

Internet Engineering Task Force  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2018

D. Hiremagalur, Ed.  
G. Grammel, Ed.  
Juniper  
G. Galimberti, Ed.  
Cisco  
R. Kunze  
Deutsche Telekom  
D. Beller  
Nokia  
October 30, 2017

Extension to the Link Management Protocol (LMP/DWDM -rfc4209) for Dense  
Wavelength Division Multiplexing (DWDM) Optical Line Systems to manage  
the application code of optical interface parameters in DWDM application  
draft-dharinigert-ccamp-dwdm-if-lmp-05

## Abstract

This memo defines extensions to LMP(rfc4209) for managing Optical parameters associated with Wavelength Division Multiplexing (WDM) systems in accordance with the Interface Application Identifier approach defined in ITU-T Recommendation G.694.1.[ITU.G694.1] and its extensions.

## Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

## 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 May 3, 2018.

## Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

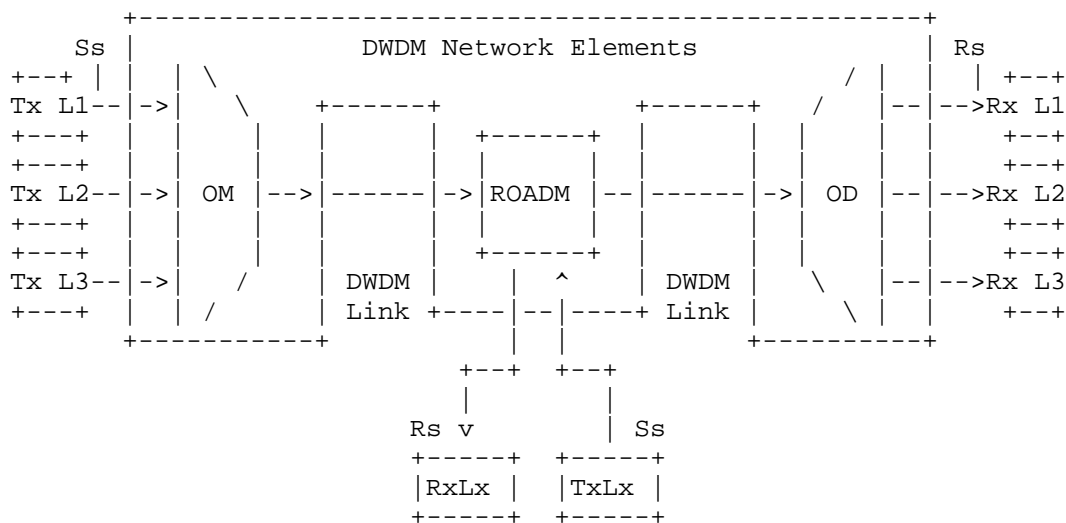
1. Introduction . . . . .	2
2. DWDM line system . . . . .	3
3. Use Cases . . . . .	4
4. Extensions to LMP-WDM Protocol . . . . .	4
5. General Parameters - OCh_General . . . . .	5
6. ApplicationIdentifier - OCh_ApplicationIdentifier . . . . .	6
7. OCh_Ss - OCh transmit parameters . . . . .	9
8. OCh_Rs - receive parameters . . . . .	9
9. Security Considerations . . . . .	10
10. IANA Considerations . . . . .	10
11. Contributors . . . . .	11
12. References . . . . .	11
12.1. Normative References . . . . .	11
12.2. Informative References . . . . .	12
Authors' Addresses . . . . .	13

## 1. Introduction

This extension addresses the use cases described by "draft-ietf-ccamp-dwdm-if-mng-ctrl-fwk-07". LMP [RFC4902] provides link property correlation capabilities that can be used between a transceiver device and an Optical Line System (OLS) device. Link property correlation is a procedure by which, intrinsic parameters and capabilities are exchanged between two ends of a link. Link property correlation as defined in RFC3591 allows either end of the link to supervise the received signal and operate within a commonly understood parameter window. Here the term 'link' refers in particular to the attachment link between OXC and OLS (see Figure 1). The relevant interface parameters are in line with "draft-dharini-ccamp-dwdm-if-yang-03".

## 2. DWDM line system

Figure 1 shows a set of reference points (Rs and Ss), for a single-channel connection between transmitter (Tx) and receiver (Rx) devices. Here the DWDM network elements in between those devices include an Optical Multiplexer (OM) and an Optical Demultiplexer (OD). In addition it may include one or more Optical Amplifiers (OA) and one or more Optical Add-Drop Multiplexers (OADM).

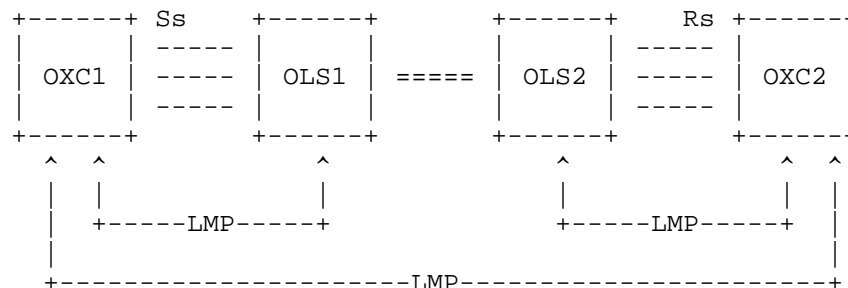


Ss = Sender reference point at the DWDM network element tributary output  
Rs = Receiver reference point at the DWDM network element tributary input  
Lx = Lambda x  
OM = Optical Mux  
OD = Optical Demux  
ROADM = Reconfigurable Optical Add Drop Mux

from Fig. 5.1/G.698.2

Figure 1: Linear Single Channel approach

Figure 2 Extended LMP Model ( from [RFC4209] )



OXC           : is an entity that contains transponders  
 OLS           : generic optical system, it can be -  
               Optical Mux, Optical Demux, Optical Add  
               Drop Mux, Amplifier etc.  
 OLS to OLS   : represents the Optical Multiplex section  
               <xref target="ITU.G709"/>  
 Rs/Ss         : reference points in between the OXC and the OLS

Figure 2: Extended LMP Model

### 3. Use Cases

The use cases are described in draft-ietf-ccamp-dwdm-if-mng-ctrl-fwk

### 4. Extensions to LMP-WDM Protocol

This document defines extensions to [RFC4209] to allow a set of characteristic parameters, to be exchanged between a router or optical switch (e.g. OTN cross connect) and the optical line system to which it is attached. In particular, this document defines additional Data Link sub-objects to be carried in the LinkSummary message defined in [RFC4204] and [RFC6205]. The OXC and OLS systems may be managed by different Network management systems and hence may not know the capability and status of their peer. These messages and their usage are defined in subsequent sections of this document.

The following new messages are defined for the WDM extension for ITU-T G.698.2 [ITU.G698.2]/ITU-T G.698.1 [ITU.G698.1]/ITU-T G.959.1 [ITU.G959.1]

- OCh\_General (sub-object Type = TBA)
- OCh\_ApplicationIdentifier (sub-object Type = TBA)
- OCh\_Ss (sub-object Type = TBA)
- OCh\_Rs (sub-object Type = TBA)

## 5. General Parameters - OCh\_General

These are a set of general parameters as described in [G698.2] and [G.694.1]. Please refer to the "draft-galikunze-ccamp-dwdm-if-snmp-mib-01" and "draft-dharini-ccamp-dwdm-if-yang-00" for more details about these parameters and the [RFC6205] for the wavelength definition.

The general parameters are

1. Central Frequency - (Tera Hz) 4 bytes (see RFC6205 sec.3.2)
2. Number of Application Identifiers (A.I.) Supported
3. Single-channel Application Identifier in use
4. Application Identifier Type in use
5. Application Identifier in use

Figure 3: The format of the this sub-object (Type = TBA, Length = TBA) is as follows:

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Length										(Reserved)																			
Central Frequency																																							
Number of Application Identifiers Supported																				(Reserved)																			
Single-channel Application Identifier Number in use										A.I. Type in use										A.I. length																			
Single-channel Application Identifier in use																																							
Single-channel Application Identifier in use																																							
Single-channel Application Identifier in use																																							

A.I. Type in use: STANDARD, PROPRIETARY

A.I. Type in use: STANDARD

Refer to G.698.2 recommendation : B-DScW-ytz(v)

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Single-channel Application Code																																							
Single-channel Application Code																																							
Single-channel Application Code																																							

A.I. Type in use: PROPRIETARY

Note: if the A.I. type = PROPRIETARY, the first 6 Octets of the Application Identifier in use are six characters of the PrintableString must contain the Hexadecimal representation of an OUI (Organizationally Unique Identifier) assigned to the vendor whose implementation generated the Application Identifier; the remaining octets of the PrintableString are unspecified.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
OUI																																							
OUI cont.																				Vendor value																			
Vendor Value																																							

Figure 3: OCh\_General

## 6. ApplicationIdentifier - OCh\_ApplicationIdentifier

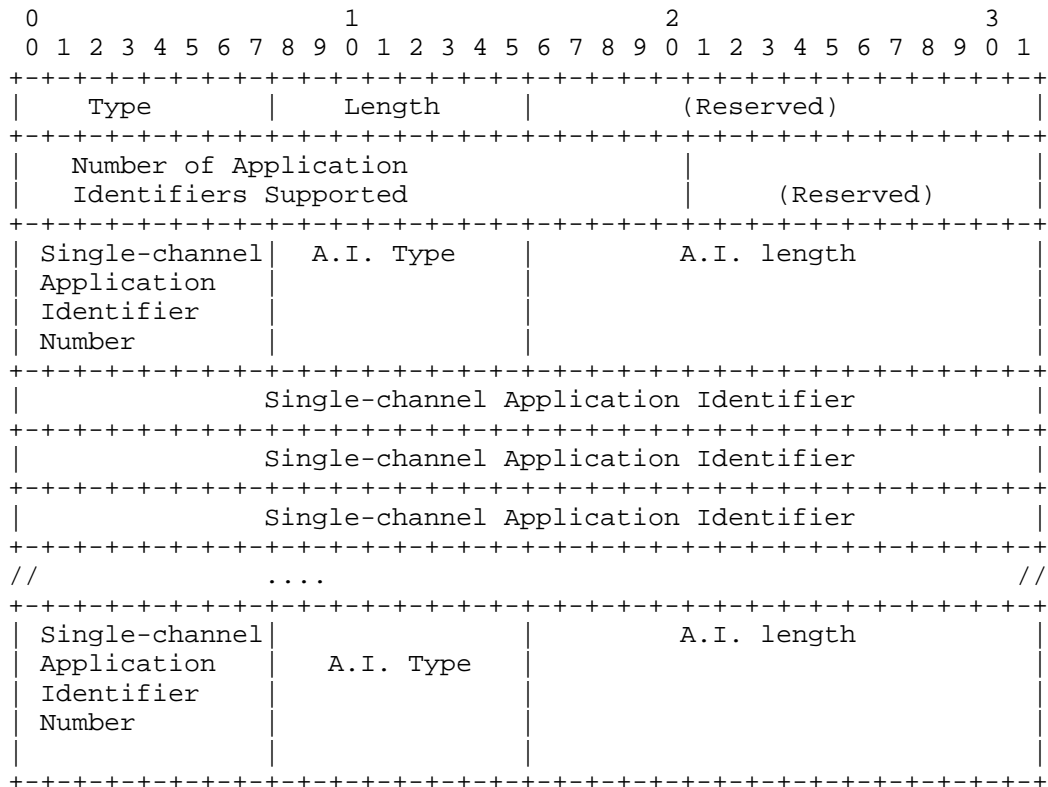
This message is to exchange the application identifiers supported as described in [G698.2]. There can be more than one Application Identifier supported by the transmitter/receiver in the OXC. The number of application identifiers supported is exchanged in the "OCh\_General" message. (from [G698.1]/[G698.2]/[G959.1] and G.874.1)

The parameters are

1. Number of Application Identifiers (A.I.) Supported
2. Single-channel application identifier Number  
uniquely identifies this entry - 8 bits
3. Application Identifier Type (A.I.) (STANDARD/PROPRIETARY)
4. Single-channel application identifier -- 96 bits  
(from [G698.1]/[G698.2]/[G959.1])

- this parameter can have multiple instances as the transceiver can support multiple application identifiers.

Figure 4: The format of the this sub-object (Type = TBA, Length = TBA) is as follows:



```

|               Single-channel Application Identifier               |
+-----+-----+-----+-----+-----+-----+-----+-----+
|               Single-channel Application Identifier               |
+-----+-----+-----+-----+-----+-----+-----+-----+
|               Single-channel Application Identifier               |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

A.I. Type in use: STANDARD, PROPRIETARY

A.I. Type in use: STANDARD

Refer to G.698.2 recommendation : B-DScW-ytz(v)

```

0               1               2               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|               Single-channel Application Code                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|               Single-channel Application Code                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|               Single-channel Application Code                     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

A.I. Type in use: PROPRIETARY

Note: if the A.I. type = PROPRIETARY, the first 6 Octets of the Application Identifier in use are six characters of the PrintableString must contain the Hexadecimal representation of an OUI (Organizationally Unique Identifier) assigned to the vendor whose implementation generated the Application Identifier; the remaining octets of the PrintableString are unspecified.

```

0               1               2               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|               OUI                                                 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|               OUI cont.                |               Vendor value |
+-----+-----+-----+-----+-----+-----+-----+-----+
|               Vendor Value                                         |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Figure 4: OCh\_ApplicationIdentifier



## 7. OCh\_Ss - OCh transmit parameters

These are the G.698.2 parameters at the Source(Ss reference points). Please refer to "draft-dharini-ccamp-dwdm-if-yang-03" for more details about these parameters.

### 1. Output power

Figure 5: The format of the OCh sub-object (Type = TBA, Length = TBA) is as follows:

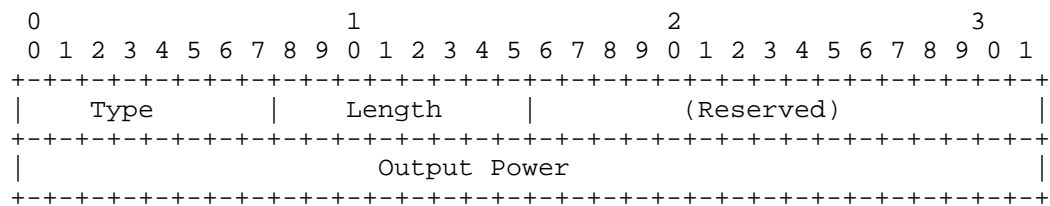


Figure 5: OCh\_Ss transmit parameters

## 8. OCh\_Rs - receive parameters

These are the G.698.2 parameters at the Sink (Rs reference points).

### 1. Current Input Power - (0.1dbm) 4bytes

Figure 6: The format of the OCh receive sub-object (Type = TBA, Length = TBA) is as follows:

The format of the OCh receive/OLS Sink sub-object (Type = TBA, Length = TBA) is as follows:

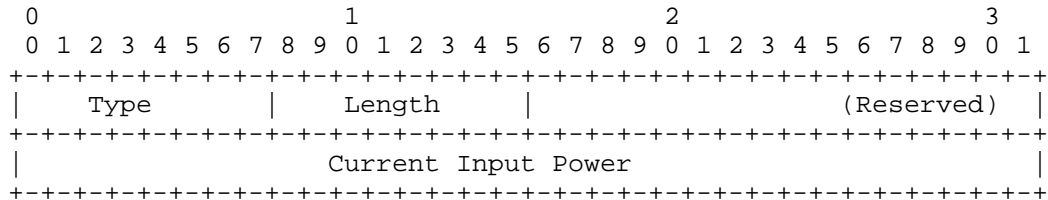


Figure 6: OCh\_Rs receive parameters

## 9. Security Considerations

LMP message security uses IPsec, as described in [RFC4204]. This document only defines new LMP objects that are carried in existing LMP messages, similar to the LMP objects in [RFC:4209]. This document does not introduce new security considerations.

## 10. IANA Considerations

LMP <xref target="RFC4204"/> defines the following name spaces and the ways in which IANA can make assignments to these namespaces:

- LMP Message Type
  - LMP Object Class
  - LMP Object Class type (C-Type) unique within the Object Class
  - LMP Sub-object Class type (Type) unique within the Object Class
- This memo introduces the following new assignments:

LMP Sub-Object Class names:

under DATA\_LINK Class name (as defined in <xref target="RFC4204"/>)

- OCh\_General (sub-object Type = TBA)
- OCh\_ApplicationIdentifier (sub-object Type = TBA)
- OCh\_Ss (sub-object Type = TBA)
- OCh\_Rs (sub-object Type = TBA)

## 11. Contributors

Arnold Mattheus  
Deutsche Telekom  
Darmstadt  
Germany  
email a.mattheus@telekom.de

John E. Drake  
Juniper  
1194 N Mathilda Avenue  
HW-US, Pennsylvania  
USA  
jdrake@juniper.net

Zafar Ali  
Cisco  
3000 Innovation Drive  
KANATA  
ONTARIO K2K 3E8  
zali@cisco.com

## 12. References

### 12.1. Normative References

[I-D.ietf-ccamp-dwdm-if-mng-ctrl-fwk]  
Kunze, R., Grammel, G., Beller, D., Galimberti, G., and J. Meuric, "A framework for Management and Control of DWDM optical interface parameters", draft-ietf-ccamp-dwdm-if-mng-ctrl-fwk-07 (work in progress), September 2017.

[ITU.G694.1]  
International Telecommunications Union, "Spectral grids for WDM applications: DWDM frequency grid", ITU-T Recommendation G.698.2, February 2012.

[ITU.G698.2]  
International Telecommunications Union, "Amplified multichannel dense wavelength division multiplexing applications with single channel optical interfaces", ITU-T Recommendation G.698.2, November 2009.

[ITU.G709]  
International Telecommunications Union, "Interface for the Optical Transport Network (OTN)", ITU-T Recommendation G.709, February 2012.

- [ITU.G872]     International Telecommunications Union, "Architecture of optical transport networks", ITU-T Recommendation G.872, October 2012.
- [ITU.G874.1]     International Telecommunications Union, "Optical transport network (OTN): Protocol-neutral management information model for the network element view", ITU-T Recommendation G.874.1, October 2012.
- [RFC4054]     Strand, J., Ed. and A. Chiu, Ed., "Impairments and Other Constraints on Optical Layer Routing", RFC 4054, DOI 10.17487/RFC4054, May 2005, <<https://www.rfc-editor.org/info/rfc4054>>.
- [RFC4204]     Lang, J., Ed., "Link Management Protocol (LMP)", RFC 4204, DOI 10.17487/RFC4204, October 2005, <<https://www.rfc-editor.org/info/rfc4204>>.
- [RFC4209]     Fredette, A., Ed. and J. Lang, Ed., "Link Management Protocol (LMP) for Dense Wavelength Division Multiplexing (DWDM) Optical Line Systems", RFC 4209, DOI 10.17487/RFC4209, October 2005, <<https://www.rfc-editor.org/info/rfc4209>>.
- [RFC6205]     Otani, T., Ed. and D. Li, Ed., "Generalized Labels for Lambda-Switch-Capable (LSC) Label Switching Routers", RFC 6205, DOI 10.17487/RFC6205, March 2011, <<https://www.rfc-editor.org/info/rfc6205>>.

## 12.2. Informative References

- [RFC2629]     Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <<https://www.rfc-editor.org/info/rfc2629>>.
- [RFC3410]     Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, DOI 10.17487/RFC3410, December 2002, <<https://www.rfc-editor.org/info/rfc3410>>.
- [RFC4181]     Heard, C., Ed., "Guidelines for Authors and Reviewers of MIB Documents", BCP 111, RFC 4181, DOI 10.17487/RFC4181, September 2005, <<https://www.rfc-editor.org/info/rfc4181>>.

Authors' Addresses

Dharini Hiremagalur (editor)  
Juniper  
1194 N Mathilda Avenue  
Sunnyvale - 94089 California  
USA

Phone: +1408  
Email: dharinih@juniper.net

Gert Grammel (editor)  
Juniper  
Oskar-Schlemmer Str. 15  
80807 Muenchen  
Germany

Phone: +49 1725186386  
Email: ggrammel@juniper.net

Gabriele Galimberti (editor)  
Cisco  
Via S. Maria Molgora, 48 c  
20871 - Vimercate  
Italy

Phone: +390392091462  
Email: ggalimbe@cisco.com

Ruediger Kunze  
Deutsche Telekom  
Dddd, xx  
Berlin  
Germany

Phone: +49xxxxxxxxxx  
Email: RKunze@telekom.de

Dieter Beller  
Nokia  
Lorenzstrasse, 10  
70435 Stuttgart  
Germany

Phone: +4971182143125  
Email: Dieter.Beller@nokia.com

CCAMP Working Group

Internet Draft

Intended Status: Standard Track

Expires: April 27, 2018

G. Fioccola

Telecom Italia

K. Lee

Korea Telecom

Y. Lee

D. Dhody

Huawei

O. Gonzalez de Dios

Telefonica

D. Ceccarelli

Ericsson

October 27, 2017

A Yang Data Model for L1 Connectivity Service Model (L1CSM)

draft-fioccola-ccamp-llcsm-yang-00

## Abstract

This document provides a YANG data model for Layer 1 Connectivity Service Model (L1CSM).

## Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on April 27, 2018.

## Copyright Notice

TBD

Expires April 27, 2018

[Page 1]

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction.....	2
1.1. Deployment Scenarios.....	3
1.2. Terminology.....	6
1.3. Tree diagram.....	6
2. Definitions.....	7
3. L1SM YANG Model (Tree Structure).....	7
4. L1SM YANG Code.....	8
5. Security Considerations.....	19
6. IANA Considerations.....	20
7. Acknowledgments.....	20
8. References.....	21
8.1. Normative References.....	21
8.2. Informative References.....	21
9. Contributors.....	21
Authors' Addresses.....	21

## 1. Introduction

This document provides a YANG data model for L1VPN Connectivity Service Model (L1CSM). The intent of this document is to provide a transport service model exploiting Yang data model, which can be utilized by a client network controller to initiate a service request connectivity request as well as retrieving service states toward a transport network controller communicating with the client controller via a Netconf/Restconf interface.

[RFC4847] provides a framework and service level requirements for Layer 1 Virtual Private Networks (L1VPNs). It classifies service models as management-based service model, signaling-based service



model (Basic Mode) and signaling and routing service model (Enhanced Mode).

In the management-based service model, customer management systems and provider management systems communicate with each other. Customer management systems access provider management systems to request layer 1 connection setup/deletion between a pair of CEs. Customer management systems may obtain additional information, such as resource availability information and monitoring information, from provider management systems. There is no control message exchange between a CE and PE.

In the signaling-based service model (Basic Model), the CE-PE interface's functional repertoire is limited to path setup signaling only. In the Signaling and routing service model (Enhanced Mode), the CE-PE interface provides the signaling capabilities as in the Basic Mode, plus permits limited exchange of information between the control planes of the provider and the customer to help such functions as discovery of customer network routing information (i.e., reachability or TE information in remote customer sites), or parameters of the part of the provider's network dedicated to the customer.

The primary focus of this document is to describe L1CS YANG model required for the instantiation of point-to-point L1VPN service. A L1VPN is a service offered by a core layer 1 network to provide layer 1 connectivity between two or more customer sites where the customer has some control over the establishment and type of the connectivity.

### 1.1. Deployment Scenarios

Figure 1 depicts a deployment scenario of the L1VPN SDN control-based service model for an external customer instantiating L1 point-to-point connectivity to the provider.

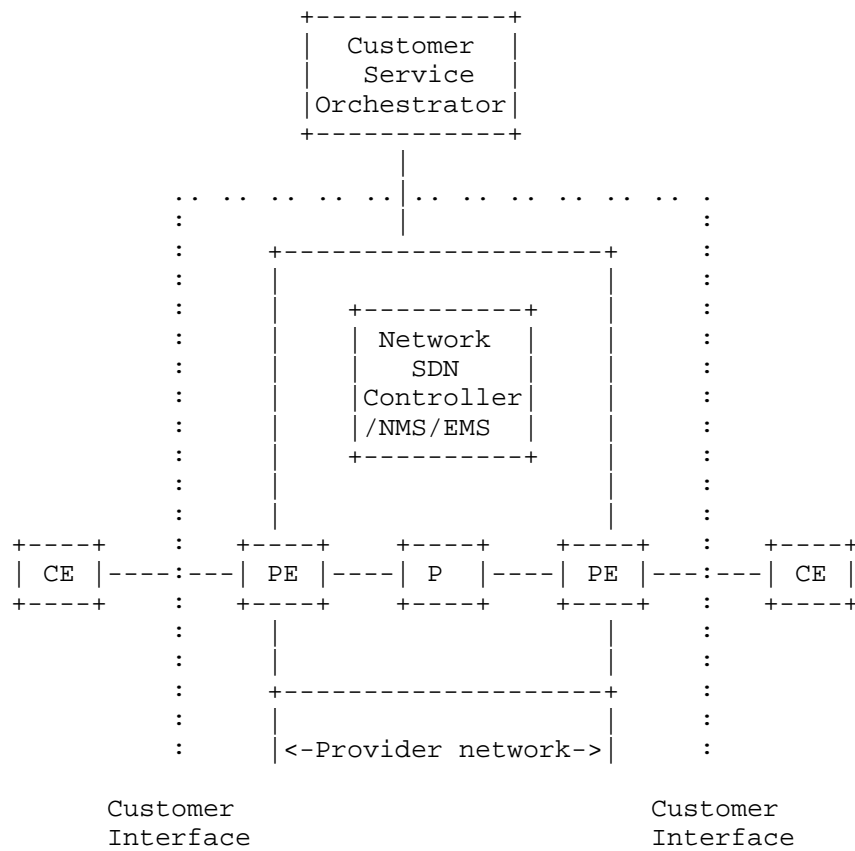


Figure 1: L1VPN SDN Controller/EMS/NMS-Based Service Model: External Customer

With this scenario, the customer service orchestrator interfaces with the network SDN controller of the provider using Customer Service Model as defined in [Service-Yang].

Figure 2 depicts another deployment scenario for internal customer (e.g., higher-layer service management department(s)) interfacing the layer 1 transport network department. With this scenario, a multi-service backbone is characterized such that each service department of a provider (e.g., L2/3 services) that receives the same provider's L1VPN service provides a different kind of higher-layer service. The customer receiving the L1VPN service (i.e., each service department) can offer its own services, whose payloads can be any layer (e.g., ATM, IP, TDM). The layer 1 transport network and each service network belong to the same organization, but may be

managed separately. The Service SDN Controller is the control/management entity owned by higher-layer service department (e.g., L2/3 VPN) whereas the Network SDN Controller is the control/management entity responsible for Layer 1 connectivity service. The CE's in Figure 2 are L2/3 devices that interface with L1 PE devices.

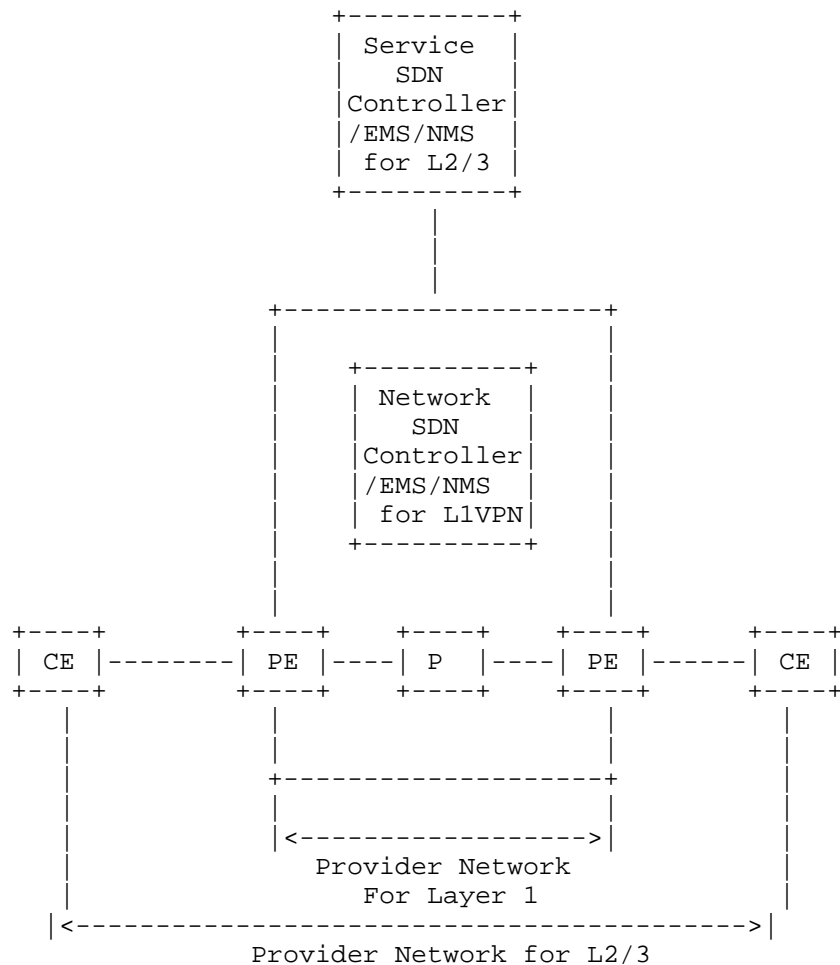


Figure 2: L1VPN SDN Controller/EMS/NMS-Based Service Model: Internal Customer

The benefit is that the same layer 1 transport network resources are shared by multiple services. A large capacity backbone network (data plane) can be built economically by having the resources shared by multiple services usually with flexibility to modify topologies, while separating the control functions for each service department. Thus, each customer can select a specific set of features that are needed to provide their own service [RFC4847].

## 1.2. Terminology

Refer to [RFC4847] and [RFC5253] for the key terms used in this document.

The following terms are defined in [RFC6241] and are not redefined here:

- o client
- o configuration data
- o server
- o state data

The following terms are defined in [RFC6020] and are not redefined here:

- o augment
- o data model
- o data node

The terminology for describing YANG data models is found in [RFC6020].

## 1.3. Tree diagram

A simplified graphical representation of the data model is presented in Section x.

The meaning of the symbols in these diagrams is as follows:

- o Brackets "[" and "]" enclose list keys.

- o Curly braces "{" and "}" contain names of optional features that make the corresponding node conditional.
- o Abbreviations before data node names: "rw" means configuration (read-write), and "ro" state data (read-only).
- o Symbols after data node names: "?" means an optional node and "\*" denotes a "list" or "leaf-list".
- o Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- o Ellipsis ("...") stands for contents of subtrees that are not shown.

## 2. Definitions

TDB

## 3. L1SM YANG Model (Tree Structure)

```

module: ietf-llcsm
  +--rw llcs
    +--rw access
      |   +--rw uni-list* [UNI-ID]
      |   |   +--rw UNI-ID          string
      |   |   +--rw protocol?       identityref
      |   |   +--rw coding?         identityref
      |   |   +--rw optical_interface? identityref
      +--rw service
        +--rw service-list* [subscriber-llvc-id]
        +--rw subscriber-llvc-id    string
        +--rw service-config
          +--rw subscriber-llvc-id?    string
          +--rw subscriber-llvc-ep-ingress? ->
/llcs/access/uni-list/UNI-ID
  +--rw subscriber-llvc-ep-egress? ->
/llcs/access/uni-list/UNI-ID
  +--rw client-protocol?            identityref
  +--rw time-start?                 yang:date-and-time
  +--rw time-interval?              int64
  +--rw CoS_Name?                   string

```

+--rw performance-metric?                    identityref

#### 4. L1SM YANG Code

The YANG code is as follows:

<CODE BEGINS> file "ietf-l1csm@2017-10-27.yang"

```
module ietf-l1csm {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-l1csm";
  prefix "l1csm";

  import ietf-yang-types {
    prefix "yang";
  }

  organization
    "Internet Engineering Task Force (IETF) CCAMP WG";

  contact
    "Editor: G. Fioccola (giuseppe.fioccola@telecomitalia.it)
     Editor: K. Lee (kwangkoog.lee@kt.com)
     Editor: Y. Lee (leeyoung@huawei.com)
     Editor: D. Dhody (dhruv.ietf@gmail.com)
     Editor: O. Gonzalez de-Dios (oscar.gonzalezdedios@telefonica.com)
     Editor: D. Ceccarelli (daniele.ceccarelli@ericsson.com)";

  description
    "this module describes Layer 1 connectivity service model for
     subscriber Layer 1 Connectivity Services and Attributes";

  revision 2017-10-27 {
    description
      "Initial revision.";
    reference "to add the draft name";
  }

  identity protocol-type {
    description
```

```
                                "base identity from which client protocol
type is derived.";
    }

    identity aGigE {
        base protocol-type;
        description
            "GigE protocol type";
    }

    identity a10GigE_WAN {
        base protocol-type;
        description
            "10GigE-WAN protocol type";
    }

    identity a10GigE_LAN {
        base protocol-type;
        description
            "10GigE-LAN protocol type";
    }

    identity a40GigE {
        base protocol-type;
        description
            "40GigE protocol type";
    }

    identity a100GigE {
        base protocol-type;
        description
            "100GigE protocol type";
    }

    identity FC-100 {
        base protocol-type;
        description
            "Fiber Channel - 100 protocol type";
    }

    identity FC-200 {
        base protocol-type;
        description
            "Fiber Channel - 200 protocol type";
    }
}
```

```
identity FC-400 {
    base protocol-type;
    description
        "Fiber Channel - 400 protocol type";
}

identity FC-800 {
    base protocol-type;
    description
        "Fiber Channel - 800 protocol type";
}

identity FC-1200 {
    base protocol-type;
    description
        "Fiber Channel - 1200 protocol type";
}

identity FC-1600 {
    base protocol-type;
    description
        "Fiber Channel - 1600 protocol type";
}

identity FC-3200 {
    base protocol-type;
    description
        "Fiber Channel - 3200 protocol type";
}

identity STM-1 {
    base protocol-type;
    description
        "SDH STM-1 protocol type";
}

identity STM-4 {
    base protocol-type;
    description
        "SDH STM-4 protocol type";
}

identity STM-16 {
    base protocol-type;
```



```
        description
            "SDH STM-16 protocol type";
    }

    identity STM-64 {
        base protocol-type;
        description
            "SDH STM-64 protocol type";
    }

    identity STM-256 {
        base protocol-type;
        description
            "SDH STM-256 protocol type";
    }

    identity OC-3 {
        base protocol-type;
        description
            "SONET OC-3 protocol type";
    }

    identity OC-12 {
        base protocol-type;
        description
            "SONET OC-12 protocol type";
    }

    identity OC-48 {
        base protocol-type;
        description
            "SONET OC-48 protocol type";
    }

    identity OC-192 {
        base protocol-type;
        description
            "SONET OC-192 protocol type";
    }

    identity OC-768 {
        base protocol-type;
        description
            "SONET OC-768 protocol type";
    }
}
```

```
        identity coding-func {
            description
                "base identity from which coding func is
derived.";
        }

        identity a1000X-PCS-36 {
            base coding-func;
            description
                "PCS clause 36 coding function that
corresponds to 1000BASE-X";
        }

        identity a10GW-PCS-49-WIS-50 {
            base coding-func;
            description
                "PCS clause 49 and WIS clause 50 coding func
that corresponds to 10GBASE-W (WAN PHY)";
        }

        identity a10GR-PCS-49 {
            base coding-func;
            description
                "PCS clause 49 coding function that
corresponds to 10GBASE-R (LAN PHY)";
        }

        identity a40GR-PCS-82 {
            base coding-func;
            description
                "PCS clause 82 coding function that
corresponds to 40GBASE-R";
        }

        identity a100GR-PCS-82 {
            base coding-func;
            description
                "PCS clause 82 coding function that
corresponds to 100GBASE-R";
        }

        /* coding func needs to expand for Fiber Channel, SONET, SDH */

        identity optical-interface-func {
```

```
        description
            "base identity from which optical-interface-
function is derived.";
    }

    identity SX-PMD-clause-38 {
        base optical-interface-func;
        description
            "SX-PMD-clause-38 Optical Interface function
for 1000BASE-X PCS-36";
    }

    identity LX-PMD-clause-38 {
        base optical-interface-func;
        description
            "LX-PMD-clause-38 Optical Interface function
for 1000BASE-X PCS-36";
    }

    identity LX10-PMD-clause-59 {
        base optical-interface-func;
        description
            "LX10-PMD-clause-59 Optical Interface
function for 1000BASE-X PCS-36";
    }

    identity BX10-PMD-clause-59 {
        base optical-interface-func;
        description
            "BX10-PMD-clause-59 Optical Interface
function for 1000BASE-X PCS-36";
    }

    identity LW-PMD-clause-52 {
        base optical-interface-func;
        description
            "LW-PMD-clause-52 Optical Interface function
for 10GBASE-W PCS-49-WIS-50";
    }

    identity EW-PMD-clause-52 {
        base optical-interface-func;
        description
            "EW-PMD-clause-52 Optical Interface function
for 10GBASE-W PCS-49-WIS-50";
    }
```

```
    }

    identity LR-PMD-clause-52 {
        base optical-interface-func;
        description
            "LR-PMD-clause-52 Optical Interface function
for 10GBASE-R PCS-49";
    }

    identity ER-PMD-clause-52 {
        base optical-interface-func;
        description
            "ER-PMD-clause-52 Optical Interface function
for 10GBASE-R PCS-49";
    }

    identity LR4-PMD-clause-87 {
        base optical-interface-func;
        description
            "LR4-PMD-clause-87 Optical Interface function
for 40GBASE-R PCS-82";
    }

    identity ER4-PMD-clause-87 {
        base optical-interface-func;
        description
            "ER4-PMD-clause-87 Optical Interface function
for 40GBASE-R PCS-82";
    }

    identity FR-PMD-clause-89 {
        base optical-interface-func;
        description
            "FR-PMD-clause-89 Optical Interface function
for 40GBASE-R PCS-82";
    }

    identity LR4-PMD-clause-88 {
        base optical-interface-func;
        description
            "LR4-PMD-clause-88 Optical Interface function
for 100GBASE-R PCS-82";
    }

    identity ER4-PMD-clause-88 {
```

```
        base optical-interface-func;
        description
            "ER4-PMD-clause-88 Optical Interface function
for 100GBASE-R PCS-82";
    }

/* optical interface func needs to expand for Fiber Channel, SONET
and SDH */

    identity performance-metriclist {
        description "list of performance metric";
    }

    identity One-way-Delay {
        base performance-metriclist;
        description "One-way-Delay";
    }

    identity One-way-Errored-Second {
        base performance-metriclist;
        description "One-way-Errored-Second";
    }

    identity One-way-Severely-Errored-Second {
        base performance-metriclist;
        description "One-way-Severely-Errored-Second";
    }

    identity One-way-Unavailable-Second {
        base performance-metriclist;
        description "One-way-Unavailable-Second";
    }

    identity One-way-Availability {
        base performance-metriclist;
        description "One-way-Availability";
    }

    grouping protocol-coding-optical_interface {
        description
            "describes <p,c,o>";
        leaf protocol {
            type identityref {
```

```

        base protocol-type;
    }
    description "Physical layer L1VC client
protocol service attribute";
}

    leaf coding {
        type identityref {
            base coding-func;
        }
        description "coding function";
    }

    leaf optical_interface {
        type identityref {
            base optical-interface-func;
        }
        description "optical-interface-function";
    }
}

grouping uni-attributes {
    description
        "uni-service-attributes";

    leaf UNI-ID {
        type string;
        description "the UNI id of UNI
Service Attributes";
    }

    uses protocol-coding-optical_interface;
}

grouping subscriber-llvc-sls-service-attribute {
    description
        "The value of the Subscriber L1VC SLS
(Service Level Specification) Service Attribute expressed in a 4-tuple of the
form.";

    leaf time-start {
        type yang:date-and-time;
        description "a time that represent
the date and time for the start of the SLS";
    }
}

```

```

    }

    leaf time-interval {
        type int64;
        units seconds;
        description "a time interval
(e.g., 1 month) that is used in conjunction with time-start to specify a
contiguous sequence of time intervals T for determining when performance
objectives are met.";
    }

    leaf CoS_Name {
        type string;
        description "a Class of Service
Name used by the Subscriber L1VC End Point Class of Service Identifier Service
Attribute.";
    }

    leaf performance-metric {
        type identityref {
            base performance-metriclist;
        }
        description "list of performance
metric";
    }
}

grouping subscriber-l1vc-service-attributes {
    description
        "subscriber layer 1 connection service
service level";

    leaf subscriber-l1vc-id {
        type string;
        description "subscriber L1VC identifier";
    }

    leaf subscriber-l1vc-ep-ingress {
        type leafref {
            path "/l1cs/access/uni-list/UNI-ID";
        }
        description "this is one end of subscriber L1VC end
point ID value = UNI-1";
    }
}

```

```
        leaf subscriber-llvc-ep-egress {
            type leafref {
                path "/llcs/access/uni-list/UNI-ID";
            }
            description "this is the other end of subscriber
L1VC end point ID value = UNI-2";
        }

        leaf client-protocol {
            type identityref {
                base protocol-type;
            }
            description "One of Ethernet, Fiber Channel, SONET,
SDH";
        }

        uses subscriber-llvc-sls-service-attribute;
    }

    grouping subscriber-attributes {
        description
            "subscriber attributes";

        uses subscriber-llvc-service-attributes;
    }

    container llcs {
        description
            "serves as a top-level container for a list of layer 1
connection services (llcs)";

        container access {
            description "UNI configurations";

            list uni-list {
                key "UNI-ID";
                description "uni identifier";
                uses uni-attributes {
```



```

        description "UNI attributes
information";
    }
}

container service {
    description "L1VC service";
    list service-list {
        key "subscriber-llvc-id";
        description
            "an unique identifier of a service";

        leaf subscriber-llvc-id {
            type string;
            description "a unique service identifier for
L1VC.";
        }
        container service-config {
            description "service-config container";

            uses subscriber-attributes;

            } //end of service-config
        } //end of service list
    } //end of service container

