "I-D.ietf-bier-pim-signaling: PIM Signaling Through BIER
        Core";
  }
```

```
     identity mld {
       base dynamic-signaling-type;
       description
         "Using MLD as multicast service signaling technology.
          This signaling protocol needs to be used in conjunction
          with the transport protocol set to BIER.";
       reference
         "I-D.ietf-bier-mld: BIER Ingress Multicast Flow Overlay
           using Multicast Listener Discovery Protocols";
     }

     identity mld-snooping {
       base dynamic-signaling-type;
       description
         "Using MLD-snooping as multicast service signaling
          technology.";
       reference
         "RFC 4541: Considerations for Internet Group Management
           Protocol (IGMP) and Multicast Listener
           Discovery (MLD) Snooping Switches";
     }

     identity evpn {
       base dynamic-signaling-type;
       description
         "Using EVPN as multicast service signaling technology.";
       reference
         "RFC 7432: BGP MPLS-Based Ethernet VPN
          RFC 9572: Updates on EVPN BUM Procedures
          RFC 9624: EVPN Broadcast, Unknown Unicast, or Multicast
           (BUM) Using Bit Index Explicit Replication (BIER)";
     }

     identity mvpn {
       base dynamic-signaling-type;
       description
         "Using MVPN as multicast service signaling technology.";
       reference
         "RFC 6513: Multicast in MPLS/BGP IP VPNs
          RFC 7716: Global Table Multicast with BGP Multicast VPN
           (BGP-MVPN) Procedures
          RFC 8556: Multicast VPN Using Bit Index Explicit
           Replication (BIER)";
     }

     identity bier {
       base transport-type;
       description
```

```
        "Using BIER as multicast transport technology.";
      reference
        "RFC 8279: Multicast Using Bit Index Explicit Replication
          (BIER)";
    }

    identity bier-te {
      base transport-type;
      description
        "Using BIER-TE as multicast transport technology.";
      reference
        "RFC 9262: Traffic Engineering for Bit Index Explicit
          Replication (BIER-TE)";
    }

    identity mldp {
      base transport-type;
      description
        "Using mLDP as multicast transport technology.";
      reference
        "RFC 6388: Label Distribution Protocol Extensions
          for Point-to-Multipoint and Multipoint-to-Multipoint
          Label Switched Paths";
    }

    identity rsvp-te-p2mp {
      base transport-type;
      description
        "Using P2MP TE as multicast transport technology.";
      reference
        "RFC 4875: Extensions to Resource Reservation Protocol
          - Traffic Engineering (RSVP-TE) for Point-to-Multipoint
          TE Label Switched Paths (LSPs)";
    }

    identity sr-p2mp {
      base transport-type;
      description
        "Using Segment Routing  as multicast transport technology.";
      reference
        "I-D.ietf-pim-sr-p2mp-policy:
           Segment Routing Point-to-Multipoint Policy";
    }

    identity pim {
      base transport-type;
      description
        "Using PIM as multicast transport technology.";
```

```
      reference
        "RFC 7761: Protocol Independent Multicast - Sparse Mode
          (PIM-SM): Protocol Specification (Revised)";
    }

    identity bidir {
      base transport-type;
      description
        "Using BIDIR-PIM as multicast transport technology.";
      reference
        "RFC 5015: Bidirectional Protocol Independent Multicast
          (BIDIR-PIM)";
    }

    identity event-type {
      description
        "The events of the multicast service.";
    }

    identity service-up {
      base event-type;
      description
        "The multicast service works.";
    }

    identity service-down {
      base event-type;
      description
        "There is something wrong with upstream or downstream node,
         and node can't work properlay.";
    }

    identity protocol-enabled {
      base event-type;
      description
        "The protocol that is used for multicast flows have been
         enabled.";
    }

    identity protocol-disabled {
      base event-type;
      description
        "The protocol that is used by multicast flows have been
         disabled.";
    }

