

MBONED WG
Internet-Draft
Intended status: Standards Track
Expires: 8 November 2025

Z. Zhang
ZTE Corporation
C. Wang
Individual
Y. Cheng
China Unicom
X. Liu
Alef Edge
M. Sivakumar
Juniper networks
7 May 2025

Multicast YANG Data Model
draft-ietf-mboned-multicast-yang-model-13

Abstract

This document provides a generic multicast YANG data model that shows the relevant technologies or protocols used by multicast streams. 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 8 November 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document.

Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
1.1. Terminology	3
1.2. Conventions Used in This Document	4
1.3. Tree Diagrams	4
1.4. Prefixes in Data Node Names	4
1.5. Usage of Multicast Model	4
1.5.1. Example	7
2. Module Structure	8
2.1. Multicast YANG data Model design	8
2.2. Model Structure	10
2.3. Multicast YANG data model Configuration	12
2.4. Multicast YANG data model State	13
2.5. Multicast YANG data model Notification	14
3. Multicast YANG data Model	14
4. Security Considerations	35
5. IANA Considerations	36
6. Acknowledgements	37
7. References	37
7.1. Normative References	37
7.2. Informative References	40
Appendix A. Data Tree Example	44
Authors' Addresses	45

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 streams. 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 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:

BABEL: [RFC8966].

BGP: Border Gateway Protocol [RFC4271].

BIER: Bit Index Explicit Replication [RFC8279].

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

IS-IS: Intermediate System to Intermediate System Routeing Exchange Protocol [RFC1195].

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].

OSPF: Open Shortest Path First [RFC2328].

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	[RFC6991]
yang	ietf-yang-types	[RFC6991]
rt-types	ietf-routing-types	[RFC8294]
rt	ietf-routing	[RFC8349]
ospf	ietf-ospf	[RFC9129]
bier	ietf-bier	[I-D.ietf-bier-bier-yang]
sr-policy	ietf-sr-policy	[I-D.ietf-spring-sr-policy-yang]

Table 1

1.5. 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.

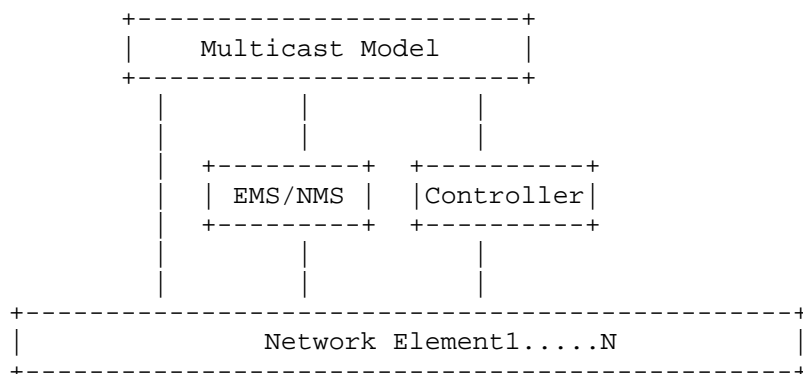


Figure 1: Usage of Multicast Model

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 overlay/ transport/ underlay information to the controller. Then the controller/ EMS/NMS can respond immediately due to the failure. Such as the changing of the failure overlay protocol to another one, as well as transport and underlay protocol. The controller can distribute new model for the flows to the network nodes. For example, a multicast flow is forwarded by BIER transport, but BIER may no longer be active, and the flow needs to be forwarded via PIM. The controller can send a model with the same multicast flow information and the associated transport protocol (set to PIM) to the ingress node.

Specifically, in section 2, it provides a human readability of the whole multicast network through diagram, which frames different multicast components and correlates them in a readable fashion. Then, based on this diagram, there is instantiated and detailed YANG model in Section 3.

The usage of this model is flexible. The multicast-keys indicate the flow characters. The flow can be L3 multicast flow, or L2 flow which is also called BUM (Broadcast, Unknown unicast, Multicast) flow in EVPN ([RFC7432]) deployment.

Among the multicast-keys, the source-address and group-address of L3 multicast flow are the most important keys. The other keys are optional, and need not be all set. 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. If mac-address and vpn-rd are set, this is EVPN use case. In case vni-value is set with associated group-address, etc., this is NVO3 (Network Virtualization over Layer 3) multicast use case.

- * When the controller manages all the ingress and egress routers for the flow, the model is sent with flow characters, ingress and egress nodes information to the ingress and egress nodes. Then the ingress and egress nodes can work without any other dynamic overlay protocols.
- * When the controller manages the ingress nodes only for the flow, the model is sent with the flow characters to the ingress nodes. The dynamic overlay protocol can be set or not. If the overlay protocol is set, the nodes use the protocol to signal the flow information with other nodes. If the overlay protocol is not set, the nodes use the local running overlay protocol to signal the flow information.
- * When the transport protocol is set in the model, the nodes encapsulate the flow according to the transport protocol. When the transport protocol is not set in the model, the nodes use the local configured transport protocol for encapsulation.
- * When the transport protocol is set in the model, the underlay protocol may be set in the model also. In case the underlay protocol is set, the nodes use the underlay protocol to signal and build the transport/forwarding layer. In case the underlay protocol is not set, the nodes use the local configured underlay protocol to signal and build the transport/forwarding layer.
- * 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].

- * The controller can also use this model to get information from the ingress node. When the received information is inconsistent with expectations, for example, a multicast stream should be forwarded through BIER transmission, but the received information shows that the multicast stream is forwarded by PIM, there may be some management inconsistencies.