} //service top container
}
```

<CODE ENDS>

## 5. Security Considerations

The configuration, state, and action data defined in this document are designed to be accessed via a management protocol with a secure transport layer, such as NETCONF [RFC6241]. The NETCONF access control model [RFC6536] provides the means to restrict access for particular NETCONF users to a preconfigured subset of all available

NETCONF protocol operations and content.

A number of configuration data nodes defined in this document are writable/deletable (i.e., "config true") These data nodes may be considered sensitive or vulnerable in some network environments.

## 6. IANA Considerations

TDB

## 7. Acknowledgments

The authors would like to thank Italo Busi for his helpful comments and valuable contributions.

## 8. References

### 8.1. Normative References

### 8.2. Informative References

[RFC4847] T. Takeda (Editor), "Framework and Requirements for Layer 1 Virtual Private Networks", RFC 4847, April 2007.

[RFC5253] T. Takeda, "Applicability Statement for Layer 1 Virtual Private Network (L1VPN) Basic Mode", RFC 5253, July 2008.

[Service-Yang] Q. Wu, et al, "Service Models Explained", draft-wu-opsawg-service-model-explained, Work in progress.

## 9. Contributors

### Contributor's Addresses

I. Busi  
Huawei  
Email: Italo.Busi@huawei.com

### Authors' Addresses

G. Fioccola  
Telecom Italia  
Email: giuseppe.fioccola@telecomitalia.it

K. Lee  
KT  
Email: kwangkoog.lee@kt.com

Y. Lee  
Huawei  
Email: leeyoung@huawei.com

D. Dhody  
Huawei

Email: dhruv.ietf@gmail.com

O. Gonzalez de Dios

Telefonica

Email: oscar.gonzalezdedios@telefonica.com

D. Ceccarelli

Ericsson

Email: daniele.ceccarelli@ericsson.com



Internet Engineering Task Force  
Internet-Draft  
Intended status: Experimental  
Expires: May 3, 2018

D. Hiremagalur, Ed.  
G. Grammel, Ed.  
Juniper  
G. Galimberti, Ed.  
Cisco  
R. Kunze  
Deutsche Telekom  
October 30, 2017

Extension to the Link Management Protocol (LMP/DWDM -rfc4209) for Dense  
Wavelength Division Multiplexing (DWDM) Optical Line Systems to manage  
the application code of optical interface parameters in DWDM application  
draft-ggalimbe-ccamp-flex-if-lmp-03

#### Abstract

This experimental memo defines extensions to LMP(rfc4209) for  
managing Optical parameters associated with Wavelength Division  
Multiplexing (WDM) adding a set of parameters related to multicarrier  
DWDM interfaces to be used in Spectrum Switched Optical Networks  
(sson).

#### Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the  
document authors. All rights reserved.

#### 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 May 3, 2018.

## Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. DWDM line system . . . . .	3
3. Use Cases . . . . .	4
4. Extensions to LMP-WDM Protocol . . . . .	4
5. Multi carrier Transceiver . . . . .	5
6. Security Considerations . . . . .	6
7. IANA Considerations . . . . .	6
8. Contributors . . . . .	7
9. References . . . . .	7
9.1. Normative References . . . . .	7
9.2. Informative References . . . . .	8
Authors' Addresses . . . . .	9

## 1. Introduction

This experimental extension addresses the use cases described by "draft-ietf-ccamp-dwdm-if-mng-ctrl-fwk" to the Spectrum Switched Optical Network applications. LMP [RFC4902] provides link property correlation capabilities that can be used between a transceiver device and an Optical Line System (OLS) device. Link property correlation is a procedure by which, intrinsic parameters and capabilities are exchanged between two ends of a link. Link property correlation as defined in RFC3591 allows either end of the link to supervise the received signal and operate within a commonly understood parameter window. Here the term 'link' refers in particular to the attachment link between OXC and OLS (see Figure 1). The relevant novelty is the interface configuration having a multiple carrier where the client signal is spread on. The parameters are not yet fully defined by ITU-T so this document can just be seen as an experimental proposal not binding operators and vendors to comply and implement them





Figure 2 Extended LMP Model ( from [RFC4209] )

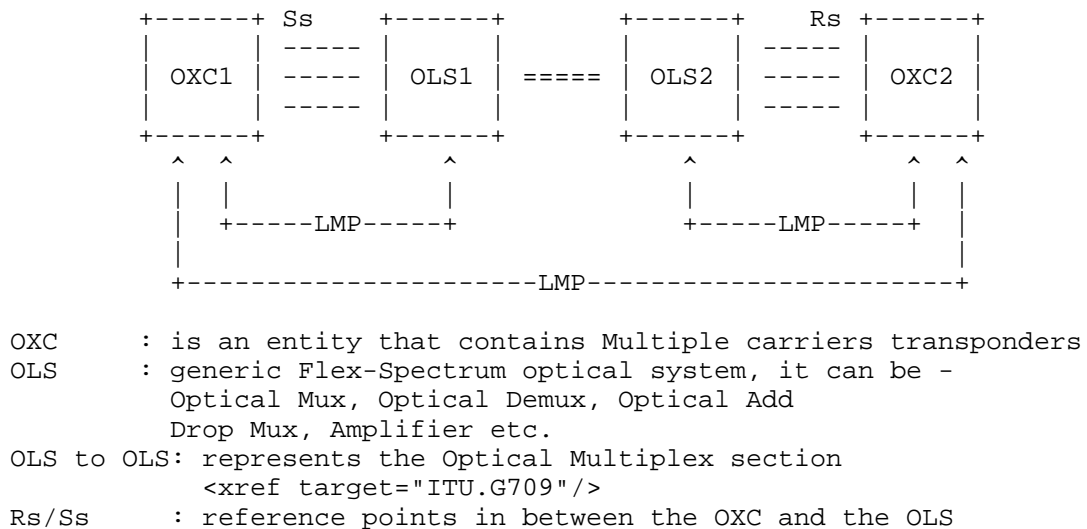


Figure 2: Extended LMP Model

### 3. Use Cases

The set of parameters exchanged between is to support the Spectrum Switched Optical Network in terms of Number of Sub-carriers available at the transceiver and their characteristics to provide the SSON control plane all the information suitable to calculate the path and the optical feasibility

### 4. Extensions to LMP-WDM Protocol

This document defines extensions to [RFC4209] to allow a set of characteristic parameters, to be exchanged between a router or optical switch and the optical line system to which it is attached. In particular, this document defines additional Data Link sub-objects to be carried in the LinkSummary message defined in [RFC4204] and [RFC6205]. The OXC and OLS systems may be managed by different Network management systems and hence may not know the capability and status of their peer. These messages and their usage are defined in subsequent sections of this document.

The following new messages are defined for the SSON extension

- Multi carrier Transceiver (sub-object Type = TBA)

## 5. Multi carrier Transceiver

These are a set of general parameters extending the description in [G698.2] and [G.694.1]. ITU-T working groups are working to detail most of parameters and an update of the TLV may be required.

The general parameters are

1. Modulation identifier: indicates the Transceiver capabilities to support a single or multiple modulation format like: BPSK (1), DC-DP-BSPSK, QPSK, DP-QPSK, QAM16, DP-QAM16, DC-DP-QAM16, 64QAM.
2. FEC: indicates the FEC types the transceiver can support
3. baud rate: number of symbols rate, basically this identify the channel frequency
4. Num Carriers: number of subcarriers the trasceiver can support and can be "mapped" in a Mediachannel
5. Bits/symbol: number of bit per simbol (aka spectral efficiency)
6. Subcarrier band (minimum distance between subcarriers) in GHz
7. Guard band (required guard band at the side of media channel)
8. Sub-carrier TX Power: output optical power the transceiver can provide
9. Sub-carrier RX Power: Input optical power Range the transceiver can support, this is known also as Sensitivity
10. Sub-carrier OSNR robustness

Figure 3: The format of the this sub-object (Type = TBA, Length = TBA) is as follows:

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Type										Length										(Reserved)																			
S		I		Modulation ID																FEC																			
baud rate										(Symbol Rate)																													
Number of subcarriers										Bit/Symbol																													
subcarrier band										guard band																													
sub-carrier TX power																																							
sub-carrier RX power HIGH																																							
sub-carrier RX power LOW																																							
Max-pol-power-difference																																							

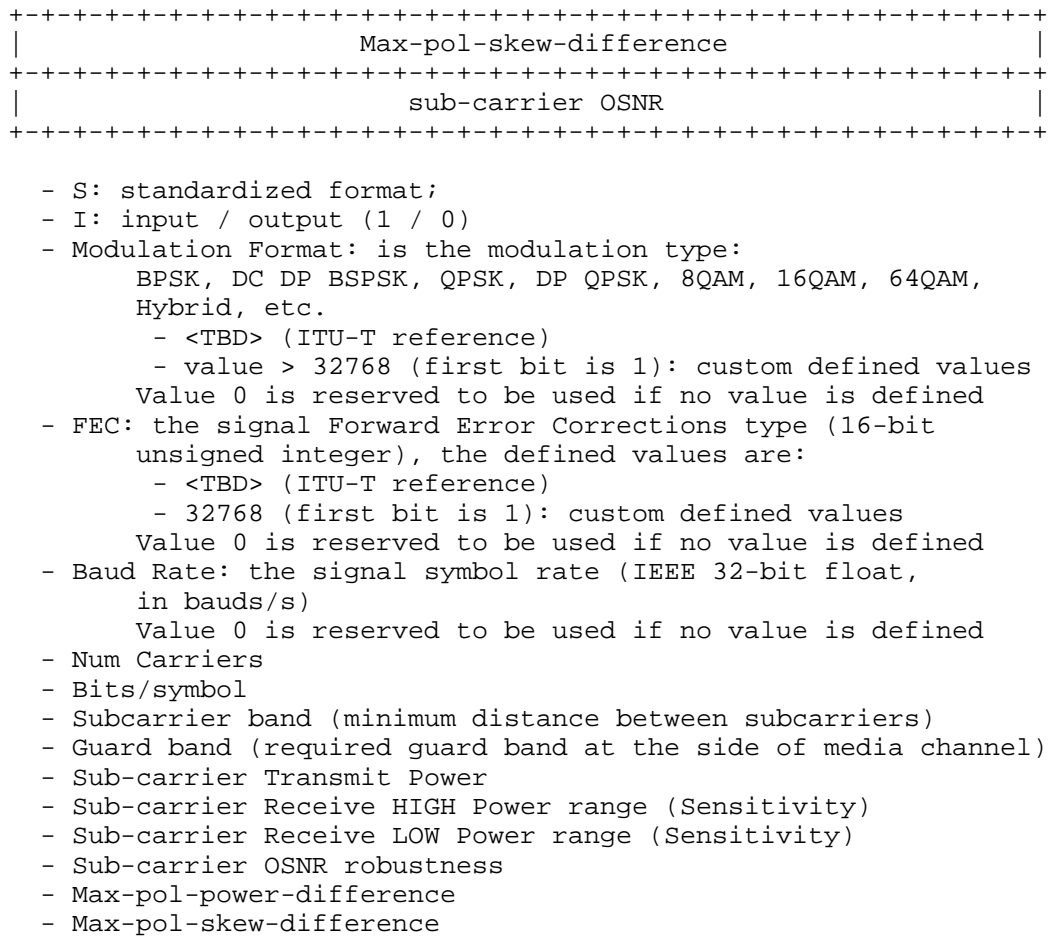


Figure 3: Multi carrier Transceiver

## 6. Security Considerations

LMP message security uses IPsec, as described in [RFC4204]. This document only defines new LMP objects that are carried in existing LMP messages, similar to the LMP objects in [RFC:4209]. This document does not introduce new security considerations.

## 7. IANA Considerations

LMP <xref target="RFC4204"/> defines the following name spaces and the ways in which IANA can make assignments to these namespaces:

- LMP Message Type
  - LMP Object Class
  - LMP Object Class type (C-Type) unique within the Object Class
  - LMP Sub-object Class type (Type) unique within the Object Class
- This memo introduces the following new assignments:

LMP Sub-Object Class names:

under DATA\_LINK Class name (as defined in <xref target="RFC4204"/>)

- Multi carrier Transceiver (sub-object Type = TBA)

## 8. Contributors

Zafar Ali  
Cisco  
3000 Innovation Drive  
KANATA  
ONTARIO K2K 3E8  
zali@cisco.com</email>

## 9. References

### 9.1. Normative References

- [I-D.ietf-ccamp-dwdm-if-mng-ctrl-fwk]  
Kunze, R., Grammel, G., Beller, D., Galimberti, G., and J. Meuric, "A framework for Management and Control of DWDM optical interface parameters", draft-ietf-ccamp-dwdm-if-mng-ctrl-fwk-07 (work in progress), September 2017.
- [ITU.G694.1]  
International Telecommunications Union, "Spectral grids for WDM applications: DWDM frequency grid", ITU-T Recommendation G.698.2, February 2012.
- [ITU.G698.2]  
International Telecommunications Union, "Amplified multichannel dense wavelength division multiplexing applications with single channel optical interfaces", ITU-T Recommendation G.698.2, November 2009.

- [ITU.G709] International Telecommunications Union, "Interface for the Optical Transport Network (OTN)", ITU-T Recommendation G.709, February 2012.
- [ITU.G872] International Telecommunications Union, "Architecture of optical transport networks", ITU-T Recommendation G.872, October 2012.
- [ITU.G874.1] International Telecommunications Union, "Optical transport network (OTN): Protocol-neutral management information model for the network element view", ITU-T Recommendation G.874.1, October 2012.
- [RFC4054] Strand, J., Ed. and A. Chiu, Ed., "Impairments and Other Constraints on Optical Layer Routing", RFC 4054, DOI 10.17487/RFC4054, May 2005, <<https://www.rfc-editor.org/info/rfc4054>>.
- [RFC4204] Lang, J., Ed., "Link Management Protocol (LMP)", RFC 4204, DOI 10.17487/RFC4204, October 2005, <<https://www.rfc-editor.org/info/rfc4204>>.
- [RFC4209] Fredette, A., Ed. and J. Lang, Ed., "Link Management Protocol (LMP) for Dense Wavelength Division Multiplexing (DWDM) Optical Line Systems", RFC 4209, DOI 10.17487/RFC4209, October 2005, <<https://www.rfc-editor.org/info/rfc4209>>.
- [RFC6205] Otani, T., Ed. and D. Li, Ed., "Generalized Labels for Lambda-Switch-Capable (LSC) Label Switching Routers", RFC 6205, DOI 10.17487/RFC6205, March 2011, <<https://www.rfc-editor.org/info/rfc6205>>.

## 9.2. Informative References

- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <<https://www.rfc-editor.org/info/rfc2629>>.
- [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, DOI 10.17487/RFC3410, December 2002, <<https://www.rfc-editor.org/info/rfc3410>>.

[RFC4181] Heard, C., Ed., "Guidelines for Authors and Reviewers of MIB Documents", BCP 111, RFC 4181, DOI 10.17487/RFC4181, September 2005, <<https://www.rfc-editor.org/info/rfc4181>>.

#### Authors' Addresses

Dharini Hiremagalur (editor)  
Juniper  
1194 N Mathilda Avenue  
Sunnyvale - 94089 California  
USA

Phone: +1408  
Email: dharinih@juniper.net

Gert Grammel (editor)  
Juniper  
Oskar-Schlemmer Str. 15  
80807 Muenchen  
Germany

Phone: +49 1725186386  
Email: ggrammel@juniper.net

Gabriele Galimberti (editor)  
Cisco  
Via S. Maria Molgora, 48 c  
20871 - Vimercate  
Italy

Phone: +390392091462  
Email: ggalimbe@cisco.com

Ruediger Kunze  
Deutsche Telekom  
Dddd, xx  
Berlin  
Germany

Phone: +49xxxxxxxxxxx  
Email: RKunze@telekom.de

Internet Engineering Task Force  
Internet-Draft  
Intended status: Experimental  
Expires: May 3, 2018

G. Galimberti, Ed.  
D. La Fauci  
Cisco  
A. Zanardi, Ed.  
L. Galvagni  
FBK-CreateNet  
October 30, 2017

Signaling extensions for Media Channel sub-carriers configuration in  
Spectrum Switched Optical Networks (SSON) in Lambda Switch Capable (LSC)  
Optical Line Systems.  
draft-ggalimbe-ccamp-flexigrid-carrier-label-02

#### Abstract

This memo defines the signaling extensions for managing Spectrum Switched Optical Network (SSON) parameters shared between the Client and the Network and inside the Network in accordance to the model described in RFC 7698. The extensions are in accordance and extending the parameters defined in ITU-T Recommendation G.694.1.[ITU.G694.1] and its extensions and G.872.[ITU.G872].

#### Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

#### 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 May 3, 2018.

## Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Client interface parameters . . . . .	3
3. Use Cases . . . . .	5
4. Signalling Extensions . . . . .	5
4.1. New LSP set-up parameters . . . . .	5
4.2. Extension to LSP set-up reservation . . . . .	7
4.3. RSVP Protocol Extensions considerations . . . . .	13
5. Security Considerations . . . . .	14
6. IANA Considerations . . . . .	14
7. Contributors . . . . .	14
8. References . . . . .	14
8.1. Normative References . . . . .	14
8.2. Informative References . . . . .	16
Authors' Addresses . . . . .	16

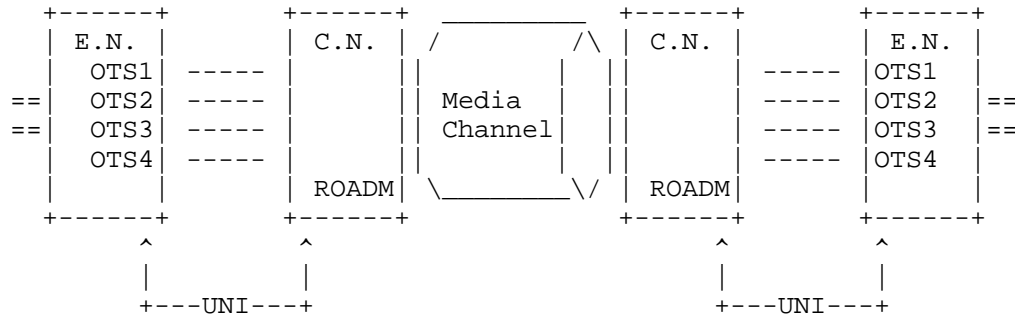
## 1. Introduction

Generalised Multiprotocol Label Switched (GMPLS) is widely used in Wavelength Switched Optical Network (WSO) to support the optical circuits set-up through the signalling between Core Nodes and Edge Nodes. This extension addresses the use cases described by [RFC7698] Ch.3.3 and supports the information, needed in Spectrum Switched Optical Network (SSO), to signal a Media Channel and the associated carriers set request. The new set of parameters is related to the Media Channel and the carrier(s) routed with it and keep the backward compatibility with the WSO signalling. In particular this memo wants do address the use cases where the SSO LSP (the Media Channel in RFC7698) carries multiple carrier (OTSi) containing same Payload. The set of the carriers can be seen as single Logical circuit. This memo can be considered as the extension of [RFC7792]. The contents



and the parameters reflect the experimental activity on IP over SSON recently done by some vendors and research consortia.

Figure 1 shows how the multiple carrier are mapped into a Media Channel. A set of parameters must be shared on the UNI to allow the GMPLS to do the proper routing and Spectrum Assignment and decide the carrier position.



E.N. = Edge Node - UNI Client  
 C.N. = Core Node - UNI Network  
 ROADM = Lambda/Spectrum switch  
 Media Channel = the optical circuit  
 OTSi = Carriers belonging to the same Network Media Channel (or Super Channel)  
 UNI = Signalig interface

from Fig. 5.1/G.698.2

Figure 1: Multi carrier LSP

## 2. Client interface parameters

The Edge Node interface can have one or multiple carriers (OTSi). All the carrier have the same characteristics and are provisionable in terms of:

Number of subcarriers:

This parameter indicates the number of subcarriers available for the super-channel in case the Transceiver can support multiple carrier circuits.

Central frequency (see G.694.1 Table 1):

This parameter indicates the Central frequency value that Ss and Rs will be set to work (in THz). See the details in Section 6/ G.694.1 or based on "n" value explanation and the following "k" values definition in case of multicarrier transceivers.

Central frequency granularity:

This parameter indicates the Central frequency granularity supported by the transceiver, this value is combined with k and n value to calculate the central frequency of the carrier or sub-carriers.

Minimum channel spacing:

This is the minimum nominal difference in frequency (in GHz) between two adjacent channels (or carriers) depending on the Transceiver characteristics.

Bit rate / Baud rate of optical tributary signals:

Optical Tributary Signal bit (for NRZ signals) rate or Symbol (for Multiple bit per symbol) rate .

FEC Coding:

This parameter indicate what Forward Error Correction (FEC) code is used at Ss and Rs (R/W) (not mentioned in G.698.2). .

Wavelength Range (see G.694.1): [ITU.G694.1]

This parameter indicate minimum and maximum wavelength spectrum in a definite wavelength Band (L, C and S).

Modulation format:

This parameter indicates the list of supported Modulation Formats and the provisioned Modulation Format..

Inter carrier skew:

This parameter indicates, in case of multi-carrier transceivers the maximum skew between the sub-carriers supported by the transceiver.

Laser Output power:

This parameter provisions the Transceiver Output power, it can be either a setting and measured value.

receiver input power:

This parameter provisions the Min and MAX input power supported by the Transceiver, i.e. Receiver Sensitivity.

The above parameters are related to the Edge Node Transceiver and are used by the Core Network GMPLS in order to calculate the optical feasibility and the spectrum allocation. The parameters can be

shared between the Client and the Network via LMP or provisioned in the Network by an EMS or an operator OSS.

### 3. Use Cases

The use cases are described in draft-ietf-ccamp-dwdm-if-mng-ctrl-fwk and [RFC7698]

### 4. Signalling Extensions

Some of the above parameters can be applied to RFC7792 (SENDER\_TSPEC/FLOWSPEC). The above parameters could be applied to [RFC4208] scenarios but they are valid also in case of non UNI scenarios. The [RFC6205] parameters remain valid.

#### 4.1. New LSP set-up parameters

When the E.N. wants to request to the C.N. a new circuit set-up request or the GMPLS want to signal in the SSON network the Optical Interface characteristics the following parameters will be provided to the C.N.:

Number of available subcarriers (c):  
This parameter is an integer.

Total bandwidth request:  
e.g. 200Gb, 400Gb, 1Tb

Policy (strict/loose):  
Strict/loose referred to B/W and subcarrier number.

Subcarrier bandwidth tunability:  
(optional) e.g. 34Ghz, 48GHz.

Figure 2: The format of the this sub-object is as follows:

The TLV define the resource constraints for the requested Media Channel.

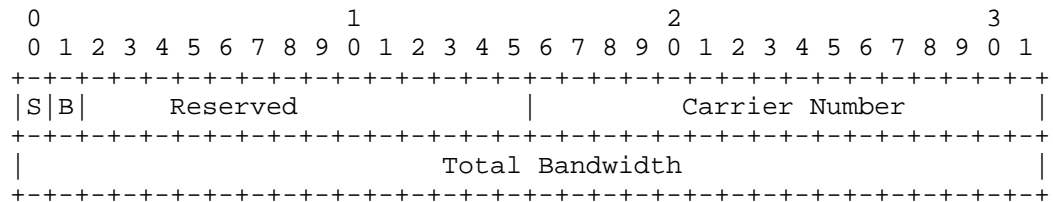


Figure 2: SSON LSP set-up request

Carrier Number: number of carrier to be allocated for the requested channel (16-bit unsigned integer)

If Carrier Number == 0 no constraint set on the number of carriers to be used

S strict number of subcarrier

- S = 0 the number of requested carriers is the maximum number that can be allocated (a lower value can be allocated if the requested bandwidth is satisfied)
- S = 1 the number of requested carriers is strict (must be > 0)

Total Bandwidth: the requested total bandwidth to be supported by the Media Channel (32-bit IEEE float, bytes/s)

If Total Bandwidth == 0: no bandwidth constraint is defined (B must be 0)

B Bandwidth constraints

- B = 0: the value is the maximum requested bandwidth (a lower value can be allocated if resources are not available)
- B = 1: the requested bandwidth is the minimum value to be allocated (a higher value can be allocated if requested by the physical constraints of the ports)

Reserved: unused bit (for future use, should be 0)

Note: bandwidth unit is defined in accordance to RFC 3471

chap. 3.1.2 Bandwidth Encoding specification. Bandwidth higher than 40Gb/s values must be defined (e.g. 100Gb/s, 150Gb/s, 400Gb/s, etc.)

TLV Usage:

Head UNI-C PATH: requested traffic constraints, the Head UNI-N node must satisfy when reserving the optical resources and defining the carriers configuration

The TLV can be omitted: no traffic constraints is defined (resources allocated by UNI-N based on a local policy)

#### 4.2. Extension to LSP set-up reservation

Once the GMPLS has calculated the Media Channel path, the Spectrum Allocation, the Sub-carrier number and frequency, the modulation format, the FEC and the Transmit power, sends back to the E.N. the path set-up confirmation providing the values of the calculated parameters:

Media Channel:

(Grid, C.S., Identifier m and n).

List of subcarriers:

This parameter indicates the subcarriers to be used for the super-channel in case the Transceiver can support multiple carrier Circuits.

Central frequency (see G.694.1 Table 1):

Grid, Identifiers, central frequency and granularity.

Central frequency granularity:

This parameter indicates the Central frequency granularity supported by the transceiver, this value is combined with K and n value to calculate the central frequency on the carrier or sub-carriers.

Bit rate / Baud rate of optical tributary signals:

Optical tributary signal bit (for NRZ signals) rate or Symbol (for Multiple bit per symbol) rate.

FEC Coding:

This parameter indicate what Forward Error Correction (FEC) code must be used by the Transceivers (not mentioned in G.698). .

Modulation format:

This parameter indicates the Modulation Formats to be set in the Transceivers.

Laser Output power:

This parameter provisions the Transceiver Output power, it can be either a setting and measured value.

Circuit Path, RRO, etc:

All these info are defined in [RFC4208].

Path Error:

e.g. no path exist, all the path error defined in [RFC4208].

Figure 3: The format of this sub-object (Type = TBA, Length = TBA) is as follows:

The TLV defines the carriers signal configuration.  
All carriers in a Media Channel MUST have the same configuration.

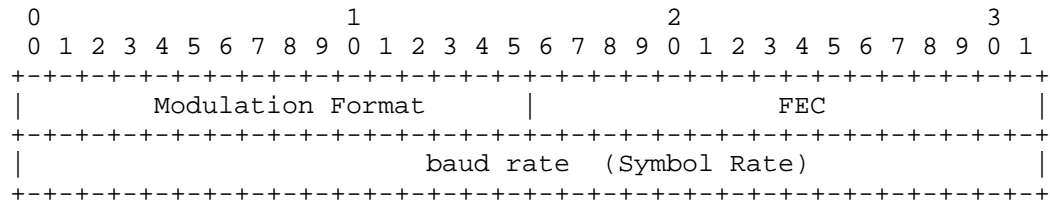


Figure 3: OCh\_General

#### Traffic Type

- Modulation Format: is the modulation type:
  - BPSK, DC DP BPSK, QPSK, DP QPSK, 8QAM, 16QAM, 64QAM, Hybrid, etc.
  - <TBD> (ITU-T reference)
  - value > 32768 (first bit is 1): custom defined values
  - Value 0 is reserved to be used if no value is defined
- FEC: the signal Forward Error Corrections type (16-bit unsigned integer), the defined values are:
  - <TBD> (ITU-T reference)
  - 32768 (first bit is 1): custom defined values
  - Value 0 is reserved to be used if no value is defined
- Baud Rate: the signal symbol rate (IEEE 32-bit float, in bauds/s)
  - Value 0 is reserved to be used if no value is defined

#### Notes:

- The request from the Head UNI-C node can specify only a subset of the parameters (e.g. the Modulation and the baud rate but not the FEC) but setting to 0 the undefined parameters.
- Custom codes (values > 0x8000) interpretation is a local installation matter.

#### TLV Usage:

- Head UNI-C PATH: used to force specific transponder configurations
- Head UNI-N RESV: set selected configuration on head node
- Tail UNI-N PATH: set selected configuration on tail node

Figure 4: The format of this sub-object (Type = TBA, Length = TBA) is as follows:

For Each carrier inside the Media Channel the TLV is used:

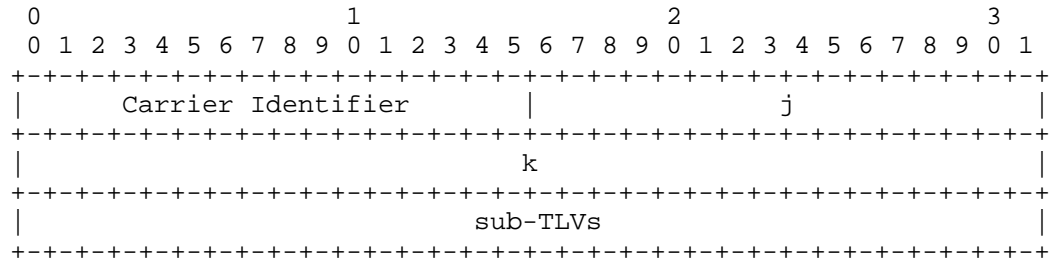


Figure 4: Sub-Carrier parameters



# Carrier set-up:

- Carrier identifier field: sub-carrier identifier inside the mediachannel. Identifies the carrier position inside the Media Channel (16-bit unsigned integer)
- J field: granularity of the channel spacing, can be a multiple of 0.01GHz. - default value is 0.1GHz.
- K field: positive or negative integer (including 0) to multiply by J and identify the Carrier Position inside the Media Channel, offset from media Channel Central frequency
- sub-TLVs: additional information related to carriers if needed.

In summary Carrier Frequency = MC-C.F. (in THz) + K \* J GHz

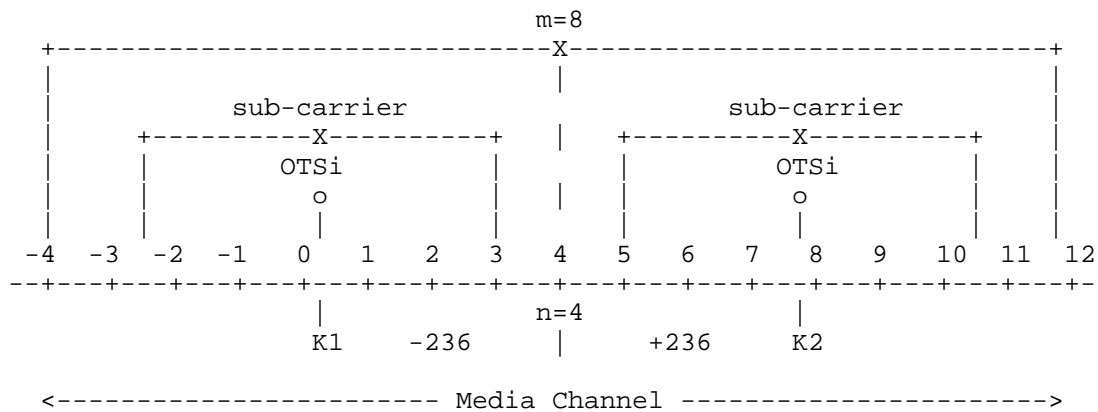


Figure 5: The format of this sub-object (Type = TBA, Length = TBD) is as follows:

The defined sub-TLVs are:

Port Identifier

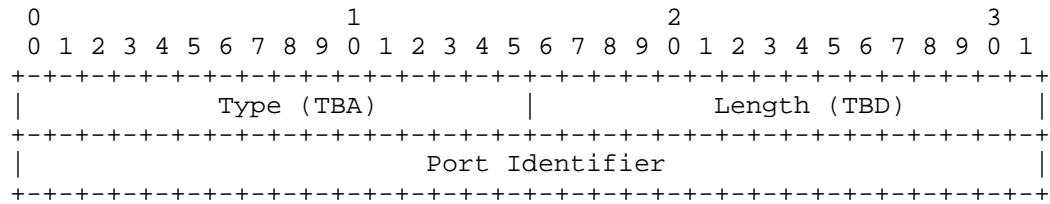


Figure 5: Port Identifier

Port Identifier: the local upstream optical logical identifier  
(32-bits integer, ifindex)

Notes:

- The Carrier Identifier is the logical circuit sub-lane position, a TLV for each value from 1 to the number of allocated carriers must be present.
- The association of a carrier to a local link optical port is a local link association (depending on the local ports physical configuration), the sub-TLV value MUST be set by head/tail nodes (with transit nodes not signaling its value).  
The local port identifier is the identifier of the local link port on the upstream node (with respect to the LSP nominal direction):
  - UNI-C port in head UNI link
  - UNI-N port in tail UNI link

TLV Usage:

- Head UNI-C PATH: used to force specific carrier frequency/ports [optional use, e.g. with external PCE scenario]
- Head UNI-N RESV: set selected configuration on head node
- Tail UNI-N PATH: set selected configuration on tail node

Figure 6: The format of this sub-object (Type = TBA, Length = TBD) is as follows:

Carrier Power:

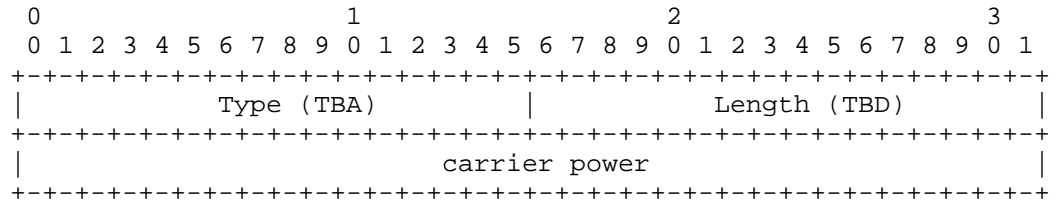


Figure 6: Carrier Power

Carrier Port: the requested carrier transmit power (32-bits IEEE Float, dBm), optionally used to notify the configured power (in UNI client side) or force the power to the to the UNI client).

TLV Usage:

- Head UNI-C PATH: used to force specific carrier frequency/ports (optional use, e.g. with external PCE scenario)
- Head UNI-N RESV: set selected configuration on head node
- Tail UNI-N PATH: set selected configuration on tail node

#### 4.3. RSVP Protocol Extensions considerations

The additional information described in the draft, is related to the Media Channel supported traffic. It could be encoded in the SENDER\_TSPEC/FLOW\_SPEC objects by extending the SSON\_SENDER\_TSPEC/SSON\_FLOW\_SPEC defined in RFC 7792 (or defining a new C-Type) with an optional TLV list or it could be encoded in a newly defined entry (new OBJECT or new LSP\_ATTRIBUTES OBJECT TLV)

This solution is consistent with other technology specific extensions (e.g. SDH), but requires the explicit handling of the extensions by all nodes.

Beside this, some of the additional information defined is local to the head/tail UNI link (e.g. the carrier/port association), while the traffic spec info should be valid end-to-end.

## 5. Security Considerations

GMPLS message security uses IPsec, as described in xxxx. This document only defines new UNI objects that are carried in existing UNI messages, similar to the UNI objects in xxx. This document does not introduce new security considerations.

## 6. IANA Considerations

T.B.D.

## 7. Contributors

Antonello Bonfanti  
Cisco  
Via Santa Maria Molgora, 48 c  
20871 - Vimercate (MB)  
Italy  
abonfant@cisco.com</email>

## 8. References

### 8.1. Normative References

- [ITU.G694.1]  
International Telecommunications Union, "Spectral grids for WDM applications: DWDM frequency grid", ITU-T Recommendation G.698.2, February 2012.
- [ITU.G698.2]  
International Telecommunications Union, "Amplified multichannel dense wavelength division multiplexing applications with single channel optical interfaces", ITU-T Recommendation G.698.2, November 2009.
- [ITU.G709]  
International Telecommunications Union, "Interface for the Optical Transport Network (OTN)", ITU-T Recommendation G.709, February 2012.
- [ITU.G872]  
International Telecommunications Union, "Architecture of optical transport networks", ITU-T Recommendation G.872, October 2012.

- [ITU.G874.1] International Telecommunications Union, "Optical transport network (OTN): Protocol-neutral management information model for the network element view", ITU-T Recommendation G.874.1, October 2012.
- [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>>.
- [RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, DOI 10.17487/RFC3473, January 2003, <<https://www.rfc-editor.org/info/rfc3473>>.
- [RFC3945] Mannie, E., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, DOI 10.17487/RFC3945, October 2004, <<https://www.rfc-editor.org/info/rfc3945>>.
- [RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and Y. Rekhter, "Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, DOI 10.17487/RFC4208, October 2005, <<https://www.rfc-editor.org/info/rfc4208>>.
- [RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS Networks", RFC 5920, DOI 10.17487/RFC5920, July 2010, <<https://www.rfc-editor.org/info/rfc5920>>.
- [RFC6163] Lee, Y., Ed., Bernstein, G., Ed., and W. Imajuku, "Framework for GMPLS and Path Computation Element (PCE) Control of Wavelength Switched Optical Networks (WSONs)", RFC 6163, DOI 10.17487/RFC6163, April 2011, <<https://www.rfc-editor.org/info/rfc6163>>.
- [RFC6205] Otani, T., Ed. and D. Li, Ed., "Generalized Labels for Lambda-Switch-Capable (LSC) Label Switching Routers", RFC 6205, DOI 10.17487/RFC6205, March 2011, <<https://www.rfc-editor.org/info/rfc6205>>.

- [RFC7698] Gonzalez de Dios, O., Ed., Casellas, R., Ed., Zhang, F., Fu, X., Ceccarelli, D., and I. Hussain, "Framework and Requirements for GMPLS-Based Control of Flexi-Grid Dense Wavelength Division Multiplexing (DWDM) Networks", RFC 7698, DOI 10.17487/RFC7698, November 2015, <<https://www.rfc-editor.org/info/rfc7698>>.
- [RFC7699] Farrel, A., King, D., Li, Y., and F. Zhang, "Generalized Labels for the Flexi-Grid in Lambda Switch Capable (LSC) Label Switching Routers", RFC 7699, DOI 10.17487/RFC7699, November 2015, <<https://www.rfc-editor.org/info/rfc7699>>.
- [RFC7792] Zhang, F., Zhang, X., Farrel, A., Gonzalez de Dios, O., and D. Ceccarelli, "RSVP-TE Signaling Extensions in Support of Flexi-Grid Dense Wavelength Division Multiplexing (DWDM) Networks", RFC 7792, DOI 10.17487/RFC7792, March 2016, <<https://www.rfc-editor.org/info/rfc7792>>.

## 8.2. Informative References

- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <<https://www.rfc-editor.org/info/rfc2629>>.
- [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, DOI 10.17487/RFC3410, December 2002, <<https://www.rfc-editor.org/info/rfc3410>>.
- [RFC4181] Heard, C., Ed., "Guidelines for Authors and Reviewers of MIB Documents", BCP 111, RFC 4181, DOI 10.17487/RFC4181, September 2005, <<https://www.rfc-editor.org/info/rfc4181>>.

## Authors' Addresses

Gabriele Galimberti (editor)  
Cisco  
Via S. Maria Molgora, 48 c  
20871 - Vimercate  
Italy

Phone: +390392091462  
Email: ggalimbe@cisco.com

Domenico La Fauci  
Cisco  
Via S. Maria Molgora, 48 c  
20871 - Vimercate  
Italy

Phone: +390392091946  
Email: dlafauci@cisco.com

Andrea Zanardi (editor)  
FBK-CreateNet  
via alla Cascata 56/D  
38123 Povo, Trento  
Italy

Phone: +390461312450  
Email: azanardi@fbk.eu

Lorenzo Galvagni  
FBK-CreateNet  
via alla Cascata 56/D  
38123 Povo, Trento  
Italy

Phone: +390461312427  
Email: lgalvagni@fbk.eu

CCAMP WG  
Internet-Draft  
Intended status: Informational  
Expires: April 23, 2018

J. Ahlberg  
Ericsson AB  
LM. Contreras  
TID  
M.Ye  
Huawei Technologies CO., Ltd  
M. Vaupotic  
Aviat Networks  
J. Tantsura  
Individual  
K. Kawada  
NEC Corporation  
X. Li  
NEC Laboratories Europe  
I. Akiyoshi  
NEC  
CJ. Bernardos  
UC3M  
D. Spreafico  
Nokia - IT  
October 20, 2017

A framework for Management and Control of microwave and  
millimeter wave interface parameters  
draft-ietf-ccamp-microwave-framework-02

Abstract

To ensure an efficient data transport, meeting the requirements requested by today's transport services, the unification of control and management of microwave and millimeter wave radio link interfaces is a precondition for seamless multilayer networking and automated network wide provisioning and operation.

This document describes the required characteristics and use cases for control and management of radio link interface parameters using a YANG Data Model. It focuses on the benefits of a standardized management model that is aligned with how other packet technology interfaces in a microwave/millimeter wave node are modeled, the need to support core parameters and at the same time allow for optional product/feature specific parameters supporting new, unique innovative features until they have become mature enough to be included in the standardized model.

The purpose is to create a framework for identification of the necessary information elements and definition of a YANG Data Model for control and management of the radio link interfaces in a microwave/millimeter wave node. Some part of the resulting model MAY be generic which COULD also be used by other technology.



#### 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 <http://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 April 23, 2018.

#### Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

# Table of Contents

1. Terminology and Definitions . . . . .	4
2. Introduction . . . . .	5
3. Conventions used in this document . . . . .	7
4. Approaches to manage and control radio link interfaces . . . . .	8
4.1. Network Management Solutions . . . . .	8
4.2. Software Defined Networking . . . . .	8
5. Use Cases . . . . .	9
5.1. Configuration Management . . . . .	9
5.1.1. Understand the capabilities & limitations . . . . .	10
5.1.2. Initial Configuration . . . . .	10
5.1.3. Radio link re-configuration & optimization . . . . .	10
5.1.4. Radio link logical configuration . . . . .	10
5.2. Inventory . . . . .	10
5.2.1. Retrieve logical inventory & configuration from device . . . . .	10
5.2.2. Retrieve physical/equipment inventory from device . . . . .	11
5.3. Status & statistics . . . . .	11
5.3.1. Actual status & performance of a radio link interface . . . . .	11
5.4. Performance management . . . . .	11
5.4.1. Configuration of historical measurements to be performed . . . . .	11
5.4.2. Collection of historical performance data . . . . .	11
5.5. Fault Management . . . . .	11
5.5.1. Configuration of alarm reporting . . . . .	11
5.5.2. Alarm management . . . . .	11
5.6. Troubleshooting and Root Cause Analysis . . . . .	11
6. Requirements . . . . .	12
7. Gap Analysis on Models . . . . .	13
7.1. Microwave Radio Link Functionality . . . . .	13
7.2. Generic Functionality . . . . .	14
7.3. Summary . . . . .	16
8. Security Considerations . . . . .	16
9. IANA Considerations . . . . .	16
10. References . . . . .	17
10.1. Normative References . . . . .	17
10.2. Informative References . . . . .	17
Authors' Addresses . . . . .	18

## 1. Terminology and Definitions

Microwave is a band of spectrum with wavelengths ranging from 1 meter to 1 millimeter and with frequencies ranging between 300 MHz and 300 GHz. Microwave radio technology is widely used for point-to-point telecommunications because of their small wavelength that allows conveniently-sized antennas to direct them in narrow beams, and their comparatively higher frequencies that allows broad bandwidth and high data transmission rates.

Millimeter wave is also known as extremely high frequency (EHF) or very high frequency (VHF) by the International Telecommunications Union (ITU), which can be used for high-speed wireless broadband communications. Millimeter wave can be used for a broad range of fixed and mobile services including high-speed, point-to-point wireless local area networks (WLANs) and broadband access. This band has short wavelengths that range from 10 millimeters to 1 millimeter, namely millimeter band or millimeter wave. The 71 - 76 GHz, 81 - 86 GHz and 92-95 GHz bands are used for point-to-point high-bandwidth communication links, which allows for higher data rates up to 10 Gbit/s but requires a license. Unlicensed short-range data links can be used on 60 GHz millimeter wave. For instance, the upcoming IEEE Wi-Fi standard 802.11ad will run on the 60 GHz spectrum with data transfer rates of up to 7 Gbit/s.

ETSI EN 302 217 series defines the characteristics and requirements of microwave/millimeter wave equipment and antennas. Especially ETSI EN 302 217-2 specifies the essential parameters for the systems operating from 1.4GHz to 86GHz.

Carrier Termination and Radio Link Terminal are two concepts defined to support modeling of microwave radio link features and parameters in a structured and yet simple manner.

Carrier Termination is an interface for the capacity provided over the air by a single carrier. It is typically defined by its transmitting and receiving frequencies.

Radio Link Terminal is an interface providing packet capacity and/or TDM capacity to the associated Ethernet and/or TDM interfaces in a node and used for setting up a transport service over a microwave/millimeter wave link.

Figure 1 provides a graphical representation of Carrier Termination and Radio Link Terminal concepts.

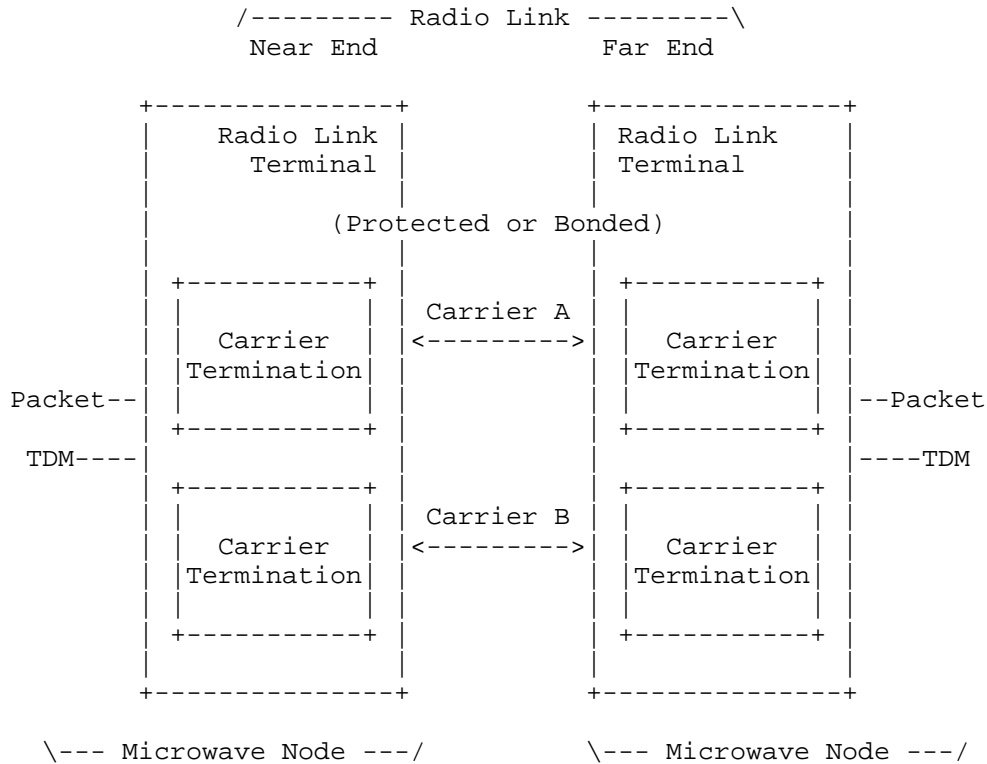


Figure 1. Radio Link Terminal and Carrier Termination

Software Defined Networking (SDN) is an emerging architecture that decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. This results in an extremely dynamic, manageable, cost-effective, and adaptable architecture that gives administrators unprecedented programmability, automation, and control. The SDN concept is widely applied for network management, the adoption of SDN framework to manage and control the microwave and millimeter wave interface is one of the key applications of this work.

## 2. Introduction

Network requirements vary between operators globally as well as within individual countries. The overall goal is however the same - to deliver the best possible network performance and quality of experience in a cost-efficient way.

Microwave/millimeter wave (hereafter referred to as microwave, but including the frequency bands represented by millimeter wave) are important technologies to fulfill this goal today, but also in the future when demands on capacity and packet features increases.

Microwave is already today able to fully support the capacity needs of a backhaul in a radio access network and will evolve to support multiple gigabits in traditional frequency bands and beyond 10 gigabits in the millimeter wave. L2 packet features are normally an integrated part of microwave nodes and more advanced L2 & L3 features will over time be introduced to support the evolution of the transport services to be provided by a backhaul/transport network. Note that the wireless access technologies such as 3/4/5G & WiFi are not within the scope of this microwave model work.

The main application for microwave is backhaul for mobile broadband. Those networks will continue to be modernized using a combination of microwave and fiber technologies. The choice of technology is a question about fiber presence and cost of ownership, not about capacity limitations in microwave.

Open and standardized interfaces are a pre-requisite for efficient management of equipment from multiple vendors, integrated in a single system/controller. This framework addresses management and control of the radio link interface(s) and the relationship to other packet interfaces, typically to Ethernet interfaces, in a microwave node. A radio link provides the transport over the air, using one or several carriers in aggregated or protected configurations. Managing and controlling a transport service over a microwave node involves both radio link and packet functionality.

Already today there are numerous IETF data models, RFCs and drafts, with technology specific extensions that cover a large part of the packet domain. Examples are IP Management [RFC7277], Routing Management [RFC8022] and Provider Bridge [PB-YANG] They are based on RFC 7223 [RFC7223], which is the IETF YANG model for Interface Management, and is an evolution of the SNMP IF-MIB [RFC2863].

Since microwave nodes will contain more and more packet functionality which is expected to be managed using those models, there are advantages if radio link interfaces can be modeled and be managed using the same structure and the same approach, specifically for use cases in which a microwave node are managed as one common entity including both the radio link and the packet functionality, e.g. at basic configuration of node & connections, centralized trouble shooting, upgrade and maintenance. All interfaces in a node, irrespective of technology, would then be accessed from the same core model, i.e. RFC 7223, and could be extended with technology specific parameters in models augmenting that core model. The relationship/connectivity between interfaces could be given by the physical equipment configuration, e.g the slot in which the Radio Link Terminal (modem) is plugged in could be associated with a specific Ethernet port due to the wiring in the backplane of the system, or it could be flexible and therefore configured via a management system or controller.

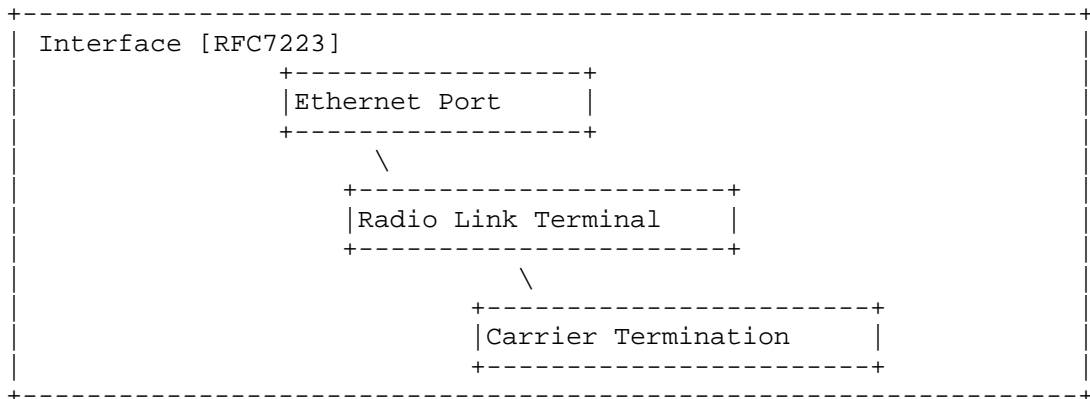


Figure 2: Relationship between interfaces in a node

There will always be certain implementations that differ among products and it is therefore practically impossible to achieve industry consensus on every design detail. It is therefore important to focus on the parameters that are required to support the use cases applicable for centralized, unified, multi-vendor management and to allow other parameters to be optional or to be covered by extensions to the standardized model. Furthermore, a standard that allows for a certain degree of freedom encourages innovation and competition which is something that benefits the entire industry. It is therefore important that a radio link management model covers all relevant functions but also leaves room for product/feature-specific extensions.

For microwave radio link functionality work has been initiated (ONF: Microwave Modeling [ONF-model], IETF: Radio Link Model [I-D.ahlbergccamp-microwave-radio-link]). The purpose of this effort is to reach consensus within the industry around one common approach, with respect to the use cases and requirements to be supported, the type and structure of the model and the resulting attributes to be included. This document describes the use cases and requirements agreed to be covered, the expected characteristics of the model and at the end includes an analysis of how the models in the two ongoing initiatives fulfill these expectations and a recommendation on what can be reused and what gaps need to be filled by a new and evolved radio link model.

### 3. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

While [RFC2119] describes interpretations of these key words in terms of protocol specifications and implementations, they are used in this document to describe requirements for the YANG Data Model for Microwave Radio Link.

#### 4. Approaches to manage and control radio link interfaces

This framework addresses the definition of an open and standardized interface for the radio link functionality in a microwave/millimeter wave node. The application of such an interface used for management and control of nodes and networks typically vary from one operator to another, in terms of the systems used and how they interact. A traditional solution is network management system, while an emerging one is SDN. SDN solutions can be used as part of the network management system, allowing for direct network programmability and automated configurability by means of a centralized SDN control and defining standardized interfaces to program the nodes.

##### 4.1. Network Management Solutions

The classic network management solutions, with vendor specific domain management combined with cross domain functionality for service management and analytics, still dominates the market. These solutions are expected to evolve and benefit from an increased focus on standardization by simplifying multi-vendor management and remove the need for vendor/domain specific management.

##### 4.2. Software Defined Networking

One of the main drivers for applying SDN from an operator perspective is simplification and automation of network provisioning as well as E2E network service management. The vision is to have a global view of the network conditions spanning across different vendors' equipment and multiple technologies.

If nodes from different vendors shall be managed by the same SDN controller via a node management interface (north bound interface, NBI), without the extra effort of introducing intermediate systems, all nodes must align their node management interfaces. Hence, an open and standardized node management interface are required in a multi-vendor environment. Such standardized interface enables a unified management and configuration of nodes from different vendors by a common set of applications.

On top of SDN applications to configure, manage and control the nodes and their associated transport interfaces including the L2 and L3 packet/Ethernet interfaces as well as the radio interfaces, there are also a large variety of other more advanced SDN applications that can be exploited and/or developed.

A potential flexible approach for the operators is to use SDN in a logical control way to manage the radio links by selecting a predefined operation mode. The operation mode is a set of logical metrics or parameters describing a complete radio link configuration, such as capacity, availability, priority and power consumption.

An example of an operation mode table is shown in Figure 3. Based on its operation policy (e.g., power consumption or traffic priority), the SDN controller selects one operation mode and translates that into the required configuration of the individual parameters for the radio link terminals and the associated carrier terminations.

ID	Description	Capacity	Availability	Priority	Power
1	High capacity	400 Mbps	99.9%	Low	High
2	High availability	100 Mbps	99.999%	High	Low

Figure 3. Example of an operation mode table

An operation mode bundles together the values of a set of different parameters. How each operation mode maps into certain set of attributes is out of scope of this document. Effort on a standardizing operation mode is required to implement a smoothly operator environment.

## 5. Use Cases

The use cases described should be the basis for identification and definition of the parameters to be supported by a YANG Data model for management of radio links, applicable for centralized, unified, multi-vendor management.

Other product specific use cases, addressing e.g. installation, on-site trouble shooting and fault resolution, are outside the scope of this framework. If required, these use cases are expected to be supported by product specific extensions to the standardized model.

### 5.1. Configuration Management

Configuration of a radio link terminal, the constituent carrier terminations and when applicable the relationship to packet/Ethernet and TDM interfaces.



#### 5.1.1.1. Understand the capabilities & limitations

Exchange of information between a manager and a device about the capabilities supported and specific limitations in the parameter values & enumerations that can be used.

Support for the XPIC (Cross Polarization Interference Cancellation) feature or not and the maximum modulation supported are two examples on information that could be exchanged.

#### 5.1.1.2. Initial Configuration

Initial configuration of a radio link terminal, enough to establish L1 connectivity over the hop to an associated radio link terminal on a device at far end. It MAY also include configuration of the relationship between a radio link terminal and an associated traffic interface, e.g. an Ethernet interface, unless that is given by the equipment configuration.

Frequency, modulation, coding and output power are examples of parameters typically configured for a carrier termination and type of aggregation/bonding or protection configurations expected for a radio link terminal.

#### 5.1.1.3. Radio link re-configuration & optimization

Re-configuration, update or optimization of an existing radio link terminal. Output power and modulation for a carrier termination and protection schemas and activation/de-activation of carriers in a radio link terminal are examples on parameters that can be re-configured and used for optimization of the performance of a network.

#### 5.1.1.4. Radio link logical configuration

Radio link terminals comprising a group of carriers are widely used in microwave technology. There are several kinds of groups: aggregation/bonding, 1+1 protection/redundancy, etc. To avoid configuration on each carrier termination directly, a logical control provides flexible management by mapping a logical configuration to a set of physical attributes. This could also be applied in a hierarchical SDN environment where some domain controllers are located between the SDN controller and the radio link terminal.

### 5.2. Inventory

#### 5.2.1. Retrieve logical inventory & configuration from device

Request from manager and response by device with information about radio interfaces, their constitution and configuration.

#### 5.2.2. Retrieve physical/equipment inventory from device

Request from manager about physical and/or equipment inventory associated with the radio link terminals and carrier terminations.

#### 5.3. Status & statistics

##### 5.3.1. Actual status & performance of a radio link interface

Manager requests and device responds with information about actual status and statistics of configured radio link interfaces and their constituent parts.

#### 5.4. Performance management

##### 5.4.1. Configuration of historical measurements to be performed

Configuration of historical measurements to be performed on a radio link interface and/or its constituent parts is a subset of the configuration use case to be supported. See 5.1 above.

##### 5.4.2. Collection of historical performance data

Collection of historical performance data in bulk by the manager is a general use case for a device and not specific to a radio link interface.

Collection of an individual counter for a specific interval is in same cases required as a complement to the retrieval in bulk as described above.

#### 5.5. Fault Management

##### 5.5.1. Configuration of alarm reporting

Configuration of alarm reporting associated specifically with radio interfaces, e.g. configuration of alarm severity, is a subset of the configuration use case to be supported. See 5.1 above.

##### 5.5.2. Alarm management

Alarm synchronization, visualization & handling, and notifications & events are generic use cases for a device and not specific to a radio link interface and should be supported accordingly.

#### 5.6. Troubleshooting and Root Cause Analysis

Information and actions required by a manager/operator to investigate and understand the underlying issue to a problem in the performance and/or functionality of a radio link terminal and the associated carrier terminations.

## 6. Requirements

For managing a microwave node including both the radio link and the packet functionality, a unified data model is desired to unify the modeling of the radio link interfaces and the packet interfaces using the same structure and the same modelling approach. If some part of model is generic for other technology usage, it should be clearly stated.

The purpose of the YANG Data Model is for management and control of the radio link interface(s) and the relationship/connectivity to other packet interfaces, typically to Ethernet interfaces, in a microwave node.

The capability of configuring and managing microwave nodes includes the following requirements for the modelling:

- 1) It MUST be possible to configure, manage and control a radio link terminal and the constituent carrier terminations.
  - a) Frequency, channel bandwidth, modulation, coding and transmitter power are examples of parameters typically configured for a carrier termination.
  - b) A radio link terminal MUST configure the associated carrier terminations and the type of aggregation/bonding or protection configurations expected for the radio link terminal.
  - c) The capability, e.g. the maximum modulation supported, and the actual status/statistics, e.g. administrative status of the carriers, SHOULD also be supported by the data model.
  - d) The definition of the features and parameters SHOULD be based on established microwave equipment and radio standards, such as ETSI EN 302 217 [EN 302 217-2] which specifies the essential parameters for microwave systems operating from 1.4GHz to 86GHz.
- 2) It MUST be possible to map different traffic types (e.g. TDM, Ethernet) to the transport capacity provided by a specific radio link terminal.
- 3) It MUST be possible to configure and collect historical measurements (for the use case described in section 5.4) to be performed on a radio link interface, e.g. minimum, maximum and average transmit power and receive level in dBm.
- 4) It MUST be possible to configure and retrieve alarms reporting associated with the radio interfaces, e.g. configuration of alarm severity, supported alarms like configuration fault, signal lost, modem fault, radio fault.

## 7. Gap Analysis on Models

The purpose of the gap analysis is to identify and recommend what existing and established models as well as draft models under definition to support the use cases and requirements specified in the previous chapters. It shall also make a recommendation on how the gaps not supported should be filled, including the need for development of new models and evolution of existing models and drafts.

For microwave radio link functionality work has been initiated (ONF: Microwave Modeling [ONF-model], IETF: Radio Link Model [I-D.ahlbergccamp-microwave-radio-link]). The analysis is expected to take these initiatives into consideration and make a recommendation on how to make use of them and how to complement them in order to fill the gaps identified.

For generic functionality, not specific for radio link, the ambition is to refer to existing or emerging models that could be applicable for all functional areas in a microwave node.

### 7.1. Microwave Radio Link Functionality

[ONF CIM] defines a CoreModel of the ONF Common Information Model. An information model describes the things in a domain in terms of objects, their properties (represented as attributes), and their relationships. The ONF information model is expressed in Unified Modeling Language (UML). The ONF CoreModel is independent of specific data plane technology. Data plane technology specific properties are acquired in a runtime solution via "filled in" cases of specification (LtpSpec etc). These can be used to augment the CoreModel to provide a data plane technology specific representation.

IETF Data Model defines an implementation and NETCONF-specific details. YANG is a data modeling language used to model the configuration and state data. It is well aligned with the structure of the Yang data models proposed for the different packet interfaces which are all based on RFC 7223. Furthermore, several YANG data models have been proposed in the IETF for other transport technologies such as optical transport; e.g., RFC 7277 [RFC7277], [I.D.zhang-ccamp-ll-topo-yang], [I.D.ietf-ospf-yang]. In light of this trend, the IETF data model is becoming a popular approach for modeling most packet transport technology interfaces and it is thereby well positioned to become an industry standard.

RFC 3444 [RFC3444] explains the difference between Information Model(IM) and Data Models(DM). IM is to model managed objects at a conceptual level for designers and operators, DM is defined at a lower level and includes many details for implementers. In addition, the protocol-specific details are usually included in DM. Since conceptual models can be implemented in different ways, multiple DMs can be derived from a single IM. To ensure better interoperability, it is better to focus on DM directly.

RFC 7223 describes an interface management model, however it doesn't include technology specific information, e.g., for radio interface. [I-D.ahlberg-ccamp-microwave-radio-link] provides a model proposal for radio interfaces, which includes support for basic configuration, status and performance but lacks full support for alarm management and interface layering, i.e. the connectivity of the transported capacity (TDM & Ethernet) with other internal technology specific interfaces in a microwave node.

The recommendation is to use the structure of the IETF: Radio Link Model [I-D.ahlberg-ccamp-microwave-radio-link] as the starting point, since it is a data model providing the wanted alignment with RFC 7223. For the definition of the detailed leafs/parameters, the recommendation is to use the IETF: Radio Link Model and the ONF: Microwave Modeling [ONF-model] as the basis and to define new ones to cover identified gaps. The parameters in those models have been defined by both operators and vendors within the industry and the implementations of the ONF Model have been tested in the Proof of Concept events in multi-vendor environments, showing the validity of the approach proposed in this framework document.

It is also recommended to add the required data nodes to describe the interface layering for the capacity provided by a radio link terminal and the associated Ethernet and TDM interfaces in a microwave node. The principles and data nodes for interface layering described in RFC 7223 should be used as a basis.

## 7.2. Generic Functionality

For generic functionality, not specific for radio link, the recommendation is to refer to existing RFCs or emerging drafts according to the table in figure 4 below. New Radio Link Model is used in the table for the cases where the functionality is recommended to be included in the new radio link model as described in chapter 7.1.

Generic Functionality	Recommendation
1. Fault Management	
Alarm Configuration	New Radio Link Model
Alarm notifications/ synchronization	[I-D.vallin-ccamp- alarm-module]
2. Performance Management	
Performance Configuration/ Activation	New Radio Link Model
Performance Collection	New Radio Link Model & XML files
3. Physical/Equipment Inventory	[I-D.ietf-netmod-entity]

Figure 4. Recommendation on how to support generic functionality

Microwave specific alarm configurations are recommended to be included in the new radio link model and could be based on what is supported in the IETF and ONF Radio Link Models. Alarm notifications and synchronization are general and is recommended to be supported by a generic model, such as [I-D.vallin-ccamp-alarm-module].

Activation of interval counters & thresholds could be a generic function but it is recommended to be supported by the new radio link specific model and can be based on both the ONF and IETF Microwave Radio Link models.

Collection of interval/historical counters is a generic function that needs to be supported in a node. File based collection via SFTP and collection via a Netconf/YANG interfaces are two possible options and the recommendation is to include support for the latter in the new radio link specific model. The ONF and IETF Microwave Radio Link models can be used as a basis also in this area.

Physical and/or equipment inventory associated with the radio link terminals and carrier terminations is recommended to be covered by a model generic for the complete node, e.g. [I-D.ietf-netmod-entity] and it is thereby outside the scope of the radio link specific model.

### 7.3. Summary

The conclusions and recommendations from the analysis can be summarized as follows:

- 1) A Microwave Radio Link YANG Data Model should be defined with a scope enough to support the use cases and requirements in chapter 5 and 6 of this document.
- 2) Use the structure in the IETF: Radio Link Model [I-D.ahlberg-ccamp-microwave-radio-link] as the starting point. It augments RFC 7223 and is thereby as required aligned with the structure of the models for management of the packet domain.
- 3) Use established microwave equipment and radio standards, such as ETSI EN 302 217 [EN 302 217-2], and the IETF: Radio Link Model [I-D.ahlberg-ccamp-microwave-radio-link] and the ONF: Microwave Modeling [ONF-model] as the basis for the definition of the detailed leafs/parameters to support the specified use cases and requirements, and proposing new ones to cover identified gaps.
- 4) Add the required data nodes to describe the interface layering for the capacity provided by a radio link terminal and the associated Ethernet and TDM interfaces, using the principles and data nodes for interface layering described in RFC 7223 as a basis.
- 5) Include support for configuration of microwave specific alarms in the Microwave Radio Link model and rely on a generic model such as [I.D.vallin-ccamp-alarm-module] for notifications and alarm synchronization.
- 6) Use a generic model such as [I-D.ietf-netmod-entity] for physical/equipment inventory.

It is furthermore recommended that the Microwave Radio Link YANG Data Model should be validated by both operators and vendors as part of the process to make it stable and mature. During the Hackathon in IETF 99, a project "SDN Applications for microwave radio link via IETF YANG Data Model" successfully validated this framework and the YANG data model [I.D.ietf-ccamp-mw-yang]. The project also received the BEST OVERALL award from the Hackathon.

### 8. Security Considerations

TBD

### 9. IANA Considerations

This memo includes no request to IANA.

## 10. References

### 10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2863] McCloghrie K. and Kastenholz F., "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000, <<http://www.rfc-editor.org/info/rfc2863>>.
- [RFC3444] Pras A., Schoenwaelder J., "On the Difference between Information Models and Data Models", RFC 3444, DOI 10.17487/RFC3444, January 2003, <<http://www.rfc-editor.org/info/rfc3444>>.
- [RFC7223] Bjorklund M., "A YANG Data Model for Interface Management", RFC 7223, DOI 10.17487/RFC7223, May 2014, <<http://www.rfc-editor.org/info/rfc7223>>.
- [RFC7277] Bjorklund M., "A YANG Data Model for IP Management", RFC 7277, DOI 10.17487/RFC7277, June 2014, <<http://www.rfc-editor.org/info/rfc7277>>.

### 10.2. Informative References

- [I-D.ahlberg-ccamp-microwave-radio-link] Ahlberg, J., Carlson, J., Lund, H., Olausson, T., Ye, M., and M. Vaupotic, "Microwave Radio Link YANG Data Models", draft-ahlberg-ccamp-microwave-radio-link-01 (work in progress), May 2016.
- [I-D.ietf-netmod-entity] Bierman A., Bjorklund M., Dong J., Romascanu D., "A YANG Data Model for Entity Management", draft-ietf-netmod-entity-05 (work in progress), October 2017.
- [I-D.vallin-ccamp-alarm-module] Vallin S. and Bjorklund M., "YANG Alarm Module", draft-vallin-ccamp-alarm-module-00 (work in progress), October 2017.
- [RFC8022] Lhotka, L. and A. Lindem, "A YANG Data Model for Routing Management", RFC 8022, DOI 10.17487/RFC8022, November 2016



[I.D.zhang-ccamp-l1-topo-yang]

Zhang X., Rao B., Sharma A., Liu X., "A YANG Data Model for Layer 1 (ODU) Network Topology", draft-zhang-ccamp-l1-topo-yang-03 (work in progress), July 2016.

[I.D.ietf-ospf-yang]

Yeung D., Qu Y., Zhang J., Bogdanovic D., Sreenivasa K., "Yang Data Model for OSPF Protocol", draft-ietf-ospf-yang-05,(work in progress), July 2016.

[ONF-model]

"Microwave Modeling - ONF Wireless Transport Group", May 2016.

[ONF CIM]

"Core Information Model", ONF TR-512, ONF, September 2016

[PB-YANG] "IEEE 802.1X and 802.1Q YANG models", Marc,H., October 2015.

[EN 302 217-2]

ETSI, "Fixed Radio Systems; Characteristics and requirements for point to-point equipment and antennas; Part 2: Digital systems operating in frequency bands from 1 GHz to 86 GHz; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU", EN 302 217-2 V3.1.1, May 2017.

[I.D.ietf-ccamp-mw-yang]

Ahlberg, J., Ye, M., Li,X., Kawada K., Bernardos C., Spreafico D., Vaupotic M., "A YANG Data Model for Microwave Radio Link", draft-ietf-ccamp-mw-yang-01,(work in progress), July 2016.

Authors' Addresses

Jonas Ahlberg  
Ericsson AB  
Lindholmspiren 11  
Goeteborg 417 56  
Sweden

Email: [jonas.ahlberg@ericsson.com](mailto:jonas.ahlberg@ericsson.com)

Luis M. Contreras  
Telefonica I+D  
Ronda de la Comunicacion, S/N  
Madrid 28050  
Spain

Email: [luismiguel.contrerasmurillo@telefonica.com](mailto:luismiguel.contrerasmurillo@telefonica.com)

Ye Min  
Huawei Technologies CO., Ltd  
No.1899, Xiyuan Avenue  
Chengdu 611731  
P.R.China

Email: [amy.yemin@huawei.com](mailto:amy.yemin@huawei.com)

Marko Vaupotic  
Aviat Networks  
Motnica 9  
Trzin-Ljubljana 1236  
Slovenia

Email: [Marko.Vaupotic@aviatnet.com](mailto:Marko.Vaupotic@aviatnet.com)

Jeff Tantsura  
Individual

Email: [jefftant.ietf@gmail.com](mailto:jefftant.ietf@gmail.com)

Koji Kawada  
NEC Corporation  
1753, Shimonumabe Nakahara-ku  
Kawasaki, Kanagawa 211-8666  
Japan

Email: k-kawada@ah.jp.nec.com

Xi Li  
NEC Laboratories Europe  
Kurfuersten-Anlage 36  
69115 Heidelberg  
Germany

Email: Xi.Li@neclab.eu

Ippei Akiyoshi  
NEC  
1753, Shimonumabe Nakahara-ku  
Kawasaki, Kanagawa 211-8666  
Japan

Email: i-akiyoshi@ah.jp.nec.com

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain

Email: cjbc@it.uc3m.es

Daniela Spreafico  
Nokia - IT  
Via Energy Park, 14  
Vimercate (MI) 20871  
Italy

Email: daniela.spreafico@nokia.com

CCAMP Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: April 26, 2018

J. Ahlberg  
Ericsson AB  
M. Ye  
Huawei Technologies  
X. Li  
NEC Laboratories Europe  
K. Kawada  
NEC Corporation  
CJ. Bernardos  
Universidad Carlos III de Madrid  
D. Spreafico  
Nokia - IT  
M. Vaupotic  
Aviat Networks  
October 23, 2017

A YANG Data Model for Microwave Radio Link  
draft-ietf-ccamp-mw-yang-02

Abstract

This document defines a YANG data model for control and management of the radio link interfaces, and their connectivity to packet (typically Ethernet) interfaces in a microwave/millimeter wave node. The data nodes for management of the interface protection functionality is broken out into a separate and generic YANG data model in order to make it available also for other interface types.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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 <http://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 April 26, 2018.

## Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Terminology and Definitions . . . . .	2
2. Introduction . . . . .	3
3. Microwave Radio Link YANG Data Model. . . . .	4
3.1. YANG Tree . . . . .	4
3.2. Explanation of the Microwave Data Model . . . . .	5
4. Microwave Radio Link YANG Module . . . . .	6
5. Interface Protection YANG Module . . . . .	30
6. Security Considerations . . . . .	36
7. IANA Considerations . . . . .	36
8. References . . . . .	37
8.1. Normative References . . . . .	37
8.2. Informative References . . . . .	37
Authors' Addresses . . . . .	38

## 1. Terminology and Definitions

The following terms are used in this document:

Carrier Termination (CT) is an interface for the capacity provided over the air by a single carrier. It is typically defined by its transmitting and receiving frequencies.

Radio Link Terminal (RLT) is an interface providing packet capacity and/or TDM capacity to the associated Ethernet and/or TDM interfaces in a node and used for setting up a transport service over a microwave/millimeter wave link.

The following acronyms are used in this document:

ACM Adaptive Coding Modulation

ATPC Automatic Transmit Power Control

CM Coding Modulation

CT Carrier Termination

RLT Radio Link Terminal

RTPC Remote Transmit Power Control

XPIC Cross Polarization Interference Cancellation

MIMO Multiple-Input Multiple-Output

## 2. Introduction

This document defines a YANG data model for management and control of the radio link interface(s) and the relationship to packet (typically Ethernet) and/or TDM interfaces in a microwave/millimeter wave node. ETSI EN 302 217 series defines the characteristics and requirements of microwave/millimeter wave equipment and antennas. Especially ETSI EN 302 217-2 [EN 302 217-2] specifies the essential parameters for the systems operating from 1.4GHz to 86GHz. The data model includes configuration and state data according to the new Network Management Datastore Architecture [NMDA].

The design of the data model follows the framework for management and control of microwave and millimeter wave interface parameters defined in [I-D.ietf-ccamp-microwave-framework]. This framework identifies the need and the scope of the YANG data model, the use cases and requirements that the model needs to support. Moreover, it provides a detailed gap analysis to identify the missing parameters and functionalities of the existing and established models to support the specified use cases and requirements, and based on that recommends how the gaps should be filled with the development of the new model.

According to the conclusion of the gap analysis, the structure of the data model is based on the structure defined in [I-D.ahlberg-ccamp-microwave-radio-link] and it augments [RFC7223bis] to align with the same structure for management of the packet interfaces. More specifically, the model will include interface layering to manage the capacity provided by a radio link terminal for the associated Ethernet and TDM interfaces, using the principles for interface layering described in RFC 7223 bis as a basis.

The data nodes for management of the interface protection functionality is broken out into a separate and generic YANG data module in order to make it available also for other interface types.

The designed YANG data model uses established microwave equipment and radio standards, such as ETSI EN 302 217-2, and the IETF: Radio Link Model[I-D.ahlberg-ccamp-microwave-radio-link] and the ONF: Microwave Modeling[ONF-model] as the basis for the definition of the detailed leafs/parameters, and proposes new ones to cover identified gaps which are analysed in[I-D.ietf-ccamp-microwave-framework].

### 3. Microwave Radio Link YANG Data Model

#### 3.1. YANG Tree