    grouping general-multicast-key {
      description
```

```
        "The general multicast keys. They are used to differentiate
         multicast service.";
      leaf vpn-rd {
        type rt-types:route-distinguisher;
        description
          "A Route Distinguisher is used to differentiate
           routes from different MVPNs.
           When the value is set to 0, it indicates that it is
           Global Table Multicast as described in RFC7716.";
        reference
          "RFC 8294: Common YANG Data Types for the Routing Area
           RFC 6513: Multicast in MPLS/BGP IP VPNs
           RFC 7716: Global Table Multicast with BGP Multicast VPN
             (BGP-MVPN) Procedures";
      }
      leaf source-address {
        type ip-multicast-source-address;
        description
          "The IP source address of the multicast flow. The
           value set to * means that the receiver interests
           in all source that relevant to one given group.";
      }
      leaf group-address {
        type rt-types:ip-multicast-group-address;
        mandatory true;
        description
          "The IP group address of multicast flow. This
           type represents a version-neutral IP multicast group
           address. The format of the textual representation
           implies the IP version.";
        reference
          "RFC 8294: Common YANG Data Types for the Routing Area";
      }
    }

    // multicast-key

    grouping bier-key {
      description
        "The key parameters set for BIER/BIER TE forwarding.";
      reference
        "RFC 8279: Multicast Using Bit Index Explicit Replication
          (BIER).";
      leaf sub-domain {
        type uint16;
        description
          "The subdomain ID that the multicast flow belongs to.";
      }
```

```
      list tad {
        key "mt-id fa-number data-plane";
        description
          "The associated Multi-Topology ID, Flex Algo number and
           data plane type.";
        leaf mt-id {
          type uint16;
          description
            "The multi-topology ID that the multicast flow belongs
             to.";
          reference
            "RFC 4915: Multi-Topology (MT) Routing in OSPF
             RFC 5120: M-ISIS: Multi Topology (MT) Routing in
               Intermediate System to Intermediate Systems (IS-ISs)";
        }
        leaf fa-number {
          type uint8;
          description
            "Flex-algo number, value between 128 and 255 inclusive.";
          reference
            "RFC 9350: IGP Flexible Algorithm";
        }
        leaf data-plane {
          type uint8;
          description
            "Data plane type used for prefix calculation.";
          reference
            "RFC 9502: IGP Flexible Algorithm in IP Networks
             I-D.ietf-lsr-flex-soft-dataplane: IGP Flex Soft
              Dataplane";
        }
      }
      leaf bitstringlength {
        type uint16;
        description
          "The bitstringlength used by BIER forwarding.";
      }
      leaf bier-encap-type {
        type identityref {
          base bier-encapsulation;
        }
        description
          "The BIER encapsulation that can be used in either MPLS
           networks or non-MPLS networks.";
      }
    }

    grouping transport-tech {
```

```
      description
        "The transport technology selected for the multicast service.
         For one specific multicast flow.
         The same multicast flow may be forwarded using multiple
         transport technologies as needed for management purposes.";
      leaf transport {
        type identityref {
          base transport-type;
        }
        description
          "The type of transport technology";
      }
      choice transport-tech-type {
        description
          "The type of transport technology";
        case bier {
          if-feature "bier";
          list bier {
            key "sub-domain";
            description
              "Using BIER as the transport technology.
               The BIER technology is introduced in RFC8279.";
            reference
              "RFC 8296: Encapsulation for Bit Index Explicit
                 Replication (BIER) in MPLS and Non-MPLS Networks";
            uses bier-key;
          }
        }
        case bier-te {
          if-feature "bier-te";
          description
            "Using BIER-TE as the transport technology.
             The BIER-TE technology is introduced in RFC9262.";
          reference
            "RFC 9262: Tree Engineering for Bit Index Explicit
               Replication (BIER-TE)";
          list bitstring {
            key "name";
            leaf name {
              type string;
              description
                "The name of the bitstring";
            }
            list bier-te-adj {
              key "adj-id";
              leaf adj-id {
                type uint16;
                description
```