1.5.1. Example

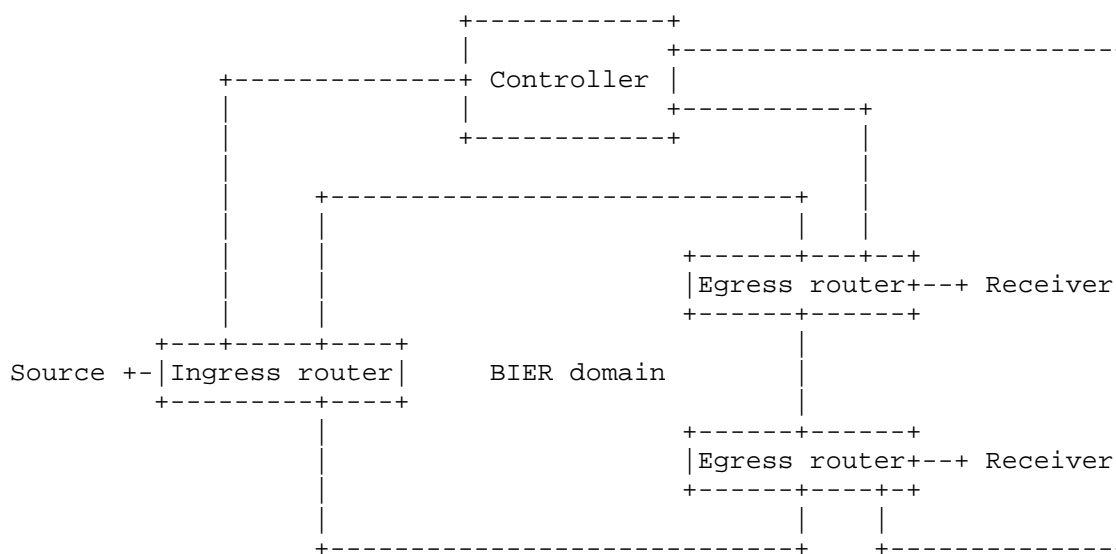


Figure 2: Example

The network administrator can use the multicast model and associated models to deploy the multicast service. For example, suppose that the flow for a multicast service is 233.252.0.0/24, the flow should be forwarded by BIER [RFC8279] with MPLS encapsulation [RFC8296]. Corresponding IGP protocol which is used to build BIER transport layer is OSPF [RFC2328].

In this model, the corresponding group-address that is in multicast-keys is set to 233.252.0.0/24, the transport technology is set to BIER. The BIER underlay protocol is set to OSPF. The model is sent to every edge router from the controller. If the BIER transport layer which depends on OSPF has not been built in the network, the multicast YANG model may work with the BIER YANG model that is defined in [I-D.ietf-bier-bier-yang]. After the BIER transport layer is built, the ingress router encapsulates the multicast flow with BIER header and sends it into the network. Intermediate routers forward the flows to all the egress nodes by BIER forwarding.

Another example for this figure is, the controller can act as the BIER overlay only. The routers in the domain build BIER forwarding plane beforehand. The controller sends the multicast group-address and/or the source-address to the edge routers in BIER domain only, without transport and underlay set in the model. Then the ingress router can encapsulate the multicast flow with BIER encapsulation automatically.

2. Module Structure

2.1. Multicast YANG data Model design

The following is the design for Multicast YANG data Model.