```

module: ietf-microwave-radio-link
  +--rw radio-link-protection-groups
  |   +--rw protection-group* [name]
  |   |   +--rw name string
  |   |   +--rw protection-architecture-type? identityref
  |   |   +--rw protection-members* if:interface-ref
  |   |   +--rw protection-operation-type? enumeration
  |   |   +--rw working-entity* if:interface-ref
  |   |   +--rw revertive-wait-to-restore? uint16
  |   |   +--rw hold-off-timer? uint16
  |   |   +--rw protection-status? identityref
  |   |   +---x protection-external-commands
  |   |   |   +---w input
  |   |   |   +---w protection-external-command? identityref
  |   +--rw xpics-pairs {xpics}?
  |   |   +--rw xpics-pair* [name]
  |   |   |   +--rw name string
  |   |   |   +--rw enabled? boolean
  |   |   |   +--rw xpics-members* if:interface-ref
  |   +--rw mimos-groups {mimos}?
  |   |   +--rw mimos-group* [name]
  |   |   |   +--rw name string
  |   |   |   +--rw enabled? boolean
  |   |   |   +--rw mimos-members* if:interface-ref
  augment /if:interfaces/if:interface:
    +--rw id? string
    +--rw mode identityref
    +--rw carrier-terminations* if:interface-ref
    +--rw rlp-groups*
    |   -> /radio-link-protection-groups/protection-group/name
    +--rw xpics-pairs* -> /xpics-pairs/xpics-pair/name
    |   {xpics}?
    +--rw mimos-groups* -> /mimos-groups/mimos-group/name
    |   {mimos}?
    +--rw tdm-connections* [tdm-type] {tdm}?
    |   +--rw tdm-type identityref
    |   +--rw tdm-connections uint16
  augment /if:interfaces/if:interface:
    +--rw carrier-id? string
    +--rw tx-enabled? boolean
    +--ro tx-oper-status? enumeration
    +--rw tx-frequency uint32
    +--rw rx-frequency? uint32
    +--rw duplex-distance? uint32
    +--rw channel-separation uint32
    +--rw polarization? enumeration
    +--rw power-mode enumeration

```

```

+--rw maximum-nominal-power          power
+--rw atpc-lower-threshold            power
+--rw atpc-upper-threshold            power
+--ro actual-transmitted-level?       power
+--ro actual-received-level?          power
+--rw coding-modulation-mode          enumeration
+--rw selected-cm                     identityref
+--rw selected-min-acm                identityref
+--rw selected-max-acm                identityref
+--ro actual-tx-cm?                   identityref
+--ro actual-snr?                     decimal64
+--ro actual-xpi?                     decimal64 {xpic}?
+--rw ct-performance-thresholds
|   +--rw received-level-alarm-threshold? power
|   +--rw transmitted-level-alarm-threshold? power
|   +--rw ber-alarm-threshold?          enumeration
+--rw if-loop?                        enumeration
+--rw rf-loop?                        enumeration
+--ro capabilities
|   +--ro min-tx-frequency?             uint32
|   +--ro max-tx-frequency?             uint32
|   +--ro min-rx-frequency?             uint32
|   +--ro max-rx-frequency?             uint32
|   +--ro minimum-power?                power
|   +--ro maximum-available-power?      power
|   +--ro available-min-acm?            identityref
|   +--ro available-max-acm?            identityref
+--ro error-performance-statistics
|   +--ro bbe?      yang:counter32
|   +--ro es?       yang:counter32
|   +--ro ses?      yang:counter32
|   +--ro uas?      yang:counter32
+--ro radio-performance-statistics
|   +--ro min-rltm? power
|   +--ro max-rltm? power
|   +--ro min-tltm? power
|   +--ro max-tltm? power

```

### 3.2. Explanation of the Microwave Data Model

The leafs in the Interface Management Module augmented by Radio Link Terminal (RLT) and Carrier Termination (CT) are not always applicable.

"/interfaces/interface/enabled" is not applicable for RLT. Enable and disable of an interface is done in the constituent CTs.

The packet related measurements "in-octets", "in-unicast-pkts", "in-broadcast-pkts", "in-multicast-pkts", "in-discards", "in-errors", "in-unknown-protos", "out-octets", "out-unicast-pkts", "out-broadcast-pkts", "out-multicast-pkts", "out-discards", "out-errors" are not within the scope of the microwave radio link domain and therefore not applicable for RLT and CT.



## 4. Microwave Radio Link YANG Module

```
<CODE BEGINS> file "ietf-microwave-radio-link.yang"

module ietf-microwave-radio-link {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-microwave-radio-link";
  prefix mrl;

  import ietf-yang-types {
    prefix yang;
  }

  import ietf-interfaces {
    prefix if;
  }

  import ietf-interface-protection {
    prefix ifprot;
  }

  import iana-if-type {
    prefix ianaift;
  }

  organization
    "Internet Engineering Task Force (IETF) CCAMP WG";
  contact
    "WG List: <mailto:ccamp@ietf.org>"

    ID-draft authors:
      Jonas Ahlberg (jonas.ahlberg@ericsson.com);
      Min Ye (amy.yemin@huawei.com);
      Xi Li (Xi.Li@neclab.eu);
      Koji Kawada (k-kawada@ah.jp.nec.com)
      Carlos J. Bernardos (cjbc@it.uc3m.es)
      Daniela Spreafico (daniela.spreafico@nokia.com)
      Marko Vaupotic (Marko.Vaupotic@aviatnet.com);

  description
    "This is a module for the entities in
    a generic microwave system.";

  revision 2017-10-23 {
    description
      "Break out protection functionality to a generic module
      and update to follow the new NMDA style.";
    reference "";
  }
}
```

```
revision 2017-06-21 {
  description
    "Updated draft revision with updates of some descriptions to
    increase clarity and some minor adjustments of the model.";
  reference "";
}
revision 2016-12-22 {
  description
    "Draft revision covering a complete scope for configuration
    and state data for radio link interfaces.";
  reference "";
}
revision 2016-10-29 {
  description
    "Draft revision.";
  reference "";
}

/*
 * Features
 */

feature xpic {
  description
    "Indicates that the device supports XPIC.";
  reference "ETSI TR 102 311";
}

feature mimo {
  description
    "Indicates that the device supports MIMO.";
  reference "ETSI TR 102 311";
}

feature tdm {
  description
    "Indicates that the device supports TDM.";
}

/*
 * Interface identities
 */

identity radio-link-terminal {
  base ianaif:iana-interface-type;
  description
    "Interface identity for a radio link terminal.";
}
```

```
identity carrier-termination {
  base ianaift:iana-interface-type;
  description
    "Interface identity for a carrier termination.";
}

/*
 * Radio-link-terminal mode identities
 */

identity rlt-mode {
  description
    "A description of the mode in which the radio link
    terminal is configured. The format is X plus Y.
    X represent the number of bonded carrier terminations.
    Y represent the number of protecting carrier
    terminations.";
}

identity one-plus-zero {
  base rlt-mode;
  description
    "1 carrier termination only.";
}

identity one-plus-one {
  base rlt-mode;
  description
    "1 carrier termination
    and 1 protecting carrier termination.";
}

identity two-plus-zero {
  base rlt-mode;
  description
    "2 bonded carrier terminations.";
}

/*
 * Coding and modulation identities
 */

identity coding-modulation {
  description
    "The coding and modulation schemes.";
}

identity half-bpsk-strong {
  base coding-modulation;
  description
    "Half BPSK strong coding and modulation scheme.";
}
```

```
identity half-bpsk {
  base coding-modulation;
  description
    "Half BPSK coding and modulation scheme.";
}

identity half-bpsk-light {
  base coding-modulation;
  description
    "Half BPSK light coding and modulation scheme.";
}

identity bpsk-strong {
  base coding-modulation;
  description
    "BPSK strong coding and modulation scheme.";
}

identity bpsk {
  base coding-modulation;
  description
    "BPSK coding and modulation scheme.";
}

identity bpsk-light {
  base coding-modulation;
  description
    "BPSK light coding and modulation scheme.";
}

identity qpsk {
  base coding-modulation;
  description
    "QPSK coding and modulation scheme.";
}

identity qam-4-strong {
  base coding-modulation;
  description
    "4 QAM strong coding and modulation scheme.";
}

identity qam-4 {
  base coding-modulation;
  description
    "4 QAM coding and modulation scheme.";
}
```

```
identity qam-4-light {
  base coding-modulation;
  description
    "4 QAM light coding and modulation scheme.";
}

identity qam-16-strong {
  base coding-modulation;
  description
    "16 QAM strong coding and modulation scheme.";
}

identity qam-16 {
  base coding-modulation;
  description
    "16 QAM coding and modulation scheme.";
}

identity qam-16-light {
  base coding-modulation;
  description
    "16 QAM light coding and modulation scheme.";
}

identity qam-32-strong {
  base coding-modulation;
  description
    "32 QAM strong coding and modulation scheme.";
}

identity qam-32 {
  base coding-modulation;
  description
    "32 QAM coding and modulation scheme.";
}

identity qam-32-light {
  base coding-modulation;
  description
    "32 QAM light coding and modulation scheme.";
}

identity qam-64-strong {
  base coding-modulation;
  description
    "64 QAM strong coding and modulation scheme.";
}
```

```
identity qam-64 {
  base coding-modulation;
  description
    "64 QAM coding and modulation scheme.";
}

identity qam-64-light {
  base coding-modulation;
  description
    "64 QAM light coding and modulation scheme.";
}

identity qam-128-strong {
  base coding-modulation;
  description
    "128 QAM strong coding and modulation scheme.";
}

identity qam-128 {
  base coding-modulation;
  description
    "128 QAM coding and modulation scheme.";
}

identity qam-128-light {
  base coding-modulation;
  description
    "128 QAM light coding and modulation scheme.";
}

identity qam-256-strong {
  base coding-modulation;
  description
    "256 QAM strong coding and modulation scheme.";
}

identity qam-256 {
  base coding-modulation;
  description
    "256 QAM coding and modulation scheme.";
}

identity qam-256-light {
  base coding-modulation;
  description
    "256 QAM light coding and modulation scheme.";
}
```

```
identity qam-512-strong {
  base coding-modulation;
  description
    "512 QAM strong coding and modulation scheme.";
}

identity qam-512 {
  base coding-modulation;
  description
    "512 QAM coding and modulation scheme.";
}

identity qam-512-light {
  base coding-modulation;
  description
    "512 QAM light coding and modulation scheme.";
}

identity qam-1024-strong {
  base coding-modulation;
  description
    "1024 QAM strong coding and modulation scheme.";
}

identity qam-1024 {
  base coding-modulation;
  description
    "1024 QAM coding and modulation scheme.";
}

identity qam-1024-light {
  base coding-modulation;
  description
    "1024 QAM light coding and modulation scheme.";
}

identity qam-2048-strong {
  base coding-modulation;
  description
    "2048 QAM strong coding and modulation scheme.";
}

identity qam-2048 {
  base coding-modulation;
  description
    "2048 QAM coding and modulation scheme.";
}
```

```
identity qam-2048-light {
  base coding-modulation;
  description
    "2048 QAM light coding and modulation scheme.";
}

identity qam-4096-strong {
  base coding-modulation;
  description
    "4096 QAM strong coding and modulation scheme.";
}

identity qam-4096 {
  base coding-modulation;
  description
    "4096 QAM coding and modulation scheme.";
}

identity qam-4096-light {
  base coding-modulation;
  description
    "4096 QAM light coding and modulation scheme.";
}

/*
 * TDM-type identities
 */

identity tdm-type {
  description
    "A description of the type of TDM connection,
    also indicating the supported capacity of the
    connection.";
}

identity E1 {
  base tdm-type;
  description
    "E1 connection, 2,048 Mbit/s.";
}

identity STM-1 {
  base tdm-type;
  description
    "STM-1 connection, 155,52 Mbit/s.";
}
```



```
/*
 * Typedefs
 */

typedef power {
  type decimal64 {
    fraction-digits 1;
  }
  description
    "Type used for power values, selected and measured.";
}

/*
 * Radio Link Terminal (RLT)
 */

augment "/if:interfaces/if:interface" {
  when "if:type = 'mrl:radio-link-terminal'";
  description
    "Addition of data nodes for radio link terminal to
    the standard Interface data model, for interfaces of
    the type 'radio-link-terminal'.";

  leaf id {
    type string;
    default "";
    description
      "ID of the radio link terminal. Used by far-end when
      checking that it's connected to the correct RLT.";
  }

  leaf mode {
    type identityref {
      base rlt-mode;
    }
    mandatory true;
    description
      "A description of the mode in which the radio link
      terminal is configured. The format is X plus Y.
      X represent the number of bonded carrier terminations.
      Y represent the number of protecting carrier
      terminations.";
  }
}
```

```
leaf-list carrier-terminations {
  type if:interface-ref;
  must "/if:interfaces/if:interface[if:name = current()]"
    + "/if:type = 'mrl:carrier-termination'" {
    description
      "The type of interface must be
       'carrier-termination'.";
  }
  min-elements 1;
  description
    "A list of references to carrier terminations
     included in the radio link terminal.";
}

leaf-list rlp-groups {
  type leafref {
    path "/mrl:radio-link-protection-groups/"
      + "mrl:protection-group/mrl:name";
  }
  description
    "A list of references to the carrier termination
     groups configured for radio link protection in this
     radio link terminal.";
}

leaf-list xpics-pairs {
  if-feature xpics;
  type leafref {
    path "/mrl:xpics-pairs/mrl:xpics-pair/mrl:name";
  }
  description
    "A list of references to the XPIC pairs used in this
     radio link terminal. One pair can be used by two
     terminals.";
  reference "ETSI TR 102 311";
}

leaf-list mimo-groups {
  if-feature mimo;
  type leafref {
    path "/mrl:mimo-groups/mrl:mimo-group/mrl:name";
  }
  description
    "A reference to the MIMO group used in this
     radio link terminal. One group can be used by more
     than one terminal.";
  reference "ETSI TR 102 311";
}
```

```
list tdm-connections {
  if-feature tdm;
  key "tdm-type";
  description
    "A list stating the number of active TDM connections
    of a specified tdm-type that is configured to be
    supported by the RLT.";
  leaf tdm-type {
    type identityref {
      base tdm-type;
    }
    description
      "The type of TDM connection, which also indicates
      the supported capacity.";
  }
  leaf tdm-connections {
    type uint16;
    mandatory true;
    description
      "Number of connections of the specified type.";
  }
}