```
                  "The link adjacency ID used for BIER TE
                   forwarding.";
              }
              description
                "The adjacencies ID used for BIER TE bitstring
                 encapsulation.";
            }
            description
              "The bitstring name and detail used for BIER TE
               forwarding encapsulation. One or more bitstring
               can be used for backup path.";
          }
        }
        case mldp {
          if-feature "mldp";
          description
            "Using MLDP as the transport technology.";
          reference
            "RFC 6388: Label Distribution Protocol Extensions
              for Point-to-Multipoint and Multipoint-to-Multipoint
              Label Switched Paths
             RFC 9658:
              Multipoint LDP Extensions for Multi-Topology Routing";
          leaf mt-id {
            type uint16;
            description
              "The multi-topology ID that the multicast flow
               belongs to.";
            reference
              "RFC 4915: Multi-Topology (MT) Routing in OSPF
               RFC 5120: M-ISIS: Multi Topology (MT) Routing in
               Intermediate System to Intermediate Systems (IS-ISs)";
          }
          leaf fa-number {
            type uint8;
            description
              "Flex-algo number, value between 128 and 255
               inclusive.";
            reference
              "RFC 9350: IGP Flexible Algorithm";
          }
        }
        case rsvp-te-p2mp {
          if-feature "p2mp-te";
          description
            "Using RSVP TE P2MP as the transport technology.";
          reference
            "RFC 4875: Extensions to Resource Reservation Protocol -
```

```
            Traffic Engineering (RSVP-TE) for Point-to-Multipoint
            TE Label Switched Paths (LSPs)";

          leaf tunnel-name {
            type string;
            description
              "The P2MP TE tunnel name.";
          }
        }
        case pim {
          if-feature "pim";
          description
            "Using PIM as the transport technology.
             By setting the corresponding TAD (Multi-Topology ID,
             FA number, and data plane type), constraint-based
             multicast path establishment can be achieved.";
          reference
            "RFC 7761: Protocol Independent Multicast - Sparse Mode
             (PIM-SM): Protocol Specification (Revised)
             I-D: ietf-pim-flex-algo: Multi-Topology in PIM";
          leaf source-address {
            type ip-multicast-source-address;
            description
              "The IP source address of the multicast flow. The
               value set to * means that the receiver interests
               in all source that relevant to one given group.";
          }
          leaf group-address {
            type rt-types:ip-multicast-group-address;
            mandatory true;
            description
              "The IP group address of multicast flow. This
               type represents a version-neutral IP multicast group
               address. The format of the textual representation
               implies the IP version.";
          }
          leaf bidir {
            if-feature "bidir";
            type boolean;
            description
              "Using BIDIR-PIM as the transport technology.
               When using the bidir technique, only the group address
               needs to be considered.";
            reference
              "RFC 5015: Bidirectional Protocol Independent Multicast
               (BIDIR-PIM)";
          }
          list tad {
```

```
            key "mt-id fa-number data-plane";
            description
              "The Multi-Topology ID, Flex Algo number and data plane
               type are used to construct the logical topology,
               which enables constraint-based forwarding.";
            leaf mt-id {
              type uint16;
              description
                "The multi-topology ID.";
              reference
                "RFC 4915: Multi-Topology (MT) Routing in OSPF
                 RFC 5120: M-ISIS: Multi Topology (MT) Routing in
                   Intermediate System to Intermediate Systems
                   (IS-ISs)";
            }
            leaf fa-number {
              type uint8;
              description
                "Flex-algo number, value between 128 and 255
                 inclusive.";
              reference
                "RFC 9350: IGP Flexible Algorithm";
            }
            leaf data-plane {
              type uint8;
              description
                "Data plane type used for prefix calculation.";
              reference
                "RFC 9502: IGP Flexible Algorithm in IP Networks
                 I-D.ietf-lsr-flex-soft-dataplane:
                   IGP Flex Soft Dataplane";
            }
          }
        }
        case ir-tunnel {
          if-feature "ir-tunnel";
          description
            "Using IR (Ingress Replication) P-tunnel for MVPN as the
             transport technology.";
          reference
            "RFC 7988: Ingress Replication Tunnels in Multicast VPN
             RFC 6514: BGP Encodings and Procedures for Multicast
               in MPLS/BGP IP VPNs";
          leaf ir-tunnel-type {
            type uint8;
            description
              "The tunnel type used by MVPN ingress replication.";
          }
```