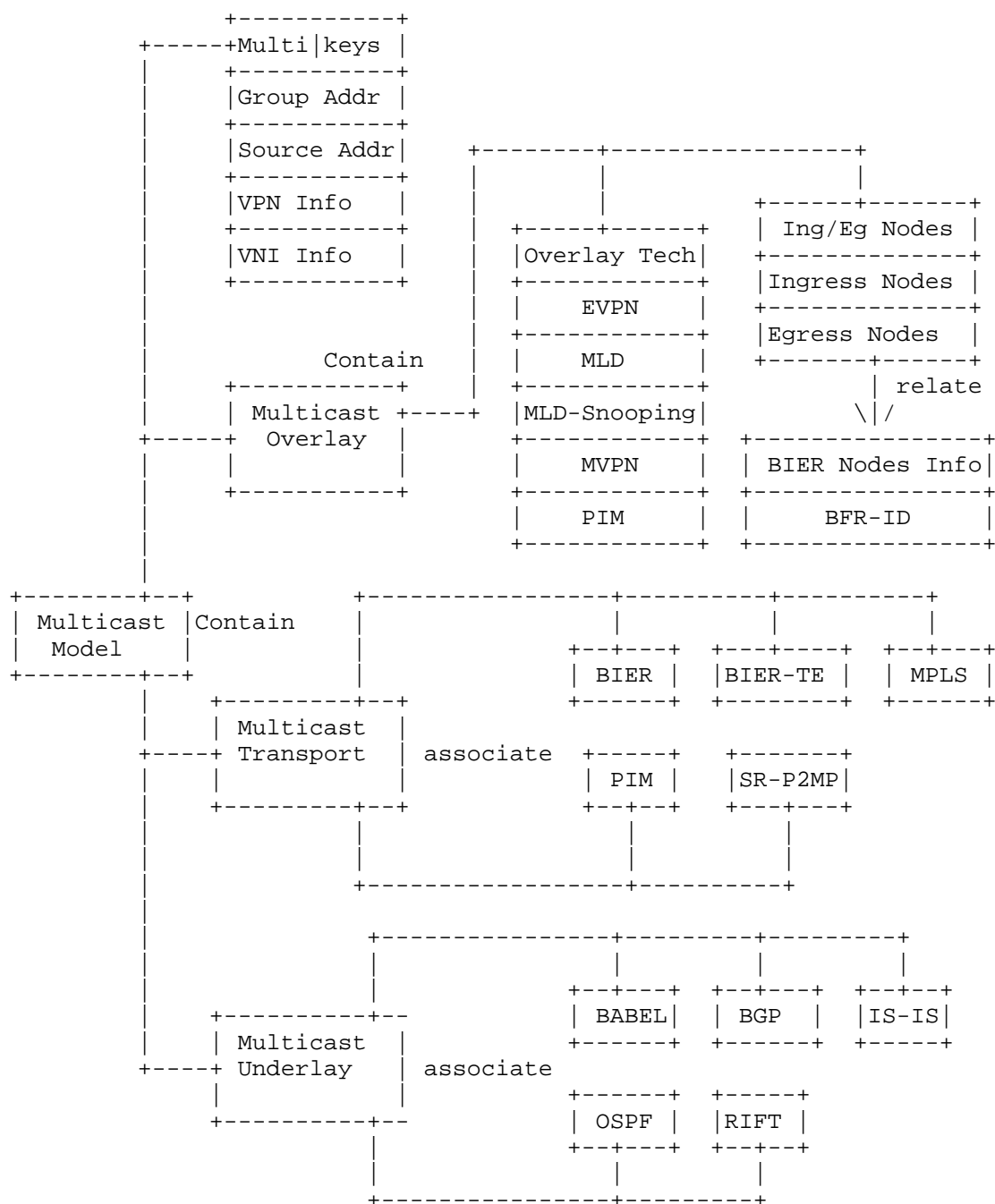


Figure 3: Multicast YANG data Model design

2.2. Model Structure

```

module: ietf-multicast
  +--rw multicast-service
    +--rw multicast-keys* [source-address group-address]
      +--rw source-address      ip-multicast-source-address
      +--rw group-address
        | rt-types:ip-multicast-group-address
      +--rw vpn-rd?              rt-types:route-distinguisher
      +--rw mac-address?         yang:mac-address
      +--rw vni-value?           uint32
      +--rw multicast-overlay
        | +--rw vni-type?        identityref
        | +--rw ingress-egress
        | | +--rw ingress-nodes*  inet:ip-address
        | | +--rw egress-nodes*   inet:ip-address
        | +--rw bier-ids {bier}?
        | | +--rw sub-domain?      uint16
        | | +--rw ingress-nodes*   uint16
        | | +--rw egress-nodes*    uint16
        | +--rw dynamic-overlay
        | | +--rw type?            identityref
        | | +--rw (overlay-tech-type)?
        | | | +--:(evpn)
        | | | +--:(mld)
        | | | | +--rw mld-instance-group?
        | | | | | rt-types:ip-multicast-group-address
        | | | +--:(mld-snooping)
        | | | | +--rw mld-snooping-group?
        | | | | | rt-types:ip-multicast-group-address
        | | | +--:(mvpn)
        | | | +--:(pim)
        | +--rw multicast-transport
        | | +--rw type?            identityref
        | | +--rw (transport-tech-type)?
        | | | +--:(bier) {bier}?
        | | | | +--rw sub-domain?      uint16
        | | | | +--rw bitstringlength? uint16
        | | | | +--rw set-identifier?   uint16
        | | | | +--rw bier-encap-type?  identityref
        | | | +--:(bier-te) {bier}?
        | | | | +--rw bitstring* [name]
        | | | | | +--rw name            string
        | | | | | +--rw bier-te-adj* [adj-id]
        | | | | | | +--rw adj-id      uint16
        | | | +--:(mldp) {mldp}?
        | | | +--:(rsvp-te-p2mp) {p2mp-te}?

```

```

|         | +--rw template-name?      te-types:te-template-name
|         +---:(pim) {pim}?
|         | +--rw source-address?     ip-multicast-source-address
|         | +--rw group-address
|         |         rt-types:ip-multicast-group-address
|         +---:(sr-p2mp) {sr}?
|         | +--rw ir-sr-policies*     leafref
+--rw multicast-underlay
|   +--rw type?                       identityref
|   +--rw (underlay-tech-type)?
|   |   +---:(ospf)
|   |   |   +--rw topology-id?        uint8
|   |   +---:(isis)
|   |   +---:(pim)
|   |       +--rw source-address?     ip-multicast-source-address
|   |       +--rw group-address
|   |           rt-types:ip-multicast-group-address
|
notifications:
+---n ingress-egress-event
|   +--ro event-type?                 identityref
|   +--ro multicast-key
|   |   +--ro source-address?         ip-multicast-source-address
|   |   +--ro group-address          rt-types:ip-multicast-group-address
|   |   +--ro vpn-rd?                 rt-types:route-distinguisher
|   |   +--ro mac-address?            yang:mac-address
|   |   +--ro vni-value?              uint32
|   +--ro dynamic-overlay
|   |   +--ro type?                   identityref
|   |   +--ro (overlay-tech-type)?
|   |   |   +---:(evpn)
|   |   |   +---:(mld)
|   |   |   |   +--ro mld-instance-group?
|   |   |   |       rt-types:ip-multicast-group-address
|   |   |   +---:(mld-snooping)
|   |   |   |   +--ro mld-snooping-group?
|   |   |   |       rt-types:ip-multicast-group-address
|   |   |   +---:(mvpn)
|   |   |   +---:(pim)
|   +--ro transport-tech
|   |   +--ro type?                   identityref
|   |   +--ro (transport-tech-type)?
|   |   |   +---:(bier) {bier}?
|   |   |   |   +--ro sub-domain?     uint16
|   |   |   |   +--ro bitstringlength? uint16
|   |   |   |   +--ro set-identifier?  uint16
|   |   |   |   +--ro bier-encap-type? identityref
|   |   |   +---:(bier-te) {bier}?