/*
 * Carrier Termination
 */

augment "/if:interfaces/if:interface" {
  when "if:type = 'mrl:carrier-termination'";
  description
    "Addition of data nodes for carrier termination to
    the standard Interface data model, for interfaces
    of the type 'carrier-termination'.";

  leaf carrier-id {
    type string;
    default "A";
    description
      "ID of the carrier. (e.g. A, B, C or D)
      Used in XPIC & MIMO configurations to check that
      the carrier termination is connected to the correct
      far-end carrier termination. Should be the same
      carrier ID on both sides of the hop.
      Defaulted when not MIMO or XPIC.";
  }
}
```

```
leaf tx-enabled {
  type boolean;
  default "false";
  description
    "Disables (false) or enables (true) the transmitter.
     Only applicable when the interface is enabled
     (interface:enabled = true) otherwise it's always
     disabled.";
}

leaf tx-oper-status {
  type enumeration {
    enum "off" {
      description "Transmitter is off.";
    }
    enum "on" {
      description "Transmitter is on.";
    }
    enum "standby" {
      description "Transmitter is in standby.";
    }
  }
  config false;
  description
    "Shows the operative status of the transmitter.";
}

leaf tx-frequency {
  type uint32;
  units "kHz";
  mandatory true;
  description
    "Selected transmitter frequency.";
}

leaf rx-frequency {
  type uint32;
  units "kHz";
  description
    "Selected receiver frequency.
     Overrides existing value in duplex-distance.
     Calculated from tx-frequency and duplex-distance if
     only duplex-distance is configured.
     Must match duplex-distance if both leaves are
     configured in a single operation.";
}
```

```
leaf duplex-distance {
  type uint32;
  units "kHz";
  description
    "Distance between Tx & Rx frequencies.
     Used to calculate rx-frequency when
     rx-frequency is not specifically configured.
     Overrides existing value in rx-frequency.
     Calculated from tx-frequency and rx-frequency if only
     rx-frequency is configured.
     Must match rx-frequency if both leaves are configured
     in a single operation.";
}

leaf channel-separation {
  type uint32;
  units "kHz";
  mandatory true;
  description
    "The amount of bandwidth allocated to a carrier. The distance
     between adjacent channels in a radio frequency channels
     arrangement";
  reference "ETSI EN 302 217-1";
}

leaf polarization {
  type enumeration {
    enum "horizontal" {
      description "Horizontal polarization.";
    }
    enum "vertical" {
      description "Vertical polarization.";
    }
    enum "not-specified" {
      description "Polarization not specified.";
    }
  }
  default "not-specified";
  description
    "Polarization - A textual description for info only.";
}

leaf power-mode {
  type enumeration {
    enum rtpc {
      description
        "Remote Transmit Power Control (RTPC).";
      reference "ETSI EN 302 217-1";
    }
  }
}
```

```
    enum atpc {
        description
            "Automatic Transmit Power Control (ATPC).";
        reference "ETSI EN 302 217-1";
    }
}
mandatory true;
description
    "A choice of Remote Transmit Power Control (RTPC)
    or Automatic Transmit Power Control (ATPC).";
}

leaf maximum-nominal-power {
    type power {
        range "-99..40";
    }
    units "dBm";
    mandatory true;
    description
        "Selected output power in RTPC mode and selected
        maximum output power in ATPC mode. Minimum output
        power in ATPC mode is the same as the system
        capability, available-min-output-power.";
    reference "ETSI EN 302 217-1";
}

leaf atpc-lower-threshold {
    when "../power-mode = 'atpc'";
    type power {
        range "-99..-30";
    }
    units "dBm";
    mandatory true;
    description
        "The lower threshold for the input power at far-end
        used in the ATPC mode.";
    reference "ETSI EN 302 217-1";
}

leaf atpc-upper-threshold {
    when "../power-mode = 'atpc'";
    type power {
        range "-99..-30";
    }
    units "dBm";
    mandatory true;
    description
        "The upper threshold for the input power at far-end
        used in the ATPC mode.";
    reference "ETSI EN 302 217-1";
}
```

```
leaf actual-transmitted-level {
  type power {
    range "-99..40";
  }
  units "dBm";
  config false;
  description
    "Actual transmitted power level (0.1 dBm resolution).";
  reference "ETSI EN 301 129";
}

leaf actual-received-level {
  type power {
    range "-99..-20";
  }
  units "dBm";
  config false;
  description
    "Actual received power level (0.1 dBm resolution).";
  reference "ETSI EN 301 129";
}

leaf coding-modulation-mode {
  type enumeration {
    enum single {
      description "a single modulation order only.";
      reference "ETSI EN 302 217-1";
    }
    enum adaptive {
      description "Adaptive coding/modulation.";
      reference "ETSI EN 302 217-1";
    }
  }
  mandatory true;
  description
    "A selection of single or
    adaptive coding/modulation mode.";
}

leaf selected-cm {
  when "../coding-modulation-mode = 'single'";
  type identityref {
    base coding-modulation;
  }
  mandatory true;
  description
    "Selected the single coding/modulation.";
}
```

```
leaf selected-min-acm {
  when "../coding-modulation-mode = 'adaptive'";
  type identityref {
    base coding-modulation;
  }
  mandatory true;
  description
    "Selected minimum coding/modulation.
    Adaptive coding/modulation shall not go
    below this value.";
}

leaf selected-max-acm {
  when "../coding-modulation-mode = 'adaptive'";
  type identityref {
    base coding-modulation;
  }
  mandatory true;
  description
    "Selected maximum coding/modulation.
    Adaptive coding/modulation shall not go
    above this value.";
}

leaf actual-tx-cm {
  type identityref {
    base coding-modulation;
  }
  config false;
  description
    "Actual coding/modulation in transmitting direction.";
}

leaf actual-snr {
  type decimal64 {
    fraction-digits 1;
    range "0..99";
  }
  units "dB";
  config false;
  description
    "Actual signal to noise plus interference ratio.
    (0.1 dB resolution).";
}

leaf actual-xpi {
  if-feature xpic;
  type decimal64 {
    fraction-digits 1;
    range "0..99";
  }
}
```



```
    units "dB";
    config false;
    description
        "The actual carrier to cross-polar interference.
        Only valid if XPIC is enabled. (0.1 dB resolution).";
    reference "ETSI TR 102 311";
}

container ct-performance-thresholds {
    description
        "Specification of thresholds for when alarms should
        be sent and cleared for various performance counters.";

    leaf received-level-alarm-threshold {
        type power {
            range "-99..-30";
        }
        units "dBm";
        default "-99";
        description
            "An alarm is sent when the received power level is
            below the specified threshold.";
        reference "ETSI EN 301 129";
    }

    leaf transmitted-level-alarm-threshold {
        type power {
            range "-99..40";
        }
        units "dBm";
        default "-99";
        description
            "An alarm is sent when the transmitted power level
            is below the specified threshold.";
        reference "ETSI EN 301 129";
    }

    leaf ber-alarm-threshold {
        type enumeration {
            enum "10e-9" {
                description "Threshold at 10e-9.";
            }
            enum "10e-8" {
                description "Threshold at 10e-8.";
            }
            enum "10e-7" {
                description "Threshold at 10e-7.";
            }
            enum "10e-6" {
                description "Threshold at 10e-6.";
            }
        }
    }
}
```

```
        enum "10e-5" {
            description "Threshold at 10e-5.";
        }
        enum "10e-4" {
            description "Threshold at 10e-4.";
        }
        enum "10e-3" {
            description "Threshold at 10e-3.";
        }
        enum "10e-2" {
            description "Threshold at 10e-2.";
        }
        enum "10e-1" {
            description "Threshold at 10e-1.";
        }
    }
    default "10e-6";
    description
        "Specification of at which BER an alarm should
        be raised.";
    reference "ETSI EN 302 217-1";
}

leaf if-loop {
    type enumeration {
        enum disabled {
            description "Disables the IF Loop.";
        }
        enum client {
            description
                "Loops the signal back to the client side.";
        }
        enum radio {
            description
                "Loops the signal back to the radio side.";
        }
    }
    default "disabled";
    description
        "Enable (client/radio) or disable (disabled)
        the IF loop, which loops the signal back to
        the client side or the radio side.";
}

leaf rf-loop {
    type enumeration {
        enum disabled {
            description "Disables the RF Loop.";
        }
    }
}
```

```
    enum client {
      description
        "Loops the signal back to the client side.";
    }
    enum radio {
      description
        "Loops the signal back to the radio side.";
    }
  }
  default "disabled";
  description
    "Enable (client/radio) or disable (disabled)
     the RF loop, which loops the signal back to
     the client side or the radio side.";
}

container capabilities {
  config false;
  description
    "Capabilities of the the installed equipment and
     some selected configurations.";

  leaf min-tx-frequency {
    type uint32;
    units "kHz";
    description
      "Minimum Tx frequency possible to use.";
  }

  leaf max-tx-frequency {
    type uint32;
    units "kHz";
    description
      "Maximum Tx frequency possible to use.";
  }

  leaf min-rx-frequency {
    type uint32;
    units "kHz";
    description
      "Minimum Rx frequency possible to use.";
  }

  leaf max-rx-frequency {
    type uint32;
    units "kHz";
    description
      "Maximum Tx frequency possible to use.";
  }
}
```

```
    leaf minimum-power {
      type power;
      units "dBm";
      description
        "The minimum output power supported.";
      reference "ETSI EN 302 217-1";
    }

    leaf maximum-available-power {
      type power;
      units "dBm";
      description
        "The maximum output power supported.";
      reference "ETSI EN 302 217-1";
    }

    leaf available-min-acm {
      type identityref {
        base coding-modulation;
      }
      description
        "Minimum coding-modulation possible to use.";
    }

    leaf available-max-acm {
      type identityref {
        base coding-modulation;
      }
      description
        "Maximum coding-modulation possible to use.";
    }
  }

  container error-performance-statistics {
    config false;
    description
      "ITU-T G.826 error performance statistics relevant for
      a microwave/millimeter wave carrier.";

    leaf bbe {
      type yang:counter32;
      units "number of block errors";
      description
        "Number of Background Block Errors (BBE) during the
        interval. A BBE is an errored block not occurring as
        part of an SES.";
      reference "ITU-T G.826";
    }
  }
```

```
leaf es {
    type yang:counter32;
    units "seconds";
    description
        "Number of Errored Seconds (ES) since last reset.
        An ES is a one-second period with one or more errored
        blocks or at least one defect.";
    reference "ITU-T G.826";
}

leaf ses {
    type yang:counter32;
    units "seconds";
    description
        "Number of Severely Errored Seconds (SES) during the
        interval. SES is a one-second period which contains
        equal or more than 30% errored blocks or at least
        one defect. SES is a subset of ES.";
    reference "ITU-T G.826";
}

leaf uas {
    type yang:counter32;
    units "seconds";
    description
        "Number of Unavailable Seconds (UAS), that is, the
        total time that the node has been unavailable during
        a fixed measurement interval.";
    reference "ITU-T G.826";
}

container radio-performance-statistics {
    config false;
    description
        "ETSI EN 301 129 radio physical interface statistics relevant
        for a carrier termination.";

    leaf min-rltm {
        type power {
            range "-99..-20";
        }
        units "dBm";
        description
            "Minimum received power level since last reset.";
        reference "ETSI EN 301 129";
    }
}
```

```
    leaf max-rltm {
      type power {
        range "-99..-20";
      }
      units "dBm";
      description
        "Maximum received power level since last reset.";
      reference "ETSI EN 301 129";
    }

    leaf min-tltm {
      type power {
        range "-99..40";
      }
      units "dBm";
      description
        "Minimum transmitted power level since last reset.";
      reference "ETSI EN 301 129";
    }

    leaf max-tltm {
      type power {
        range "-99..40";
      }
      units "dBm";
      description
        "Maximum transmitted power level since last reset.";
      reference "ETSI EN 301 129";
    }
  }
}

/*
 * Radio Link Protection Groups
 */

container radio-link-protection-groups {
  description
    "Configuration of radio link protected groups (1+1) of
    carrier terminations in a radio link. More than one
    protected group per radio-link-terminal is allowed.";

  uses ifprot:protection-groups {

    refine protection-group/protection-members {
      must "/if:interfaces/if:interface[if:name = current()]"
        + "/if:type = 'mrl:carrier-termination'" {
        description
          "The type of a protection member must be
          'carrier-termination'.";
      }
    }
  }
}
```

```
    refine protection-group/working-entity {
      must "/if:interfaces/if:interface[if:name = current()]"
        + "/if:type = 'mrl:carrier-termination'" {
        description
          "The type of a working-entity must be
           'carrier-termination'.";
      }
    }
  }
}

/*
 * XPIC & MIMO groups - Configuration data nodes
 */

container xpic-pairs {
  if-feature xpic;
  description
    "Configuration of carrier termination pairs
     for operation in XPIC mode.";
  reference "ETSI TR 102 311";

  list xpic-pair {
    key "name";
    description
      "List of carrier termination pairs in XPIC mode.";

    leaf name {
      type string;
      description
        "Name used for identification of the XPIC pair.";
    }

    leaf enabled {
      type boolean;
      default "false";
      description
        "Enable(true)/disable(false) XPIC";
    }

    leaf-list xpic-members {
      type if:interface-ref;
      must "/if:interfaces/if:interface[if:name = current()]"
        + "/if:type = 'mrl:carrier-termination'" {
        description
          "The type of a xpic-member must be
           'carrier-termination'.";
      }
      min-elements 2;
      max-elements 2;
    }
  }
}
```

```
        description
            "Association to XPIC pairs used in the radio link
            terminal.";
    }
}

container mimo-groups {
    if-feature mimo;
    description
        "Configuration of carrier terminations
        for operation in MIMO mode.";
    reference "ETSI TR 102 311";

    list mimo-group {
        key "name";
        description
            "List of carrier terminations in MIMO mode.";

        leaf name {
            type string;
            description
                "Name used for identification of the MIMO group.";
        }

        leaf enabled {
            type boolean;
            default "false";
            description
                "Enable(true)/disable(false) MIMO";
        }

        leaf-list mimo-members {
            type if:interface-ref;
            must "/if:interfaces/if:interface[if:name = current()]"
                + "/if:type = 'mrl:carrier-termination'" {
                description
                    "The type of a mimo-member must be
                    'carrier-termination'.";
            }
            min-elements 2;
            description
                "Association to a MIMO group if used in the radio
                link terminal.";
        }
    }
}

<CODE ENDS>
```



## 5. Interface Protection YANG Module

The data nodes for management of the interface protection functionality is broken out from the Microwave Radio Link Module into a separate and generic YANG data module in order to make it available also for other interface types.

<CODE BEGINS> file "ietf-interface-protection.yang"

```
module ietf-interface-protection {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-interface-protection";
  prefix ifprot;

  import ietf-interfaces {
    prefix if;
  }

  organization
    "Internet Engineering Task Force (IETF) CCAMP WG";
  contact
    "WG List: <mailto:ccamp@ietf.org>";

  ID-draft authors:
    Jonas Ahlberg (jonas.ahlberg@ericsson.com);
    Min Ye (amy.yemin@huawei.com);
    Xi Li (Xi.Li@neclab.eu);
    Koji Kawada (k-kawada@ah.jp.nec.com)
    Carlos J. Bernardos (cjbc@it.uc3m.es)
    Daniela Spreafico (daniela.spreafico@nokia.com)
    Marko Vaupotic (Marko.Vaupotic@aviatnet.com);

  description
    "This is a module for the entities in
    a generic interface protection mechanism.";

  revision 2017-10-19 {
    description
      "Draft revision.";
    reference "";
  }

  /*
   * Protection architecture type identities
   */

  identity protection-architecture-type {
    description
      "protection architecture type";
    reference "ITU-T Rec. G.808.1";
  }
```

```
identity one-plus-one-type {
  base protection-architecture-type;
  description
    "1+1, One interface protects
    another one interface.";
  reference "ITU-T Rec. G.808.1";
}

identity one-to-n-type {
  base protection-architecture-type;
  description
    "1:N, One interface protects
    n other interfaces.";
  reference "ITU-T Rec. G.808.1";
}

/*
 * Protection states identities
 */

identity protection-states {
  description
    "Identities describing the status of the protection,
    in a group of interfaces configured in
    a protection mode.";
}

identity unprotected {
  base protection-states;
  description "Not protected";
}

identity protected {
  base protection-states;
  description "Protected";
}

identity unable-to-protect {
  base protection-states;
  description "Unable to protect";
}

/*
 * protection-external-commands identities
 */

identity protection-external-commands{
  description
    "Protection external commands for trouble shooting
    purpose.";
  reference "ITU-T Rec. G.808.1";
}
```

```
identity manual-switch-working{
  base protection-external-commands;
  description
    "A switch action initiated by an operator command.
    It switches normal traffic signal to the working
    transport entity.";
  reference "ITU-T Rec. G.808.1";
}

identity manual-switch-protection{
  base protection-external-commands;
  description
    "A switch action initiated by an operator command.
    It switches normal traffic signal to the protection
    transport entity.";
  reference "ITU-T Rec. G.808.1";
}

identity forced-switch{
  base protection-external-commands;
  description
    "A switch action initiated by an operator command.
    It switches normal traffic signal to the protection
    transport entity and forces it to remain on that
    entity even when criteria for switching back to
    the original entity are fulfilled.";
  reference "ITU-T Rec. G.808.1";
}

identity lockout-of-protection{
  base protection-external-commands;
  description
    "A switch action temporarily disables access to the
    protection transport entity for all signals.";
  reference "ITU-T Rec. G.808.1";
}

identity freeze{
  base protection-external-commands;
  description
    "A switch action temporarily prevents any switch action
    to be taken and, as such, freezes the current state.
    Until the freeze is cleared, additional near-end external
    commands are rejected and fault condition changes and
    received APS messages are ignored..";
  reference "ITU-T Rec. G.808.1";
}
```

```
identity exercise{
  base protection-external-commands;
  description
    "A switch action to test if the APS communication is
    operating correctly. It is lower priority than any 'real'
    switch request..";
  reference "ITU-T Rec. G.808.1";
}

identity clear{
  base protection-external-commands;
  description
    "A action clears all switch commands.";
  reference "ITU-T Rec. G.808.1";
}

/*
 * Protection Groups
 */

grouping protection-groups {
  description
    "Configuration of protected groups (1+1) of interfaces
    providing protection for each other. More than one protected
    group per higher-layer-interface is allowed.";

  list protection-group {
    key "name";
    description
      "List of protected groups of interfaces
      in a higher-layer-interface.";

    leaf name {
      type string;
      description
        "Name used for identification of the protection group";
    }

    leaf protection-architecture-type {
      type identityref{
        base protection-architecture-type;
      }
      default "one-plus-one-type";
      description
        "The type of protection architecture used, e.g. one
        interface protecting one or several other interfaces.";
      reference "ITU-T Rec. G.808.1";
    }
  }
}
```

```
leaf-list protection-members {
  type if:interface-ref;
  min-elements 2;
  description
    "Association to a group of interfaces configured for
    protection and used by a higher-layer-interface.";
}

leaf protection-operation-type {
  type enumeration {
    enum "non-revertive" {
      description
        "In non revertive operation, the traffic does not
        return to the working interface if the switch requests
        are terminated.";
      reference "ITU-T Rec. G.808.1";
    }
    enum "revertive" {
      description
        "In revertive operation, the traffic always
        returns to (or remains on) the working interface
        if the switch requests are terminated.";
      reference "ITU-T Rec. G.808.1";
    }
  }
  default "non-revertive";
  description
    "The type of protection operation, i.e. revertive
    or non-revertive operation.";
}

leaf-list working-entity {
  when "../protection-operation-type = 'revertive'";
  type if:interface-ref;
  min-elements 1;
  description
    "The interfaces over which the traffic normally should
    be transported over when there is no need to use the
    protecting interface.";
}

leaf revertive-wait-to-restore {
  when "../protection-operation-type = 'revertive'";
  type uint16;
  units "seconds";
  default "0";
  description
    "The time to wait before switching back to the working
    interface if protection-operation-type is revertive.";
  reference "ITU-T Rec. G.808.1";
}
```

```
leaf hold-off-timer {
    type uint16;
    units "milliseconds";
    default "0";
    description
        "Time interval after the detection of a fault and its
         confirmation as a condition requiring the protection
         switching procedure.";
    reference "ITU-T Rec. G.808.1";
}

leaf protection-status {
    type identityref {
        base protection-states;
    }
    description
        "Status of the protection, in a group of interfaces
         configured in a protection mode.";
    reference "ITU-T Rec. G.808.1";
}

action protection-external-commands {
    input {
        leaf protection-external-command {
            type identityref {
                base protection-external-commands;
            }
            description
                "Execution of protection external commands for
                 trouble shooting purpose.";
        }
    }
}

}
}
}

<CODE ENDS>
```

## 6. Security Considerations

The YANG module defined in this memo is designed to be accessed via the NETCONF protocol [RFC6241]. The lowest NETCONF layer is the secure transport layer and the mandatory-to-implement secure transport is SSH [RFC6242]. The NETCONF access control model [RFC6536] provides the means to restrict access for particular NETCONF users to a pre-configured subset of all available NETCONF protocol operations and content.

There are a number of data nodes defined in the YANG module which are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., <editconfig>) to these data nodes without proper protection can have a negative effect on network operations.

The security considerations of [RFC7223bis] also apply to this document.

## 7. IANA Considerations

TBD.

## 8. References

### 8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC7223bis] Bjorklund, M., "A YANG Data Model for Interface Management", draft-bjorklund-netmod-rfc7223bis-00 (work in progress), September 2017.
- [EN 302 217-2] ETSI, "Fixed Radio Systems; Characteristics and requirements for point to-point equipment and antennas; Part 2: Digital systems operating in frequency bands from 1 GHz to 86 GHz; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU", EN 302 217-2 V3.1.1, May 2017.

### 8.2. Informative References

- [NMDA] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., Wilton, R. "Network Management Datastore Architecture", draft-ietf-netmod-revised-datastores-05 (work in progress), October 2017.
- [I-D.ahlberg-ccamp-microwave-radio-link] Ahlberg, J., Carlson, J., Lund, H., Olausson, T., Ye, M., and M. Vaupotic, "Microwave Radio Link YANG Data Models", draft-ahlberg-ccamp-microwave-radio-link-01 (work in progress), May 2016.
- [I-D.ietf-ccamp-microwave-framework] Ahlberg, J., Contreras, L., Ye, M., Vaupotic, M., Tantsura, J., Kawada, K., Li, X., Akiyoshi, I., C. Bernardos, and D. Spreafico, "A framework for Management and Control of microwave and millimeter wave interface parameters", draft-ietf-ccamp-microwave-framework-02 (work in progress), October 2017.
- [ONF-model] "Microwave Modeling - ONF Wireless Transport Group", May 2016.
- [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, <<http://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, <<http://www.rfc-editor.org/info/rfc6242>>.
- [RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <<http://www.rfc-editor.org/info/rfc6536>>.

## Authors' Addresses

Jonas Ahlberg  
Ericsson AB  
Lindholmspiren 11  
Goeteborg 417 56  
Sweden

Email: [jonas.ahlberg@ericsson.com](mailto:jonas.ahlberg@ericsson.com)

Ye Min  
Huawei Technologies  
No.1899, Xiyuan Avenue  
Chengdu 611731  
P.R.China

Email: [amy.yemin@huawei.com](mailto:amy.yemin@huawei.com)

Xi Li  
NEC Laboratories Europe  
Kurfursten-Anlage 36  
Heidelberg 69115  
Germany

Email: [Xi.Li@neclab.eu](mailto:Xi.Li@neclab.eu)

Koji Kawada  
NEC Corporation  
1753, Shimonumabe Nakahara-ku  
Kawasaki, Kanagawa 211-8666  
Japan

Email: [k-kawada@ah.jp.nec.com](mailto:k-kawada@ah.jp.nec.com)

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain

Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)

Daniela Spreafico  
Nokia - IT  
Via Energy Park, 14  
Vimercate (MI) 20871  
Italy

Email: [daniela.spreafico@nokia.com](mailto:daniela.spreafico@nokia.com)

Marko Vaupotic  
Aviat Networks  
Motnica 9  
Trzin-Ljubljana 1236  
Slovenia

Email: [Marko.Vaupotic@Aviatnet.com](mailto:Marko.Vaupotic@Aviatnet.com)

CCAMP Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2018

H. Zheng  
Z. Fan  
Huawei Technologies  
A. Sharma  
Google  
X. Liu  
Jabil  
S. Belotti  
Nokia  
Y. Xu  
CAICT  
L. Wang  
China Mobile  
O. Gonzalez de Dios  
Telefonica  
October 30, 2017

A YANG Data Model for Optical Transport Network Topology  
draft-ietf-ccamp-otn-topo-yang-02

Abstract

A transport network is a server-layer network designed to provide connectivity services for a client-layer network to carry the client traffic transparently across the server-layer network resources. A transport network can be constructed from equipments utilizing any of a number of different transport technologies such as the evolving Optical Transport Networks (OTN) or packet transport as provided by the MPLS-Transport Profile (MPLS-TP).

This document describes a YANG data model to describe the topologies of an Optical Transport Network (OTN). It is independent of control plane protocols and captures topological and resource related information pertaining to OTN. This model enables clients, which interact with a transport domain controller via a REST interface, for OTN topology related operations such as obtaining the relevant topology resource information.

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 May 3, 2018.

#### Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

#### Table of Contents

1. Introduction . . . . .	2
2. Terminology and Notations . . . . .	3
3. YANG Data Model for OTN Topology . . . . .	4
3.1. the YANG Tree . . . . .	4
3.2. Explanation of the OTN Topology Data Model . . . . .	4
3.3. The YANG Code . . . . .	5
4. IANA Considerations . . . . .	9
5. Manageability Considerations . . . . .	9
6. Security Considerations . . . . .	9
7. Acknowledgements . . . . .	10
8. Contributors . . . . .	10
9. References . . . . .	10
9.1. Normative References . . . . .	10
9.2. Informative References . . . . .	11
Authors' Addresses . . . . .	12

#### 1. Introduction

A transport network is a server-layer network designed to provide connectivity services for a client-layer network to carry the client traffic transparently across the server-layer network resources. A transport network can be constructed of equipments utilizing any of a number of different transport technologies such as the Optical

Transport Networks (OTN) or packet transport as provided by the MPLS-Transport Profile (MPLS-TP).

This document defines a data model of an OTN network topology, using YANG [RFC7950]. The model can be used by an application exposing to a transport controller via a REST interface. Furthermore, it can be used by an application for the following purposes (but not limited to):

- o To obtain a whole view of the network topology information of its interest;
- o To receive notifications with regard to the information change of the OTN topology;
- o To enforce the establishment and update of a network topology with the characteristic specified in the data model, e.g., by a client controller;

The YANG model defined in this document is independent of control plane protocols and captures topology related information pertaining to an Optical Transport Networks (OTN)-electrical layer, as the scope specified by [RFC7062] and [RFC7138]. Furthermore, it is not a stand-alone model, but augmenting from the TE topology YANG model defined in [I-D.ietf-teas-yang-te-topol]. Following TE topology YANG model, the YANG model defined in this document is interface independent. The applicability of models to interfaces is described in [I-D.zhang-teas-actn-yang].

Optical network technologies, including fixed Dense Wavelength Switched Optical Network (WSON) and flexible optical networks (a.k.a., flexi-grid networks), are covered in [I-D.ietf-ccamp-wson-yang] and [I-D.vergara-ccamp-flexigrid-yang], respectively.

## 2. Terminology and Notations

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in the YANG data tree presented later in this document is defined in [I-D.ietf-netmod-yang-tree-diagrams]. They are provided below for reference.

- o Brackets "[" and "]" enclose list keys.
- o Abbreviations before data node names: "rw" means configuration (read-write) and "ro" state data (read-only).

- o Symbols after data node names: "?" means an optional node, "!" means a presence container, and "\*" denotes a list and leaf-list.
- o Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- o Ellipsis ("...") stands for contents of subtrees that are not shown.

### 3. YANG Data Model for OTN Topology

#### 3.1. the YANG Tree

```

module: ietf-otn-topology
  augment /nw:networks/nw:network/nw:network-types/tet:te-topology:
    +--rw otn-topology!
  augment /nw:networks/nw:network/nt:link/tet:te
    /tet:te-link-attributes:
      +--rw available-odu-info* [priority]
      |   +--rw priority      uint8
      |   +--rw odulist* [odu-type]
      |   |   +--rw odu-type      identityref
      |   |   +--rw number?      uint16
      |   |   +--rw tpn-range?   string
      |   +--rw ts-range?      string
      +--rw tsg?                identityref
      +--rw distance?           uint32
  augment /nw:networks/nw:network/nw:node/nt:termination-point
    /tet:te:
      +--rw supported-payload-types* [index]
      |   +--rw index          uint16
      |   +--rw payload-type?  string

```

#### 3.2. Explanation of the OTN Topology Data Model

As can be seen, from the data tree shown in Section 3.1, the YANG module presented in this document augments from a more generic Traffic Engineered (TE) network topology data model, i.e., the `ietf-te-topology.yang` as specified in [I-D.ietf-teas-yang-te-topo]. The entities and their attributes, such as node, termination points and links, are still applicable for describing an OTN topology and the model presented in this document only specifies with technology-specific attributes/information. For example, if the data plane complies with ITU-T G.709 (2012) standards, the switching-capability

and encoding attributes MUST be filled as OTN-TDM and G.709 ODUk(Digital Path) respectively.

Note the model in this document re-uses some attributes defined in `ietf-transport-types.yang`, which is specified in [I-D.ietf-ccamp-otn-tunnel-model].

One of the main augmentations in this model is that it allows to specify the type of ODU container and the number a link can support per priority level. For example, for a ODU3 link, it may advertise 32\*ODU0, 16\*ODU1, 4\*ODU2 available, assuming only a single priority level is supported. If one of ODU2 resource is taken to establish a ODU path, then the availability of this ODU link is updated as 24\*ODU0, 12\*ODU1, 3\*ODU2 available. If there are equipment hardware limitations, then a subset of potential ODU type SHALL be advertised. For instance, an ODU3 link may only support 4\*ODU2.

### 3.3. The YANG Code

```
<CODE BEGINS> file "ietf-otn-topology@2017-10-30.yang"

module ietf-otn-topology {
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-otn-topology";
  prefix "otntopo";

  import ietf-network {
    prefix "nw";
  }

  import ietf-network-topology {
    prefix "nt";
  }

  import ietf-te-topology {
    prefix "tet";
  }

  import ietf-otn-types {
    prefix "otn-types";
  }

  organization
    "IETF CCAMP Working Group";
  contact
    "WG Web: <http://tools.ietf.org/wg/ccamp/>
```

WG List: <mailto:ccamp@ietf.org>

Editor: Haomian Zheng  
<mailto:zhenghaomian@huawei.com>

Editor: Zheyu Fan  
<mailto:fanzheyu2@huawei.com>

Editor: Anurag Sharma  
<mailto:ansha@google.com>

Editor: Xufeng Liu  
<mailto:Xufeng\_Liu@jabil.com>

Editor: Sergio Belotti  
<mailto:sergio.belotti@nokia.com>

Editor: Yunbin Xu  
<mailto:xuyunbin@ritt.cn>

Editor: Lei Wang  
<mailto:wangleiyj@chinamobile.com>

Editor: Oscar Gonzalez de Dios  
<mailto:oscar.gonzalezdedios@telefonica.com>;

description

"This module defines a protocol independent Layer 1/ODU topology data model.";

```
revision 2017-10-30 {  
  description  
    "Revision 0.5";  
  reference  
    "draft-ietf-ccamp-otn-topo-yang-02.txt";  
}
```

```
/*  
 * Groupings  
 */  
grouping otn-link-attributes {  
  description "link attributes for OTN";  
  
  list available-odu-info {  
    key "priority";  
    max-elements "8";  
    description "List of ODU type and number on this link";  
    leaf priority {
```



```

    type uint8 {
        range "0..7";
    }
    description "priority";
}
list odulist {
    key "odu-type";
    description
        "the list of available ODUs per priority level";
    leaf odu-type {
        type identityref {
            base otn-types:tributary-protocol-type;
        }
        description "the type of ODU";
    }
    leaf number {
        type uint16;
        description "the number of odu type supported";
    }
    leaf tpn-range {
        type string {
            pattern "([1-9][0-9]{0,3}(-[1-9][0-9]{0,3})?"
                + "(, [1-9][0-9]{0,3}(-[1-9][0-9]{0,3})?)*)";
        }
        description
            "A list of available tributary port number range
            between 1 and 9999.
            For example 1-20,25,50-1000";
        reference "RFC 7139: GMPLS Signaling Extensions for Control
            of Evolving G.709 Optical Transport Networks";
    }
}
leaf ts-range {
    type string {
        pattern "([1-9][0-9]{0,3}(-[1-9][0-9]{0,3})?"
            + "(, [1-9][0-9]{0,3}(-[1-9][0-9]{0,3})?)*)";
    }
    description
        "A list of available tributary slot range
        between 1 and 9999.
        For example 1-20,25,50-1000";
    reference "RFC 7139: GMPLS Signaling Extensions for Control
        of Evolving G.709 Optical Transport Networks";
}
}
leaf tsgr {
    type identityref {
        base otn-types:tributary-slot-granularity;
    }
}

```

```

    }
    description "Tributary slot granularity.";
    reference
      "G.709/Y.1331, February 2016: Interfaces for the
      Optical Transport Network (OTN)";
  }
  leaf distance {
    type uint32;
    description "distance in the unit of kilometers";
  }
}

grouping otn-tp-attributes {
  description "tp attributes for OTN";
  list supported-payload-types {
    key "index";
    description
      "Supported payload types of a TP. The payload type is defined
      as the generalized PIDs in GMPLS.";
    leaf index {
      type uint16;
      description "payload type index";
    }
    leaf payload-type {
      type string;
      description "the payload type supported by this client tp";
      reference
        "http://www.iana.org/assignments/gmpls-sig-parameters
        /gmpls-sig-parameters.xhtml";
    }
  }
}

/*
 * Data nodes
 */
augment "/nw:networks/nw:network/nw:network-types/"
  + "tet:te-topology" {
  container otn-topology {
    presence "indicates a topology type of Optical Transport
    Network (OTN)-electrical layer.";
    description "otn topology type";
  }
  description "augment network types to include otn newtork";
}

augment "/nw:networks/nw:network/nt:link/tet:te/"
  + "tet:te-link-attributes" {

```

```
    when "../../../nw:network-types/tet:te-topology/"
      + "otntopo:otn-topology" {
      description "Augment only for otn network.";
    }
    description "Augment link configuration";
    uses otn-link-attributes;
  }

  augment "/nw:networks/nw:network/nw:node/nt:termination-point/"
    + "tet:te" {
    when "../../../nw:network-types/tet:te-topology/"
      + "otntopo:otn-topology" {
      description "Augment only for otn network";
    }
    description "OTN TP attributes config in ODU topology.";
    uses otn-tp-attributes;
  }
}
```

<CODE ENDS>

#### 4. IANA Considerations

TBD.

#### 5. Manageability Considerations

TBD.

#### 6. Security Considerations

The data following the model defined in this document is exchanged via, for example, the interface between an orchestrator and a transport network controller. The security concerns mentioned in [I-D.ietf-teas-yang-te-topo] for using ietf-te-topology.yang model also applies to this document.

The YANG module defined in this document can be accessed via the RESTCONF protocol defined in [RFC8040], or maybe via the NETCONF protocol [RFC6241].

There are a number of data nodes defined in the YANG module which are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., POST) to these data nodes without proper protection can have a negative effect on network operations.

Editors note: to list specific subtrees and data nodes and their sensitivity/vulnerability.

## 7. Acknowledgements

We would like to thank Igor Bryskin, Zhe Liu, and Daniele Ceccarelli for their comments and discussions.

## 8. Contributors

Baoquan Rao  
Huawei Technologies  
Email: raobaoquan@huawei.com

Xian Zhang  
Huawei Technologies  
Email: zhang.xian@huawei.com

Huub van Helvoort  
Hai Gaoming BV  
the Netherlands  
Email: huubatwork@gmail.com

Victor Lopez  
Telefonica  
Email: victor.lopezalvarez@telefonica.com

Yunbo Li  
China Mobile  
Email: liyunbo@chinamobile.com

Dieter Beller  
Nokia  
Email: dieter.beller@nokia.com

Yanlei Zheng  
China Unicom  
Email: zhengyl@dimpt.com

## 9. References

### 9.1. Normative References

[I-D.ietf-ccamp-otn-tunnel-model]  
zhenghaomian@huawei.com, z., Fan, Z., Sharma, A., Rao, R., Belotti, S., Lopezalvarez, V., and Y. Li, "OTN Tunnel YANG Model", draft-ietf-ccamp-otn-tunnel-model-00 (work in progress), July 2017.

- [I-D.ietf-teas-yang-te-topo]  
Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Dios, "YANG Data Model for Traffic Engineering (TE) Topologies", draft-ietf-teas-yang-te-topo-13 (work in progress), October 2017.
- [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>>.
- [RFC7138] Ceccarelli, D., Ed., Zhang, F., Belotti, S., Rao, R., and J. Drake, "Traffic Engineering Extensions to OSPF for GMPLS Control of Evolving G.709 Optical Transport Networks", RFC 7138, DOI 10.17487/RFC7138, March 2014, <<https://www.rfc-editor.org/info/rfc7138>>.
- [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>>.
- [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>>.

## 9.2. Informative References

- [I-D.ietf-ccamp-wson-yang]  
Lee, Y., Dhody, D., Zhang, X., Guo, A., Lopezalvarez, V., King, D., Yoon, B., and R. Vilata, "A Yang Data Model for WSON Optical Networks", draft-ietf-ccamp-wson-yang-08 (work in progress), October 2017.
- [I-D.ietf-netmod-yang-tree-diagrams]  
Bjorklund, M. and L. Berger, "YANG Tree Diagrams", draft-ietf-netmod-yang-tree-diagrams-02 (work in progress), October 2017.
- [I-D.vergara-ccamp-flexigrid-yang]  
Madrid, U., Perdices, D., Lopezalvarez, V., Dios, O., King, D., Lee, Y., and G. Galimberti, "YANG data model for Flexi-Grid Optical Networks", draft-vergara-ccamp-flexigrid-yang-05 (work in progress), July 2017.

[I-D.zhang-teas-actn-yang]

Lee, Y., zhenghaomian@huawei.com, z., Yoon, B., Dios, O., Shin, J., and S. Belotti, "Applicability of YANG models for Abstraction and Control of Traffic Engineered Networks", draft-zhang-teas-actn-yang-05 (work in progress), June 2017.

[RFC7062] Zhang, F., Ed., Li, D., Li, H., Belotti, S., and D. Ceccarelli, "Framework for GMPLS and PCE Control of G.709 Optical Transport Networks", RFC 7062, DOI 10.17487/RFC7062, November 2013, <<https://www.rfc-editor.org/info/rfc7062>>.

#### Authors' Addresses

Haomian Zheng  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base, Bantian, Longgang District  
Shenzhen, Guangdong 518129  
P.R.China

Email: zhenghaomian@huawei.com

Zheyu Fan  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base, Bantian, Longgang District  
Shenzhen, Guangdong 518129  
P.R.China

Email: fanzheyu2@huawei.com

Anurag Sharma  
Google  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Email: ansha@google.com

Xufeng Liu  
Jabil

Email: Xufeng\_Liu@jabil.com

Sergio Belotti  
Nokia

Email: [sergio.belotti@nokia.com](mailto:sergio.belotti@nokia.com)

Yunbin Xu  
CAICT

Email: [xuyunbin@rict.cn](mailto:xuyunbin@rict.cn)

Lei Wang  
China Mobile

Email: [wangleiyj@chinamobile.com](mailto:wangleiyj@chinamobile.com)

Oscar Gonzalez de Dios  
Telefonica

Email: [oscar.gonzalezdedios@telefonica.com](mailto:oscar.gonzalezdedios@telefonica.com)

CCAMP Working Group

Internet Draft

Intended status: Standard Track

Y. Lee (Editor)

D. Dhody

X. Zhang

A. Guo

Huawei

V. Lopez

Telefonica

D. King

U. of Lancaster

B. Yoon

ETRI

Ricard Vilalta

CTTC

Expires: April 8, 2018

October 9, 2017

## A Yang Data Model for WSON Optical Networks

draft-ietf-ccamp-wson-yang-08.txt

### Abstract

This document provides a YANG data model for the routing and wavelength assignment (RWA) TE topology in wavelength switched optical networks (WSONs).

### Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>



The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on April 8, 2018.

#### Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

#### Table of Contents

1. Introduction.....	2
2. YANG Model (Tree Structure).....	3
3. IETF-WSN-Topology YANG Model.....	4
4. IETF-TE-WSN-Types YANG Model.....	12
5. Security Considerations.....	14
6. IANA Considerations.....	15
7. Acknowledgments.....	15
8. References.....	16
8.1. Normative References.....	16
8.2. Informative References.....	16
9. Contributors.....	16
Authors' Addresses.....	16

#### 1. Introduction

This document provides a YANG data model for the routing and wavelength assignment (RWA) Traffic Engineering (TE) topology in wavelength switched optical networks (WSNs). The YANG model described in this document is a WSON technology-specific Yang model based on the information model developed in [RFC7446] and the two

encoding documents [RFC7581] and [RFC7579] that developed protocol independent encodings based on [RFC7446]. This document augments the the generic TE topology draft [TE-TOPO].

What is not in scope of this document is both impairment-aware WSON and flex-grid.

This document defines two YANG models: ietf-wson-topology (Section 3) and ietf-te-wson-types (Section 4).

## 2. YANG Model (Tree Structure)

```

module: ietf-wson-topology
  augment /nd:networks/nd:network/nd:network-types/tet:te-topology:
    +-rw wson-topology!
  augment /nd:networks/nd:network/nd:node/tet:te/tet:config/tet:te-node-
attributes/tet:connectivity-matrices/tet:connectivity-matrix:
    +-rw wavelength-availability-range?   te-wson-types:wavelength-range-type
  augment /nd:networks/nd:network/nd:node/tet:te/tet:state/tet:te-node-
attributes/tet:connectivity-matrices/tet:connectivity-matrix:
    +-ro wavelength-availability-range?   te-wson-types:wavelength-range-type
  augment /nd:networks/nd:network/lnk:link/tet:te/tet:config/tet:te-link-attri-
butes:
    +-rw channel-num?                     int32
    +-rw first-channel-frequency?          decimal64
    +-rw channel-spacing?                  decimal64
    +-rw available-wavelength-info* [priority]
      +-rw priority                        uint8
      +-rw wavelength-availability-range? te-wson-types:wavelength-range-typ
e
  augment /nd:networks/nd:network/lnk:link/tet:te/tet:state/tet:te-link-attri-
butes:
    +-ro channel-num?                     int32
    +-ro first-channel-frequency?          decimal64
    +-ro channel-spacing?                  decimal64
    +-ro available-wavelength-info* [priority]
      +-ro priority                        uint8
      +-ro wavelength-availability-range? te-wson-types:wavelength-range-typ
e
  augment /nd:networks/nd:network/nd:node/tet:te/tet:config/tet:te-node-attri-
butes:
    +-rw wson-node
      +-rw node-type? identityref
  augment /nd:networks/nd:network/nd:node/tet:te/tet:state/tet:te-node-attri-
butes:
    +-ro wson-node
      +-ro node-type? identityref
  augment /nd:networks/nd:network/nd:node/tet:te/tet:tunnel-termination-
point/tet:config:
    +-rw available-operational-mode*      te-wson-types:operational-mode
    +-rw operational-mode?                 te-wson-types:operational-mode
  augment /nd:networks/nd:network/nd:node/tet:te/tet:tunnel-termination-
point/tet:state:
    +-ro available-operational-mode*      te-wson-types:operational-mode

```

+-ro operational-mode?

te-wson-types:operational-mode

### 3. IETF-WSON-Topology YANG Model

```
<CODE BEGINS> file "ietf-wson-topology@2017-10-09.yang"

module ietf-wson-topology {
  //TODO: FIXME
  //yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-wson-topology";

  prefix "wson";

  import ietf-network {
    prefix "nd";
  }

  import ietf-network-topology {
    prefix "lnk";
  }

  import ietf-inet-types {
    prefix "inet";
  }

  import ietf-te-topology {
    prefix "tet";
  }
}
```

```
import ietf-te-wson-types { //Modified
prefix "te-wson-types";
}

//NOT NEEDED
/*import ietf-transport-types {
prefix "tran-types";
} */

organization
    "IETF CCAMP Working Group";

contact
    "Editor:    Young Lee  <leeyoung@huawei.com>";

description
    "This module contains a collection of YANG definitions
for
    RWA WSON.