```
        }
        case sr-p2mp {
          if-feature "sr-p2mp";
          description
            "Using SR P2MP as the transport technology.
             The ingress replication and the SR P2MP
             function should not be used at the same time.";
          reference
            "RFC 9524: Segment Routing Replication for Multipoint
               Service Delivery
             I-D.ietf-pim-sr-p2mp-policy: Segment Routing
               Point-to-Multipoint Policy";
        }
        // sr-p2mp
        case native {
          description
            "When this type is set, it indicates that it is a
             normal multicast and no additional transport
             forwarding is required.";
        }
      }
    }

    // transport
    /*signaling*/

    grouping signaling-tech {
      leaf signaling {
        type identityref {
          base dynamic-signaling-type;
        }
        description
          "The type of signaling technology.";
      }
      choice protocol-type {
        description
          "The type of dynamic signaling technology.";
        case evpn {
          description
            "EVPN technology is used for multicast service
             signaling.
             When BIER is used as a transport technology, there is
             specific draft listed below that explain how to
             perform signaling.";
          reference
            "RFC 7432: BGP MPLS-Based Ethernet VPN
             RFC 9624: EVPN Broadcast, Unknown Unicast, or
             Multicast (BUM) Using Bit Index Explicit Replication
```

```
            (BIER)";
        }
        case mld {
          description
            "MLD/IGMP can be used as multicast service signaling.
             When BIER is used as a transport technology, there is
             specific draft listed below that explain how to
             perform signaling.";
          reference
            "I-D:ietf-bier-mld: BIER Ingress Multicast Flow Overlay
             using Multicast Listener Discovery Protocols";
        }
        case mld-snooping {
          description
            "MLD/IGMP snooping can be used as multicast service
             signaling.";
          reference
            "RFC 4541:Considerations for Internet Group Management
              Protocol (IGMP) and Multicast Listener Discovery (MLD)
              Snooping Switches";
        }
        case mvpn {
          description
            "MVPN technology is used for multicast service signaling.
             When BIER is used as a transport technology, there is
             specific draft listed below that explain how to
             perform signaling.";
          reference
            "RFC 6513: Multicast in MPLS/BGP IP VPNs
             RFC 7716: Global Table Multicast with BGP Multicast VPN
              (BGP-MVPN) Procedures
             RFC 8556: Multicast VPN Using Bit Index Explicit
              Replication (BIER)";
        }
        case pim {
          description
            "PIM can be used as multicast service signaling.
             When BIER is used as a transport technology, there is
             specific draft listed below that explain how to
             perform signaling.";
          reference
            "RFC 7761: Protocol Independent Multicast - Sparse Mode
              (PIM-SM): Protocol Specification (Revised)
             I-D.ietf-bier-pim-signaling: PIM Signaling Through BIER
              Core";
        }
      }
      description
```

```
        "The dynamic signaling protocols.";
    }

    // signaling-tech

    container multicast-service {
      description
        "Multicast service YANG data model. Includes the flow's
         key value, upstream and downstream neighbors,
         and related information.";
      list multicast-flow {
        key "vpn-rd source-address group-address";
        description
          "Multicast flow information, including keys, upstream and
           downstream nodes, possible signaling protocols, and
           transport protocols.";
        uses general-multicast-key;
        container upstream {
          description
            "Upstream node neighbor information and the signaling
             protocol used in the multicast flow.";
          list neighbor {
            key "neighbor-address";
            description
              "The IP address of the upstream node for the multicast
               flow. It can be the ingress node for MVPN, EVPN, and
               BIER.
               In MVPN and EVPN, this is the address of the ingress
               PE; in BIER, it is the BFR prefix of the BFIR.
               To achieve redundant ingress node protection, two or
               more ingress nodes can exist.";
            leaf neighbor-address {
              type inet:ip-address;
              description
                "The IP address of the neighbor.";
            }
            leaf vni-type {
              type identityref {
                base tunnel-encap-type;
              }
              description
                "The encapsulated type for the multicast flow.";
            }
            uses signaling-tech;
          }
        }
        // upstream
```