```

```

|         |--ro bitstring* [name]
|         |--ro name          string
|         |--ro bier-te-adj* [adj-id]
|         |--ro adj-id       uint16
|         +---:(mldp) {mldp}?
|         +---:(rsvp-te-p2mp) {p2mp-te}?
|         |   |--ro template-name?    te-types:te-template-name
|         +---:(pim) {pim}?
|         |   |--ro source-address?    ip-multicast-source-address
|         |   |--ro group-address
|         |   |   rt-types:ip-multicast-group-address
|         +---:(sr-p2mp) {sr}?
|         |--ro ir-sr-policies*    leafref
+--ro underlay-tech
  |--ro type?                      identityref
  +--ro (underlay-tech-type)?
    +---:(ospf)
    |   |--ro topology-id?          uint8
    +---:(isis)
    +---:(pim)
      |--ro source-address?    ip-multicast-source-address
      |--ro group-address
      |   rt-types:ip-multicast-group-address

```

2.3. Multicast YANG data model Configuration

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

This model includes multicast service keys and three layers: the multicast overlay, the transport layer and the multicast underlay information. Multicast keys include the features of multicast flow, such as (multicast source and multicast group) information. In data center network, for fine-grained to gather the nodes belonging to the same virtual network, there may need VNI-related information to assist.

Multicast overlay defines the multicast flows information, and the nodes (ingress and/or egress) information. If the transport layer is BIER, there may define BIER information including (Subdomain, ingress-node BFR-id, egress-nodes BFR-id). When the nodes (ingress and/or egress) information are not defined, there may need overlay multicast signaling technology, such as MLD or MVPN, to collect these nodes information. The model can be sent to the ingress nodes only. For example, regardless of the dynamic overlay protocol used, the ingress node advertises the multicast flow information to all neighbors in the BIER domain. When the ingress node receives the signaling from some egress nodes, the ingress node sends the flow to the signaling egress nodes.

Multicast transport layer defines the type of transport technologies that can be used to forward multicast flow, including BIER forwarding type, MPLS forwarding type, or PIM forwarding type and so on. The multicast YANG data model can be used with the corresponding protocol model to indicate the transport technology used for the multicast flow.

Multicast underlay defines the type of underlay technologies, such as OSPF, IS-IS, BGP, PIM or BABEL and so on. Normally, the underlying protocols operate independently. In some cases, this multicast YANG data model can work with the corresponding protocol models.

The configuration modeling branch is composed of the keys, overlay layer, transport layer and underlay layer.

2.4. Multicast YANG data model State

Multicast model states are the same with the configuration. The main parts are the key and overlay layer, usually the transport layer and underlay layer work independently. In most cases, network administrators can use this model to obtain multicast flows and related protocol information such as transport layer, underlay layer, and overlay layer.

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 [RFC8407].