    Copyright (c) 2016 IETF Trust and the persons identified
as
    authors of the code.  All rights reserved.

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

revision 2017-10-09 {
    description
        "version 8.";

    reference
        "RFC XXX: A Yang Data Model for WSON Optical
Networks ";
```

```
}

typedef wson-topology-id {
    type inet:uri;
    description
        "The WSON Topology ID";
}

grouping wson-topology-type {
    description "wson-topology type";
    container wson-topology {
        presence "indicates a topology of wson";
        description
            "Container to identify wson topology type";
    }
}

grouping wson-node-attributes {
    description "WSOON node attributes";
    container wson-node {
        description "WSOON node attributes.";
        leaf node-type {
            type identityref {
                base te-wson-types:wson-node-type;
            }
            description "WSOON node type.";
        }
    }
}

grouping wson-wavelength-availability-range{
    description "wavelength availability range";

    leaf wavelength-availability-range{
        type te-wson-types:wavelength-range-type;
        description
            "range that indicates if a wavelength is
            available or not on each channel at
            specified priority level.";
    }
}
```

```

    grouping wson-link-attributes {
      description "WSON link attributes";
      leaf channel-num {
        type int32;
        description "Number of OCh channels available";
      }
      leaf first-channel-frequency {
        type decimal64 {
          fraction-digits 5;
        }
        units THz;
        description "First channel frequency in the grid";
      }
      leaf channel-spacing {
        type decimal64 {
          fraction-digits 5;
        }
        units GHz;
        description "This is fixed channel spacing for
WSON,
e.g, 12.5, 25, 50, 100, ..";
      }
      list available-wavelength-info{
        key "priority";
        max-elements "8";

        description
this link";
          "List of available wavelength channels on

        leaf priority {
          type uint8 {
            range "0..7";
          }
          description "priority";
        }
        uses wson-wavelength-availability-range;
      }
    }
  }

```

```
    grouping wson-tp-attributes {
      description "wson-tp-attributes";

      leaf client-facing {
        type empty;
        description
          "if present, it means this tp is a client-
facing tp.
          adding/dropping client signal flow.";
      }

      /*
      //can it be fully covered by interface-switching-capability of base
      TE model?
      leaf-list supported-client-signals {
        type identityref {
          base tran-types:client-signal;
        }
        description
          "Supported client signals at this TP";
      }
      */
    }

    grouping wson-ttp-attributes {
      description "WSON tunnel termination point (e.g.
tranponder)
      attributes";
      leaf-list available-operational-mode {
        type te-wson-types:operational-mode;
        description "List of all vendor-specific supported
mode identifiers";
      }

      leaf operational-mode {
        type te-wson-types:operational-mode;
        description "Vendor-specific mode identifier";
      }
    }
```

```

/* AUGMENTS */

augment "/nd:networks/nd:network/nd:network-types"
  + "/tet:te-topology" {
    description "wson-topology augmented";
    uses wson-topology-type;
  }

//FIXING NMDA
augment "/nd:networks/nd:network/nd:node/tet:te"
  + "/tet:te-node-attributes/tet:connectivity-matrices"
  + "/tet:connectivity-matrix" {
    when "/nd:networks/nd:network/nd:network-types"
      + "/tet:te-topology/wson:wson-topology" {
      description
        "This augment is only valid for WSON
connectivity
matrix.";
    }
    description "WSON connectivity matrix config
augmentation";
    uses wson-wavelength-availability-range;
  }

//REMOVING
/*
augment "/nd:networks/nd:network/nd:node/tet:te/tet:state"
  + "/tet:te-node-attributes/tet:connectivity-matrices"
  + "/tet:connectivity-matrix" {
    when "/nd:networks/nd:network/nd:network-types"
      + "/tet:te-topology/wson-topology" {
      description
        "This augment is only valid for WSON
connectivity
matrix.";
    }
    description "WSON connectivity matrix state augmentation";
    uses wson-wavelength-availability-range;
  }*/

//FIXING NMDA

```



```
augment "/nd:networks/nd:network/lnk:link/tet:te"
  + "/tet:te-link-attributes" {
  when "/nd:networks/nd:network/nd:network-types"
    + "/tet:te-topology/wson:wson-topology" {
    description
      "This augment is only valid for WSON.";
  }
  description "WSON Link augmentation.";

  uses wson-link-attributes;
}

//REMOVING
/*
augment "/nd:networks/nd:network/lnk:link/tet:te/tet:state"
  + "/tet:te-link-attributes" {
  when "/nd:networks/nd:network/nd:network-types"
    + "/tet:te-topology/wson:wson-topology" {
    description
      "This augment is only valid for WSON.";
  }
  description "WSON Link augmentation.";

  uses wson-link-attributes;
}*/

//FIXING NMDA
augment "/nd:networks/nd:network/nd:node/tet:te"
  + "/tet:te-node-attributes" {
  when "/nd:networks/nd:network/nd:network-types"
    + "/tet:te-topology/wson:wson-topology" {
    description
      "This augment is only valid for WSON.";
  }
  description "WSON Node augmentation.";

  uses wson-node-attributes;
}

//REMOVING
/*
```

```
augment "/nd:networks/nd:network/nd:node/tet:te/tet:state"
  + "/tet:te-node-attributes" {
    when "/nd:networks/nd:network/nd:network-types"
      + "/tet:te-topology/wson:wson-topology" {
      description
        "This augment is only valid for WSON.";
    }
    description "WSON Node augmentation.";

    uses wson-node-attributes;
  }*/

//FIXING NMDA
augment "/nd:networks/nd:network/nd:node/tet:te"
  + "/tet:tunnel-termination-point" {
    when "/nd:networks/nd:network/nd:network-types"
      + "/tet:te-topology/wson:wson-topology" {
      description
        "This augment is only valid for WSON.";
    }
    description "WSON tunnel termination point
augmentation.";

    uses wson-ttp-attributes;
  }

//removing
/*augment "/nd:networks/nd:network/nd:node/tet:te"
  + "/tet:tunnel-termination-point/tet:state" {
    when "/nd:networks/nd:network/nd:network-types"
      + "/tet:te-topology/wson:wson-topology" {
      description
        "This augment is only valid for WSON.";
    }
    description "WSON tunnel termination point
augmentation.";

    uses wson-ttp-attributes;
  }*/
```

```
}  
<CODE ENDS>
```

#### 4. IETF-TE-WSON-Types YANG Model

```
<CODE BEGINS> file "ietf-te-wson-types@2017-10-09.yang"  
  module ietf-te-wson-types {  
    namespace "urn:ietf:params:xml:ns:yang:ietf-te-wson-types";  
    prefix "te-wson-types";  
  
    organization  
      "IETF CCAMP Working Group";  
    contact  
      "WG Web: <http://tools.ietf.org/wg/ccamp/>  
      WG List: <mailto:ccamp@ietf.org>  
  
      Editor: Aihua Guo  
        <mailto:aihuaguo@huawei.com>  
  
      Editor: Young Lee  
        <mailto:leeyoung@huawei.com>";  
  
    description  
      "This module defines WSON types.";  
  
    revision "2017-10-09" {  
      description  
        "Revision 0.1";  
      reference "TBD";  
    }  
  
    typedef operational-mode {  
      type string;  
      description  
        "Vendor-specific mode that guarantees interoperability.  
        It must be an string with the following format:  
        B-DSw-ytz(v) where all these attributes are conformant  
        to the ITU-T recommendation";  
      reference "ITU-T G.698.2 (11/2009) Section 5.3";  
    }
```

```
identity wson-node-type {
    description
        "WSON node type.";
    reference
        "";
}

identity wson-node-foadm {
    base wson-node-type;
    description
        "Fixed OADM node.";
}

identity wson-node-roadm {
    base wson-node-type;
    description
        "ROADM or OXC node.";
}

identity wson-node-ila {
    base wson-node-type;
    description
        "ILA (In-Line Amplifier) node.";
}

//ADDED
typedef wavelength-range-type {
    type string {
        pattern "([1-9][0-9]{0,3}(-[1-9][0-9]{0,3})?" +
            "(,[1-9][0-9]{0,3}(-[1-9][0-9]{0,3})?)*)";
    }
    description
        "A list of WDM channel numbers (starting at 1)
        in ascending order. For example: 1,12-20,40,50-80";
}

identity wavelength-assignment {
    description "Wavelength selection base";
}
```

```
identity unspecified-wavelength-assignment {
    base wavelength-assignment;
    description "No method specified";
}

identity first-fit-wavelength-assignment {
    base wavelength-assignment;
    description "All the available wavelengths are numbered,
        and this WA method chooses the available wavelength
        with the lowest index.";
}

identity random-wavelength-assignment {
    base wavelength-assignment;
    description "This WA method chooses an available
        wavelength randomly.";
}

identity least-loaded-wavelength-assignment {
    base wavelength-assignment;
    description "This WA method selects the wavelength that
        has the largest residual capacity on the most loaded
        link along the route (in multi-fiber networks).";
}

}
```

<CODE ENDS>

## 5. Security Considerations

TDB

## 6. IANA Considerations

TDB

## 7. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

## 8. References

### 8.1. Normative References

[TE-TOPO] X. Liu, et al., "YANG Data Model for TE Topologies", work in progress: draft-ietf-teas-yang-te-topo.

### 8.2. Informative References

[RFC7446] Y. Lee, G. Bernstein, D. Li, W. Imajuku, "Routing and Wavelength Assignment Information Model for Wavelength Switched Optical Networks", RFC 7446, February 2015.

[RFC7579] G. Bernstein, Y. Lee, D. Li, W. Imajuku, "General Network Element Constraint Encoding for GMPLS Controlled Networks", RFC 7579, June 2015.

[RFC7581] G. Bernstein, Y. Lee, D. Li, W. Imajuku, "Routing and Wavelength Assignment Information Encoding for Wavelength Switched Optical Networks", RFC 7581, June 2015.

## 9. Contributors

### Authors' Addresses

Young Lee (ed.)  
Huawei Technologies  
5340 Legacy Drive, Building 3  
Plano, TX 75023  
USA

Phone: (469) 277-5838  
Email: leeyoung@huawei.com

Dhruv Dhody  
Huawei Technologies India Pvt. Ltd,  
Near EPIP Industrial Area, Kundalahalli Village, Whitefield,  
Bangalore - 560 037 [H1-2A-245]

Email: dhruv.dhody@huawei.com

Xian Zhang  
Huawei Technologies

Email: zhang.xian@huawei.com

Aihua Guo  
Huawei Technologies  
Email: aihuaguo@huawei.com

Victor Lopez  
Telefonica  
Email: victor.lopezalvarez@telefonica.com

Daniel King  
University of Lancaster  
Email: d.king@lancaster.ac.uk

Bin Yeong Yoon  
ETRI  
218 Gaijeongro, Yuseong-gu  
Daejeon, Korea  
Email: byyun@etri.re.kr

Ricard Vilalta  
CTTC  
Email: ricard.vilalta@cttc.es





Common Control and Measurement Plane  
Internet-Draft  
Intended status: Informational  
Expires: May 3, 2018

I. Hussain  
R. Valiveti  
Infinera Corp  
Q. Wang  
ZTE  
L. Andersson  
M. Chen  
H. Zheng  
Huawei  
October 30, 2017

GMPLS Routing and Signaling Framework for Flexible Ethernet (FlexE)  
draft-izh-ccamp-flex-e-fwk-04

Abstract

This document specifies GMPLS control plane requirements, framework, and architecture for FlexE technology.

As different from earlier Ethernet data planes FlexE allows for decoupling of the Ethernet Physical layer (PHY) and Media Access Control layer (MAC) rates.

Study Group 15 (SG15) of the ITU-T has endorsed the FlexE Implementation Agreement from Optical Networking Forum (OIF) and included it, by reference, in some of their Recommendations.

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 May 3, 2018.

## Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
1.1. Requirements Language . . . . .	4
2. Terminology . . . . .	4
3. FlexE Reference Model . . . . .	5
4. Requirements . . . . .	6
5. GMPLS Controlled FlexE . . . . .	7
5.1. Types of LSPs in a FlexE capable network . . . . .	8
5.2. Signaling Channel . . . . .	8
5.3. MPLS LSP in the FlexE Data Plane . . . . .	8
5.4. Configuring the data plane in FlexE capable nodes . . . . .	10
5.4.1. Configure/Establish a FlexE Group/Link . . . . .	10
5.4.2. Configure/Establish a FlexE Client . . . . .	11
5.4.3. Advertise FlexE Groups and FlexE lts . . . . .	11
6. Framework and Architecture . . . . .	11
6.1. FlexE Framework . . . . .	12
6.2. FlexE Architecture . . . . .	12
6.2.1. Architecture Components . . . . .	12
6.2.2. FlexE Layer Model . . . . .	12
6.2.2.1. FlexE Group structure . . . . .	13
6.2.2.2. FlexE Client mapping . . . . .	13
7. Control Plane . . . . .	13
7.1. GMPLS Routing . . . . .	14
7.2. GMPLS Signaling . . . . .	14
7.2.1. LSP setup with pre-configured FlexE infrastructure . . . . .	15
7.2.2. LSP setup with partially configured FlexE infrastructure . . . . .	16
7.2.3. LSP setup with non-configured FlexE infrastructure . . . . .	17
7.2.4. Packet Label Switching Data Plane . . . . .	17
8. Operations, Administration, and Maintenance (OAM) . . . . .	19
9. Acknowledgements . . . . .	19
10. IANA Considerations . . . . .	19

11. Security Considerations . . . . .	19
12. Contributors . . . . .	19
13. References . . . . .	19
13.1. Normative References . . . . .	19
13.2. Informative References . . . . .	20
Authors' Addresses . . . . .	21

## 1. Introduction

Ethernet MAC rates were until recently constrained to match the rates of the Ethernet PHY(s). Work within the OIF allows MAC rates to be different from PHY rates. An OIF implementation agreement [OIFFLEXE1] allows for complete decoupling of the MAC and PHY rates.

SG15 in ITU-T has endorsed the OIF FlexE data plane and parts of [G.872], [G.709], [G.798] and [G.8021] depends on or are based on the FlexE data plane.

This includes support for:

- a. MAC rates which are greater than the rate of a single PHY; multiple PHYs are bonded to achieve this
- b. MAC rates which are less than the rate of a PHY (sub-rate)
- c. support for channelization within a single PHY, or over a group of bonded PHYs.

The capabilities supported by the first version of the FlexE data plane are:

- a. Support a large rate Ethernet MAC over bonded Ethernet PHYs, e.g. supporting a 200G MAC over 2 bonded 100GBASE-R PHY(s)
- b. Support a sub-rate Ethernet MAC over a single Ethernet PHY, e.g. supporting a 50G MAC over a 100GBASE-R PHY
- c. Support a collection of flexible Ethernet clients over a single Ethernet PHY, e.g. supporting two MACs with the rates 25G, and one with rate 50G over a single 100GBASE-R PHY
- d. Support a sub-rate Ethernet MAC over bonded PHYs, e.g. supporting a 150G Ethernet client over 2 bonded 100GBASE-R PHY(s)
- e. Support a collection of Ethernet MAC clients over bonded Ethernet PHYs, e.g. supporting a 50G, and 150G MAC over 2 bonded Ethernet PHY(s)

Networks which support FlexE Ethernet interfaces include a basic building block, this is true also when the interfaces are bonded. This building block consists of two FlexE Shim functions, located at opposite ends of a link, and the logical point to point links that carry the Ethernet PHY signals between the two FlexE Shim Functions.

These logical point-to-point links may be realized in a variety of ways:

- a. direct point-to-point links with no intervening transport network.
- b. Ethernet PHY(s) may be transparently transported via an Optical Transport Network (OTN), as defined by ITU-T in [G.709] and [G.798]. The OTN set of client mappings has been extended to support the use cases identified in the OIF FlexE implementation agreement.

This draft considers the variants in which the two peer FlexE devices are both customer-edge devices, or when one is a customer-edge and the other is provider edge devices. This list of use cases will help identify the Control Plane (i.e. Routing and Signaling) extensions that may be required.

### 1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

## 2. Terminology

- a. CE (Customer Edge) - the group of functions that support the termination/origination of data received from or sent to the network
- b. Ethernet PHY: an entity representing Physical Coding Sublayer (PCS), Physical Media Attachment (PMA), and Physical Media Dependent (PMD) layers.
- c. FlexE Calendar: The total capacity of a FlexE Group is represented as a collection of slots which have a granularity of 5G. The calendar for a FlexE Group composed of  $n$  100G PHYs is represented as an array of  $20n$  slots (each representing 5G of bandwidth). This calendar is partitioned into sub-calendars, with 20 slots per 100G PHY. Each FlexE client is mapped into one or more calendar slots (based on the bandwidth the FlexE client flow will need).

- d. FlexE Client: An Ethernet flow based on a MAC data rate that may or may not correspond to any Ethernet PHY rate.
- e. FlexE Group: A FlexE Group is composed of from 1 to n Ethernet PHYs. In the first version of FlexE each PHY is identified by a number in the range {1-254}.
- f. FlexE Shim: the layer that maps or demaps the FlexE client flows carried over a FlexE Group.
- g. LMP: Link Management Protocol
- h. LSP: Label Switched Path
- i. OTN: Optical Transport Network
- j. SG15: ITU-T Study Group 15 (Transport, Access and Home).
- k. TE: Traffic Engineering
- l. TED: Traffic Engineering Database

### 3. FlexE Reference Model

The figure below gives a simplified FlexE reference model.

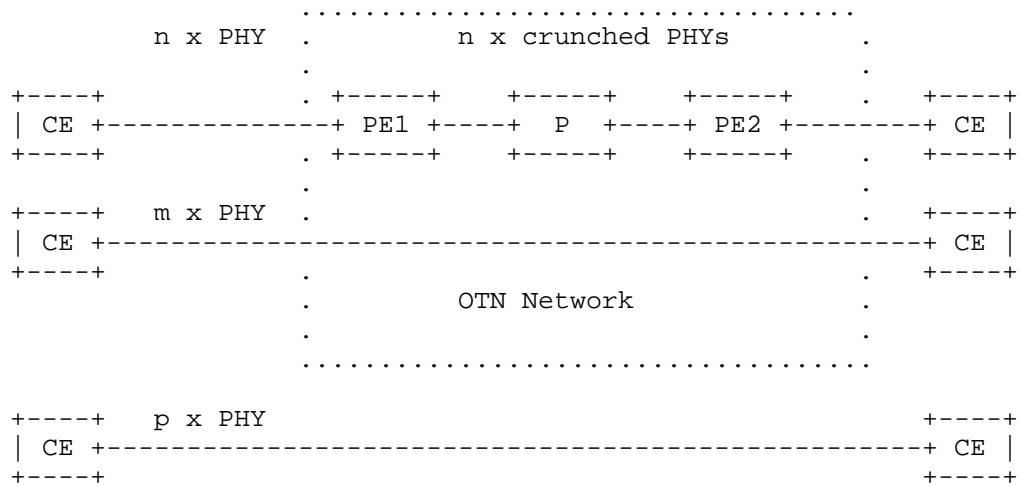


Figure 1: FlexE Reference Model

The services offered by Flexible Ethernet are essentially the same as for traditional Ethernet, connection less Ethernet transport. However, when the relationship between the PHY and MAC layer are setup by a GMPLS control plane there is a strong connection oriented aspect.

#### 4. Requirements

This section summarizes the control plane requirements for FlexE Group and FlexE Client signaling and routing.

- Req-1 The solution SHALL support the creation of a FlexE Group, consisting of one or more (i.e., in the 1 to 254 range) 100GE Ethernet PHY(s).

There are several alternatives that can meet this requirement, e.g. routing and signaling protocols, or a centralized controller/management system with network access to the FlexE mux/demux at each FlexE Group termination point.

- Req-2 The solution SHOULD be able to verify that the collection of Ethernet PHY(s) included in a FlexE Group have the same characteristics (e.g. number of PHYs, rate of PHYs, etc.) at the peer FlexE shims.

- Req-3 The solution SHALL support the ability to delete a FlexE Group.
- Req-4 The solution SHALL support the ability to administratively lock/unlock a FlexE Group.
- Req-5 It SHALL be possible to add/remove PHY(s) to/from an operational FlexE group while the group has been administratively locked.
- Req-6 The solution SHALL support the ability to advertise and discover information about FlexE capable nodes, and the FlexE Groups and FlexE Clients they support.
- Req-7 The system SHALL allow the addition (or removal) of one or more FlexE clients on a FlexE Group. The addition (or removal) of a FlexE client flow SHALL NOT affect the services for the other FlexE client signals.
- Req-8 The system SHALL allow the FlexE client signals to flexibly span the set of Ethernet PHY(s) which comprise the FlexE Group.
- Req-9 The solution SHALL support FlexE client flow resizing without affecting any existing FlexE clients within the same FlexE Group.
- Req-10 The solution SHALL support establishment of MPLS LSPs that requires the support of a FlexE infrastructure.

## 5. GMPLS Controlled FlexE

The high level goals for using a GMPLS control plane for FlexE can be summarized as:

- o Set up a FlexE Group
- o Set up a FlexE Client
- o Advertise FlexE Groups and FlexE Clients
- o Set up of a higher layer LSP that requires to be run over a FlexE infrastructure.



### 5.1. Types of LSPs in a FlexE capable network

The FlexE infrastructure may be established in three different ways

- o The FlexE Groups and FlexE Client may be pre-configured
- o Only the FlexE groups may be pre-configured, while the setup of the FlexE client is triggered by the request to setup a MPLS LSP
- o The setup of both FlexE Group and FlexE Client may be triggered by the request to setup an MPLS LSP.

### 5.2. Signaling Channel

In the type of equipment for which FlexE was first specified an out of band signaling channel is not commonly available. If that is the case, and the GMPLS FlexE control plane will be used, the FlexE Group will have to setup by e.g. a management system and a FlexE Client on that FlexE Group (also configured) will have to allocated as a signaling channel.

Further details of the setup of the FlexE Groups, FlexE Clients and MPLS LSPs over a FlexE infrastructure will be found in Section 7.2.

### 5.3. MPLS LSP in the FlexE Data Plane

FlexE is a true link layer technology, i.e. it is not switched, this means that the FlexE Groups and FlexE Clients are terminated on the next-hop node, and that the switching needs to take place on a higher layer.

The FlexE technology can be used to establish link layer connectivity with high and deterministic bandwidth. However, there is no way to, in a deterministic way, allocate certain traffic to a specific FlexE Client. A GMPLS control plane can do this.

A GMPLS controlled FlexE capable node may be thought of using the traditional model of a node with a separation between control and data plane.

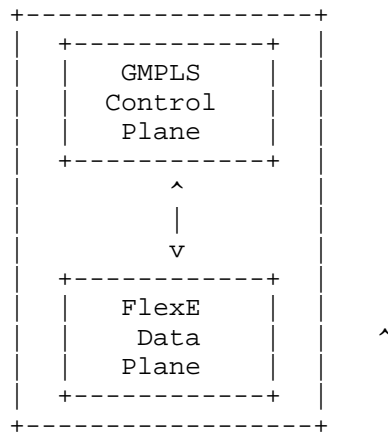


Figure 2: GMPLS controlled FlexE Node

The GMPLS control plane will speak extended standard GMPLS protocols with its neighbours and peers.

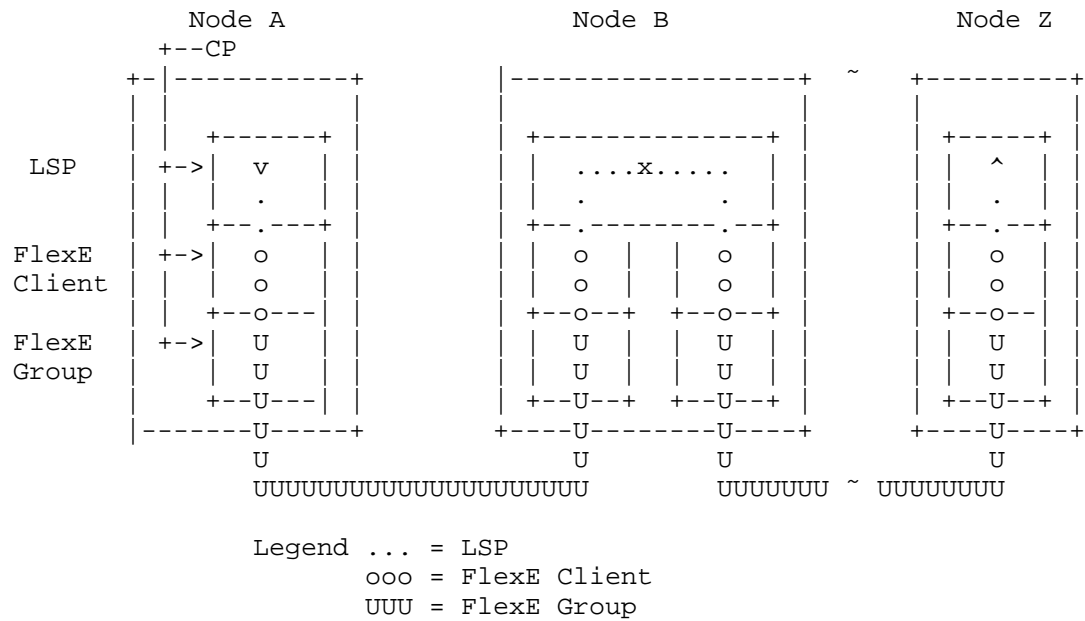


Figure 3: GMPLS controlled network with FlexE infrastructure

Figure 3 describes how an MPLS LSP is mapped over a FlexE Client and FlexE Group.

#### 5.4. Configuring the data plane in FlexE capable nodes

In Figure 3 we show an LSP, a FlexE Client and a FlexE Group, the LSP is there because while the FlexE Channel and Group are not switched, switching in our example takes place on the LSP level. This section will discuss establishment of FlexE Clients and Groups, and mapping of the LSP onto a FlexE Client.

The establishment of a LSP over a FlexE system is very similar to how this is done in any other system. Building on information gathered through the routing system and using the GMPLS signaling to establish the LSP.

##### 5.4.1. Configure/Establish a FlexE Group/Link

Consider the setup of a FlexE Group between node A and B, corresponding to the row of U's from node A to B in Figure 3. The FlexE group is considered to consist of n PHYs, but does not have any FlexE Clients defined from start.

When this is done by the GMPLS control plane, two conditions need to be fulfilled (1) there need to be a data channel defined between node A and B; and (2) a FlexE capable IGP-TE protocol needs to be running in the network.

Node A will send an RSVP-TE message to node B with the information describing the FlexE Group to be setup. This information might be thought of as the "FlexE Group Label" (or part of the FlexE label). It will contain at least the following information:

- o A FlexE Group Identifier (FGid).
- o The number of active FlexE Channels (numFC), where 0 indicates that zero clients are active.
- o Number of PHYs that the FlexE Group is composed of, for each PHY
  - \* PHY identifier
  - \* PHY bandwidth
  - \* slot granularity/number of slots
  - \* available and unavailable slots

When node B receives the RSVP-TE message it checks that it can setup the requested FlexE Group. If the check turns positive, node send an acknowledgment to node A and the FlexE Group is setup.

A more detailed description of how to setup a FlexE Group, will be included in the draft dealing with signaling in detail.

#### 5.4.2. Configure/Establish a FlexE Client

Consider the situation where a FlexE Group is already established (as described in Section 5.4.1) and an m G FlexE Client is needed. Similar to the establishment of the FlexE Group, node A will send a RSV-TE message to node B.

This RSVP-TE message include at least the following information:

- o FlexE Group Identifier
- o FlexE Client Identifier
- o from which PHYs the slots will allocated, i.e. slots might come from more than one PHY.
- o Information per PHY
  - \* PHY bandwidth
  - \* slot granularity
  - \* available/unavailable slots
  - \* allocated slots

A more detailed description of how to setup a FlexE Channel, will be included in the draft dealing with signaling in detail.

#### 5.4.3. Advertise FlexE Groups and FlexE lts

Once the FlexE Group and FlexE CLielts are configured they can be advertised into the routing system as normal routing adjacencies, including the FlexE specific TE information.

### 6. Framework and Architecture

This section discusses FlexE framework and architecture. Framework is taken to mean how FlexE interoperates with other parts of the data communication system. Architecture is taken to mean how functional groups and elements within FlexE work together to deliver the

expected FlexE services. Framework is taken to mean how FlexE interacts with its environment.

### 6.1. FlexE Framework

The service offered by Flexible Ethernet is a transport service very similar (or even identical) to the service offered by Ethernet.

There are two major additions supported by FlexE:

- o FlexE is intended to support high bandwidth and FlexE can offer granular bandwidth from 5Gbits/s and a bandwidth as high as the FlexE Group allows.
- o As FlexE groups and clients are setup as a configuration activity, by a centralized controller or by a GMPLS control plane the service is connection oriented.

### 6.2. FlexE Architecture

#### 6.2.1. Architecture Components

This section discusses the different parts of FlexE signaling and routing and how these parts interoperate.

The FlexE routing mechanism is used to provide resource available information for setup of higher layer LSPs, like Ethernet PHYs' information, partial-rate support information. Based on the resource available information advertised by routing protocol, an end-to-end FlexE connection is computed, and then the signaling protocol is used to set up the end-to-end connection.

FlexE signaling mechanism is used to setup LSPs.

MPLS forwarding over a FlexE infrastructure is different from forwarding over other infrastructures. When MPLS runs over a FlexE infrastructure it is possible that there are more than FlexE Client that meet the next-hop requirements, often it is possible to use any suitable FlexE Client for a hop between two nodes. If the mapping between a MPLS encapsulated packet and the FlexE Client, this mapping need to be explicit when the LSP is set up, and the MPLS label will be used to find the correct FlexE Client.

#### 6.2.2. FlexE Layer Model

The FlexE layer model is similar Ethernet model, the Ethernet PHY layer corresponds to the "FlexE Group", and the MAC layer corresponds to the "FlexE Client".

As different from earlier Ethernet the combination of FlexE Group and Client allows for a huge freedom when it comes to define the bandwidth of an Ethernet connectivity.

#### 6.2.2.1. FlexE Group structure

The FlexE Group might be supported by virtually any transport network, including the Ethernet PHY. While the Ethernet PHY offers a fixed bandwidth the FlexE Group has been structured into 5 Gbit/s slots. This means that the FlexE Group can support FlexE clients of a variety of bandwidths.

The first version is defined for 20 slots of 5 Gbit/s over a 100 Gbit/s PHY. The 100 Gbit/s PHYs can be bonded to give higher bandwidth.

#### 6.2.2.2. FlexE Client mapping

A FlexE client is an Ethernet flow based on a MAC data rate that may or may not correspond to any Ethernet PHY rate. The FlexE Shim is the layer that maps or demaps the FlexE client flows carried over a FlexE group. As defined in [OIFFLEXE1], MAC rates of 10, 40, and any multiple of 25 Gbit/s are supported. This means that if there is a 100 Gbit/s FlexE Group between A and B, a FlexE client of 10, 25, 40, 50, 75 and 100 Gbit/s can be created.

However, by bonding, for example 5 PHYs of 100 Gbit/s to a single FlexE group, FlexE clients of 500 Gbit/s can be supported.

### 7. Control Plane

This section discusses the procedures and extensions needed to the GMPLS Control Plane to establish FlexE LSPs.

There are several ways to establish FlexE groups, allocate slots for FlexE clients, and setup higher layer LSPs. A configuration tool, a centralized controller or the GMPLS control plane can all be used.

To create the FlexE GMPLS control plane Groups, FlexE Clients and higher layer LSPs, extensions to the following protocols may be needed:

- o "RSVP-TE: Extensions to RSVP for LSP Tunnels" (RSVP-TE) [RFC3209]
- o "Link Management Protocol" (LMP) [RFC4204]
- o "Path Computation Element (PCE) Communication Protocol" (PCEP) [RFC5440]

- o IS-IS Extensions for Traffic Engineering (ISIS-TE) [RFC5305]
- o "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)" (OSPF-TE) [RFC4203]
- o "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP" (BGP-LS) [RFC7752]

A FlexE control plane YANG model will also be needed.

Section 7.2 and Section 7.1 discusses the role of the GMPLS control plane when primarily setting up LSPs.

When discussing the signaling and routing procedures we assume that the FlexE group has been established prior to executing the procedures needed to establish an LSP. Technically it is possible to establish FlexE group, allocate FlexE client slots and LSP with a single exchange of GMPLS signaling messages.

#### 7.1. GMPLS Routing

To establish an LSP the Traffic Engineering (TE) information is the most critical information, e.g. resource utilization on interfaces and link, including the availability of slots on the FlexE groups. The GMPLS routing protocols needs to be extended to handle this information. The Traffic Engineering Database (TED) will keep an updated version of this information.

The FlexE capable nodes will be identified by IP-addresses, and the routing and traffic engineering information will be flooded to all nodes within the routing domain using TCP/IP.

When an LSP over the FlexE infrastructure is about to be setup, e.g. R1 - R4 - R5 in Figure 4 the information in the TED is used verify that resources are available. When it is conformed that the LSP is established the TED is updated, marking the resources used for the new LSP as used. Similarly when a LSP is taken down the resources are marked as free.

#### 7.2. GMPLS Signaling

As described in Section 5 the state of the FlexE infrastructure may effect the actions needed to setup an LSP in a FlexE capable network. The FlexE infrastructure maybe be:

1. fully pre-configured

2. partially pre-configured, i.e. the FlexE Group may be pre-configured, but not the FlexE Clients
3. not pre-configured, i.e. the setup of FlexE Group and FlexE Client will be triggered because of the request to setup an LSP.

Figure 4 will be used to illustrate the different cases.

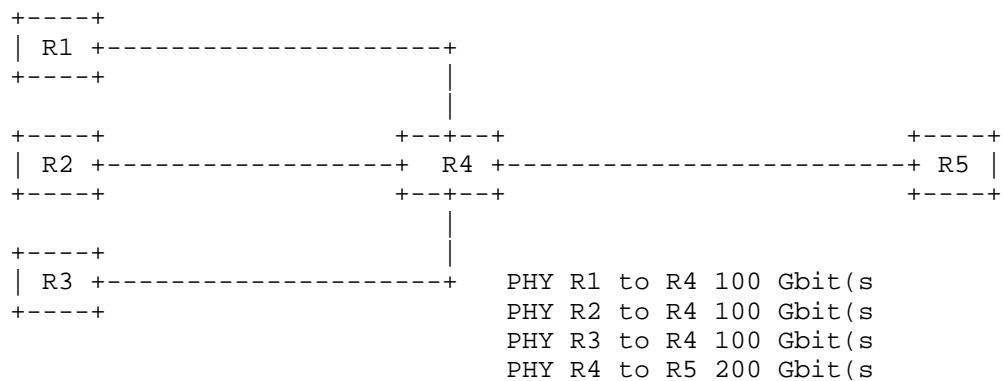


Figure 4: FlexE LSP Example

The text in Section 7.2 is not a specification of the GMPLS signaling extensions for FlexE capable network, it is a description to illustrate the expected features of such a protocol. Nor do we discuss failure scenarios.

#### 7.2.1. LSP setu with pre-configured FlexE infrastructure

In this first example, referencing Figure 4, one 100 Gbit/s FlexE group is configured between R1 and R4, between R2 and R4, and between R3 and R4. Between R4 and R5 there is a 200 Gbit/s FlexE Group.

Over each 100 Gbit/s FlexE Group there are four 5 Gbit/s, two 20 Gbit/s and one 40 Gbit/s FlrxE Clients configured. Over the 200 Gbit/s FlexE Group there are eoght 5 Gbit/s, four 20 Gbit/s and tow 40 Gbit/s FlrxE Clients configured.

One of the 5 Gbit/s FlexE Clients on each FlexE Groups are used as signaling channel.



To establish the for example a 200 Mbit/s MPLS LSP the normal GMPLS request/response procedures are followed. R1 sends the request to R4, R4 allocate resources on one of the FlexE Ckients, forward the request to R5. R5 responds to R4 indicating the label and the FlexE Client the traffic should be sent over, R4 does the same for R1.

The only difference between the standard signaling and what happens here is that there the assigned label will be used to find the right FlexE Client.

#### 7.2.2. LSP setup with partially configured FlexE infrastructure

In the second example, also referencing Figure 4, the FlexE Groups are set up in the same way as in the first example, however only one 5 Gbit/s FlexE Client per FlexE Group are established by configuration. This FlexE Client will be used for signaling.

When preparing to send the request that a 5 Gbit/s MPLS LSP shall be set up R1 discovers that there are no feasible FlexE Client between R1 aand R4. R1 therefore sends the request to establish such a FlexE Client, when receiving the request R4 allocates resources for the FlexE Client on the FlexE Group. There may be different strategies for allocating the bandwidth for this FlexE client. Such strategies are out of scope for this document. R1 then sends the information about the FlexE Client to R1, and both ends establish the FlexE Client.

When the FlexE Client between R1 and R4 is established, R1 proceeds to send the request for an MPLS LSP to R4. R4 will discover that a feasible FlexE Client is missing between R4 and R5. The same procedur s for setting up the FlexE Client between R1 and R4 is repeated for R4 and R5. When there is a feasible FlexE Client available the signaling to set up the MPLS LSP continues as normal.

The label allocated for the MPLS LSP will be used to find the correct FlexE Client.

When a FlexE Clients is set up in this way they can be announced into the routing system in two different ways. First, they can be made generally available, i.e. it will be free to use for anyone that want to set up LSPs over the FlexE Group between R1 and R4 and between R4 and R5. Second, the use of the FlexE Clients may be restricted to the application that initially did set up the FlexE Client.

### 7.2.3. LSP setup with non-configured FlexE infrastructure

This example also refers to Figure 4 as different from the earlier example no FlexE Group or FlexE Client configuration is done prior to the first request for an MPLS LSP over the FlexE infrastructure.

To make the set up of LSPs in a FlexE network where no FlexE Groups or FlexE Clients have been configured two conditions need to be fulfilled. First an out of band signaling channel must be available. Second the FlexE Capabilities must be announced in to the IGP and/or centralized controller.

If these two conditions are fulfilled, the set up of an MPLS LSP progress pretty much as in the partially configured network. The difference is that the set up of both the FlexE Group and FlexE Client are triggered by the request to set up an MPLS LSP.

As in the partially configured case FlexE Clients can be announced into the routing system in two different modes, either they are generally available. It or they are reserved for the applications that first established them.

### 7.2.4. Packet Label Switching Data Plane

This section discusses how the FlexE LSP data plane works. In general it can be said that the interface offered by the FlexE Shim and the FlexE client is equivalent to the interface offered by the Ethernet MAC.

Figure 5 below illustrates the FlexE packet switching data plane procedures.

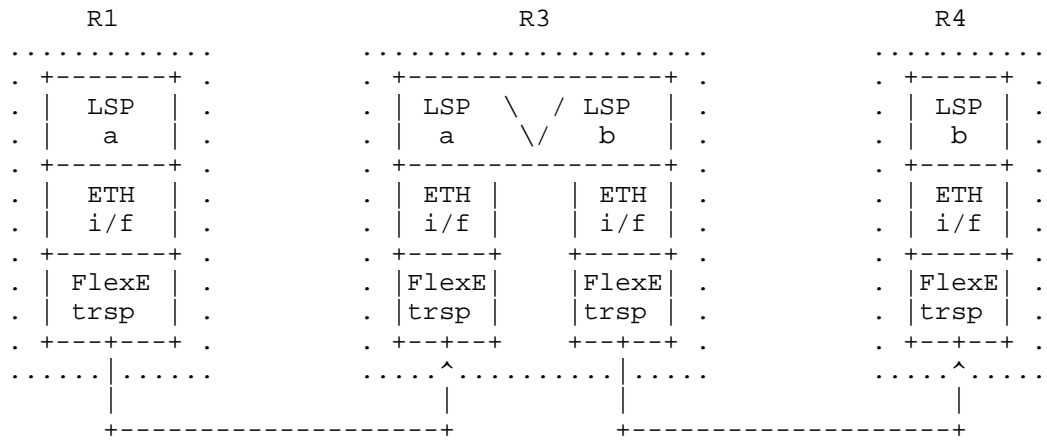


Figure 5: LSP over FlexE Data Plane

The data plane processes packets like this:

- o The LSP encapsulating and forwarding function in node R1 receives a packet that needs to be encapsulated as an MPLS packet with the label "a". The label "a" is used to figure out which FlexE emulated Ethernet interfaces the label encapsulated packet need to be forwarded over.
- o The Ethernet interfaces, by means of FlexE transport, forwards the packet to node R3. Node R3 swaps the label "a" to label "b" and uses "b" to decide over which interface to send the packet.
- o Node R3 forwards the packet to node R, which terminates the LSP.

Sending MPLS encapsulated packets over a FlexE Client is similar to send them over an Ethernet 802.1 interface. The critical differences are:

- o FlexE channelized sub-interfaces guarantee a deterministic bandwidth for an LSP.
- o When a application that originally establish a FlexE Client reserve it for use by that application only, it is possible to create unfringeable bandwidth end-to-end for an MPLS LSP.
- o FlexE infrastructure allows for creating very large end to end bandwidth

## 8. Operations, Administration, and Maintenance (OAM)

To be added in a later version.

## 9. Acknowledgements

## 10. IANA Considerations

This memo includes no request to IANA.

Note to the RFC Editor: This section should be removed before publishing.

## 11. Security Considerations

To be added in a later version.

## 12. Contributors

Khuzema Pithewan, Infinera Corp, kpithewan@infinera.com

Fatai Zhang, Huawei, zhangfatai@huawei.com

Jie Dong, Huawei, jie.dong@huawei.com

Zongpeng Du, Huawei, duzongpeng@huawei.com

Xian Zhang, Huawei, zhang.xian@huawei.com

James Huang, Huawei, james.huang@huawei.com

Qiwon Zhong, Huawei, zhongqiwen@huawei.com

Yongqing Zhu China Telecom zhuyq@gsta.com

Huanan Chen China Telecom chenhuanan@gsta.com

## 13. References

### 13.1. Normative References

- [G.709] ITU, "Optical Transport Network Interfaces  
(<http://www.itu.int/rec/T-REC-G.709-201606-P/en>)", July  
2016.

- [G.798] ITU, "Characteristics of optical transport network hierarchy equipment functional blocks (<http://www.itu.int/rec/T-REC-G.798-201212-I/en>)", February 2014.
- [G.8021] ITU, "Characteristics of Ethernet transport network equipment functional blocks", November 2016.
- [G.872] ITU, "Architecture of optical transport networks", January 2017.
- [OIFFLEXE1] OIF, "FLEX Ethernet Implementation Agreement Version 1.0 (OIF-FLEXE-01.0)", March 2016.
- [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>>.

### 13.2. Informative References

- [RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <<https://www.rfc-editor.org/info/rfc3209>>.
- [RFC4203] Kompella, K., Ed. and Y. Rekhter, Ed., "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, DOI 10.17487/RFC4203, October 2005, <<https://www.rfc-editor.org/info/rfc4203>>.
- [RFC4204] Lang, J., Ed., "Link Management Protocol (LMP)", RFC 4204, DOI 10.17487/RFC4204, October 2005, <<https://www.rfc-editor.org/info/rfc4204>>.
- [RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, DOI 10.17487/RFC5305, October 2008, <<https://www.rfc-editor.org/info/rfc5305>>.
- [RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <<https://www.rfc-editor.org/info/rfc5440>>.

[RFC7752] Gredler, H., Ed., Medved, J., Previdi, S., Farrel, A., and S. Ray, "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP", RFC 7752, DOI 10.17487/RFC7752, March 2016, <<https://www.rfc-editor.org/info/rfc7752>>.

#### Authors' Addresses

Iftekhar Hussain  
Infinera Corp  
169 Java Drive  
Sunnyvale, CA 94089  
USA

Email: [IHussain@infinera.com](mailto:IHussain@infinera.com)

Radha Valiveti  
Infinera Corp  
169 Java Drive  
Sunnyvale, CA 94089  
USA

Email: [rvaliveti@infinera.com](mailto:rvaliveti@infinera.com)

Qilei Wang  
ZTE  
Nanjing  
CN

Email: [wang.qilei@zte.com.cn](mailto:wang.qilei@zte.com.cn)

Loa Andersson  
Huawei  
Stockholm  
Sweden

Email: [loa@pi.nu](mailto:loa@pi.nu)

Mach Chen  
Huawei  
CN

Email: [mach.chen@huawei.com](mailto:mach.chen@huawei.com)

Haomian Zheng  
Huawei  
CN

Email: [zhenghaomian@huawei.com](mailto:zhenghaomian@huawei.com)

CCAMP Working Group  
Internet Draft  
Intended status: Standard Track  
Expires: April 29, 2018

Y. Lee  
D. Dhody  
Huawei

V. Lopez  
Telefonica

D. King  
U. of Lancaster

B. Yoon  
ETRI

R. Vilalta  
CTTC

October 29, 2017

## A Yang Data Model for WSON Tunnel

draft-lee-ccamp-wson-tunnel-model-02.txt

### Abstract

This document provides a YANG data model for WSON TE tunnel.

### Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on December 29, 2017.



## Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction.....	2
2. YANG Model (Tree Structure).....	2
3. TE Tunnel Model for WSON.....	3
4. Security Considerations.....	5
5. IANA Considerations.....	6
6. Acknowledgments.....	6
7. References.....	7
7.1. Normative References.....	7
7.2. Informative References.....	7
8. Contributors.....	7
Authors' Addresses.....	7

## 1. Introduction

This document provides a YANG data model for WSON tunnel model. The YANG model described in this document is a WSON technology-specific Yang Tunnel model based on the information model developed in [RFC7446] and the two encoding documents [RFC7581] and [RFC7579] that developed protocol independent encodings based on [RFC7446].

This document augments the generic TE tunnel model [TE-Tunnel].

## 2. YANG Model (Tree Structure)