```
        list downstream {
          key "signaling transport";
          description
            "Downstream node neighbor information, the signaling
             protocol and transport protocol used by the multicast
             flow. For different downstream neighbor, different
             signaling and transport technology may be used.";

          list neighbor {
            key "neighbor-address";
            description
              "The IP address of the downstream node for the multicast
               flow. It can be the egress node for MVPN, EVPN, and
               BIER.
               In MVPN and EVPN, this is the address of the egress PE;
               in BIER, it is the BFR prefix of the BFER.";
            leaf neighbor-address {
              type inet:ip-address;
              description
                "The IP address of the neighbor.";
            }
          }
          uses signaling-tech;
          uses transport-tech;
        }
        // downstream
      }
      // multicast-flow
    }

    /*Notifications*/

    notification ingress-egress-event {
      leaf event-type {
        type identityref {
          base event-type;
        }
        description
          "The event type.";
      }
      list multicast-flow {
        key "vpn-rd source-address group-address";
        description
          "Multicast flow information, including keys, upstream and
           downstream nodes, possible signaling protocols, and
           transport protocols.";

        uses general-multicast-key;
```

```
        container upstream {
          description
            "Upstream node neighbor information and the signaling
             protocol used in the multicast flow.";

          leaf neighbor-address {
            type inet:ip-address;
            description
              "The IP address of the neighbor.";
          }
          leaf signaling {
            type identityref {
              base dynamic-signaling-type;
            }
            description
              "The type of signaling technology";
          }
        }
        // upstream
        list downstream {
          key "signaling transport";
          description
            "Downstream node neighbor information, the signaling
             protocol and transport protocol used by the multicast
             flow. For different downstream neighbor, different
             signaling and transport technology may be used.";

          leaf neighbor-address {
            type inet:ip-address;
            description
              "The IP address of the neighbor.";
          }
          leaf signaling {
            type identityref {
              base dynamic-signaling-type;
            }
            description
              "The type of signaling technology";
          }
          leaf transport {
            type identityref {
              base transport-type;
            }
            description
              "The type of transport technology";
          }
        }
        // downstream
```