2.5. Multicast YANG data model Notification

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

3. Multicast YANG data Model

This module references [RFC1195], [RFC2328], [RFC4271], [RFC4541], [RFC4875], [RFC5340], [RFC6388], [RFC6513], [RFC6991], [RFC7348], [RFC7432], [RFC7637], [RFC7716], [RFC7761], [RFC8279], [RFC8294], [RFC8296], [RFC8343], [RFC8344], [RFC8349], [RFC8556], [RFC8639], [RFC8641], [RFC8926], [RFC8966], [RFC9128], [RFC9129], [RFC9130], [RFC9262], [RFC9130], [RFC9524], [RFC9572], [RFC9624], [RFC9692], [I-D.ietf-bier-bier-yang], [I-D.ietf-bess-evpn-yang], [I-D.ietf-bess-mvpn-yang], [I-D.ietf-bier-mld], [I-D.ietf-bier-bierin6], [I-D.ietf-bier-pim-signaling], [I-D.ietf-spring-sr-policy-yang].

```
<CODE BEGINS> file "ietf-multicast@2025-05-06.yang"
module ietf-multicast {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-multicast";
  prefix ietf-multicast;

  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-routing-types {
    prefix rt-types;
    reference
      "RFC 8294: Common YANG Data Types for the Routing Area";
  }
  import ietf-routing {
    prefix rt;
    reference
      "RFC 8349: A YANG Data Model for Routing Management
      (NMDA Version)";
  }
}
```

```
import ietf-te-types {
  prefix te-types;
  reference
    "RFC 8776: Common YANG Data Types for Traffic Engineering";
}
import ietf-bier {
  prefix bier;
  reference
    "I-D.ietf-bier-bier-yang: YANG Data Model for BIER Protocol";
}
import ietf-sr-policy {
  prefix sr-policy;
  reference
    "I-D.ietf-spring-sr-policy-yang: YANG Data Model for Segment
      Routing Policy";
}

organization
  " IETF MBONED (MBONE Deployment) Working Group";
contact
  "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 indicates the overlay, transport protocol
  used by a multicast flow. And the underlay protocol used for
  the transport layer building.

  Copyright (c) 2025 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; 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 2025-05-06 {
  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 sr {
  description
    "Cooperation with Segment Routing technology.";
  reference
    "RFC 8402: Segment Routing Architecture";
}

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)";
    }

    /*
    *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.";
    }

    typedef tree-sid {
        type union {
            type rt-types:mpls-label;
            type inet:ip-prefix;
        }
        description
            "The type of the Segment Identifier of a Replication segment
            is a SR-MPLS label or a SRv6 SID.";
    }
```

```
/*
 * Identities
 */

identity multicast-service {
  base rt:control-plane-protocol;
  description
    "Identity for the multicast model.";
}

identity overlay-type {
  description
    "Base identity for the type of multicast overlay technology.";
}

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

identity underlay-type {
  description
    "Identity for the multicast underlay 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 overlay-pim {
  base overlay-type;
  description
    "Using PIM as multicast overlay technology.";
  reference
    "I-D.ietf-bier-pim-signaling:
    PIM Signaling Through BIER Core";
}

identity mld {
  base overlay-type;
  description
    "Using MLD as multicast overlay technology.";
  reference
    "I-D.ietf-bier-mld:
    BIER Ingress Multicast Flow Overlay
    using Multicast Listener Discovery Protocols";
}

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

identity evpn {
  base overlay-type;
  description
    "Using EVPN as multicast overlay 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 overlay-type;
    description
      "Using MVPN as multicast overlay 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 bgp {
  base underlay-type;
  description
    "Using BGP as underlay technology to build the multicast
      transport layer. For example, using BGP as BIER underlay.";
  reference
    "I-D.ietf-bier-idr-extensions: BGP Extensions for BIER.";
}

identity ospf {
  base underlay-type;
  description
    "Using OSPF as multicast underlay technology.
      For example, using OSPF as BIER underlay.";
  reference
    "RFC 8444:
      OSPFv2 Extensions for Bit Index Explicit Replication (BIER),
      I-D.ietf-bier-ospfv3-extensions:
      OSPFv3 Extensions for BIER.";
```

```
}

identity isis {
  base underlay-type;
  description
    "Using IS-IS as multicast underlay technology.
     For example, using IS-IS as BIER underlay.";
  reference
    "RFC 8401:
     Bit Index Explicit Replication (BIER) Support via IS-IS";
}

identity babel {
  base underlay-type;
  description
    "Using BABEL as multicast underlay technology.
     For example, using BABEL as BIER underlay.";
  reference
    "RFC 8966: The Babel Routing Protocol
     I-D.zhang-bier-babel-extensions: BIER in BABEL";
}

identity rift {
  base underlay-type;
  description
    "Using RIFT as multicast underlay technology.
     For example, using RIFT as BIER underlay.";
  reference
    "RFC 9692: RIFT: Routing in Fat Trees.
     I-D.zhang-bier-rift: Supporting BIER with RIFT";
}

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

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

identity event-down {
  base event-type;
  description
    "There is something wrong with ingress or egress node,
     and node can't work properly.";
```

```
}

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 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.";
  }
}

grouping optional-multicast-key {
  description
    "The optional 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.";
    reference
        "RFC 8294: Common YANG Data Types for the Routing Area.
        RFC 6513: Multicast in MPLS/BGP IP VPNs.";
    }
    leaf mac-address {
        type yang:mac-address;
        description
            "The mac address of flow. In the EVPN situation, the L2
            flow that is called
            BUM (Broadcast, Unknown Unicast, Multicast)
            can be sent to the other PEs that
            are in a same broadcast domain.";
        reference
            "RFC 6991: Common YANG Data Types.
            RFC 7432: BGP MPLS-Based Ethernet VPN.";
    }
    leaf vni-value {
        type uint32;
        description
            "The value of VXLAN network identifier, virtual subnet ID
            or virtual net identifier. This value and vni-type is used
            to indicate a specific virtual multicast service.";
    }
}

// multicast-key

grouping encap-type {
    description
        "The encapsulation type used for flow forwarding.
        This encapsulation acts as the inner encapsulation,
        as compare to the outer multicast-transport encapsulation.";
    choice encap-type {
        case mpls {
            description
                "The BIER forwarding depends on mpls.";