```
module: ietf-wson-tunnel
```

```

augment /te:te/te:tunnels/te:tunnel:
  +--rw src-client-signal?  identityref
  +--rw dst-client-signal?  identityref
augment /te:te/te:tunnels/te:tunnel/te:state:
  +--ro src-client-signal?  identityref
  +--ro dst-client-signal?  identityref
augment /te:te/te:globals/te:named-path-constraints/te:named-path-
constraint:
  +--rw wavelength-assignment?  identityref
augment /te:tunnels-rpc/te:input/te:tunnel-info/tepc:request-list:
  +---- src-client-signal?      identityref
  +---- dst-client-signal?      identityref
  +---- wavelength-assignment?  identityref

```

### 3. TE Tunnel Model for WSON

<CODE BEGINS> file "ietf-te-wson@2017-10-29.yang"

```

module ietf-wson-tunnel {
  //TODO: FIXME
  //yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-wson-tunnel";
  prefix "wson-tunnel";

  import ietf-te { prefix "te"; }
  import ietf-transport-types { prefix "tran-types"; }
  import ietf-te-wson-types { prefix "wson-types"; }
  import ietf-te-path-computation { prefix "tepc"; }

  organization
    "IETF CCAMP Working Group";

  contact
    "WG Web:    <http://tools.ietf.org/wg/ccamp/>
    WG List:    <mailto:ccamp@ietf.org>

    WG Chair: Daniele Ceccarelli
               <mailto:daniele.ceccarelli@ericsson.com>

    WG Chair: Fatai Zhang
               <mailto:zhangfatai@huawei.com>

```

```
Editor: Young Lee <leeyoung@huawei.com>
Editor: Dhruv Dhody <dhruv.ietf@gmail.com>
Editor: Ricard Vilalta <ricard.vilalta@cttc.es>;
description
    "This module defines a model for WSON Tunnel Services.";

revision "2017-10-29" {
    description
        "Updates to version 2";
    reference "version 2";
}

grouping wson-tunnel-endpoint {
    description "Parameters for OTN tunnel.";

    leaf src-client-signal {
        type identityref {
            base tran-types:client-signal;
        }
        description
            "Client signal at the source endpoint of
            the tunnel.";
    }

    leaf dst-client-signal {
        type identityref {
            base tran-types:client-signal;
        }
        description
            "Client signal at the destination endpoint of
            the tunnel.";
    }
}

grouping wson-path-constraints {
    description
        "Global named path constraints configuration
        grouping for WSON tunnel";

    leaf wavelength-assignment {
        type identityref {
            base wson-types:wavelength-assignment;
        }
    }
}
```

```
        description "Wavelength Allocation Method";
    }
}

augment "/te:te/te:tunnels/te:tunnel" {
    description
        "Augment with additional parameters required for WSON
        tunnel.";
    uses wson-tunnel-endpoint;
}

augment "/te:te/te:tunnels/te:tunnel/te:state" {
    description
        "Augment with additional parameters required for WSON
        tunnel.";
    uses wson-tunnel-endpoint;
}

augment "/te:te/te:globals/te:named-path-constraints/"
+ "te:named-path-constraint" {
    description
        "Augment with additional constraints WSON
        tunnel.";
    uses wson-path-constraints;
}

augment "/te:tunnels-rpc/te:input/te:tunnel-info/"
+ "tepc:request-list" {
    description
        "Augment with additional constraints WSON
        tunnel.";
    uses wson-tunnel-endpoint;
    uses wson-path-constraints;
}

}
```

<CODE ENDS>

#### 4. Security Considerations

The configuration, state, and action data defined in this document

are designed to be accessed via a management protocol with a secure transport layer, such as NETCONF [RFC6241]. The NETCONF access control model [RFC6536] provides the means to restrict access for particular NETCONF users to a preconfigured subset of all available NETCONF protocol operations and content.

A number of configuration data nodes defined in this document are writable/deletable (i.e., "config true") These data nodes may be considered sensitive or vulnerable in some network environments.

## 5. IANA Considerations

This document registers the following namespace URIs in the IETF XML registry [RFC3688]:

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

This document registers the following YANG modules in the YANG Module

Names registry [RFC7950]:

```
-----
name:          ietf-wson-tunnel
namespace:     urn:ietf:params:xml:ns:yang:ietf-wson-tunnel
reference:     RFC XXXX (TDB)
-----
```

## 6. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

## 7. References

### 7.1. Normative References

[TE-TOPO] X. Liu, et al., "YANG Data Model for TE Topologies", work in progress: draft-ietf-teas-yang-te-topo.

### 7.2. Informative References

[RFC7446] Y. Lee, G. Bernstein, D. Li, W. Imajuku, "Routing and Wavelength Assignment Information Model for Wavelength Switched Optical Networks", RFC 7446, February 2015.

[RFC7579] G. Bernstein, Y. Lee, D. Li, W. Imajuku, "General Network Element Constraint Encoding for GMPLS Controlled Networks", RFC 7579, June 2015.

[RFC7581] G. Bernstein, Y. Lee, D. Li, W. Imajuku, "Routing and Wavelength Assignment Information Encoding for Wavelength Switched Optical Networks", RFC 7581, June 2015.

## 8. Contributors

### Authors' Addresses

Young Lee (ed.)  
Huawei Technologies  
5340 Legacy Drive, Building 3  
Plano, TX 75023  
USA

Phone: (469) 277-5838  
Email: leeyoung@huawei.com

Dhruv Dhody  
Huawei Technologies India Pvt. Ltd,  
Near EPIP Industrial Area, Kundalahalli Village, Whitefield,  
Bangalore - 560 037 [H1-2A-245]

Email: dhruv.dhody@huawei.com

Victor Lopez  
Telefonica  
Email: victor.lopezalvarez@telefonica.com

Daniel King  
University of Lancaster  
Email: d.king@lancaster.ac.uk

Bin Yeong Yoon  
ETRI  
218 Gaijeongro, Yuseong-gu  
Daejeon, Korea  
Email: byyun@etri.re.kr

Ricard Vilalta  
CTTC  
Email: ricard.vilalta@cttc.es





Internet Engineering Task Force  
Internet-Draft  
Intended status: Informational  
Expires: May 3, 2018

Q. Wang, Ed.  
ZTE  
R. Valiveti, Ed.  
Infinera Corp  
H. Zheng, Ed.  
Huawei  
H. Helvoort  
Hai Gaoming B.V  
S. Belotti  
Nokia  
October 30, 2017

GMPLS Routing and Signaling Framework for B100G  
draft-merge-ccamp-otn-b100g-fwk-02

Abstract

The 2016 revision of G.709 introduces support for OTU links with rates larger than 100G. This document provides a framework to address the GMPLS routing and signalling extensions that enable GMPLS to setup paths through network that contain these newly introduced OTUCn links.

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 May 3, 2018.

Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
1.1. Scope . . . . .	3
2. Terminology . . . . .	3
2.1. Requirements Language . . . . .	3
2.2. OTN terminology used in this document . . . . .	3
3. Overview of B100G in G.709 . . . . .	4
3.1. OTUCn . . . . .	4
3.1.1. Carrying OTUCn between 3R points . . . . .	5
3.2. ODUCn . . . . .	7
3.3. OTUCn-M . . . . .	9
3.4. OPUCn Time Slot Granularity . . . . .	9
3.5. Structure of OPUCn MSI with Payload type 0x22 . . . . .	10
3.6. Client Signal Mappings . . . . .	10
4. Usecases . . . . .	12
4.1. 100GE Client Service with a homogeneous chain of OTUC1 links . . . . .	13
4.2. 100GE Client Service with a mix of ODU4, and ODUC1 connections . . . . .	14
4.3. Transport of non-OTN Client Signal over ODUCn connection . . . . .	14
4.3.1. 400GE Client Service with a mix of OTUCn links . . . . .	14
4.3.2. FlexE aware transport over OTUCn links . . . . .	15
4.3.3. FlexE Client transport over OTUCn links . . . . .	16
4.4. Multihop ODUCn link . . . . .	17
4.5. Use of OTUCn-M links . . . . .	18
4.6. Intermediate State of ODU mux . . . . .	19
5. GMPLS Implications . . . . .	19
5.1. OTN ODUCn/OTUCn hierarchy . . . . .	19
5.2. OTUCn/OTUCn-M/ODUCn LSP . . . . .	20
5.3. Implications for GMPLS Signaling . . . . .	20
5.4. Implications for GMPLS Routing . . . . .	21
6. Acknowledgements . . . . .	22
7. Authors (Full List) . . . . .	22
8. Contributors . . . . .	23
9. IANA Considerations . . . . .	24
10. Security Considerations . . . . .	24
11. References . . . . .	24
11.1. Normative References . . . . .	24
11.2. Informative References . . . . .	25

Authors' Addresses	25
--------------------	----

## 1. Introduction

The current GMPLS routing [RFC7138] and signaling extensions [RFC7139] includes coverage for all the OTN capabilities that were defined in the 2012 version of G.709 [ITU-T\_G709\_2012].

The 2016 version of G.709 [ITU-T\_G709\_2012] introduces support for higher rate OTU signals, termed OTUCn (which have a nominal rate of  $n \times 100$  Gbps). The newly introduced OTUCn represent a very powerful extension to the OTN capabilities, and one which naturally scales to transport any newer clients with bit rates in excess of 100G, as they are introduced.

This document presents an overview of the changes introduced in [ITU-T\_G709\_2016] and analyzes them to identify the extensions that would be required in GMPLS routing and signaling to enable the new OTN capabilities.

### 1.1. Scope

For the purposes of the B100G control plane discussion, the OTN should be considered as a combination of ODU and OTSi layers. Note that [ITU-T\_G709\_2016] is deprecating the use of the term "Och" for B100G entities, and leaving it intact only for maintaining continuity in the description of the signals with bandwidth upto 100G. This document focuses on only the control of the ODU layer. The control of the OTSi layer is out of scope of this document.

## 2. Terminology

### 2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

### 2.2. OTN terminology used in this document

- a. OPUCn: Optical Payload Unit -Cn.
- b. ODUCn: Optical Data Unit - Cn.
- c. OTUCn: Fully standardized Optical Transport Unit - Cn.
- d. OTUCn-M: This signal is an extension of the OTUCn signal introduced above. This signal contains the same amount of

overhead as the OTUCn signal, but contains a reduced amount of payload area. Specifically the payload area consists of M 5G tributary slots (where M is strictly less than  $20 \cdot n$ ).

- e. PSI: OPU Payload structure Indicator. This is a multi-frame message and describes the composition of the OPU signal. This field is a concatenation of the Payload type (PT) and the Multiplex Structure Indicator (MSI) defined below.
- f. MSI: Multiplex Structure Indicator. This structure indicates the grouping of the tributary slots in an OPU payload area to realize a client signal that is multiplexed into an OPU. The individual clients multiplexed into the OPU payload area are distinguished by the Tributary Port number (TPN).
- g. GMP: Generic Mapping Procedure.

Detailed description of these terms can be found in [ITU-T\_G709\_2016].

### 3. Overview of B100G in G.709

This section provides an overview of new features in [ITU-T\_G709\_2016].

#### 3.1. OTUCn

In G.709 [ITU-T\_G709\_2012], the standard mechanism for transporting a client signal is to first map it into an ODU signal (of the appropriate rate), and then switch the resulting ODU signal through the OTN network. In the course of its traversal through the OTN network, the ODU signal generated by the mapper is either (a) multiplexed into higher-order ODU, and then encapsulated to form an OTU or (b) directly encapsulated into an OTU signal that defines the section layer. The option (b), i.e. direct encapsulation into an OTU was possible only for ODU1/ODU2/ODU3/ODU4; ODU signals with other rates (e.g. ODUFlex) would first have to be processed per option (a) above. The term "client signal" is generic in the sense that it encompasses both Constant Bit rate (CBR) clients (e.g. 10GBASE-R, SONET OC-768), or packet traffic -- where the goal is to transfer the payload from end-to-end (without regard for bit transparency at the PCS layer). Given that OTU4 was the highest rate section layer signal supported in [ITU-T\_G709\_2012], the client signal rates were limited to be less than 100G (if ODU-VCAT was not used).

In order to carry client signals with rates greater than 100Gbps, [ITU-T\_G709\_2016] takes a general and scalable approach that decouples the rates of OTU signals from the client rate evolution.

The new OTU signal is called OTUCn; this signal is defined to have a rate of (approximately)  $n \times 100\text{G}$ . The following are the key characteristics of the OTUCn signal:

- a. The OTUCn signal contains one ODUCn, which in turn contains one OPUCn signal. The OTUCn and ODUCn signals perform digital section roles only (see [ITU-T\_G709\_2016]:Section 6.1.1). The OTUCn and ODUCn can be seen as being analogous to the regenerator section, and multiplex section in SDH respectively.
- b. The OTUCn signals can be viewed as being formed by interleaving  $n$  OTUC signals (where are labeled 1, 2, ...,  $n$ ), each of which has the format of a standard OTUK signal without the FEC columns (per [ITU-T\_G709\_2016]:Figure 7-1). The ODUCn, and OPUCn have a similar structure, i.e. they can be seen as being formed by interleaving  $n$  instances of ODUC, OPUC signals (respectively) The OTUC signal contains the ODUC, and OPUC signals, just as in the case of fixed rate OTUs defined in G.709 [ITU-T\_G709\_2016].
- c. Each of the OTUC "slices" have the same overhead (OH) as the standard OTUK signal in G.709 [ITU-T\_G709\_2016]. The combined signal OTUCn has  $n$  instances of OTUC OH, ODUC OH, and OPUC OH.
- d. The OTUC signal has a slightly higher rate compared to the OTU4 signal (without FEC); this is to ensure that the OPUC payload area can carry an ODU4 signal.

#### 3.1.1.1. Carrying OTUCn between 3R points

As explained above, within G.709 [ITU-T\_G709\_2016], the OTUCn, ODUCn and OPUCn signal structures are presented in a (physical) interface independent manner, by means of  $n$  OTUC, ODUC and OPUC instances that are marked #1 to # $n$ . Specifically, the definition of the OTUCn signal does not cover aspects such as FEC, modulation formats, etc. These details are defined as part of the adaptation of the OTUCn layer to the optical layer(s). The specific interleaving of OTUC/ODUC/OPUC signals onto the optical signals is interface specific and specified for OTN interfaces with standardized application codes in the interface specific recommendations (G.709.x).

The following scenarios of OTUCn transport need to be considered (see Figure 1):

- a. inter-domain interfaces: These types of interfaces are used for connecting OTN edge nodes to (a) client equipment (e.g. routers) or (b) hand-off points from other OTN networks. ITU-T has standardized the Flexible OTN (FlexO) interfaces to support these functions. Recommendation [ITU-T\_G709.1] specifies a flexible

interoperable short-reach OTN interface over which an OTUCn ( $n \geq 1$ ) is transferred, using bonded FlexO interfaces which belong to a FlexO group. The FlexO group supports physical interface bonding, management of the group members, overhead for communication between FlexO peers etc. (these overheads are separate from the GCC0 channel defined over OTUCn). In its current form, Recommendation [ITU-T\_G709.1] is limited to the case of transporting OTUCn signals using  $n$  100G Ethernet PHY(s). The mechanisms for transporting the OTUCn signals over 100G optical interfaces are specified in [ITU-T\_G709.1] and are not repeated here. When the PHY(s) for the emerging set of Ethernet signals, e.g. 200GbE and 400GbE, become available, new recommendations can define the required adaptations.

- b. intra-domain interfaces: In these cases, the OTUCn is transported using a proprietary (vendor specific) encapsulation, FEC etc. In future, it may be possible to transport OTUCn for intra-domain links using future variants of FlexO.

=====

OTUCn signal		
Inter+Domain Interface (IrDI) FlexO (G.709.1)	Intra+Domain Interface (IaDI) FlexO (G.709.x) (Future)	Intra+Domain Interface Proprietary Encap, FEC etc.

=====

Figure 1: OTUCn transport possibilities

It is possible for an OTUCn signal to be transported via multiple hops of lower-layer adaptation (see Figure 2). In this scenario, the OTUCn spans multiple optical paths joined by a FlexO segment. An end-to-end OTUCn LSP needs to be setup after the optical circuits are established. The information about the FlexO interfaces (and group) are configured at the FlexO endpoints, and there is no dynamic setup.

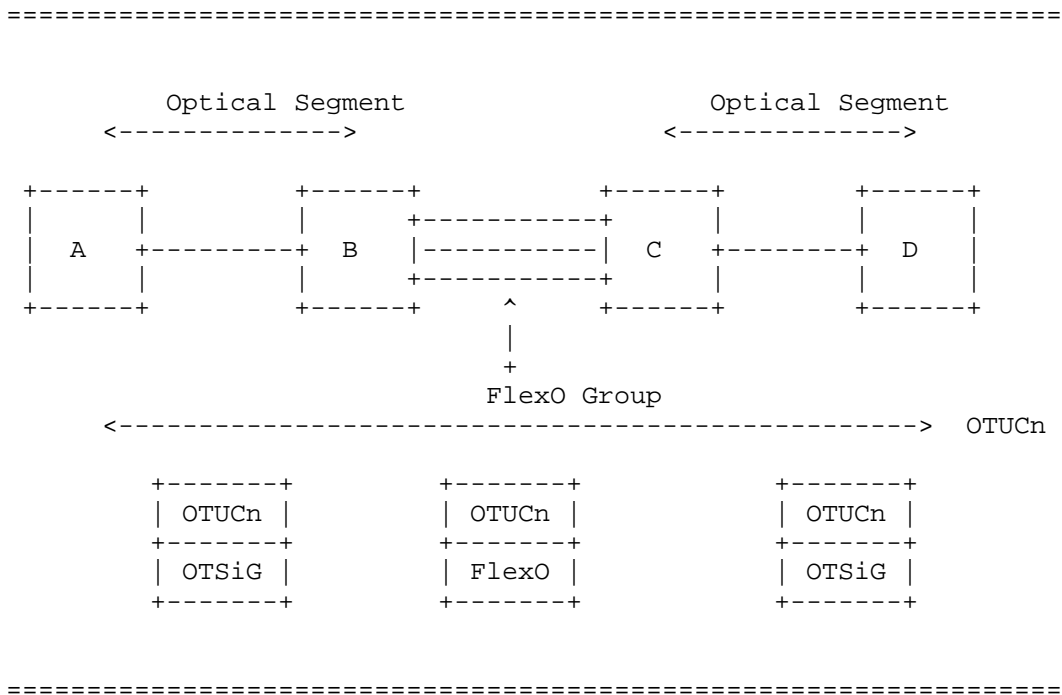


Figure 2: OTUCn transport - Multihop

This document views FlexO (even if there are some digital sub-layers involved in the adaptation) and other OTUCn transport mechanisms as "lower layers", and are therefore considered out-of-scope. The OTUCn layer operates independent of the method used to transport the signal.

### 3.2. ODUCn

The ODUCn signal [ITU-T\_G709\_2016] can be viewed as being formed by the appropriate interleaving of content from n ODUC signal instances. The ODUC frames have the same structure as a standard ODU -- in the sense that it has the same Overhead (OH) area, and the payload area -- but has a higher rate since its payload area can embed an ODU4 signal. The ODUCn signal can be formed in one of the following ways:

By multiplexing lower-rate (i.e. both low-order and high-order) ODUC signals.

Each of the n instances of ODUC can carry the NULL signal (as specified in [ITU-T\_G709\_2016]: Section 17.5.1)

Each of the  $n$  instances of ODUC can carry the PN-11 PRBS test sequence (as specified in [ITU-T\_G709\_2016]: Section 17.5.2)

It is conceivable that vendors might implement proprietary mappings (Payload Type values of 0x80-x8F) of non-OTN client signals. An interoperable control plane cannot make use of these proprietary ODUCn signals, and hence this case isn't considered in this document.

The ODUCn signals have a rate that is captured in Table 1.

ODU Type	ODU Bit Rate
ODUCn	$n \times 239/226 \times 99,532,800 \text{ kbit/s} = n \times 105,258,138.053 \text{ kbit/s}$

Table 1: ODUCn rates

The ODUCn is a multiplex section ODU signal, and is mapped into an OTUCn signal which provides the regenerator section layer. In some scenarios, the ODUCn, and OTUCn signals will be co-terminous, i.e. they will have identical source/sink locations. [ITU-T\_G709\_2016] and [ITU-T\_G872] allow for the ODUCn signal to pass through a digital regenerator node which will terminate the OTUCn layer, but will pass the regenerated (but otherwise untouched) ODUCn towards a different OTUCn interface where a fresh OTUCn layer will be initiated (see Figure 3). In this case, an ODUCn LSP needs to be set up to traverse the 3 OTUCn segments.

Specifically, the OPUCn signal flows through these regenerators unchanged. That is, the set of client signals, their TPNs, trib-slot allocation remains unchanged. Note however that the ODUCn Overhead (OH) might be modified if TCM sub-layers are instantiated in order to monitor the performance of the repeater hops. In this sense, the ODUCn should not be seen as a general ODU which can be switched via an ODUk cross-connect.



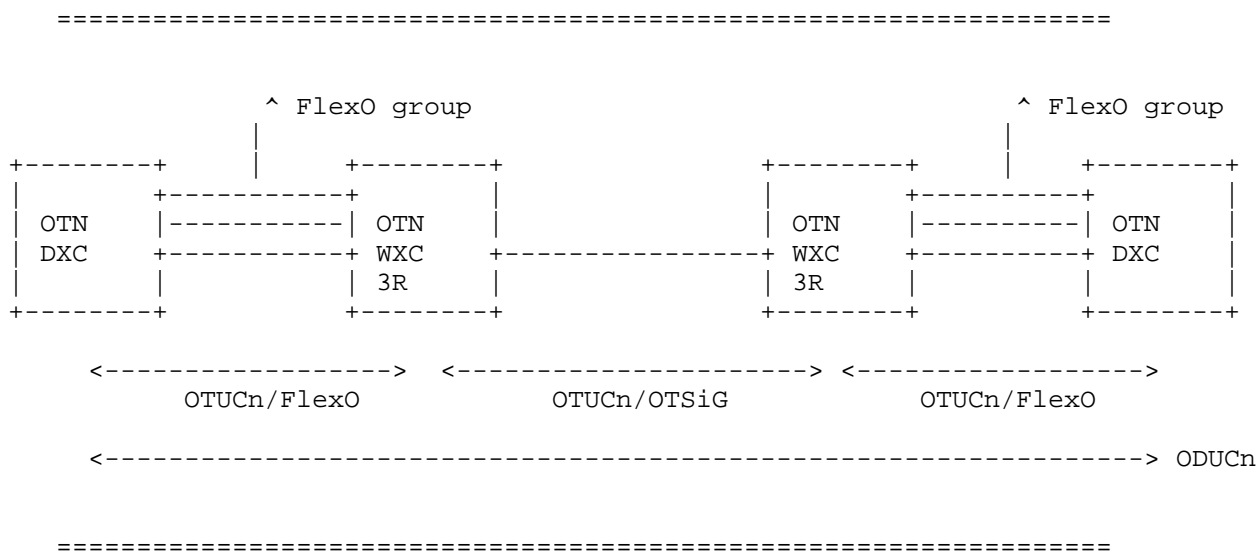


Figure 3: Multi-hop ODUCn signal

### 3.3. OTUCn-M

The standard OTUCn signal has the same rate as that of the ODUcN signal as captured in Table 1. This implies that the OTUCn signal can only be transported over wavelength groups which have a total capacity of multiples of (approximately) 100G. Modern DSPs support a variety of bit rates per wavelength, depending on the reach requirements for the optical link. With this in mind, ITU-T supports the notion of a reduced rate OTUCn signal, termed the OTUCn-M. The OTUCn-M signal is derived from the OTUCn signal by retaining all the n instances of overhead (one per OTUC slice) and crunching the OPUC tributary slots marked as "unavailable".

### 3.4. OPUCn Time Slot Granularity

[ITU-T\_G709\_2012] introduced the support for 1.25G granular tributary slots in OPU2, OPU3, and OPU4 signals. With the introduction of higher rate signals such as the OPUCn, it is no longer practical for the optical networks (and the datapath hardware) to support a very large number of flows at such a fine granularity. ITU-T has defined the OPUC with a tributary slot granularity of 5G. This means that the ODUCn signal has  $20 \times n$  tributary slots (of 5Gbps capacity).

### 3.5. Structure of OPUCn MSI with Payload type 0x22

As mentioned above, the OPUCn signal has  $20 \times n$  5G tributary slots. The OPUCn contains  $n$  PSI structures, one per OPUC instance. The PSI structure consists of the Payload Type (of 0x22), followed by a Reserved Field (1 byte), followed by the MSI. The OPUCn MSI field has a fixed length of  $40 \times n$  bytes and indicates the ODTU content of each TS of an OPUCn. Two bytes are used for each of the  $20 \times n$  tributary slots, and each such information structure has the following format ([ITU-T\_G709\_2016] G.709:Section 20.4.1):

- a. The TS availability bit 1 indicates if the tributary slot is available or unavailable
- b. The TS occupation bit 9 indicates if the tributary slot is allocated or unallocated

### 3.6. Client Signal Mappings

Note that [ITU-T\_G709\_2016] introduces support for OTUCn signals with rates of  $n \times 100\text{G}$  and also introduces support for client signals with rates larger than 100G (e.g. the future 400GBASE-R client being standardized by IEEE, higher packet streams from NPUs). The approach taken by the ITU-T to map non-OTN client signals to the appropriate ODU containers is as follows:

- a. All client signals with rates less than 100G are mapped as specified in [ITU-T\_G709\_2016]:Clause 17. These mappings are identical to those specified in the earlier revision of G.709 [ITU-T\_G709\_2012]. Thus, for example, the 100GBASE-X/10GBASE-R signals are mapped to ODU0/ODU2e respectively (see Table 2 -- based on Table 7-2 in [ITU-T\_G709\_2016])
- b. Always map the new and emerging client signals to ODUFlex signals of the appropriate rates (see Table 2 -- based on Table 7-2 in [ITU-T\_G709\_2016])
- c. Drop support for ODU Virtual Concatenation. This simplifies the network, and the supporting hardware since multiple different mappings for the same client are no longer necessary. Note that legacy implementations that transported sub-100G clients using ODU VCAT shall continue to be supported.
- d. ODUFlex signals are low-order signals only. If the ODUFlex entities have rates of 100G or less, they can be transported using either an ODUk ( $k=1..4$ ) or an ODUCn server layer. On the other hand, ODUFlex connections with rates greater than 100G will require the server layer to be ODUCn. The ODUCn signals must be

adapted to an OTUCn signal. Figure 4 illustrates the hierarchy of the digital signals defined in [ITU-T\_G709\_2016].

ODU Type	ODU Bit Rate
ODU0	1,244,160 Kbps
ODU1	$239/238 \times 2,488,320$ Kbps
ODU2	$239/237 \times 9,953,280$ Kbps
ODU2e	$239/237 \times 10,312,500$ Kbps
ODU3	$239/236 \times 39,813,120$ Kbps
ODU4	$239/227 \times 99,532,800$ Kbps
ODUflex for CBR client signals	$239/238 \times$ Client signal Bit rate
ODUflex for GFP-F mapped packet traffic	Configured bit rate
ODUflex for IMP mapped packet traffic	$s \times 239/238 \times 5\,156\,250$ kbit/s: $s=2,8,5*n$ , $n \geq 1$
ODUflex for FlexE aware transport	$103\,125\,000 \times 240/238 \times n/20$ kbit/s, where n is total number of available tributary slots among all PHYs which have been crunched and combined.

Note that this table doesn't include ODUCn -- since it cannot be generated by mapping a non-OTN signal. An ODUCn is always formed by multiplexing multiple LO-ODUs.

Table 2: Types and rates of ODUs usable for client mappings

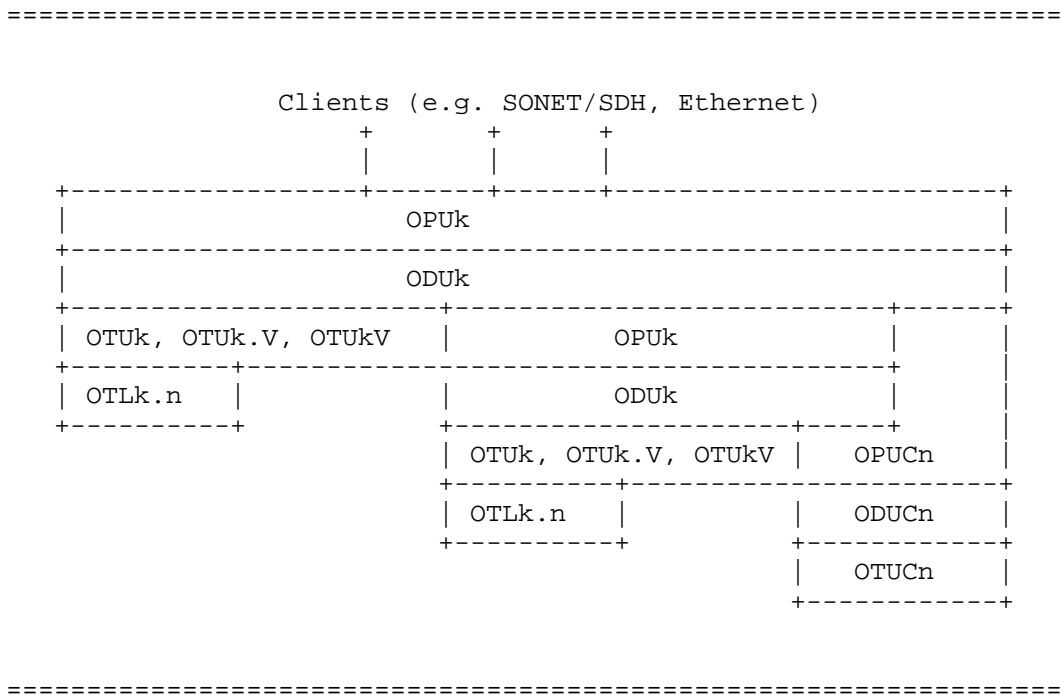


Figure 4: Digital Structure of OTN interfaces (from G.709:Figure 6-1)

#### 4. Usecases

This section introduces various usecases that provide the rationale for the requirements that any solution must satisfy. At a later point in time, it is possible to consolidate these usecases so that all the multiplexing (and demultiplexing) variants are encountered along the path of an end-to-end ODU circuit.

Note-1: These usecases present scenarios in which OTUCn links are depicted. These illustrations do not highlight how the OTUCn is transported between the 3R points. That is, these usecases do not cover cases in which a standard FlexO interface (e.g. as defined in [ITU-T\_G709.1]) is used, or whether a vendor specific mapping of OTUCn to OTSiG (as defined in [ITU-T\_G872]) is used. In other words, multiple variants of these usecases based on FlexO usage (or not) are not included in this document.

#### 4.1. 100GE Client Service with a homogeneous chain of OTUC1 links

In the scenario illustrated in Figure 5 a 100GBASE-R client is mapped into an ODU4 at NE1. The resulting ODU4 signal is multiplexed into the ODU4 server layer (using GMP) and further encapsulated to form the OTUC1 signal. The links NE1-NE2, and NE2-NE3 are both OTUC1 links -- and they can carry one 100GE client mapped into an ODU4 server layer. Actions performed at NE2 are: (a) terminate OTUC1, and ODU4 towards NE1 (b) demultiplex the ODU4 signal from ODU4 (c) map the ODU4 signal onto a different ODU4/OTUC1 towards NE3. NE3 performs the inverse sequence of steps performed at NE1, and recovers the 100GBASE-R client from the ODU4 signal. Note that the ODU4 and ODU4 signals are not "interoperable" and that the ODU4 is a server layer to the ODU4 signal.

This illustration is also applicable to the usecase in which members of a FlexE group are transported in a flexe-unaware mode in the transport network. Although this illustration included only OTUC1 signals, any higher rate OTUCn signal can be substituted for these signals. In this particular scenario, there are two adjacent ODU4 hops, and the NE2 demultiplexes (and multiplexes) the ODU4 onto the ODU4. It is possible to construct an alternative scenario in the case when NE2 acts as a regenerator, and doesn't terminate the ODU4 signals in the two hops, and instead repeats the ODU4 signal; this scenario is specifically discussed in Section 4.4.

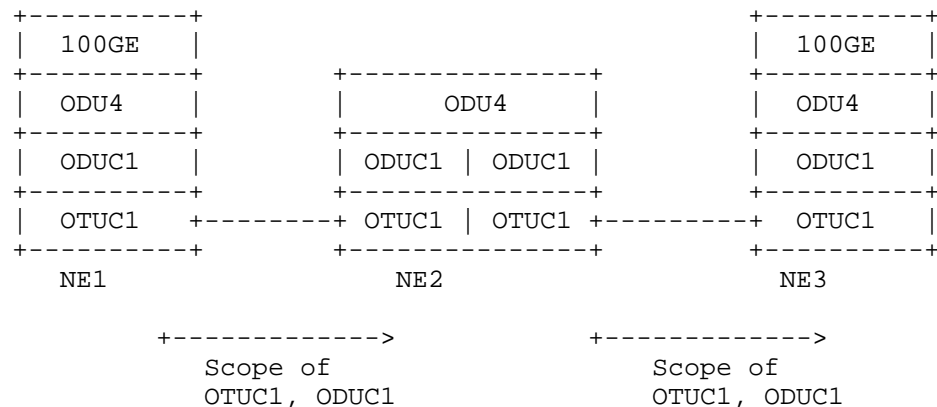


Figure 5: 100GE Client service

#### 4.2. 100GE Client Service with a mix of ODU4, and ODUC1 connections

In the scenario illustrated in Figure 6 a 100GBASE-R client is mapped into an ODU4 at NE1. The resulting ODU4 signal is encapsulated with an OTU layer to form the OTU4 signal. Actions performed at NE2 are: (a) terminate OTU4 layer, and extract the ODU4 signal (b) map the ODU4 signal onto a different ODUC1/OTUC1 towards NE3. NE3 performs the same set of actions that were performed by NE3 in Figure 5. This usecase illustrates a scenario in which an ODU4 signal can span between network elements regardless of whether they support the OTUCn interfaces or not.

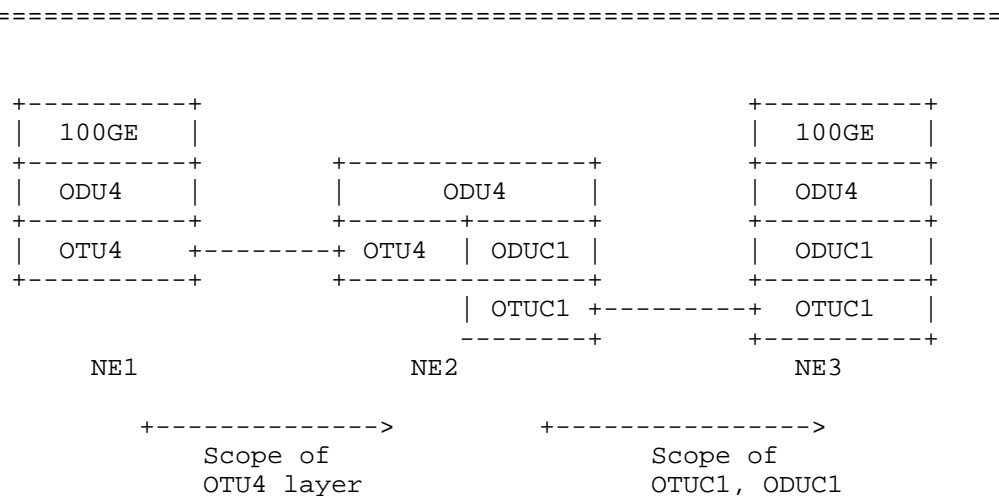


Figure 6: 100GE Client Service with a mix of OTU4, and OTUC1 links

#### 4.3. Transport of non-OTN Client Signal over ODUCn connection

Editor Note: this section may not be needed, as this section mainly describes the setup of client signal over ODUFlex, then over ODUCn. Setup of ODUk/ODUFlex can reuse mechanisms defined in RFC7139.

##### 4.3.1. 400GE Client Service with a mix of OTUCn links

In the scenario illustrated in Figure 7 a 400GBASE-R client is mapped into an ODUFlex at NE1. The resulting ODUFlex signal is multiplexed into an ODUC4 (using GMP), and then transformed into an OTUC4 signal. The links between NE1-NE2, and NE2-NE3 are OTUC4 and OTUC6 (respectively). Actions performed at NE2 are: (a) terminate OTUC4,

and ODU4 towards NE1 (b) demultiplex the ODUflex signal from ODU4 (c) map the ODUflex signal onto ODU6/OTUC6 towards NE3. NE3 performs the inverse sequence of steps performed at NE1, and recovers the 400GBASE-R client from the ODUflex signal.

Although not specifically illustrated in this figure, the 200G of spare capacity in the NE2-NE3 links can be used to carry other client signals.. Although the scenario illustrated in Figure 7 is specific to 400GE, the treatment for packet clients at other rates (e.g. 25G, 50G, 200G) follows a very similar processing sequence. In the case of 25GBASE-R clients, the 25GE client signal will be mapped to an ODUflex, and can be multiplexed into an ODU4 signal, or an ODUcn signal as illustrated here.

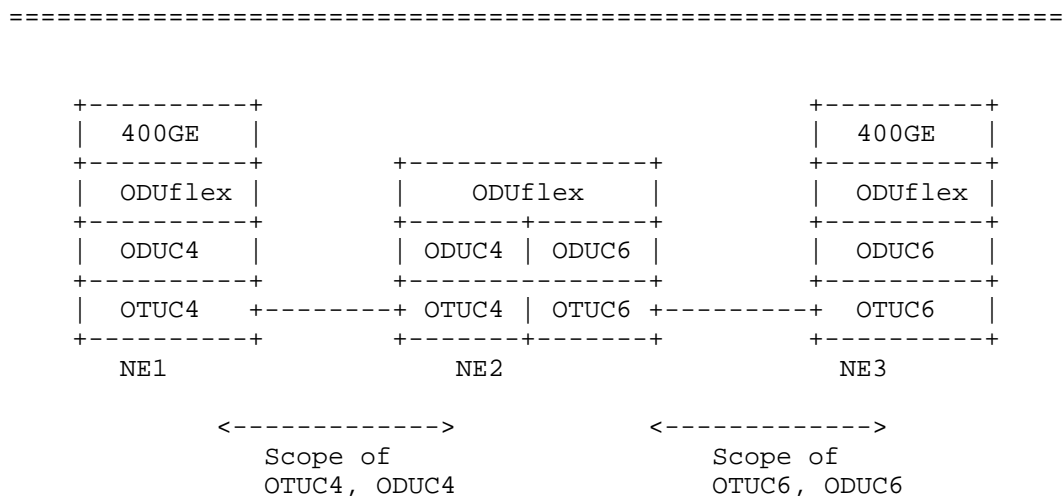


Figure 7: 400GE transport over OTUCn links

#### 4.3.2. FlexE aware transport over OTUCn links

In the scenario illustrated in Figure 8 NE1 interfaces to a client equipment which includes the FlexE SHIM functions which originate/terminate a FlexE group. The transport network edge node NE2 is FlexE aware -- but doesn't terminate the FlexE group. NE1 may (as defined in the FlexE draft [I-D.izh-ccamp-flex-e-fwk]), crunch the unavailable tributary slots in the FlexE PHY signals, and map the resultant stream to one or more ODUflex signals. The links between NE1-NE2, and NE2-NE3 are OTUC4 and OTUC6 (respectively). Actions

performed at NE2 are: (a) terminate OTUC4, and ODU4 towards NE1 (b) demultiplex the ODUflex signal from ODU4 (c) map the ODUflex signal onto ODU6/OTUC6 towards NE3. NE3 recovers the Crunched and combined PHY(s) from the ODUflex signal, re-adds the unavailable calendar slots, and outputs the resulting stream towards the FlexE PHY(s).

In the scenario illustrated in Figure 8 the lowest rate OTUCn link is the OTUC4 link between NE1-NE2. This means that the size of the FlexE group is at most 4. FlexE groups with greater sizes can be handled by utilizing appropriate OTUCn links. Note that at most 400G of the capacity of OTUC6 (or 600G) NE2-NE3 link is occupied by the ODUflex signal; the remaining bandwidth can be allocated to other client signals.

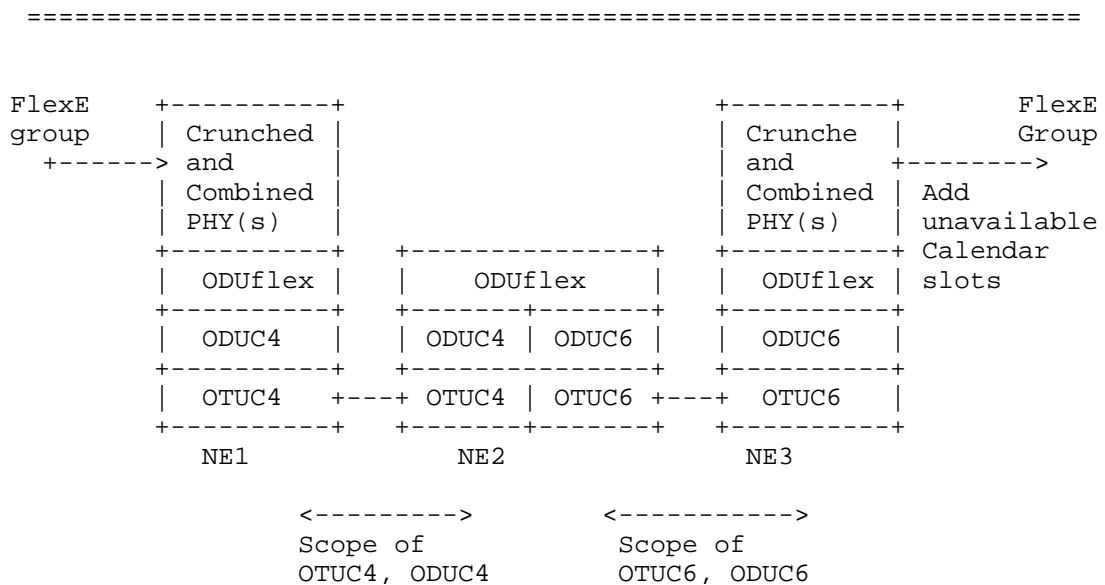


Figure 8: FlexE aware transport over OTUCn links

#### 4.3.3. FlexE Client transport over OTUCn links

This use case (see Figure 9) concerns the scenario in which a FlexE group is terminated at the transport network edge node (via the FlexE SHIM function), and the FlexE clients are demultiplexed, and independently transported through the OTN network. In the scenario illustrated in Figure 9 the lowest rate OTUCn link is the OTUC4 link



between NE1-NE2. This means that the maximum bit rate of the FlexE client is at most 400G. FlexE clients with greater sizes can be handled by utilizing appropriate OTUCn links. This figure illustrates the case in which one FlexE client is transported between NE1 and NE3. Other FlexE clients recovered at NE1 can routed independently to NE3, or to other network elements.

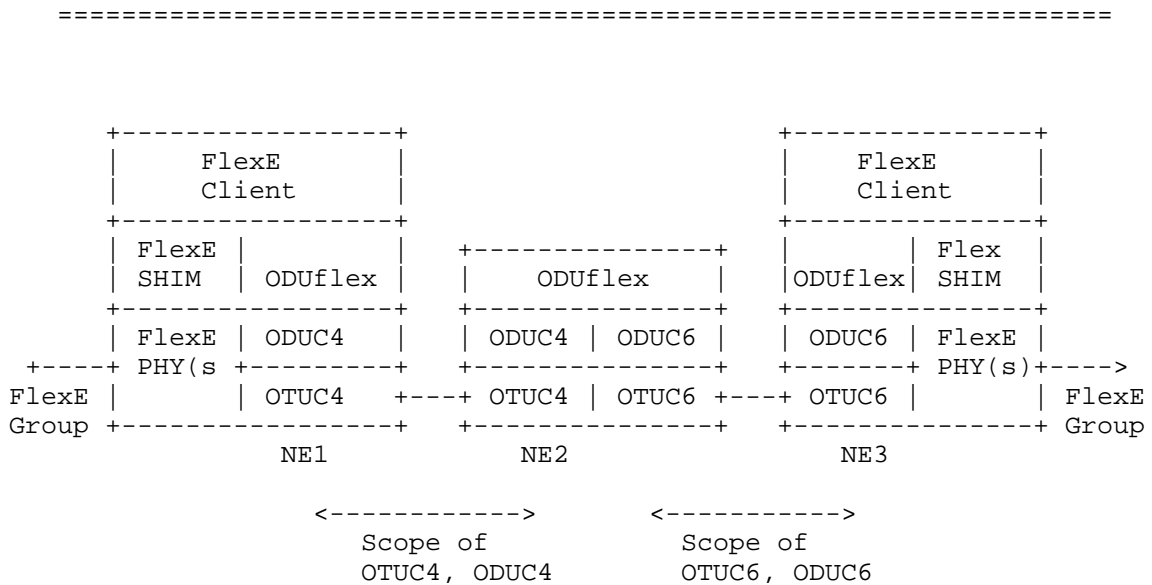


Figure 9: FlexE client transport over OTUCn links

#### 4.4. Multihop ODUCn link

As mentioned in the introductory section, the ODUCh is not a switchable entity. The ODUCh layer is a server layer, which more-or-less occupies the position of a section layer in OTN networks. As such, the ODUCh signal must be terminated and the contained low-order ODU flows can be switched independently to other OTN interfaces. G.709 and G.872 however allow for digital regenerators to terminate the OTUCh layer, and reinject the ODUCh layer towards another interface (where a new OTUCh section layer is started). This scenario is illustrated in Figure 10. In this figure, NE3 is the regenerator. The ODUCh signal is terminated at NE2, and NE4. At the regeneration points, all the clients embedded inside the ODUCh signal are not touched (i.e. no TS changes can occur). More specifically, the OPUC2 signal is not modified in any way. However, the ODUCh OH

may be modified if intrusive TCM monitoring points are applied to the ODUC2 signal at NE3. It is for this reason that the ODUC2 entity must be visible at NE3.

In scenarios involving multi-hop ODUCn links, GMPLS signalling will be required to setup multiple ODUCn LSPs, each covering a regenerator section (since an end-to-end ODUCn LSP is not possible except in very simple configurations). A LO-ODU can then be switched across multiple ODUCn LSPs (possibly with different rates).

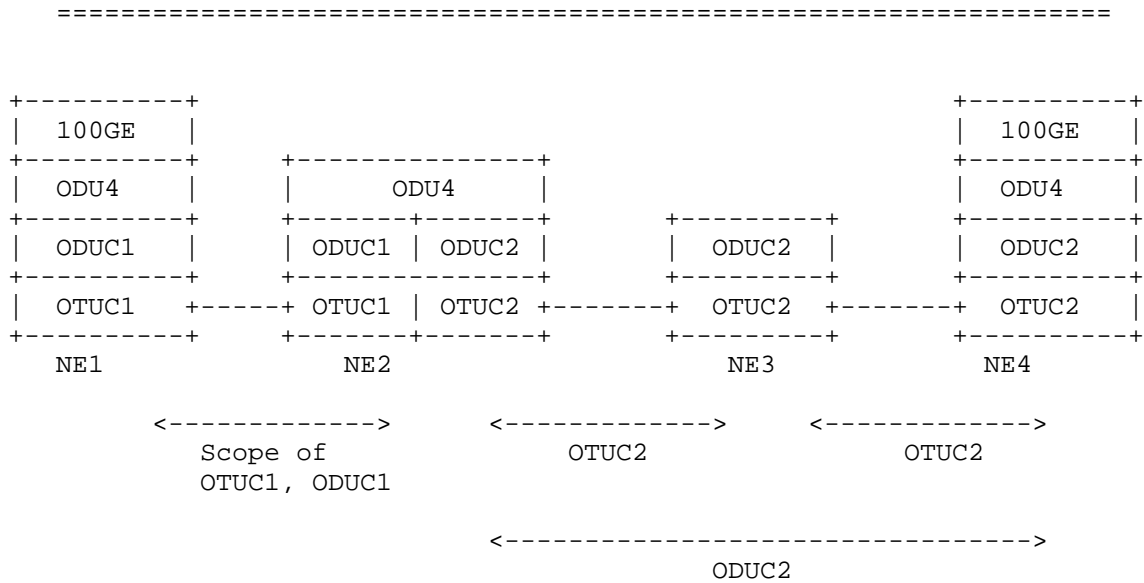


Figure 10: Multihop ODUCn link

#### 4.5. Use of OTUCn-M links

The scenario illustrated in Figure 11 is a variant of the basic usecase presented in Figure 5. The only difference is that the second hop of the ODU4 connection makes use of a OTUC2-30 link which has a capacity of 150G.

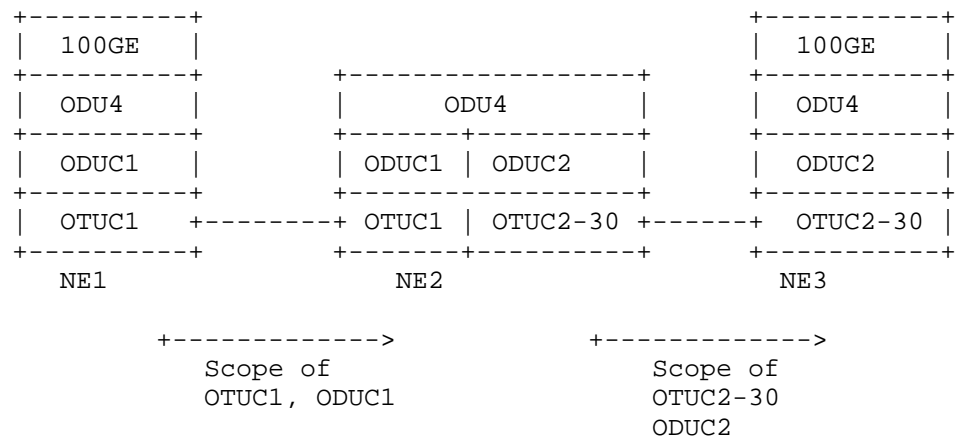


Figure 11: 100GE Client service over OTUCn-M links

#### 4.6. Intermediate State of ODU mux

The ODUCn links have a tributary slot granularity of 5G -- and this makes it a bit inefficient if a small number of ODU0 flows have to be switched across an ODUCn links. In these cases, it is conceivable that the intermediate nodes may offer the convenience of a intermediate-stage multiplexing, whereby multiple ODU0 flows are first multiplexed into a higher rate container (e.g. ODU2), and then multiplexed into an ODUCn signal. This however assumes that all these ODU0 flows are co-routed in the network. If this assumption cannot be made, the only solution is to multiplex these ODU0 flows into higher rate flows, from the source of the traffic. This usecase isn't elaborated in this document. We can add details if required.

### 5. GMPLS Implications

#### 5.1. OTN ODUCn/OTUCn hierarchy

As described in [ITU-T\_G872], the digital layers of the OTN are divided into the OTU layer and a hierarchy of one or more ODU layers. As an ODUCn cannot be used to support non-OTN client signals, the OTN client signals (e.g. ODU0, ODU1, ODU2, ODU2e, ODU3, ODU4, ODUflex) are first multiplexed into an ODUCn container, then the ODUCn

container is then mapped into OTUCn (see Figure 1). The signal hierarchy supported by the ODUCn and OTUCn needs to be taken into consideration in control plane Routing and Signaling.

ODUCn based connection management is concerned with controlling the connectivity of ODUCn paths. According to [ITU-T\_G872], the intermediate nodes with ODUCn do not support the switching of ODUCn tributary slot. Intermediate ODUCn points are only considered as a forwarding node. Once an ODUCn path is used to transport client signal, the TS occupied will not change across the ODUCn network.

### 5.2. OTUCn/OTUCn-M/ODUCn LSP

OTUCn/OTUCn-M Link is different from traditional OTUk link. The OTUk link is already configured once two matched OTU interfaces are connected. But for setup of OTUCn link, the first thing that needs to do is to bond several different OTUC instances together as one group, which is seen as one OTUCn link. Control plane mechanisms are needed to finish the bonding of these instances.

For transportation of client signal over ODUCn signal, an ODUCn LSP is also needed to be configured with control plane mechanisms in advance.

Once an ODUCn LSP is set up, the signaling mechanism defined in [RFC7139] can be reused to set up OTUk LSP over ODUCn link. Setup of OTUk LSP over ODUCn LSP is out of the scope of this document.

### 5.3. Implications for GMPLS Signaling

[RFC7139] extends the base RSVP-TE signaling specification [RFC4328] to define RSVP-TE signaling extensions that can be used to control OTN networks built in accordance with [ITU-T\_G709\_2012]. [ITU-T\_G709\_2016] introduced some new containers, such as OPUCn, ODUCn, and OTUCn. The mechanisms defined in [RFC7139] do not support these new OTN features. Therefore, GMPLS signaling protocols MUST be extended to support this new functionality. The following summarizes key aspects that should be considered for GMPLS signaling extensions:

- a. Per the description in clause 7 of [ITU-T\_G872], "the digital layers of the OTN are divided into the OTU layer and a hierarchy of one or more ODU layers". In B100G links, the ODUCn layer is the bottom of the ODU hierarchy, and an ODUCn (induced) LSP needs to be established before the LO-ODUs can flow across this link. The traffic parameters in a signaling message should be extended to support the new signal type(s) for the ODUCn signals. This approach keeps the treatment for ODUCn signals consistent with that of other ODU(s).

- b. Support the new TS granularity: the signaling protocol should be able to identify the TS granularity (i.e., the new 5 Gbps TS granularity) to be used for establishing a Hierarchical LSP that will be used to carry service LSP(s) requiring a specific TS granularity.
- c. A new label format MUST carry the information about one or more OTUC/ODUC instances to be bonded together.
- d. Support for LSP setup of OTUCn sub rates (OTUCn-M) path: based on previous extensions, there should be new signal mechanism to declare the OTUCn-m information. The GMPLS signalling protocol SHALL support the setup of OTUCn sub rates (OTUCn-M) LSP, which includes the negotiation of unavailable slots number, slots position and allocation of slot resources.
- e. The GMPLS signalling protocol should be able to specify the new ODUCn/OTUCn signal types and related traffic information. The traffic parameters should be extended in a signalling message to support the new ODUCn/OTUCn signal types

#### 5.4. Implications for GMPLS Routing

The path computation process needs to select a suitable route for an ODUCn/OTUCn/OTUCn-M connection request. In order to perform the path computation, it needs to evaluate the available bandwidth/slots available on one or more candidate links. The routing protocol SHOULD be extended to carry sufficient information to represent ODU Traffic Engineering (TE) topology.

The Interface Switching Capability Descriptors defined in [RFC4203] present a new constraint for LSP path computation. [RFC4203] defines the Switching Capability, related Maximum LSP Bandwidth, and Switching Capability specific information. [RFC7138] updates the ISCD to support ODU4, ODU2e and ODUFlex. The new Switching Capability specific information provided in [RFC7138] have to be adapted to support new features contained in [G709-2016]. The following requirements should be considered:

- a. Support for carrying the link multiplexing capability: As discussed in Section 3.1.2, many different types of low-order ODU(s) (e.g. ODUFlex, ODU4) can be multiplexed into the ODUCn. An ODUCn path may support one or more types of ODUk signals. The routing protocol should be capable of carrying this multiplexing capability.
- b. Support for advertising 5G Tributary Slot Granularity introduced [ITU-T\_G709\_2016].

- c. Support for advertisement of available bandwidth in an ODUCn path.

6. Acknowledgements

7. Authors (Full List)

Qilei Wang (editor)

ZTE

Nanjing, China

Email: wang.qilei@zte.com.cn

Radha Valiveti (editor)

Infinera Corp

Sunnyvale, CA, USA

Email: rvaliveti@infinera.com

Haomian Zheng (editor)

Huawei

CN

EMail: zhenghaomian@huawei.com

Huub van Helvoort

Hai Gaoming B.V

EMail: huubatwork@gmail.com

Sergio Belotti

Nokia

EMail: sergio.belotti@nokia.com

Iftekhar Hussain

Infinera Corp

Sunnyvale, CA, USA

Email: IHussain@infinera.com

Daniele Ceccarelli

Ericsson

Email: daniele.ceccarelli@ericsson.com

#### 8. Contributors

Rajan Rao, Infinera Corp, Sunnyvale, USA, rrao@infinera.com

Fatai Zhang, Huawei, zhangfatai@huawei.com

Italo Busi, Huawei, italo.busi@huawei.com

Zheyu Fan, Huawei, fanzheyu2@huawei.com

Yuanbin Zhang, ZTE, Beijing, zhang.yuanbin@zte.com.cn

Zafar Ali, Cisco Systems, zali@cisco.com

Daniel King, d.king@lancaster.ac.uk

Manoj Kumar, Cisco Systems, manojk2@cisco.com

Antonello Bonfanti, Cisco Systems, abonfant@cisco.com

Akshaya Nadahalli, Cisco Systems, anadahal@cisco.com

## 9. IANA Considerations

This memo includes no request to IANA.

## 10. Security Considerations

None.

## 11. References

### 11.1. Normative References

- [ITU-T\_G709.1]  
ITU-T, "ITU-T G.709.1: Flexible OTN short-reach interface; 2016", , 2016.
- [ITU-T\_G709\_2012]  
ITU-T, "ITU-T G.709: Optical Transport Network Interfaces; 02/2012", <http://www.itu.int/rec/T-REC-G.709-201202-S/en>, February 2012.
- [ITU-T\_G709\_2016]  
ITU-T, "ITU-T G.709: Optical Transport Network Interfaces; 07/2016", <http://www.itu.int/rec/T-REC-G.709-201606-P/en>, July 2016.
- [ITU-T\_G872]  
ITU-T, "ITU-T G.872: The Architecture of Optical Transport Networks; 2017", <http://www.itu.int/rec/T-REC-G.872/en>, January 2017.
- [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>>.
- [RFC4328] Papadimitriou, D., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control", RFC 4328, DOI 10.17487/RFC4328, January 2006, <<https://www.rfc-editor.org/info/rfc4328>>.
- [RFC7138] Ceccarelli, D., Ed., Zhang, F., Belotti, S., Rao, R., and J. Drake, "Traffic Engineering Extensions to OSPF for GMPLS Control of Evolving G.709 Optical Transport Networks", RFC 7138, DOI 10.17487/RFC7138, March 2014, <<https://www.rfc-editor.org/info/rfc7138>>.



[RFC7139] Zhang, F., Ed., Zhang, G., Belotti, S., Ceccarelli, D., and K. Pithewan, "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks", RFC 7139, DOI 10.17487/RFC7139, March 2014, <<https://www.rfc-editor.org/info/rfc7139>>.

## 11.2. Informative References

[I-D.izh-ccamp-flex-e-fwk]  
Hussain, I., Valiveti, R., Pithewan, K., Wang, Q., Andersson, L., Zhang, F., Chen, M., Dong, J., Du, Z., zhenghaomian@huawei.com, z., Zhang, X., Huang, J., and Q. Zhong, "GMPLS Routing and Signaling Framework for Flexible Ethernet (FlexE)", draft-izh-ccamp-flex-e-fwk-00 (work in progress), October 2016.

## Authors' Addresses

Qilei Wang (editor)  
ZTE  
Nanjing  
CN

Email: wang.qilei@zte.com.cn

Radha Valiveti (editor)  
Infinera Corp  
Sunnyvale  
USA

Email: rvaliveti@infinera.com

Haomian Zheng (editor)  
Huawei  
CN

Email: zhenghaomian@huawei.com

Huub van Helvoort  
Hai Gaoming B.V

Email: huubatwork@gmail.com

Sergio Belotti  
Nokia

Email: [sergio.belotti@nokia.com](mailto:sergio.belotti@nokia.com)

CCAMP Working Group  
Internet-Draft  
Intended status: Standards Track

Z. Fan  
Huawei Technologies  
R. Valiveti  
I. Hussain  
Infinera  
Q. Wang  
ZTE  
Z. Ali  
Cisco  
October 30, 2017

Expires: April 30, 2018

## OSPF Extensions for the GMPLS Control of OTN B100G Network

draft-merge-ccamp-otn-b100g-routing-ext-00

### Abstract

ODUCn signal is recently introduced to OTN to support B100G feature. This document provides the OSPF extensions to control the OTN B100G Network.

### Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April XX, 2018.

### Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction .....	2
1.1. Requirements Language .....	3
2. Terminology .....	3
3. Overview of OSPF-TE Extensions for Support ODUCn .....	3
4. ISCD Format Extensions .....	3
4.1. Switching Capability Specific Information .....	4
4.1.1. Modification of Type 1 Container .....	4
4.1.2. Type 3 Container for advertising Unreserved ODUCn ..	5
5. Examples .....	6
5.1. Multiplexing ODUk over ODUCn .....	6
5.2. Advertising Unavailable TS Information of ODUCn .....	7
6. Security Considerations .....	9
7. IANA considerations .....	9
8. Contributors' Addresses .....	9
9. References .....	10
9.1. Normative References .....	10
9.2. Informative References .....	10
Authors' Addresses .....	10

## 1. Introduction

G.709 edition 5 [G709-2016] introduces ODUCn signal to support beyond 100G data rate. ODUCn signal, as a HO ODU, can carry OTN signals such as ODUk and ODUFlex. The tributary slot granularity of ODUCn is 5 Gbps. The OSPF-TE extensions defined in [RFC7138] cannot support the OTN B100G features.

B100G framework document [I-D.merge-ccamp-otn-b100g-fwk] provides the requirements of protocol extensions to support the GMPLS control of OTN B100G. This document provides OSPF-TE extensions to support the control of ODUCn.

Note: This document considers routing information for OTN electrical layer only. Routing information for OTN optical layer (i.e., OCh, OTSiA, and FlexO interfaces) is beyond the scope of this document.

### 1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

## 2. Terminology

OPUCn: Optical Payload Unit-Cn

ODUCn: Optical Data Unit-Cn

OTUCn: completely standardized Optical Transport Unit-Cn

OTUCn-M: Optical Transport Unit-Cn with n OxUC overhead instances and M 5G tributary slots

TS: Tributary Slot

TSG: Tributary Slot Granularity

## 3. Overview of OSPF-TE Extensions for Support ODUCh

As described in [I-D.merge-ccamp-otn-b100g-fwk], OSPF-TE should be extended to advertise the 5G tributary slot granularity, the multiplexing capabilities of ODUCh, and the available bandwidth information of ODUCh.

The advertisement of ODUCh information is used to synchronize the two end nodes of an ODUCh link. If the two ends have different tributary slot granularities, this ODUCh link should not be setup. If the two ends have different multiplexing hierarchies for ODUCh, the supported ODUk multiplexing should be the ODUk supported by both ends. If the two ends mark different tributary slots as unavailable, each end node should calculate the actual available TS (i.e., the intersection of available TS from two ends), and convert the actual available bandwidth to equivalent available ODUk bandwidth.

## 4. ISCD Format Extensions

As defined in [RFC4203], ISCD is used to describe the switching capability. Although ODUCh is not switchable, as discussed in Section 3, we still need advertise some capabilities to the other end of the ODUCh link. We re-use the OTN-TDM switching capability

defined in [RFC7138]. A new LSP encoding type is defined for ODUCn in [I-D.merge-ccamp-bl00g-signaling].

#### 4.1. Switching Capability Specific Information

Besides ODUCn signal, [G709-2016] also introduces ODUFlex for FlexE-aware signal and ODUFlex with IMP. Three new signal type need to be defined:

- o TBA1 - ODUCh
- o TBA2 - ODUflex (IMP)
- o TBA3 - ODUflex (FlexE-aware)

The Bandwidth sub-TLV defined in [RFC7138] contains two types. As ODUcn is a HO ODU, the multiplexing hierarchy is affected to have more stages. Type 1 Bandwidth sub-TLV need to be modified, and a new type Bandwidth sub-TLV is needed for ODUcn.

#### 4.1.1. Modification of Type 1 Container

The multiplexing hierarchy is represented by stages in [RFC7138]. As ODUk can be multiplexed into ODUCn, one more multiplexing stage can be introduced in both type 1 (fixed container) and type 2 (flexible container) Bandwidth sub-TLV. The extreme case for type 1 is that ODU0->ODU1->ODU2->ODU3->ODU4->ODUCn, which contains 5 stages. The original one-row space for stage field could be insufficient. Therefore, the Stage field needs to be modified to support multiplexing to ODUCn. The modified format of type 1 Bandwidth sub-TLV is depicted in the following figure:

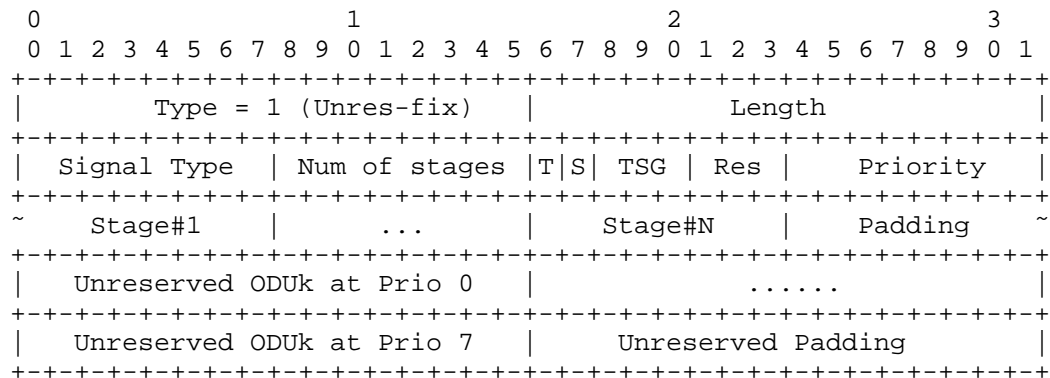


Figure 1: Modified Bandwidth sub-TLV for Type 1 containers

## 4.1.2. Type 3 Container for advertising Unreserved ODUCn

The format of the Bandwidth sub-TLV for ODUCn is depicted in the following figure:

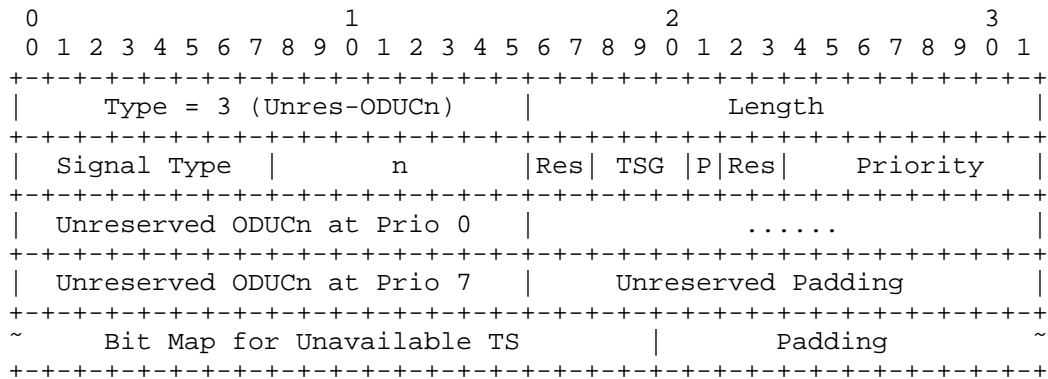


Figure 2: Extended Bandwidth sub-TLV for Type 3 containers

- o Signal Type (8 bits): Same as the definition in [RFC7138]. The value can only be ODUCn signal.
- o n (8 bits): Indicates the number of ODUC instance in an ODUCn signal.
- o Flags (8 bits):
  - \* P Flag (bit 22): Indicates whether the advertised ODUCn link is mapped to sub-rate OTUCn-M, which means some TS in this link are marked as unavailable. When ODUCn contains unavailable TS, P MUST be set, while when ODUCn does not contain unavailable TS, P MUST be cleared.
- o TSG (3 bits): Inherits the definition in [RFC7138] by adding a new value indicating the 5 Gbps TSG:
  - \* 4 - 5 Gbps only
- Priority (8 bits): Same as the definition in [RFC7138].

Unreserved ODUCn (16 bits): Indicates the Unreserved Bandwidth at a particular priority level. This field MUST be set to the number of the specific ODUCn, which is identified by the Signal Type field, the n field, and the Bit Map for Unavailable TS field, for a particular priority level. One field MUST be present for each bit set in the Priority field, and the fields are ordered to match the

Priority field. Fields MUST NOT be present for priority levels that are not indicated in the Priority field.

Unreserved Padding (16 bits): Same as the definition in [RFC7138].

Bit Map for Unavailable TS (variable): Indicates which tributary slots are marked as unavailable due to the bandwidth limitation from lower layer connection, which is different from occupied/allocated TS. The total number of unavailable TS can be calculated by summing this field. The length of this field is derived from the n field (the length is 20 x n). The sequence of this field follows the joint sequence of the tributary slots in the ODUCn and the order of ODUC instances. The first 20 bits are respectively for ODUC#1, the second 20 bits are respectively for ODUC#2, and so on. Each bit in the bit map represents the corresponding tributary slot in the ODUCn with a value of 1 or 0 indicating whether the tributary slot is marked as unavailable or not. When P bit is cleared, the Bit Map field is not required and MUST NOT be included.

Padding (variable): Are added after the Bit Map field to make the whole label a multiple of four bytes if necessary. Padding bits MUST be set to 0 and MUST be ignored on receipt.

## 5. Examples

The examples in the following pages are not normative and are not intended to imply or mandate any specific implementation.

### 5.1. Multiplexing ODUk over ODUCn

This example shows the advertisement of the ISCD for ODUCn. An OTUC2 link is considered with supported priorities 0,3 and multiplexing hierarchy ODU4->ODUC2.

The format of the advertised ISCD is depicted by the following figure:

```

      0              1              2              3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| SwCap=OTN_TDM | Encoding=ODUCn |   Reserved (all zeros)   |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Max LSP Bandwidth at priority 0 = 200 Gbps                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Max LSP Bandwidth at priority 1 = 0                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Max LSP Bandwidth at priority 2 = 0                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```



```

|           Max LSP Bandwidth at priority 3 = 200 Gbps           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Max LSP Bandwidth at priority 4 = 0                 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Max LSP Bandwidth at priority 5 = 0                 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Max LSP Bandwidth at priority 6 = 0                 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Max LSP Bandwidth at priority 7 = 0                 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Type = 1 (Unres-fix)           |           Length = 12           |
+-----+-----+-----+-----+-----+-----+-----+-----+
| SigType=ODU4 | #stages = 1 |X|X| 3 |0 0 0|1 0 0 1 0 0 0 0|
+-----+-----+-----+-----+-----+-----+-----+-----+
| Stage#1=ODUCn |           Padding (all zeros)           |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Unreserved ODU4 at Prio 0 = 2 | Unreserved ODU4 at Prio 3 = 2 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Type = 3 (Unres-ODUCn)           |           Length = 8           |
+-----+-----+-----+-----+-----+-----+-----+-----+
| SigType=ODUCn | n = 2 |0 0| 4 |0|0 0|1 0 0 1 0 0 0 0|
+-----+-----+-----+-----+-----+-----+-----+-----+
| Unreserved ODUC2 at Prio 0 =1 | Unreserved ODUC2 at Prio 3 =1 |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Figure 3: ISCD for ODU4 over OTUC2 link

The Max LSP Bandwidth is filled with the bandwidth of ODUC2 (i.e., 200 Gbps).

According to the multiplexing hierarchy, the advertised ODU4 has one stage to ODUCn. The number of unreserved ODU4 is 2 in this example.

The advertised ODUC2 has signal type as ODUCn, n as 2, and P bit cleared. The TSG value is 4, which means 5 Gbps granularity. The number of unreserved ODUC2 is 1 in this example.

## 5.2. Advertising Unavailable TS Information of ODUCn

This example shows the advertisement of unavailable TS information. An OTUC2-30 link is considered with supported priorities 0,3 and multiplexing hierarchy ODU4->ODUC2.

The format of the advertised ISCD is depicted by the following figure:

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
| SwCap=OTN_TDM | Encoding=ODUCn |   Reserved (all zeros)   |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 0 = 150 Gbps   |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 1 = 0         |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 2 = 0         |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 3 = 150 Gbps   |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 4 = 0         |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 5 = 0         |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 6 = 0         |
+-----+-----+-----+-----+
|               Max LSP Bandwidth at priority 7 = 0         |
+-----+-----+-----+-----+
|   Type = 1 (Unres-fix)   |   Length = 12   |
+-----+-----+-----+-----+
| SigType=ODU4 | #stages = 1 |X|X| 3 |0 0 0|1 0 0 1 0 0 0 0|
+-----+-----+-----+-----+
| Stage#1=ODUCn |   Padding (all zeros)   |
+-----+-----+-----+-----+
| Unreserved ODU4 at Prio 0 = 1 | Unreserved ODU4 at Prio 3 = 1 |
+-----+-----+-----+-----+
|   Type = 3 (Unres-ODUCn)   |   Length = 16   |
+-----+-----+-----+-----+
| SigType=ODUCn |   n = 2   |0 0| 4 |1|0 0|1 0 0 1 0 0 0 0|
+-----+-----+-----+-----+
| Unreserved ODUC2 at Prio 0 =1 | Unreserved ODUC2 at Prio 3 =1 |
+-----+-----+-----+-----+
|0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1|
+-----+-----+-----+-----+
|0 0 0 1 0 0 0 1|   Padding (all zeros)   |
+-----+-----+-----+-----+

```

Figure 4: ISCD for ODU4 over OTUC2-30 link

The Max LSP Bandwidth is filled with 150 Gbps, as ODUC2 has 10 unavailable tributary slots.

As the bandwidth of ODUC2 is reduced, the number of unreserved ODU4 is 1 in this example.

The advertised ODUC2 has signal type as ODUCn, n as 2, and P bit set. The TSG value is 4, which means 5 Gbps granularity. The number of unreserved ODUC2 is 1 in this example. The Bit Map field indicates which tributary slot is marked as unavailable, where the marking policy is vendor specific. In this example, bit-4, bit-8, bit-12, bit-16, bit-20, bit-24, bit-28, bit-32, bit-36, and bit-40 are set, which means the corresponding tributary slots are marked as unavailable.

## 6. Security Considerations

TBD.

## 7. IANA considerations

TBD.

## 8. Contributors' Addresses

Haomian Zheng  
Huawei Technologies

Email: zhenghaomian@huawei.com

Sergio Belotti  
Nokia

Email: sergio.belotti@nokia.com

Yunbin Xu  
CAICT

Email: xuyunbin@ritr.cn

Rajan Rao  
Infinera

Email: rrao@infinera.com

Huub van Helvoort  
Hai Gaoming B.V

Email: huubatwork@gmail.com

## 9. References

### 9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to indicate requirements levels", RFC 2119, March 1997.
- [G709-2016] ITU-T, "Interface for the Optical Transport Network (OTN)", G.709/Y.1331 Recommendation, June 2016.
- [RFC7138] Ceccarelli D., Zhang, F., Belotti, S., Rao, R., and J. Drake, "Traffic Engineering Extensions to OSPF for GMPLS Control of Evolving G.709 Optical Transport Networks", RFC7138, March 2014.
- [RFC4203] Kompella, K., Ed., and Y. Rekhter, Ed., "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC4203, October 2005.

### 9.2. Informative References

- [I-D.merge-ccamp-otn-b100g-fwk] Wang, Q., Ed., Valiveti, R., Ed., Zheng, H., Ed., Helvoort, H., and S. Belotti, "GMPLS Routing and Signaling Framework for B100G", draft-merge-ccamp-otn-b100g-fwk-02 (work in process), July 2017.
- [I-D.merge-ccamp-b100g-signaling] Wang, Q., Ed., Zheng, H., Valiveti, R., Helvoort, H., and Z. Ali, " GMPLS Signalling Extensions for control of B100G OTUCn/ODUCn Network ", draft-merge-ccamp-100g-signalling-00 (work in process), October 2017.

## Authors' Addresses

Zheyu Fan  
Huawei Technologies

Email: fanzheyu2@huawei.com

Radhakrishna Valiveti  
Infinera

Email: rvaliveti@infinera.com

Iftekhhar Hussain  
Infinera

Email: IHussain@infinera.com

Qilei Wang  
ZTE

Email: wang.qilei@zte.com.cn

Zafar Ali  
Cisco

Email: zali@cisco.com



CCAMP Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: September 12, 2017

X. Zhang  
K. Xiang  
Huawei Technologies  
A. Sharma  
R. Rao  
Infinera  
March 11, 2017

OTN Tunnel YANG Model  
draft-sharma-ccamp-otn-tunnel-model-01

Abstract

This document describes the YANG data model for OTN Tunnels.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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 <http://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 September 12, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology and Notations . . . . .	2
3. Model Overview . . . . .	3
3.1. Mux Service in Multi-Domain OTN Network . . . . .	3
3.2. Bookended and Non-BookEnded OTN Tunnel . . . . .	4
3.3. Network and Client side tunnel services . . . . .	4
3.4. OTN Tunnel YANG Tree . . . . .	4
3.5. OTN Tunnel YANG Code . . . . .	5
3.6. Transport Types YANG Code . . . . .	10
4. Security Considerations . . . . .	19
5. IANA Considerations . . . . .	19
6. Acknowledgements . . . . .	19
7. Normative References . . . . .	19
Authors' Addresses . . . . .	19

## 1. Introduction

OTN transport networks can carry various types of client services. In many cases, the client signal is carried over an OTN tunnel across connected domains in a multi-domain network. These OTN services can either be transported or switched in the OTN network. If an OTN tunnel is switched, then additional parameters need to be provided to create a Mux OTN service.

This document provides YANG model for creating OTN tunnel. The model augments the TE Tunnel model, which is an abstract model to create TE Tunnels.

## 2. Terminology and Notations

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in the YANG data tree presented later in this draft is defined in . They are provided below for reference.

- o Brackets "[" and "]" enclose list keys.
- o Abbreviations before data node names: "rw" means configuration (read-write) and "ro" state data (read-only).



- o Symbols after data node names: "?" means an optional node, "!" means a presence container, and "\*" denotes a list and leaf-list.
- o Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- o Ellipsis ("...") stands for contents of subtrees that are not shown.

### 3. Model Overview

#### 3.1. Mux Service in Multi-Domain OTN Network

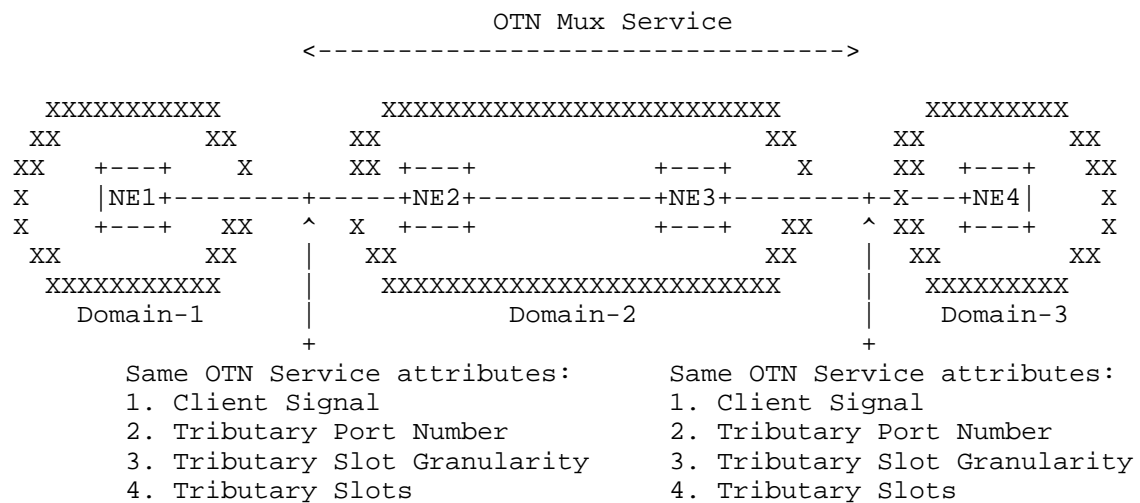


Figure 1: OTN Mux Service in a multi-domain network topology

Figure 1 shows a multi-domain OTN network with three domains. In this example, user wants to setup an end-to-end OTN service that passes through Domain-2. In order to create an OTN mux service in Domain-2, user will need to specify the exact details of the client side LO-ODU on NE2 and NE3, so that these service endpoints can be paired with the LO-ODU endpoints on NE1 and NE4, respectively.

Let's assume that ODU4 is the client side HO-ODU on NE2 and NE3, and the client signal is ODU2. User will need to specify the OTN client signal (ODU2 in this example), the Tributary Port Number (TPN), Tributary Slot Granularities (TSG) and tributary slots to be used.

As shown in the figure above, these service parameters must be the same between NE1 and NE2, and NE3 and NE4.

Once the OTN Mux service is setup in Domain-2, the incoming signal from either NE1 and/or NE4 will be switched inside Domain-2, and delivered to NE at the other end.

### 3.2. Bookended and Non-BookEnded OTN Tunnel

OTN tunnel model provides support for both bookended and non-bookended OTN tunnels.

For bookended tunnels, the same client signal is present on source and destination endpoints. For example, ODU2e bookended tunnel will have the same ODU2e client signal at both source and destination endpoints.

For non-bookended tunnels, different client signals are present on source and destination endpoints. For example, the client signal can be ODU2e on the source endpoint and the handoff at the destination can be 10GbE-LAN client signal.

### 3.3. Network and Client side tunnel services

The OTN tunnel model provides support for both network to network and client to client tunnels. For network to network tunnel, network termination points on source and destination node represent source and destination endpoints. For client to client tunnel, client termination points on source and destination node represent source and destination endpoints.

If a client to client tunnel needs to use one or more HO (or server) network to network tunnels, ERO and routing constraints, defined in the base TE model, can be used to route the client tunnel over one or more server tunnels.

