Workgroup: TEAS Working Group
Internet-Draft:
draft-dhody-teas-te-traffic-yang-04
Published: 4 March 2024
Intended Status: Standards Track
Expires: 5 September 2024
Authors: D. Dhody
Huawei

Traffic Mapping YANG model for Traffic Engineering (TE)

Abstract

This document provides a YANG data model to map traffic to Traffic Engineering (TE) paths. This model providers operator a seamless control and management of which traffic to send on the underlying TE resources.

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 5 September 2024.

Table of Contents

1. Introduction

Data models are a representation of objects that can be configured or monitored within a system. Within the IETF, YANG [RFC7950] is the language of choice for documenting data models, and YANG models have been produced to allow configuration or modeling of a variety of network devices, protocol instances, and network services.

There are various YANG models to establish paths in the network, such as:

*TE Tunnels [I-D.ietf-teas-yang-te]

*Segment Routing (SR) Policy [I-D.ietf-spring-sr-policy-yang]

*Service Function Chaining (SFC)

*Virtual Network (VN)

*IETF Network Slice

These models do not include an exact mechanism to describe the traffic that needs to be mapped to the paths. Thus an operator lacks a way to simply use the YANG model to tell requirements such as the traffic from source X on port Y should go on a TE path with delay less than Z. The YANG model defined in this document fills this gap.

To achieve this goal, the YANG model defined in this document utilizes the concept borrowed from:

- BGP FlowSpec: Where the description of traffic flows is done by the combination of multiple Flow Specification Components and their dissemination as traffic flow specifications (Flow Specifications) is described for BGP in [RFC8955]. In BGP, a Flow Specification is comprised of traffic filtering rules and is associated with actions to perform on the packets that match the Flow Specification. The BGP routers that receive a Flow Specification can classify received packets according to the traffic filtering rules and can direct packets based on the associated actions.

- Path Computation Element (PCE) FlowSpec: Extends the idea to PCE Communication Protocol (PCEP) [RFC9168].

- Access Control List (ACL): A basic elements used to configure device-forwarding behavior in form of a user-ordered set of rules that is used to filter traffic on a networking device. Each rule is represented by an Access Control Entry (ACE). Each ACE has a group of match criteria and a group of actions [RFC8519].

- Flow: Elements in the packet in IP/UDP/TCP header to match particular flows.

The YANG model includes two key concepts:

- Traffic Description: The various fields that needs to be matched to identify a traffic flow.

- Action: The associated action that needs to be taken. For the purpose of this YANG model the action is to simply point to the TE resource in form of the TE tunnel, SR Policy etc.

Note: The RFC Editor will replace XXXX with the number assigned to the RFC once this draft becomes an RFC.

2. Conventions

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

2.1. Tree Diagrams

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in these diagrams is defined in [RFC8340].

2.2. Prefixes in Data Node Names

In this document, names of data nodes 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]
te	ietf-te	[I-D.ietf-teas-yang-te]
rt	ietf-routing	[RFC8349]
sr-policy	ietf-sr-policy	[I-D.ietf-spring-sr-policy-yang]
ietf-nss	ietf-network-slice-service	[I-D.ietf-teas-ietf-network-slice-nbi-yang]
acl	ietf-access-control-list	[RFC8519]
packet-fields	ietf-packet-fields	[RFC8519]
vpn-common	ietf-vpn-common	[RFC9181]

Table 1

2.3. References in the Model

Following documents are referenced in the model defined in this document -

Document	Reference
YANG Data Model for Network Access Control Lists (ACLs)	[RFC8519]
A YANG Data Model for Traffic Engineering Tunnels and Interfaces	[I-D.ietf-teas-yang-te]
YANG Data Model for Segment Routing Policy	[I-D.ietf-spring-sr-policy-yang]

Table 2

3. Discussion Items

For describing the traffic, currently the YANG models uses:

* The match criteria grouping from the [I-D.ietf-teas-ietf-network-slice-nbi-yang]. If this document gets WG backing, then it might be a good idea to move the grouping to this document instead.