            reference
                "RFC 8296: Encapsulation for Bit Index Explicit
                Replication (BIER) in MPLS and Non-MPLS Networks.";
        }
        case eth {
            description
                "The BIER forwarding depends on ethernet.";
            reference
                "RFC 8296: Encapsulation for Bit Index Explicit
                Replication (BIER) in MPLS and Non-MPLS Networks.";
        }
    }
}
```



```
    case ipv6 {
      description
        "The BIER forwarding depends on IPv6.";
      reference
        "I-D.ietf-bier-bierin6: BIER in IPv6 (BIERin6)";
    }
    description
      "The encapsulation type in BIER.";
  }
}

// encap-type
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.";
  }
  leaf bitstringlength {
    type uint16;
    description
      "The bitstringlength used by BIER forwarding.";
  }
  leaf set-identifier {
    type uint16;
    description
      "The set identifier used by the multicast flow.";
  }
  leaf bier-encap-type {
    type identityref {
      base bier: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.";
  leaf type {
```

```
    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";
      description
        "Using BIER as the transport technology.
        The BIER technology is introduced in RFC8279.
        The parameters are consistent with the definition in
        BIER YANG data model.";
      reference
        "RFC 8296: Encapsulation for Bit Index Explicit
        Replication (BIER) in MPLS and Non-MPLS Networks
        I-D.ietf-bier-bier-yang:
        YANG Data Model for BIER Protocol.";
      uses bier-key;
    }
    case bier-te {
      if-feature "bier";
      description
        "Using BIER-TE as the transport technology.
        The BIER-TE technology is introduced in RFC9262.
        The parameters are consistent with the definition in
        BIER and BIER TE YANG data model.";
      reference
        "RFC 9262: Tree Engineering for Bit Index Explicit
        Replication (BIER-TE)
        I-D.ietf-bier-bier-yang: YANG Data Model for BIER Protocol
        I-D.ietf-bier-te-yang: A YANG data model for Traffic
        Engineering for Bit Index Explicit Replication
        (BIER-TE)";
      //uses bier-key;
      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";
}
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)
        RFC 8776: Common YANG Data Types for Traffic Engineering";
    leaf template-name {
        type te-types:te-template-name;
        description
            "A type for the name of a TE node template or TE link
            template.";
    }
}
}
case pim {
    if-feature "pim";
    description
        "Using PIM as the transport technology.";
    reference
        "RFC 7761: Protocol Independent Multicast - Sparse Mode
        (PIM-SM): Protocol Specification (Revised)";
    uses pim;
}
```

```
}
case sr-p2mp {
  if-feature "sr";
  description
    "Using SR P2MP as the transport technology.
    The ingress replication and the treesid
    function will not be used at the same time.";
  reference
    "RFC 8402: Segment Routing Architecture
    RFC 9524: Segment Routing Replication for Multipoint
    Service Delivery
    I-D.ietf-pim-sr-p2mp-policy: Segment Routing
    Point-to-Multipoint Policy
    I-D.ietf-spring-sr-policy-yang: YANG Data Model for
    Segment Routing Policy";
  leaf-list ir-sr-policies {
    type leafref {
      path "/rt:routing/"
        + "sr-policy:segment-routing/"
        + "sr-policy:traffic-engineering/"
        + "sr-policy:attributes/"
        + "sr-policy:segment-lists/"
        + "sr-policy:segment-list/"
        + "sr-policy:name";
    }
    description
      "The segment list used for ingress replication.";
  }
}
// sr-p2mp
}

// underlay-tech

grouping underlay-tech {
  description
    "The underlay technology selected for the transport layer.
    The underlay technology has no straight relationship with
    the multicast overlay, it is used for transport path
    building, for example BIER forwarding path building.";
  leaf type {
    type identityref {
      base underlay-type;
    }
    description
      "The type of underlay technology";
  }
}
```

```
choice underlay-tech-type {
  description
    "The type of underlay technology";
  case ospf {
    description
      "Using OSPF as the underlay technology.
      If OSPF protocol supports multiple topology feature,
      the associated topology name may be assigned.
      In case the topology name is assigned, the specific
      OSPF topology is used for underly to building the
      transport layer.";
    reference
      "RFC 4915: Multi-Topology Routing
      RFC 9129: YANG Data Model for the OSPF Protocol";
    leaf topology-id {
      type uint8;
      description
        "The MT-ID for the topology enabled in OSPF protocol";
    }
  }
  case isis {
    description
      "Using IS-IS as the underlay technology.
      If IS-IS protocol supports multiple topology feature,
      the associated topology name may be assigned.
      In case the topology name is assigned, the specific
      IS-IS topology is used for underly to building the
      transport layer.";
    reference
      "RFC 5120: M-IS-IS: Multi Topology Routing in IS-IS
      RFC 9130: YANG Data Model for the IS-IS Protocol";
  }
  case pim {
    description
      "Using PIM as the underlay technology.";
    reference
      "RFC 7761: Protocol Independent Multicast - Sparse Mode
      (PIM-SM): Protocol Specification (Revised)";
    uses pim;
  }
}

// underlay-tech

/*overlay*/
grouping overlay-tech {
  container dynamic-overlay {
```

```
leaf type {
  type identityref {
    base overlay-type;
  }
  description
    "The type of overlay technology";
}
choice overlay-tech-type {
  description
    "The type of overlay technology";
  case evpn {
    description
      "EVPN technology is used for multicast overlay.";
    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 overlay
       when BIER is used as transport technology.";
    reference
      "I-D:ietf-bier-mld: BIER Ingress Multicast Flow Overlay
       using Multicast Listener Discovery Protocols";
    leaf mld-instance-group {
      type rt-types:ip-multicast-group-address;
      description
        "The multicast address used for multiple MLD instance
         support.";
    }
  }
  case mld-snooping {
    description
      "MLD/IGMP snooping can be used as multicast overlay
       when BIER is used as transport technology.";
    reference
      "RFC 9166:A YANG Data Model for Internet Group
       Management Protocol (IGMP) and Multicast Listener
       Discovery (MLD) Snooping";
    leaf mld-snooping-group {
      type rt-types:ip-multicast-group-address;
      description
        "The multicast address used for MLD-snooping.";
    }
  }
}
case mvpn {
```

```
    description