```
      }
      // multicast-flow
      description
        "Notification events for the upstream or downstream nodes.
         Like node failure, signaling/ transport module
         loading/ unloading. And the potential failure about some
         multicast flows and associated
         signaling/ transport technologies.";
    }
  }
  <CODE ENDS>
```

4. Security Considerations

The "multicast-service" YANG module defines a data model that is designed to be accessed via YANG-based management protocols, such as NETCONF [RFC6241] and RESTCONF [RFC8040]. These YANG-based management protocols (1) have to use a secure transport layer (e.g., SSH [RFC4252], TLS [RFC8446], and QUIC [RFC9000]) and (2) have to use mutual authentication.

The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular Network Configuration Protocl (NETCONF) or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., "config true", which is the default). All writable data nodes are likely to be reasonably sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) and delete operations to these data nodes without proper protection or authentication can have a negative effect on network operations. The following subtrees and data nodes have particular sensitivities/vulnerabilities:

’upstream’ and ’downstream’

* These data nodes in this model specifies the configuration for the multicast service at the top level. Modifying the configuration can cause multicast service to be deleted or reconstructed.

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. Specifically, the following subtrees and data nodes have particular sensitivities/ vulnerabilities:

'upstream' and 'downstream'

* Unauthorized access to any data node of the above tree can disclose the operational state information of multicast service on this device.

The YANG module defines a set of identities, types, and groupings. These nodes are intended to be reused by other YANG modules. The module by itself does not expose any data nodes that are writable, data nodes that contain read-only state, or RPCs. As such, there are no additional security issues related to the YANG module that need to be considered.

Modules that use the groupings that are defined in this document should identify the corresponding security considerations. For example, reusing some of these groupings will expose privacy-related information (e.g., 'transport-tech').

5. IANA Considerations

RFC Ed.: Please replace all occurrences of 'XXXX' with the actual RFC number (and remove this note).

IANA is requested to register the following URI in the "ns" subregistry within the "IETF XML Registry" [RFC3688]:

URI: urn:ietf:params:xml:ns:yang:ietf-multicast

Registrant Contact: The IESG

XML: N/A, the requested URI is an XML namespace.

IANA is requested to register the following YANG module in the "YANG Module Names" subregistry [RFC6020] within the "YANG Parameters" registry.

name: ietf-multicast

Maintained by IANA? N

namespace: urn:ietf:params:xml:ns:yang:ietf-multicast

prefix: ietf-multicast

reference: RFC XXXX

6. Acknowledgements

The authors would like to thank Stig Venaas, Jake Holland, Min Gu, Gyan Mishra, Jeffrey Zhang for their valuable comments and suggestions.

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>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[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>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://www.rfc-editor.org/info/rfc8342>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <https://www.rfc-editor.org/info/rfc8641>.

7.2. Informative References

[I-D.ietf-bier-bierin6]
Zhang, Z., Zhang, Z. J., Wijnands, I., Mishra, M. P., Bidgoli, H., and G. S. Mishra, "Supporting BIER in IPv6 Networks (BIERin6)", Work in Progress, Internet-Draft, draft-ietf-bier-bierin6-13, 23 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-bier-bierin6-13>.

[I-D.ietf-bier-mld]
Pfister, P., Wijnands, I., Venaas, S., Wang, C., Zhang, Z., and M. Stenberg, "BIER Ingress Multicast Flow Overlay using Multicast Listener Discovery Protocols", Work in Progress, Internet-Draft, draft-ietf-bier-mld-08, 2 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-bier-mld-08>.

[I-D.ietf-bier-pim-signaling]
Bidgoli, H., Xu, F., Kotalwar, J., Wijnands, I., Mishra, M. P., and Z. J. Zhang, "PIM Signaling Through BIER Core", Work in Progress, Internet-Draft, draft-ietf-bier-pim-signaling-13, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-bier-pim-signaling-13>.

[I-D.ietf-lsr-flex-soft-dataplane]
Ginsberg, L., Psenak, P., and Z. Zhang, "IGP Flex Soft Dataplane", Work in Progress, Internet-Draft, draft-ietf-lsr-flex-soft-dataplane-00, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lsr-flex-soft-dataplane-00>.

[I-D.ietf-mboned-redundant-ingress-failover]
Shepherd, G., Zhang, Z., Liu, Y., Cheng, Y., and G. S. Mishra, "Multicast Redundant Ingress Router Failover", Work in Progress, Internet-Draft, draft-ietf-mboned-redundant-ingress-failover-09, 2 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-mboned-redundant-ingress-failover-09>.

[I-D.ietf-pim-flex-algo]
Zhang, Z., Xu, B., Venaas, S., Zhang, Z. J., and H. Bidgoli, "Multi-Topology in PIM", Work in Progress, Internet-Draft, draft-ietf-pim-flex-algo-00, 15 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-pim-flex-algo-00>.

[I-D.ietf-pim-sr-p2mp-policy]
Parekh, R., Voyer, D., Filsfils, C., Bidgoli, H., and Z. J. Zhang, "Segment Routing Point-to-Multipoint Policy", Work in Progress, Internet-Draft, draft-ietf-pim-sr-p2mp-policy-22, 4 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pim-sr-p2mp-policy-22>.

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, <https://www.rfc-editor.org/info/rfc4252>.

[RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, DOI 10.17487/RFC4541, May 2006, <https://www.rfc-editor.org/info/rfc4541>.

[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>.

[RFC4915] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915, DOI 10.17487/RFC4915, June 2007, <https://www.rfc-editor.org/info/rfc4915>.

[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>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

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

[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>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/info/rfc7348>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <https://www.rfc-editor.org/info/rfc7432>.

[RFC7637] Garg, P., Ed. and Y. Wang, Ed., "NVGRE: Network Virtualization Using Generic Routing Encapsulation", RFC 7637, DOI 10.17487/RFC7637, September 2015, <https://www.rfc-editor.org/info/rfc7637>.

[RFC7716] Zhang, J., Giuliano, L., Rosen, E., Ed., Subramanian, K., and D. Pacella, "Global Table Multicast with BGP Multicast VPN (BGP-MVPN) Procedures", RFC 7716, DOI 10.17487/RFC7716, December 2015, <https://www.rfc-editor.org/info/rfc7716>.

[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>.

[RFC7951] Lhotka, L., "JSON Encoding of Data Modeled with YANG", RFC 7951, DOI 10.17487/RFC7951, August 2016, <https://www.rfc-editor.org/info/rfc7951>.

[RFC7988] Rosen, E., Ed., Subramanian, K., and Z. Zhang, "Ingress Replication Tunnels in Multicast VPN", RFC 7988, DOI 10.17487/RFC7988, October 2016, <https://www.rfc-editor.org/info/rfc7988>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[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>.

[RFC8279] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast Using Bit Index Explicit Replication (BIER)", RFC 8279, DOI 10.17487/RFC8279, November 2017, <https://www.rfc-editor.org/info/rfc8279>.

[RFC8294] Liu, X., Qu, Y., Lindem, A., Hopps, C., and L. Berger, "Common YANG Data Types for the Routing Area", RFC 8294, DOI 10.17487/RFC8294, December 2017, <https://www.rfc-editor.org/info/rfc8294>.

[RFC8296] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Tantsura, J., Aldrin, S., and I. Meilik, "Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks", RFC 8296, DOI 10.17487/RFC8296, January 2018, <https://www.rfc-editor.org/info/rfc8296>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[RFC8349] Lhotka, L., Lindem, A., and Y. Qu, "A YANG Data Model for Routing Management (NMDA Version)", RFC 8349, DOI 10.17487/RFC8349, March 2018, <https://www.rfc-editor.org/info/rfc8349>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8556] Rosen, E., Ed., Sivakumar, M., Przygienda, T., Aldrin, S., and A. Dolganow, "Multicast VPN Using Bit Index Explicit Replication (BIER)", RFC 8556, DOI 10.17487/RFC8556, April 2019, <https://www.rfc-editor.org/info/rfc8556>.

[RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", RFC 8639, DOI 10.17487/RFC8639, September 2019, <https://www.rfc-editor.org/info/rfc8639>.

[RFC8926] Gross, J., Ed., Ganga, I., Ed., and T. Sridhar, Ed., "Geneve: Generic Network Virtualization Encapsulation", RFC 8926, DOI 10.17487/RFC8926, November 2020, <https://www.rfc-editor.org/info/rfc8926>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RFC9128] Liu, X., McAllister, P., Peter, A., Sivakumar, M., Liu, Y., and F. Hu, "YANG Data Model for Protocol Independent Multicast (PIM)", RFC 9128, DOI 10.17487/RFC9128, October 2022, <https://www.rfc-editor.org/info/rfc9128>.

[RFC9179] Hopps, C., "A YANG Grouping for Geographic Locations", RFC 9179, DOI 10.17487/RFC9179, February 2022, <https://www.rfc-editor.org/info/rfc9179>.

[RFC9262] Eckert, T., Ed., Menth, M., and G. Cauchie, "Tree Engineering for Bit Index Explicit Replication (BIER-TE)", RFC 9262, DOI 10.17487/RFC9262, October 2022, <https://www.rfc-editor.org/info/rfc9262>.

[RFC9350] Psenak, P., Ed., Hegde, S., Filsfils, C., Talaulikar, K., and A. Gulko, "IGP Flexible Algorithm", RFC 9350, DOI 10.17487/RFC9350, February 2023, <https://www.rfc-editor.org/info/rfc9350>.

[RFC9502] Britto, W., Hegde, S., Kaneriya, P., Shetty, R., Bonica, R., and P. Psenak, "IGP Flexible Algorithm in IP Networks", RFC 9502, DOI 10.17487/RFC9502, November 2023, <https://www.rfc-editor.org/info/rfc9502>.

[RFC9524] Voyer, D., Ed., Filsfils, C., Parekh, R., Bidgoli, H., and Z. Zhang, "Segment Routing Replication for Multipoint Service Delivery", RFC 9524, DOI 10.17487/RFC9524, February 2024, <https://www.rfc-editor.org/info/rfc9524>.

[RFC9572] Zhang, Z., Lin, W., Rabadan, J., Patel, K., and A. Sajassi, "Updates to EVPN Broadcast, Unknown Unicast, or Multicast (BUM) Procedures", RFC 9572, DOI 10.17487/RFC9572, May 2024, <https://www.rfc-editor.org/info/rfc9572>.

[RFC9624] Zhang, Z., Przygienda, T., Sajassi, A., and J. Rabadan, "EVPN Broadcast, Unknown Unicast, or Multicast (BUM) Using Bit Index Explicit Replication (BIER)", RFC 9624, DOI 10.17487/RFC9624, August 2024, <https://www.rfc-editor.org/info/rfc9624>.

[RFC9658] Wijnands, IJ., Mishra, M., Ed., Raza, K., Zhang, Z., and A. Gulko, "Multipoint LDP Extensions for Multi-Topology Routing", RFC 9658, DOI 10.17487/RFC9658, October 2024, <https://www.rfc-editor.org/info/rfc9658>.

[RFC9907] Bierman, A., Boucadair, M., Ed., and Q. Wu, "Guidelines for Authors and Reviewers of Documents Containing YANG Data Models", BCP 216, RFC 9907, DOI 10.17487/RFC9907, March 2026, <https://www.rfc-editor.org/info/rfc9907>.

[RFC9911] Sch旦nw辰lder, J., Ed., "Common YANG Data Types", RFC 9911, DOI 10.17487/RFC9911, December 2025, <https://www.rfc-editor.org/info/rfc9911>.

Appendix A. Data Tree Example

This section contains an example of an instance data tree in JSON encoding [RFC7951], containing configuration data.

The configuration example:

```
{
  "ietf-multicast:multicast-service":{
    "multicast-flow":[
      {
        "vpn-rd":"0:65532:4294967292",
        "source-address":"*",
        "group-address":"233.252.0.10",
        "upstream":{
          "neighbor":[
            {
```

```
                        "neighbor-address":"198.51.100.10",
                        "vni-type":"tunnel-encap-vxlan",
                        "signaling":"mvpn"
                      }
                    ]
                  }
                },
                {
                  "vpn-rd":"0:65532:4294967292",
                  "source-address":"*",
                  "group-address":"233.252.0.11",
                  "downstream":[
                    {
                      "signaling":"mvpn",
                      "transport":"bier",
                      "neighbor":[
                        {
                          "neighbor-address":"198.51.100.20"
                        },
                        {
                          "neighbor-address":"198.51.100.30"
                        }
                      ],
                      "bier":[
                        {
                          "sub-domain":1,
                          "tad":[
                            {
                              "mt-id":0,
                              "fa-number":200,
                              "data-plane":3
                            }
                          ],
                          "bier-encap-type":"bier-encap-ipv6"
                        }
                      ]
                    }
                  ]
                }
              ]
            }
          }
```


Authors' Addresses

Zheng Zhang
ZTE Corporation
China
Email: zhang.zheng@zte.com.cn

Cui(Linda) Wang
Individual
Australia
Email: lindawangjoy@gmail.com

Ying Cheng
China Unicom
Beijing
China
Email: chengying10@chinaunicom.cn

Xufeng Liu
Alef Edge
Email: xufeng.liu.ietf@gmail.com

Mahesh Sivakumar
Juniper networks
1133 Innovation Way
Sunnyvale, CALIFORNIA 94089,
United States of America
Email: sivakumar.mahesh@gmail.com