* The ACL Name. Should that be ACE instead?

* The match action granularity in case of IETF network slice and VN needs to be discussed.

* The match action for SFC is not handled yet.

4. Tree Structure

```
module: ietf-traffic-map
  +--rw traffic-map
     +--rw maps* [id]
        +--rw id         string
        +--rw traffic
        |  +--rw id?                      string
        |  +--rw (type)?
        |     +--:(match-criteria)
        |     |  +--rw match-criterion* [index]
        |     |     +--rw index         uint32
        |     |     +--rw match-type    identityref
        |     |     +--rw value*        string
        |     +--:(acl)
        |     |  +--rw acl?               -> /acl:acls/acl/name
        |     +--:(flowspec)
        |     +--:(interface)
        |     |  +--rw node?              string
        |     |  +--rw if-name?           string
        |     +--:(flow)
        |     |  +--rw (l3)?
        |     |  |  +--:(ipv4)
        |     |  |  |  +--rw ipv4
        |     |  |  |        ...
        |     |  |  +--:(ipv6)
        |     |  |     +--rw ipv6
        |     |  |           ...
        |     |  +--rw (l4)?
        |     |     +--:(tcp)
        |     |     |  +--rw tcp
        |     |     |        ...
        |     |     +--:(udp)
        |     |        +--rw udp
        |     |              ...
        |     +--:(other)
        +--rw action
        |  +--rw te-tunnel*   te:tunnel-ref
        |  +--rw sr-policy* [headend policy-color-ref policy-endpoint-re
        |  |  +--rw headend               inet:ip-address-no-zone
        |  |  +--rw policy-color-ref      leafref
        |  |  +--rw policy-endpoint-ref   leafref
        |  +--rw other
        +--ro stats
           +--ro matched-packets?   yang:counter64
           +--ro matched-octets?    yang:counter64
```