      "MVPN technology is used for multicast overlay.
      The global table multicast can also be achieved.";
    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 overlay
      when BIER is used as transport technology.";
    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 overlay technologies and associated parameter
  that may be set.";
}
description
  "The overlay technology used for multicast service.";
}

// overlay-tech
/*transport*/

grouping pim {
  description
    "The required information of pim transportation.";
  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 7761: Protocol Independent Multicast - Sparse Mode
        (PIM-SM): Protocol Specification (Revised).";
}

container multicast-service {
    description
        "The model of multicast YANG data. Include keys, overlay,
        transport and underlay.";
    list multicast-keys {
        key "source-address group-address";
        uses general-multicast-key;
        uses optional-multicast-key;
        container multicast-overlay {
            description
                "The overlay information of multicast service.
                Overlay technology is used to exchange multicast
                flows information. Overlay technology may not be
                used in SDN controlled situation. Different overlay
                technologies can be chosen according to different
                deploy consideration.";
            leaf vni-type {
                type identityref {
                    base tunnel-encap-type;
                }
                description
                    "The encapsulated type for the multicast flow,
                    it is used to carry the virtual network identifier
                    for the multicast service.
                    When this type is set, the associated vni-value
                    MUST be set.";
            }
        }
        container ingress-egress {
            description
                "The ingress and egress nodes address collection.
                The ingress node may use the egress nodes set
                directly to encapsulate the multicast flow by
                transport technology.";
            leaf-list ingress-nodes {
                type inet:ip-address;
                description
                    "The ip address of ingress node for one or more
                    multicast flow. Or the ingress node of MVPN,
                    EVPN and BIER.
                    In MVPN, this is the address of ingress
```



```
    PE; in BIER, this is the BFR-prefix of BFIR.
    Two or more ingress nodes may exist for the
    redundant ingress node protection.";
  }
  leaf-list egress-nodes {
    type inet:ip-address;
    description
      "The ip address of egress nodes for the multicast flow.
      Or the egress node of MVPN, EVPN and BIER.
      In MVPN, this is the address of egress PE;
      in BIER, this is the BFR-prefix of BFER.";
  }
}
container bier-ids {
  if-feature "bier";
  description
    "The BFR-ids of ingress and egress BIER nodes for
    one or more multicast flows. This overlay is used
    with BIER transport technology. The egress nodes
    set can be used to encapsulate the multicast flow
    directly in the ingress node.";
  reference
    "RFC 8279: Multicast Using Bit Index Explicit
    Replication (BIER)";
  leaf sub-domain {
    type uint16;
    description
      "The sub-domain that this multicast flow belongs to.";
  }
  leaf-list ingress-nodes {
    type uint16;
    description
      "The BFR-ID of the ingress node.";
  }
  leaf-list egress-nodes {
    type uint16;
    description
      "The BFR-ID of the egress node.";
  }
}
uses overlay-tech;
}
container multicast-transport {
  description
    "The transportation of multicast service. Transport
    protocol is responsible for delivering multicast
    flows from ingress nodes to egress nodes with or
    without specific encapsulation. Different transport
```

```
        technology can be chosen according to different
        deploy consideration. Once a transport technology
        is chosen, associated protocol should be triggered
        to run.";
    uses transport-tech;
}
container multicast-underlay {
    description
        "The underlay of multicast service. Underlay protocol
        is used to build transport layer. Underlay protocol
        need not be assigned in ordinary network since
        existed underlay protocol fits well, but it can be
        assigned in particular networks for better
        controll. Once an underlay technology is chosen,
        associated protocol should be triggered to run.";
    uses underlay-tech;
}
description
    "The model of multicast YANG data. Include keys,
    overlay, transport and underlay.";
}
}

/*Notifications*/

notification ingress-egress-event {
    leaf event-type {
        type identityref {
            base event-type;
        }
        description
            "The event type.";
    }
    container multicast-key {
        uses general-multicast-key;
        uses optional-multicast-key;
        description
            "The associated multicast keys that are influenced by
            ingress or egress node failure.";
    }
    uses overlay-tech;
    container transport-tech {
        description
            "The modules can be used to forward multicast flows.";
        uses transport-tech;
    }
    container underlay-tech {
        description
```

```
        "There is something wrong with the module which is
        used to build multicast transport layer.";
    uses underlay-tech;
}
description
    "Notification events for the ingress or egress nodes. Like
    node failure, overlay/ transport/ underlay module
    loading/ unloading. And the potential failure about some
    multicast flows and associated
    overlay/ transport/ underlay 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] or RESTCONF [RFC8040]. These protocols have to use a secure transport layer (e.g., SSH [RFC6242], TLS [RFC8446], and QUIC [RFC9000]) and have to use mutual authentication.

The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular 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:

multicast-service

- * 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:

multicast-service

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

This YANG module uses groupings from other YANG modules that define nodes that may be considered sensitive or vulnerable in network environments. Refer to the Security Considerations of respective for information as to which nodes may be considered sensitive or vulnerable in network environments.

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-type').

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 for their valuable comments and suggestions.

7. References

7.1. Normative References