5. YANG Model

```
<CODE BEGINS> file "ietf-traffic-map@2024-03-04.yang"
module ietf-traffic-map {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-traffic-map";
  prefix tm;

  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-te {
    prefix te;
    reference
      "I-D.ietf-teas-yang-te: A YANG Data Model for Traffic
       Engineering Tunnels and Interfaces";
  }
  import ietf-routing {
    prefix rt;
    reference
      "RFC8349: A YANG Data Model for Routing Management";
  }
  import ietf-sr-policy {
    prefix sr-policy;
    reference
      "I-D.ietf-spring-sr-policy-yang: YANG Data Model for Segment
       Routing Policy";
  }
  import ietf-network-slice-service {
    prefix ietf-nss;
    reference
      "I-D.ietf-teas-ietf-network-slice-nbi-yang: IETF
       Network Slice Service YANG Model";
  }
  import ietf-packet-fields {
    prefix packet-fields;
    reference
      "RFC 8519: YANG Data Model for Network Access
       Control Lists (ACLs)";
  }
  import ietf-access-control-list {
    prefix acl;
    reference
      "RFC 8519: YANG Data Model for Network Access Control
```

```
     Lists (ACLs)";
}
import ietf-vpn-common {
  prefix vpn-common;
  reference
    "RFC 9181: A Common YANG Data Model for Layer 2 and
     Layer 3 VPNs";
}

organization
  "IETF Traffic Engineering Architecture and Signaling (TEAS)
   Working Group";
contact
  "WG Web:  <https://datatracker.ietf.org/wg/teas/about/>
   WG List:  <mailto:teas@ietf.org>
   Editor: Dhruv Dhody <dhruv.ietf@gmail.com>";
description
  "This module contains a YANG module to map traffic to
   Traffic Engineering (TE) paths.

   Copyright (c) 2022 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.";

revision 2024-03-04 {
  description
    "initial version.";
  reference
    "RFC XXXX: Traffic Mapping YANG model for Traffic
     Engineering (TE)";
}

grouping traffic-description {
  description
    "The traffic description";
  leaf id {
    type string;
    description
      "The identifier for Traffic Description";
  }
```

```
choice type {
  description
    "The various ways the traffic can be described";
  case match-criteria {
    description
      "Use the match criteria";
    list match-criterion {
      key "index";
      description
        "List of traffic match criteria.";
      leaf index {
        type uint32;
        description
          "The entry index.";
      }
      leaf match-type {
        type identityref {
          base ietf-nss:service-match-type;
        }
        mandatory true;
        description
          "Identifies an entry in the list of the
           match criteria.";
      }
      leaf-list value {
        type string;
        description
          "Describes the slice service match criteria, e.g.
           IP address, VLAN, etc.";
      }
    }
  }
  case acl {
    description
      "Reference to ACL";
    leaf acl {
      type leafref {
        path "/acl:acls/acl:acl/acl:name";
      }
      description
        "The ACL Name. The action part of the ACL is not
         used.";
      reference
        "RFC8519: YANG Data Model for Network Access Control
         Lists (ACLs)";
    }
  }
  case flowspec {
    description
```

```
    "Based on FlowSpec component type - TODO";
}
case interface {
  description
    "All traffic received on an interface";
  leaf node {
    type string;
    description
      "The node identifier";
  }
  leaf if-name {
    type string;
    description
      "The interface name on the node";
  }
}
case flow {
  description
    "Match particular flows";
  choice l3 {
    description
      "Either IPv4 or IPv6.";
    container ipv4 {
      description
        "Rule set that matches the IPv4 header.";
      uses packet-fields:acl-ip-header-fields;
      uses packet-fields:acl-ipv4-header-fields;
    }
    container ipv6 {
      description
        "Rule set that matches the IPv6 header.";
      uses packet-fields:acl-ip-header-fields;
      uses packet-fields:acl-ipv6-header-fields;
    }
  }
  choice l4 {
    description
      "Includes Layer-4-specific information.
       This version focuses on TCP and UDP.";
    container tcp {
      description
        "Rule set that matches the TCP header.";
      uses packet-fields:acl-tcp-header-fields;
      uses vpn-common:ports;
    }
    container udp {
      description
        "Rule set that matches the UDP header.";
      uses packet-fields:acl-udp-header-fields;
```

```
          uses vpn-common:ports;
        }
      }
    }
    case other {
      description
        "TODO";
    }
  }
}

grouping te-ref {
  description
    "Reference to TE paths";
  leaf-list te-tunnel {
    type te:tunnel-ref;
    description
      "Reference to TE Tunnels";
    reference
      "I-D.ietf-teas-yang-te: A YANG Data Model for Traffic
       Engineering Tunnels and Interfaces";
  }
  list sr-policy {
    key "headend policy-color-ref policy-endpoint-ref";
    description
      "SR Policy";
    reference
      "I-D.ietf-spring-sr-policy-yang: YANG Data Model for
       Segment Routing Policy";
    /*Headend needs to be added*/
    leaf headend {
      type inet:ip-address-no-zone;
      description
        "SR Policy headend";
    }
    leaf policy-color-ref {
      type leafref {
        path "/rt:routing/sr-policy:segment-routing"
           + "/sr-policy:traffic-engineering/sr-policy:policies"
           + "/sr-policy:policy/sr-policy:color";
      }
      description
        "Reference to sr-policy color";
    }
    leaf policy-endpoint-ref {
      type leafref {
        path "/rt:routing/sr-policy:segment-routing"
           + "/sr-policy:traffic-engineering/sr-policy:policies"
           + "/sr-policy:policy/sr-policy:endpoint";
```

```
      }
      description
        "Reference to sr-policy endpoint";
    }
  }
  container other {
    description
      "To dp - VN, IETF Network Slice, SFC etc";
  }
}

/* Configuration data nodes */

container traffic-map {
  description
    "AP configurations";
  list maps {
    key "id";
    description
      "traffic map identifier";
    leaf id {
      type string;
      description
        "The identifier for Traffic Maps";
    }
    container traffic {
      description
        "The traffic description";
      uses traffic-description;
    }
    container action {
      description
        "The action is limited to identifying the TE resource";
      uses te-ref;
    }
    container stats {
      config false;
      description
        "Statistics";
      leaf matched-packets {
        type yang:counter64;
        description
          "The number of packets that matched the traffic
           description";
      }
      leaf matched-octets {
        type yang:counter64;
        description
          "The number of octets (byte) that matched the traffic
```

```
            description";
          }
        }
      }
    }
}

<CODE ENDS>
```

6. Security Considerations

TBD

7. IANA Considerations

IANA is requested to make the following allocation for the URIs in the "ns" subregistry within the "IETF XML Registry" [RFC3688]:

```
---------------------------------------------------------------------
URI: urn:ietf:params:xml:ns:yang:ietf-traffic-map
Registrant Contact: The IESG.
XML: N/A, the requested URI is an XML namespace.
---------------------------------------------------------------------
```

IANA is requested to make the following allocation for the YANG module in the "YANG Module Names" registry [RFC6020]:

```
---------------------------------------------------------------------
name:         ietf-traffic-map
namespace:    urn:ietf:params:xml:ns:yang:ietf-traffic-map
prefix:       tm
reference:    RFC XXXX
---------------------------------------------------------------------
```

8. References

8.1. Normative References

[I-D.ietf-spring-sr-policy-yang] Raza, S., Sawaya, R., 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-02, 23 September 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-policy-yang-02>.

[I-D.ietf-teas-ietf-network-slice-nbi-yang] Wu, B., Dhody, D., Rokui, R., Saad, T., and J. Mullooly, "A YANG Data Model for the RFC AAAA Network Slice Service", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slice-nbi-yang-09, 17 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-nbi-yang-09>.

[I-D.ietf-teas-yang-te] Saad, T., Gandhi, R., Liu, X., Beeram, V. P., and I. Bryskin, "A YANG Data Model for Traffic Engineering Tunnels, Label Switched Paths and Interfaces", Work in Progress, Internet-Draft, draft-ietf-teas-yang-te-36, 2 February 2024, <https://

datatracker.ietf.org/doc/html/draft-ietf-teas-yang-te-36>.

[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/rfc/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/rfc/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/rfc/rfc6020>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/rfc/rfc6991>.

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

[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/rfc/rfc8174>.

[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/rfc/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/rfc/rfc8349>.

[RFC8519] Jethanandani, M., Agarwal, S., Huang, L., and D. Blair, "YANG Data Model for Network Access Control Lists (ACLs)", RFC 8519, DOI 10.17487/RFC8519, March 2019, <https://www.rfc-editor.org/rfc/rfc8519>.

[RFC9181] Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., and Q. Wu, "A Common YANG Data Model for Layer 2 and Layer 3 VPNs", RFC 9181, DOI 10.17487/RFC9181, February 2022, <https://www.rfc-editor.org/rfc/rfc9181>.

8.2. Informative References

[RFC8955] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <https://www.rfc-editor.org/rfc/rfc8955>.

[RFC9168] Dhody, D., Farrel, A., and Z. Li, "Path Computation Element Communication Protocol (PCEP) Extension for Flow Specification", RFC 9168, DOI 10.17487/RFC9168, January 2022, <https://www.rfc-editor.org/rfc/rfc9168>.

Appendix A. Acknowledgments

Thanks to Adrian Farrel for the motivation behind this document.

Appendix B. Examples

TO be added in future revisions.

Author's Address

Dhruv Dhody
Huawei
India

Email: dhruv.ietf@gmail.com