- [RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, DOI 10.17487/RFC1195, December 1990, <<https://www.rfc-editor.org/info/rfc1195>>.
- [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>>.
- [RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <<https://www.rfc-editor.org/info/rfc2328>>.
- [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <<https://www.rfc-editor.org/info/rfc4271>>.
- [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>>.
- [RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008, <<https://www.rfc-editor.org/info/rfc5340>>.

- [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>>.
- [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>>.
- [RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <<https://www.rfc-editor.org/info/rfc6242>>.
- [RFC6388] Wijnands, IJ., Ed., Minei, I., Ed., Kompella, K., and B. Thomas, "Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths", RFC 6388, DOI 10.17487/RFC6388, November 2011, <<https://www.rfc-editor.org/info/rfc6388>>.
- [RFC6513] Rosen, E., Ed. and R. Aggarwal, Ed., "Multicast in MPLS/BGP IP VPNs", RFC 6513, DOI 10.17487/RFC6513, February 2012, <<https://www.rfc-editor.org/info/rfc6513>>.
- [RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <<https://www.rfc-editor.org/info/rfc6991>>.
- [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>>.
- [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>>.
- [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>>.

- [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>>.
- [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>>.
- [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>>.
- [RFC8343] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 8343, DOI 10.17487/RFC8343, March 2018, <<https://www.rfc-editor.org/info/rfc8343>>.

- [RFC8344] Bjorklund, M., "A YANG Data Model for IP Management", RFC 8344, DOI 10.17487/RFC8344, March 2018, <<https://www.rfc-editor.org/info/rfc8344>>.
- [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>>.
- [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>>.

7.2. Informative References

- [I-D.ietf-bess-evpn-yang]
Brissette, P., Shah, H. C., Hussain, I., Tiruveedhula, K., and J. Rabadan, "Yang Data Model for EVPN", Work in Progress, Internet-Draft, draft-ietf-bess-evpn-yang-07, 11 March 2019, <<https://datatracker.ietf.org/doc/html/draft-ietf-bess-evpn-yang-07>>.
- [I-D.ietf-bess-mvpn-yang]
Liu, Y., Guo, F., Litkowski, S., Liu, X., Kebler, R., and M. Sivakumar, "Yang Data Model for Multicast in MPLS/BGP IP VPNs", Work in Progress, Internet-Draft, draft-ietf-bess-mvpn-yang-05, 20 February 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-bess-mvpn-yang-05>>.
- [I-D.ietf-bier-bier-yang]
Chen, R., hu, F., Zhang, Z., dai.xianxian@zte.com.cn, and M. Sivakumar, "YANG Data Model for BIER Protocol", Work in Progress, Internet-Draft, draft-ietf-bier-bier-yang-10, 11 February 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-bier-bier-yang-10>>.

`[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-bierin6-11, 2 March 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-bier-bierin6-11>>.

`[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-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-06, 20 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-mboned-redundant-ingress-failover-06>>.

`[I-D.ietf-pim-sr-p2mp-policy]`

Voyer, D., Filsfils, C., Parekh, R., Bidgoli, H., Zhang, Z. J., and M. P. Mishra, "Segment Routing Point-to-Multipoint Policy", Work in Progress, Internet-Draft, draft-ietf-pim-sr-p2mp-policy-11, 2 February 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-pim-sr-p2mp-policy-11>>.

`[I-D.ietf-spring-sr-policy-yang]`

Raza, S. K., Saleh, T., Shunwan, Z., Voyer, D., Durrani, M., Matsushima, S., and V. P. Beeram, "YANG Data Model for Segment Routing Policy", Work in Progress, Internet-Draft, draft-ietf-spring-sr-policy-yang-04, 22 November 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-policy-yang-04>>.

- [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <<https://www.rfc-editor.org/info/rfc3688>>.
- [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>>.
- [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>>.
- [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>>.
- [RFC8407] Bierman, A., "Guidelines for Authors and Reviewers of Documents Containing YANG Data Models", BCP 216, RFC 8407, DOI 10.17487/RFC8407, October 2018, <<https://www.rfc-editor.org/info/rfc8407>>.
- [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>>.
- [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>>.
- [RFC8776] Saad, T., Gandhi, R., Liu, X., Beeram, V., and I. Bryskin, "Common YANG Data Types for Traffic Engineering", RFC 8776, DOI 10.17487/RFC8776, June 2020, <<https://www.rfc-editor.org/info/rfc8776>>.
- [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>>.

- [RFC8966] Chroboczek, J. and D. Schinazi, "The Babel Routing Protocol", RFC 8966, DOI 10.17487/RFC8966, January 2021, <<https://www.rfc-editor.org/info/rfc8966>>.
- [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>>.
- [RFC9129] Yeung, D., Qu, Y., Zhang, Z., Chen, I., and A. Lindem, "YANG Data Model for the OSPF Protocol", RFC 9129, DOI 10.17487/RFC9129, October 2022, <<https://www.rfc-editor.org/info/rfc9129>>.
- [RFC9130] Litkowski, S., Ed., Yeung, D., Lindem, A., Zhang, J., and L. Lhotka, "YANG Data Model for the IS-IS Protocol", RFC 9130, DOI 10.17487/RFC9130, October 2022, <<https://www.rfc-editor.org/info/rfc9130>>.
- [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>>.
- [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>>.
- [RFC9692] Przygienda, T., Ed., Head, J., Ed., Sharma, A., Thubert, P., Rijsman, B., and D. Afanasiev, "RIFT: Routing in Fat Trees", RFC 9692, DOI 10.17487/RFC9692, April 2025, <<https://www.rfc-editor.org/info/rfc9692>>.

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-keys":[
      {
        "vpn-rd":"0:65532:4294967292",
        "source-address":"*",
        "group-address":"233.252.0.10",
        "mac-address": "00:00:5e:00:53:01",
        "vni-value":0,
        "multicast-overlay":{
          "vni-type":"nvgre",
          "ingress-egress":{
            "ingress-nodes":[
              {
                "ingress-node":"198.51.100.10"
              }
            ],
            "egress-nodes":[
              {
                "egress-node":"203.0.113.5"
              }
            ]
          }
        },
        "multicast-transport":{
          "type": "ietf-multicast:bier",
          "bier":{
            "sub-domain":0,
            "bitstringlength":256,
            "set-identifier":0
          }
        },
        "multicast-underlay":{
          "type": "ietf-multicast:ospf",
          "ospf":{
            "topology":"2"
          }
        }
      }
    ]
  }
}

```

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