### 3.4. OTN Tunnel YANG Tree

```

module: ietf-otn-tunnel
augment /te:te/te:tunnels/te:tunnel/te:config:
  +--rw payload-treatment?      enumeration
  +--rw src-client-signal?      identityref
  +--rw src-tpn?                uint16
  +--rw src-tsg?                identityref
  +--rw src-tributary-slot-count? uint16
  +--rw src-tributary-slots
  |   +--rw values*            uint8
  +--rw dst-client-signal?      identityref
  +--rw dst-tpn?                uint16
  +--rw dst-tsg?                identityref
  +--rw dst-tributary-slot-count? uint16
  +--rw dst-tributary-slots
  |   +--rw values*            uint8
augment /te:te/te:tunnels/te:tunnel/te:state:
  +--ro payload-treatment?      enumeration
  +--ro src-client-signal?      identityref
  +--ro src-tpn?                uint16
  +--ro src-tsg?                identityref
  +--ro src-tributary-slot-count? uint16
  +--ro src-tributary-slots
  |   +--ro values*            uint8
  +--ro dst-client-signal?      identityref
  +--ro dst-tpn?                uint16
  +--ro dst-tsg?                identityref
  +--ro dst-tributary-slot-count? uint16
  +--ro dst-tributary-slots
  |   +--ro values*            uint8

```

### 3.5. OTN Tunnel YANG Code

```

<CODE BEGINS>file "ietf-otn-tunnel@2017-03-11.yang"

module ietf-otn-tunnel {
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-otn-tunnel";
  prefix "otn-tunnel";

  import ietf-te { prefix "te"; }
  import ietf-transport-types { prefix "tran-types"; }
  //import yang-ext { prefix ext; revision-date 2013-07-09; }

  organization

```

```
"IETF CCAMP Working Group";

contact
  "WG Web: <http://tools.ietf.org/wg/ccamp/>
  WG List: <mailto:ccamp@ietf.org>

  Editor: Anurag Sharma
          <mailto:AnSharma@infinera.com>

  Editor: Rajan Rao
          <mailto:rrao@infinera.com>

  Editor: Xian Zhang
          <mailto:zhang.xian@huawei.com>

  Editor: Kun Xiang
          <mailto:xiangkun@huawei.com>";

description
  "This module defines a model for OTN Tunnel Services.";

revision "2017-03-11" {
  description
    "Revision 0.3";
  reference "TBD";
}

grouping otn-tunnel-endpoint {
  description "Parameters for OTN tunnel.";

    leaf payload-treatment {
      type enumeration {
        enum switching;
        enum transport;
      }
      default switching;
      description
        "Treatment of the incoming payload. Payload can
        either be switched, or transported as is.";
    }

    leaf src-client-signal {
      type identityref {
        base tran-types:client-signal;
      }
      description
        "Client signal at the source endpoint of
        the tunnel.";
    }
  }
}
```

```
    }

    leaf src-tpn {
      type uint16 {
        range "0..4095";
      }
      description
        "Tributary Port Number. Applicable in case of mux
        services.";
      reference
        "RFC7139: GMPLS Signaling Extensions for Control of
        Evolving G.709 Optical Transport Networks.";
    }

    leaf src-tsg {
      type identityref {
        base tran-types:tributary-slot-granularity;
      }
      description
        "Tributary slot granularity. Applicable in case of mux
        services.";
      reference
        "G.709/Y.1331, February 2016: Interfaces for the
        Optical Transport Network (OTN)";
    }

    leaf src-tributary-slot-count {
      type uint16;
      description
        "Number of tributary slots used at the source.";
    }

    container src-tributary-slots {
      description
        "A list of tributary slots used by the client
        service. Applicable in case of mux services.";
      leaf-list values {
        type uint8;
        description
          "Tributary tributary slot value.";
        reference
          "G.709/Y.1331, February 2016: Interfaces for the
          Optical Transport Network (OTN)";
      }
    }

    leaf dst-client-signal {
      type identityref {
```

```
        base tran-types:client-signal;
    }
    description
        "Client signal at the destination endpoint of
        the tunnel.";
}

leaf dst-tpn {
    type uint16 {
        range "0..4095";
    }
    description
        "Tributary Port Number. Applicable in case of mux
        services.";
    reference
        "RFC7139: GMPLS Signaling Extensions for Control of
        Evolving G.709 Optical Transport Networks.";
}

leaf dst-tsg {
    type identityref {
        base tran-types:tributary-slot-granularity;
    }
    description
        "Tributary slot granularity. Applicable in case of mux
        services.";
    reference
        "G.709/Y.1331, February 2016: Interfaces for the
        Optical Transport Network (OTN)";
}

leaf dst-tributary-slot-count {
    type uint16;
    description
        "Number of tributary slots used at the destination.";
}

container dst-tributary-slots {
    description
        "A list of tributary slots used by the client
        service. Applicable in case of mux services.";
    leaf-list values {
        type uint8;
        description
            "Tributary slot value.";
        reference
            "G.709/Y.1331, February 2016: Interfaces for the
            Optical Transport Network (OTN)";
    }
}
```

```

    }
  }
}

/*
Note: Comment has been given to authors of TE Tunnel model to add
tunnel-types to the model in order to identify the technology
type of the service.

grouping otn-service-type {
  description
    "Identifies the OTN Service type.";
  container otn-service {
    presence "Indicates OTN Service.";
    description
      "Its presence identifies the OTN Service type.";
  }
} // otn-service-type

augment "/te:te/te:tunnels/te:tunnel/te:tunnel-types" {
  description
    "Introduce OTN service type for tunnel.";
  ext:augment-identifier otn-service-type-augment;
  uses otn-service-type;
}
*/

/*
Note: Comment has been given to authors of TE Tunnel model to add
list of endpoints under config to support P2MP tunnel.
*/
augment "/te:te/te:tunnels/te:tunnel/te:config" {
  description
    "Augment with additional parameters required for OTN
    service.";
  //ext:augment-identifier otn-tunnel-endpoint-config-augment;
  uses otn-tunnel-endpoint;
}

augment "/te:te/te:tunnels/te:tunnel/te:state" {
  description
    "Augment with additional parameters required for OTN
    service.";
  //ext:augment-identifier otn-tunnel-endpoint-state-augment;
  uses otn-tunnel-endpoint;
}

/*

```

Note: Comment has been given to authors of TE Tunnel model to add tunnel-lifecycle-event to the model. This notification is reported for all lifecycle changes (create, delete, and update) to the tunnel or lsp.

```
augment "/te:tunnel-lifecycle-event" {
  description
    "OTN service event";
  uses otn-service-type;
  uses otn-tunnel-params;

  list endpoint {
    key
      "endpoint-address tp-id";
    description
      "List of Tunnel Endpoints.";
    uses te:tunnel-endpoint;
    uses otn-tunnel-params;
  }
}
*/
}
```

<CODE ENDS>

### 3.6. Transport Types YANG Code

```
<CODE BEGINS> file "ietf-transport-types@2016-10-25.yang"

module ietf-transport-types {
  namespace "urn:ietf:params:xml:ns:yang:ietf-transport-types";
  prefix "tran-types";

  organization
    "IETF CCAMP Working Group";
  contact
    "WG Web: <http://tools.ietf.org/wg/ccamp/>
    WG List: <mailto:ccamp@ietf.org>

    Editor: Anurag Sharma
           <mailto:AnSharma@infinera.com>

    Editor: Rajan Rao
           <mailto:rrao@infinera.com>

    Editor: Xian Zhang
```



```
<mailto:zhang.xian@huawei.com>";

description
  "This module defines transport types.";

revision "2016-10-25" {
  description
    "Revision 0.2";
  reference "TBD";
}

identity tributary-slot-granularity {
  description
    "Tributary slot granularity.";
  reference
    "G.709/Y.1331, February 2016: Interfaces for the
      Optical Transport Network (OTN)";
}

identity tsg-1.25G {
  base tributary-slot-granularity;
  description
    "1.25G tributary slot granularity.";
}

identity tsg-2.5G {
  base tributary-slot-granularity;
  description
    "2.5G tributary slot granularity.";
}

identity tributary-protocol-type {
  description
    "Base identity for protocol framing used by
      tributary signals.";
}

identity prot-OTU1 {
  base tributary-protocol-type;
  description
    "OTU1 protocol (2.66G)";
}

/*
identity prot-OTU1e {
  base tributary-protocol-type;
  description
    "OTU1e type (11.04G)";
}
```

```
    }

    identity prot-OTU1f {
        base tributary-protocol-type;
        description
            "OTU1f type (11.27G)";
    }
    /*
    identity prot-OTU2 {
        base tributary-protocol-type;
        description
            "OTU2 type (10.70G)";
    }

    identity prot-OTU2e {
        base tributary-protocol-type;
        description
            "OTU2e type (11.09G)";
    }

    /*
    identity prot-OTU2f {
        base tributary-protocol-type;
        description
            "OTU2f type (11.31G)";
    }
    /*

    identity prot-OTU3 {
        base tributary-protocol-type;
        description
            "OTU3 type (43.01G)";
    }

    /*
    identity prot-OTU3e1 {
        base tributary-protocol-type;
        description
            "OTU3e1 type (44.57G)";
    }

    identity prot-OTU3e2 {
        base tributary-protocol-type;
        description
            "OTU3e2 type (44.58G)";
    }
    /*
```

```
identity prot-OTU4 {
    base tributary-protocol-type;
    description
        "OTU4 type (111.80G)";
}

identity prot-OTUCn {
    base tributary-protocol-type;
    description
        "OTUCn type (beyond 100G)";
}

identity prot-ODU0 {
    base tributary-protocol-type;
    description
        "ODU0 protocol (1.24G).";
}

identity prot-ODU1 {
    base tributary-protocol-type;
    description
        "ODU1 protocol (2.49G).";
}

/*
identity prot-ODU1e {
    base tributary-protocol-type;
    description
        "ODU1e protocol (10.35G).";
}

identity prot-ODU1f {
    base tributary-protocol-type;
    description
        "ODU1f protocol (10.56G).";
}
*/

identity prot-ODU2 {
    base tributary-protocol-type;
    description
        "ODU2 protocol (10.03G).";
}

identity prot-ODU2e {
    base tributary-protocol-type;
    description
        "ODU2e protocol (10.39G).";
}
```

```
    }

    /*
    identity prot-ODU2f {
        base tributary-protocol-type;
        description
            "ODU2f protocol (10.60G).";
    }
    */

    identity prot-ODU3 {
        base tributary-protocol-type;
        description
            "ODU3 protocol (40.31G).";
    }

    /*
    identity prot-ODU3e1 {
        base tributary-protocol-type;
        description
            "ODU3e1 protocol (41.77G).";
    }

    identity prot-ODU3e2 {
        base tributary-protocol-type;
        description
            "ODU3e2 protocol (41.78G).";
    }
    */

    identity prot-ODU4 {
        base tributary-protocol-type;
        description
            "ODU4 protocol (104.79G).";
    }

    identity prot-ODUFlex-cbr {
        base tributary-protocol-type;
        description
            "ODU Flex CBR protocol for transporting constant bit
            rate signal.";
    }

    identity prot-ODUFlex-gfp {
        base tributary-protocol-type;
        description
            "ODU Flex GFP protocol for transporting stream of packets
            using Generic Framing Procedure.";
```

```
    }

    identity prot-ODUCn {
        base tributary-protocol-type;
        description
            "ODUCn protocol (beyond 100G).";
    }

    identity prot-1GbE {
        base tributary-protocol-type;
        description
            "1G Ethernet protocol";
    }

    identity prot-10GbE-LAN {
        base tributary-protocol-type;
        description
            "10G Ethernet LAN protocol";
    }

    identity prot-40GbE {
        base tributary-protocol-type;
        description
            "40G Ethernet protocol";
    }

    identity prot-100GbE {
        base tributary-protocol-type;
        description
            "100G Ethernet protocol";
    }

    identity client-signal {
        description
            "Base identity from which specific client signals for the
            tunnel are derived.";
    }

    identity client-signal-1GbE {
        base client-signal;
        description
            "Client signal type of 1GbE";
    }

    identity client-signal-10GbE-LAN {
        base client-signal;
        description
            "Client signal type of 10GbE LAN";
    }
```

```
    }

    identity client-signal-10GbE-WAN {
        base client-signal;
        description
            "Client signal type of 10GbE WAN";
    }

    identity client-signal-40GbE {
        base client-signal;
        description
            "Client signal type of 40GbE";
    }

    identity client-signal-100GbE {
        base client-signal;
        description
            "Client signal type of 100GbE";
    }

    identity client-signal-OC3_STM1 {
        base client-signal;
        description
            "Client signal type of OC3 & STM1";
    }

    identity client-signal-OC12_STM4 {
        base client-signal;
        description
            "Client signal type of OC12 & STM4";
    }

    identity client-signal-OC48_STM16 {
        base client-signal;
        description
            "Client signal type of OC48 & STM16";
    }

    identity client-signal-OC192_STM64 {
        base client-signal;
        description
            "Client signal type of OC192 & STM64";
    }

    identity client-signal-OC768_STM256 {
        base client-signal;
        description
            "Client signal type of OC768 & STM256";
    }
```

```
    }

    identity client-signal-ODU0 {
        base client-signal;
        description
            "Client signal type of ODU0 (1.24G)";
    }

    identity client-signal-ODU1 {
        base client-signal;
        description
            "ODU1 protocol (2.49G)";
    }

    identity client-signal-ODU2 {
        base client-signal;
        description
            "Client signal type of ODU2 (10.03G)";
    }

    identity client-signal-ODU2e {
        base client-signal;
        description
            "Client signal type of ODU2e (10.39G)";
    }

    identity client-signal-ODU3 {
        base client-signal;
        description
            "Client signal type of ODU3 (40.31G)";
    }

    /*
    identity client-signal-ODU3e2 {
        base client-signal;
        description
            "Client signal type of ODU3e2 (41.78G)";
    }
    */

    identity client-signal-ODU4 {
        base client-signal;
        description
            "Client signal type of ODU4 (104.79G)";
    }

    identity client-signal-ODUFlex-cbr {
        base client-signal;
```

```
        description
            "Client signal type of ODU Flex CBR";
    }

    identity client-signal-ODUFlex-gfp {
        base client-signal;
        description
            "Client signal type of ODU Flex GFP";
    }

    identity client-signal-ODUCn {
        base client-signal;
        description
            "Client signal type of ODUCn (beyond 100G).";
    }

    identity client-signal-FC400 {
        base client-signal;
        description
            "Client signal type of Fibre Channel FC400.";
    }

    identity client-signal-FC800 {
        base client-signal;
        description
            "Client signal type of Fibre Channel FC800.";
    }

    identity client-signal-FICON-4G {
        base client-signal;
        description
            "Client signal type of Fibre Connection 4G.";
    }

    identity client-signal-FICON-8G {
        base client-signal;
        description
            "Client signal type of Fibre Connection 8G.";
    }
}
<CODE ENDS>
```



## 4. Security Considerations

TBD.

## 5. IANA Considerations

TBD.

## 6. Acknowledgements

TBD.

## 7. Normative References

- [G.709] "Interfaces for the Optical Transport Network(OTN)", G.709/Y.1331 Recommendation , June 2016.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <<http://www.rfc-editor.org/info/rfc6020>>.
- [RFC7139] Zhang, F., Ed., Zhang, G., Belotti, S., Ceccarelli, D., and K. Pithewan, "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks", RFC 7139, DOI 10.17487/RFC7139, March 2014, <<http://www.rfc-editor.org/info/rfc7139>>.

## Authors' Addresses

Xian Zhang  
Huawei Technologies  
F3-5-B R&D Center, Huawei Industrial Base, Bantian, Longgang District  
Shenzhen, Guangdong 518129  
P.R.China

Email: [zhang.xian@huawei.com](mailto:zhang.xian@huawei.com)

Kun Xiang  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base, Bantian, Longgang District  
Shenzhen, Guangdong 518129  
P.R.China

Email: xiangkun@huawei.com

Anurag Sharma  
Infinera

Email: ansharma@infinera.com

Rajan Rao  
Infinera  
169 Java Drive  
Sunnyvale, CA 94089  
USA

Email: rrao@infinera.com

CCAMP Working Group  
Internet Draft  
Intended status: Informational

I. Busi (Ed.)  
Huawei  
D. King (Ed.)  
Lancaster University

Expires: January 2018

July 3, 2017

Analysis of Transport North Bound Interface Use Case 1  
draft-tnbidt-ccamp-transport-nbi-analysis-uc1-00

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on December 3, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Abstract

This document analyses how YANG models being defined by IETF (TEAS and CCAMP WG in particular) can be used to support Use Case 1 (single-domain with single-layer) scenarios as referenced later in this document.

## Table of Contents

1. Introduction.....	2
1.1. Assumptions.....	3
1.2. Feedbacks provided to the IETF Working Groups.....	3
2. Conventions used in this document.....	4
3. High-level Overview.....	5
3.1. Topology Abstraction.....	5
3.1.1. ODU White Topology Abstraction.....	5
3.2. Service Configuration.....	7
3.2.1. ODU Transit Service.....	7
3.2.2. OTN Client Private Line Service.....	9
3.2.3. EPL over ODU Service.....	9
4. Topology Abstraction: detailed JSON examples.....	10
4.1. ODU White Topology Abstraction.....	10
5. Service Configuration: detailed JSON examples.....	10
5.1. ODU Transit Service.....	10
6. Security Considerations.....	10
7. IANA Considerations.....	10
8. Conclusions.....	11
9. References.....	11
9.1. Normative References.....	11
9.2. Informative References.....	11
10. Acknowledgments.....	11
Appendix A. Validating a JSON fragment against a YANG Model.....	13
A.1. DSDL-based approach.....	13
A.2. Why not using a XSD-based approach.....	13
A.3. JSON Code: use-case-1-topology-01.json.....	14
A.4. JSON Code: use-case-1-odu2-service-01.json.....	14

## 1. Introduction

This document analyses how YANG models being developed by IETF (TEAS and CCAMP WG) can be used to support Use Case 1 (single-domain with single-layer) scenarios as described in [TNBI- UseCases].

### 1.1. Assumptions

This document is analyzing how existing models developed by the IETF can be used at the MPI between the Transport PNC and the MDSC to support the use case 1 scenarios as defined in section 3 of [TNBI-UseCases].

This document assumes the applicability of the YANG models to the ACTN interfaces as defined in [ACTN-YANG] and therefore considers the TE Topology YANG model defined in [TE-TOPO], with the OTN Topology augmentation defined in [OTN-TOPO] and the TE Tunnel YANG model defined in [TE-TUNNEL], with the OTN Tunnel augmentation defined in [OTN-TUNNEL].

The analysis of how to use the attributes in the I2RS Topology YANG model, defined in [I2RS-TOPO], is for further study.

Moreover this document is making the following assumptions, still to be validated with TEAS WG:

1. The MDSC can request, at the MPI, the Transport PNC to setup a Transit Tunnel Segment using the TE Tunnel YANG model: in this case, since the endpoints of the E2E Tunnel are outside the domain controlled by the Transport PNC, the MDSC would not specify any source or destination TTP (i.e., it would leave the source, destination, src-tp-id and dst-tp-id attributes empty) and it would use the explicit-route-object list to specify the ingress and egress links of the Transit Tunnel Segment.
2. The Transport PNC provides to the MDSC, at the MPI, the list of available timeslots on the access links using the TE Topology YANG model and OTN Topology augmentation. The TE Topology YANG model in [TE-TOPO] is being updated to report the label set information.

### 1.2. Feedbacks provided to the IETF Working Groups

The analysis done in this version of this document has triggered the following feedbacks to TEAS WG:

- o On-going discussion about how to use the TE Tunnel YANG model in [TE-TUNNEL] to support tunnel segments.
- o Need to change TE Tunnel YANG model in [TE-TUNNEL] to clarify that the router-id and interface-id attributes in the unnumbered explicit-route-object corresponds to the te-node-id and te-tp-id attributes identifying an LTP in the TE Topology YANG model.

- o Need to add information about the label set (e.g., list of available timeslots) in the TE Topology and TE Tunnel YANG models.
- o Some detailed fixes to the TE Tunnel YANG model in [TE-TUNNEL] have also been identified during the validation of the JSON examples against the TE Tunnel YANG model.

## 2. Conventions used in this document

This document provides some detailed JSON code examples to describe how the YANG models being developed by IETF (TEAS and CCAMP WG in particular) can be used.

The examples are provided using JSON because JSON code is easier for humans to read and write.

Different objects need to have an identifier. The convention used to create mnemonic identifiers is to use the object name (e.g., S3 for node S3), followed by its type (e.g., NODE), separated by an "-", followed by "-ID". For example the mnemonic identifier for node S3 would be S3-NODE-ID.

JSON language does not support the insertion of comments that have been instead found to be useful when writing the examples. This document inserts comments into the JSON code as JSON name/value pair with the JSON name string starting with the "://" characters. For example, when describing the example of a TE Topology instance representing the ODU Abstract Topology exposed by the Transport PNC, the following comment has been added to the JSON code:

```
"// comment": "ODU Abstract Topology @ MPI",
```

The JSON code examples provided in this document have been validated against the YANG models following the validation process described in Appendix A, which would not consider the comments.

In order to have successful validation of the examples, some numbering scheme has been defined to assign identifiers to the different entities which would pass the syntax checks. In that case, to simplify the reading, another JSON name/value pair, formatted as a comment and using the mnemonic identifiers is also provided. For example, the identifier of node S3 (S3-NODE-ID) has been assumed to be "10.0.0.3" and would be shown in the JSON code example using the two JSON name/value pair:

```
"// te-node-id": "S3-NODE-ID",
```

```
"te-node-id": "10.0.0.3",
```

The first JSON name/value pair will be automatically removed in the first step of the validation process while the second JSON name/value pair will be validate against the YANG model definitions.

### 3. High-level Overview

Use Case 1 is described in [TNBI-UseCases] as a single-domain with single layer network scenario supporting different types of services. This section provides an high-level overview of how IETF YANG models can be used to support these uses cases at the MPI between the Transport PNC and the MDSC.

Section 3.1 describes the topology abstraction provided to the MDSC by the Transport PNC at the MPI.

Section 3.2 describes how the difference services, defined in section 3.3 of [TNBI-UseCases], can be requested to the Transport PNC by the MDSC at the MPI.

#### 3.1. Topology Abstraction

##### 3.1.1. ODU White Topology Abstraction

In case the Transport PNC exports to the MDSC a white topology, at the MPI there will be one TE Topology instance for the ODU layer (called "ODU Topology") containing one TE Node (called "ODU Node") for each physical node, as shown in Figure 1 below.

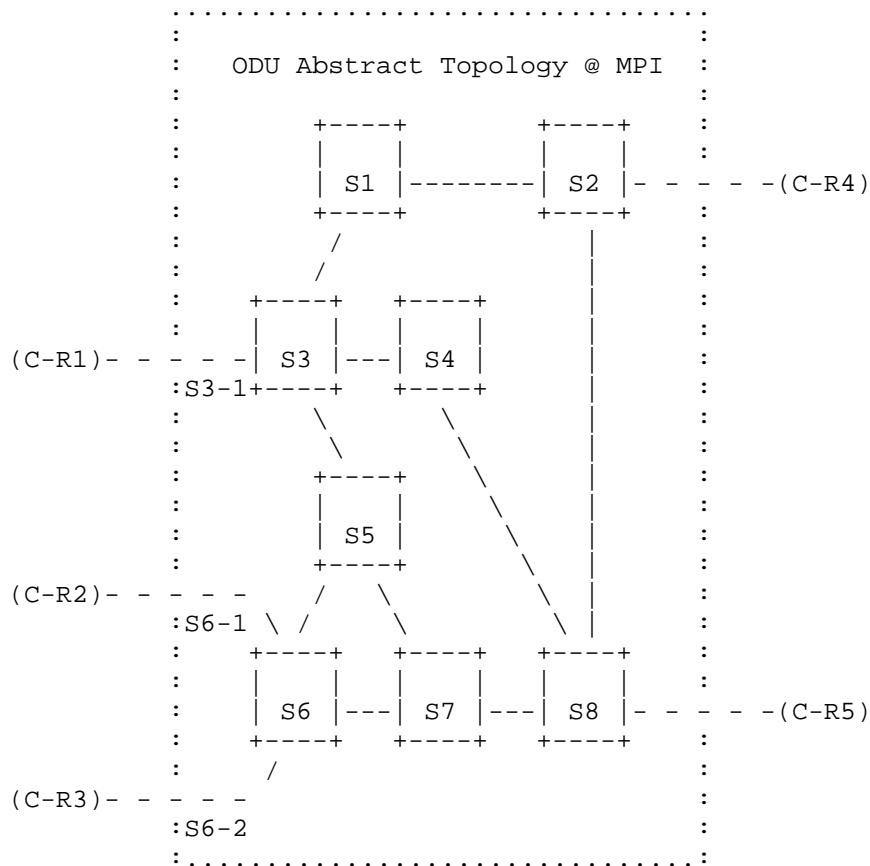


Figure 1 White Topology Abstraction (ODU Topology)

The ODU Nodes in Figure 1 are using with the same names as the physical nodes to simplify the description of the mapping between the ODU Nodes exposed by the Transport PNCs at the MPI and the physical nodes in the data plane.

As described in section 3.2 of [TNBI-UseCases], it is assumed that the physical links between the physical nodes are pre-configured up to the OTU4 trail using mechanisms which are outside the scope of this document. The Transport PNC exports to the MDSC via the MPI, one TE Link (called "ODU Link") for each of these physical links.

Access links in Figure 1 are shown as ODU Links: the modeling of the access links for other access technologies is currently an open issue.



The "external-domain" container allows the MDSC to glue together the ODU Topology provided by the Transport PNC with the information provided by the IP PNC to know which access link is connected with each link/router in the IP domain (e.g., that C-R1 is connected with the access link terminating on S3-1 LTP in the ODU Topology).

### 3.2. Service Configuration

#### 3.2.1. ODU Transit Service

In this case, the access links are configured as ODU Link, as described in section 3.1.1 above.

As described in section 3.3.1 of [TNBI-UseCases], the MDSC needs to setup an ODU2 trail, supporting an IP link, between C-R1 and C-R3.

From the topology information described in section 3.1.1 above, the MDSC can know that C-R1 is attached to the access link terminating on S3-1 LTP in the ODU Topology and that C-R3 is attached to the access link terminating on S6-2 LTP in the ODU Topology.

Based on the assumption 1) in section Error! Reference source not found., MDSC would then request Transport PNC to setup an ODU2 (Transit Segment) Tunnel between S3-1 and S6-2 LTPs:

- o Source and Destination TTP are not specified (since it is a Transit Tunnel)
- o Ingress and egress points are indicated in the explicit-route-objects of the primary path:
  - o The first element of the explicit-route-objects references the access link terminating on S3-1 LTP
  - o Last element of the explicit-route-objects references the access link terminating on S6-2 LTP

The configuration of the timeslots used by the ODU2 connection within the transport network domain (i.e., on the internal links) is a matter of the Transport PNC and its interactions with the physical network elements and therefore is outside the scope of this document.

However, the configuration of the timeslots used by the ODU2 connection at the edge of the transport network domain (i.e., on the access links) needs to take into account not only the timeslots available on the physical nodes at the edge of the transport network domain (e.g., S3 and S6) but also on the devices, outside of the

transport network domain, connected through these access links (e.g., C-R1 and C-R3).

Based on the assumption 2) in section Error! Reference source not found., MDSC, when requesting the Transport PNC to setup the (Transit Segment) ODU2 Tunnel, it would also configure the timeslots to be used on the access links. The MDSC can know the timeslots which are available on the edge OTN Node (e.g., S3 and S6) from the OTN Topology information exposed by the Transport PNC at the MPI as well as the timeslots which are available on the devices, outside of the transport network domain, connected through these access links (e.g., C-R1 and C-R3) by means which are outside the scope of this document.

The Transport PNC performs path computation and sets up the ODU2 cross-connections within the physical nodes S3, S5 and S6, as shown in section 4.3.1 of [TNBI-UseCases].

The Transport PNC reports the status of the created ODU2 (Transit Segment) Tunnel and its path within the ODU Topology as shown in Figure 2 below:

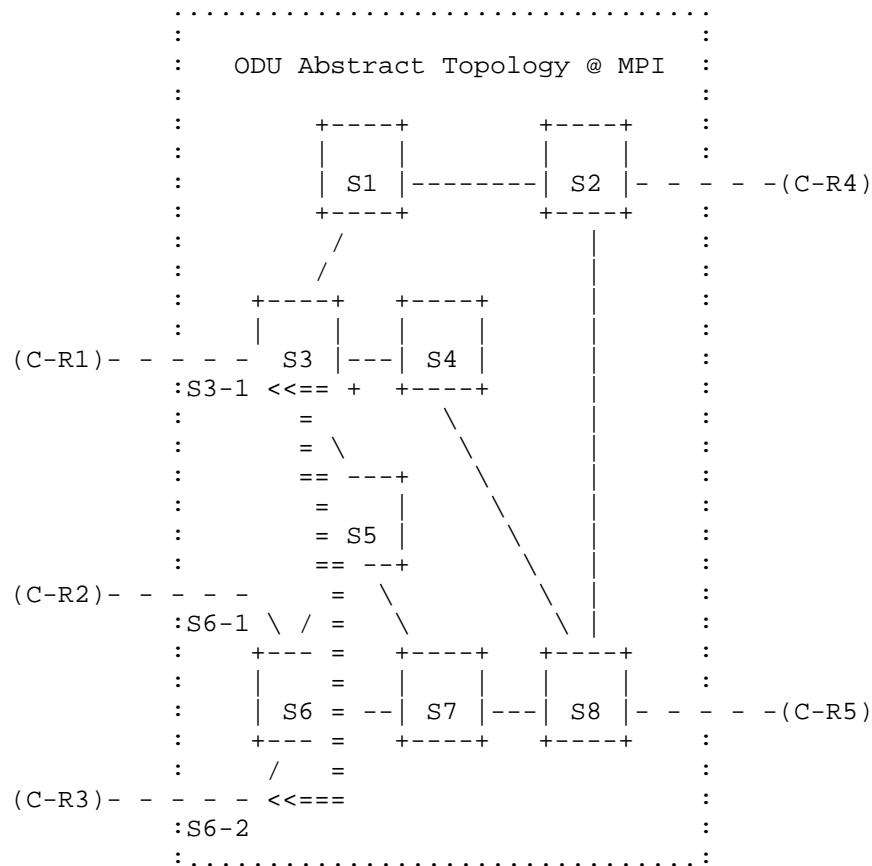


Figure 2 ODU2 Transit Tunnel

### 3.2.2. OTN Client Private Line Service

To be added

### 3.2.3. EPL over ODU Service

To be added

#### 4. Topology Abstraction: detailed JSON examples

##### 4.1. ODU White Topology Abstraction

Section 3.1.1 describes how the Transport PNC can provide a white topology abstraction to the MDSC via the MPI. Figure 1 is an example of such ODU Topology.

This section provides the detailed JSON code describing this ODU Topology, using the [TE-TOPO] and [OTN-TOPO] YANG models.

Note that this example is based on -09 version of [TE-TOPO] and on the -00 version of [OTN-TOPO]. Further changes to align with latest updates of these YANG models will be provided in the future version of this document.

JSON code "use-case-1-topology-01.json" has been provided at in the appendix of this document.

#### 5. Service Configuration: detailed JSON examples

##### 5.1. ODU Transit Service

Section 3.2.1 describes how the MDSC can request a Transport PNC, via the MPI, to setup an ODU2 transit service over an ODU Topology described in section 3.1.1.

This section provides the detailed JSON code describing this ODU Topology, using the [TE-TUNNEL] and [OTN-TUNNEL] YANG models.

Note that this example is based on -06 version of [TE-TUNNEL] and on the -02 version of [OTN-TUNNEL]. Further changes to align with latest updates of these YANG models will be provided in the future version of this document.

JSON code "use-case-1-odu2-service-01.json" has been provided at in the appendix of this document.

#### 6. Security Considerations

This section is for further study

#### 7. IANA Considerations

This document requires no IANA actions.

## 8. Conclusions

This section is for further study

## 9. References

### 9.1. Normative References

- [TNBI-UseCases] Busi, I., King, D. et al, "Transport Northbound Interface Use Cases", draft-tnbidt-ccamp-transport-nbi-use-cases, work in progress.
- [TE-TOPO] Liu, X. et al., "YANG Data Model for TE Topologies", draft-ietf-teas-yang-te-topo, work in progress.
- [OTN-TOPO] Zheng, H. et al., "A YANG Data Model for Optical Transport Network Topology", draft-ietf-ccamp-otn-topo-yang, work in progress.
- [TE-TUNNEL] Saad, T. et al., "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te, work in progress.
- [OTN-TUNNEL] Zheng, H. et al., "OTN Tunnel YANG Model", draft-sharma-ccamp-otn-tunnel-model, work in progress.

### 9.2. Informative References

- [ACTN-YANG] Zhang, X. et al., "Applicability of YANG models for Abstraction and Control of Traffic Engineered Networks", draft-zhang-teas-actn-yang, work in progress.
- [I2RS-TOPO] Clemm, A. et al., "A Data Model for Network Topologies", draft-ietf-i2rs-yang-network-topo, work in progress.

## 10. Acknowledgments

The authors would like to thank all members of the Transport NBI Design Team involved in the definition of use cases, gap analysis and guidelines for using the IETF YANG models at the Northbound Interface (NBI) of a Transport SDN Controller.

The authors would like to thank Xian Zhang, Anurag Sharma, Sergio Belotti, Tara Cummings, Michael Scharf, Karthik Sethuraman, Oscar

Gonzalez de Dios, Hans Bjursrom and Italo Busi for having initiated the work on gap analysis for transport NBI and having provided foundations work for the development of this document.

The authors would like to thank the authors of the TE Topology and Tunnel YANG models [TE-TOPO] and [TE-TUNNEL], in particular Igor Bryskin, Vishnu Pavan Beeram, Tarek Saad and Xufeng Liu, for their support in addressing any gap identified during the analysis work.

This document was prepared using 2-Word-v2.0.template.dot.

## Appendix A. Validating a JSON fragment against a YANG Model

The objective is to have a tool that allows validating whether a piece of JSON code is compliant with a YANG model without using a client/server.

### A.1. DSDL-based approach

The idea is to generate a JSON driver file (JTOX) from YANG, then use it to translate JSON to XML and validate it against the DSDL schemas, as shown in Figure 3.

Useful link: <https://github.com/mbj4668/pyang/wiki/XmlJson>

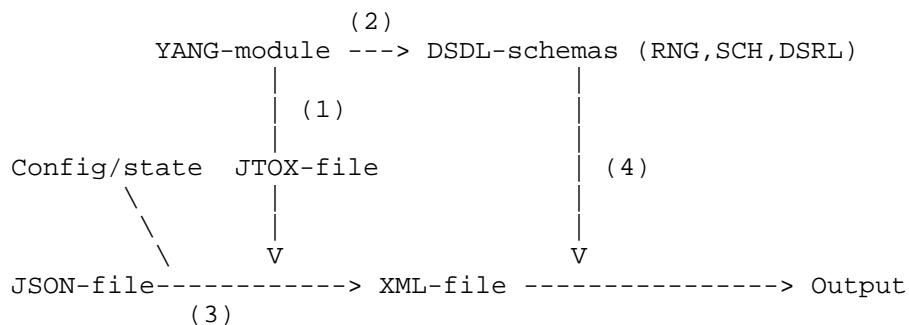


Figure 3 - DSDL-based approach for JSON code validation

In order to allow the use of comments following the convention defined in section 0 without impacting the validation process, these comments will be automatically removed from the JSON-file that will be validate.

### A.2. Why not using a XSD-based approach

This approach has been analyzed and discarded because no longer supported by pyang.

The idea is to convert YANG to XSD, JSON to XML and validate it against the XSD, as shown in Figure 4:

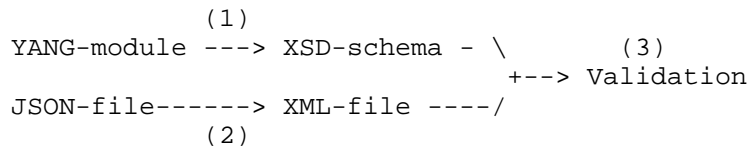


Figure 4 - XSD-based approach for JSON code validation

The pyang support for the XSD output format was deprecated in 1.5 and removed in 1.7.1. However pyang 1.7.1 is necessary to work with YANG 1.1 so the process shown in Figure 4 will stop just at step (1).

#### A.3. JSON Code: use-case-1-topology-01.json

The JSON code for this use case is currently located on GitHub at:

<https://github.com/danielkinguk/transport-nbi/blob/master/Internet-Drafts/Use-Case-1-Analysis/use-case-1-topology-01.json>

#### A.4. JSON Code: use-case-1-odu2-service-01.json

The JSON code for this use case is currently located on GitHub at:

<https://github.com/danielkinguk/transport-nbi/blob/master/Internet-Drafts/Use-Case-1-Analysis/use-case-1-odu2-service-01.json>



Authors' Addresses

Italo Busi (Editor)  
Huawei  
Email: italo.busi@huawei.com

Daniel King (Editor)  
Lancaster University  
Email: d.king@lancaster.ac.uk

Sergio Belotti  
Nokia  
Email: sergio.belotti@nokia.com

Gianmarco Bruno  
Ericsson  
Email: gianmarco.bruno@ericsson.com

Carlo Perocchio  
Ericsson  
Email: carlo.perocchio@ericsson.com



CCAMP Working Group  
Internet Draft  
Intended status: Informational

Haomian Zheng  
Italo Busi  
Huawei  
Yunbin Xu  
CAICT  
Ricard Vilalta  
CTTC

Expires: April 2018

October 30, 2017

Analysis of Transport North Bound Interface Use Case 3  
draft-tnbidt-ccamp-transport-nbi-analysis-uc3-00

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on April 30, 2018.

Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Abstract

This document analyses how YANG models being defined by IETF (TEAS and CCAMP WG in particular) can be used to support Use Case 3 (multi-domain with single-layer) scenarios as referenced later in this document.

## Table of Contents

1. Introduction.....	3
1.1. Assumptions.....	3
1.2. Feedbacks provided to the IETF Working Groups.....	3
2. Conventions used in this document.....	3
3. Scenario Overview.....	3
3.1. Topology Abstractions.....	4
3.1.1. Single Domain Topology.....	5
3.1.2. Multi-domain Topology Stitching.....	6
3.2. Multi-domain Service Configuration.....	7
3.2.1. Procedure Description.....	7
3.2.2. ODU Transit Service.....	9
3.2.3. EPL over ODU Service.....	9
3.2.4. Other OTN Client Services.....	9
3.3. Protection Scenarios.....	9
3.3.1. Linear Protection (end-to-end).....	9
3.3.2. Segmented Protection.....	9
4. Topology Abstraction: detailed JSON examples.....	10
5. Service Configuration: detailed JSON examples.....	10
5.1. ODU Transit Service.....	10
6. Security Considerations.....	10
7. IANA Considerations.....	10
8. Conclusions.....	10
9. References.....	10
9.1. Normative References.....	10
9.2. Informative References.....	11
10. Acknowledgments.....	11

## 1. Introduction

This document analyses how YANG models developed by IETF (TEAS and CCAMP WG) can be used to support Use Case 3 (multi-domain with single-layer) scenarios as described in [TNBI-UseCases].

### 1.1. Assumptions

This document is using the ACTN [ACTN-Fwk] as an architecture that deploys the IETF models. The motivation of this draft is to analyze how existing IETF models can be used on the MPI between the PNC and the MDSC to support the use case 3 scenarios as defined in section 6 of [TNBI-UseCases].

This document assumes the applicability of the YANG models to the ACTN interfaces as defined in [ACTN-YANG] and therefore considers the TE Topology YANG model defined in [TE-TOPO], with the OTN Topology augmentation defined in [OTN-TOPO] and the TE Tunnel YANG model defined in [TE-TUNNEL], with the OTN Tunnel augmentation defined in [OTN-TUNNEL].

In this document, the assumptions made in section 1 of [TNBI-UseCase-1] still apply. In summary, it is assumed that 1) MDSC uses the explicit-route-object list on MPI to specify the ingress/egress links for a tunnel segment request, and 2) label and TS availability information are reported from PNC to MDSC.

### 1.2. Feedbacks provided to the IETF Working Groups

The analysis done in this version of this document has triggered the following feedbacks to TEAS WG:

- o Updates to the plug-id definition in [TE-TOPO] to support plug-id also when auto-discovery (e.g., LMP based) mechanisms are used on inter-domain links

## 2. Conventions used in this document

The conventions defined in section 2 of [TNBI-UseCase-1] still apply in this document.

## 3. Scenario Overview

Use Case 3 is described in [TNBI-Use Cases] as a multi-domain with single layer network scenario supporting different types of services. This section provides a high-level overview of how IETF YANG models

can be used to support these uses cases at the MPI between the Transport PNC and the MDSC.

Section 3.1 describes the different topology abstractions provided to the MDSC by each PNC via its own MPI. The reference network and controlling hierarchy is defined in section 6.1 of [TNBI-Use Cases].

Section 3.2 describes how the difference services, defined in section 6.3 of [TNBI-UseCases], can be setup by the MDSC by coordinating requests to each PNC via their own MPIs.

Section 3.3 describes how the protection scenarios can be deployed, including end-to-end protection and segment protection, for both intra-domain and inter-domain scenario.

### 3.1. Topology Abstractions

The reference network is shown in Figure 1, which is the same as Figure 3 of [TNBI-UseCases]:

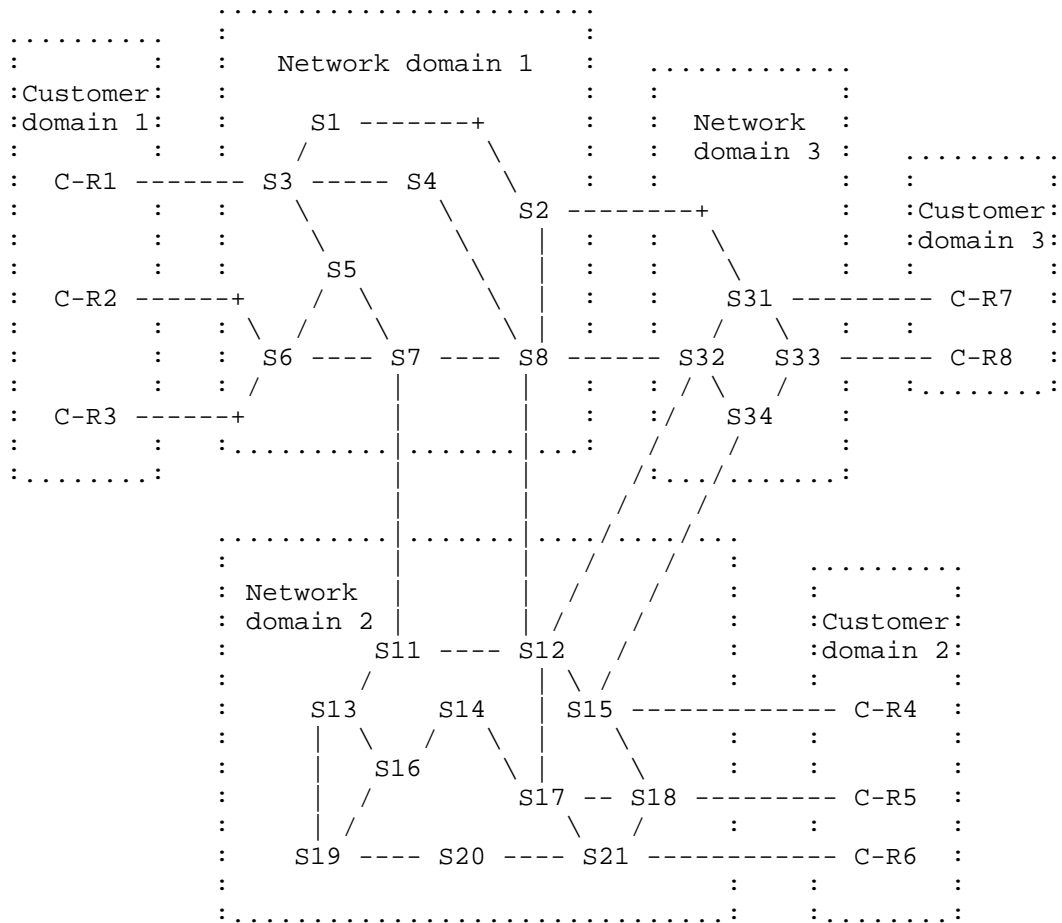


Figure 1 Reference Topology

The network is portioned in three domains with inter-domain links connecting the domains with each other. The controlling hierarchy is shown in Figure 3 of [TNBI-UseCases]: the three PNCs are responsible for the topology abstraction and device configuration for their respective domains, and the MDSC is used to coordinate the 3 domains.

### 3.1.1. Single Domain Topology

Each PNC reports its respective topology to the MDSC with different abstraction method, as described in section 6.2 of [TNBI-UseCases].

The physical topology of domain 1 and the topology abstraction (i.e., white topology abstraction) provided by PNC1 are the same as those described in section 3.1.1 of [TNBI-UseCase-1] for the single domain topology abstraction use case.

PNC2 provides a "type A grey topology abstraction": only one abstract node (i.e., AN2), with only inter-domain and access links, is reported at the MPI2.

PNC3 provides a "type B grey topology abstraction": two abstract nodes (i.e., AN31 and AN32), with internal links, inter-domain links and access links, are reported at the MPI3.

### 3.1.2. Multi-domain Topology Stitching

As assumed in the beginning of this section, MDSC does not have any knowledge of the topologies of each domain until each PNC reports its own abstraction topology, so the MDSC needs to merge together the abstract topologies provided by different PNCs, at the MPIs, to build its own topology view, as described in section 4.3 of [TE-TOPO].

Given the topologies reported from multiple PNCs, the MDSC need to stitch the multi-domain topology and obtain the full map of topology. The topology of each domain main be in an abstracted shape (refer to section 5.2 of [ACTN-Fwk]for different level of abstraction), while the inter-domain link information MUST be complete and fully configured by the MDSC.

The inter-domain link information is reported to the MDSC by the two PNCs, controlling the two ends of the inter-domain link.

The MDSC needs to understand how to "stitch" together these inter-domain links.

One possibility is to use the plug-id information, defined in [TE-TOPO]: two inter-domain links reporting the same plug-id value can be merged as a single intra-domain link within any MDSC native topology. The value of the reported plug-id information can be either assigned by a central network authority, and configured within the two PNC domains, or it can be discovered using automatic discovery mechanisms (e.g., LMP-based, as defined in [RFC6898]).

In case the plug-id values are assigned by a central authority, it is under the central authority responsibility to assign unique values.

In case the plug-id values are automatically discovered, the information discovered by the automatic discovery mechanisms needs to



be encoded as a bit string within the plug-id value. This encoding is implementation specific but the encoding rules need to be consistent across all the PNCs.

In case of co-existence within the same network of multiple sources for the plug-id (e.g., central authority and automatic discovery or even different automatic discovery mechanisms), it is RECOMMENDED that the plug-id namespace is partitioned to avoid that different sources assign the same plug-id value to different inter-domain link. The encoding of the plug-id namespace within the plug-id value is implementation specific but needs to be consistent across all the PNCs.

Another possibility is to pre-configure, either in the adjacent PNCs or in the MDSC, the association between the inter-domain link identifiers (topology-id, node-id and tp-id) assigned by the two adjacent PNCs to the same inter-domain link.

This option requires further investigation.

### 3.2. Multi-domain Service Configuration

Multi-domain service configuration can be found in section 6.3 of [TNBI-Usecases].

As an example, the objective in this section is to configure a transport service between C-R1 and C-R5. The cross-domain routing is assumed to be C-R1 <-> S3 <-> S2 <-> S31 <-> S33 <-> S34 <-> S15 <-> S18 <-> C-R5.

According to the different client signal type, there is different adaptation required. In this document, we are trying our best to reuse what has been defined in [TNBI-UseCase-1], which is the single domain case.

#### 3.2.1. Procedure Description

The service configuration procedure is assumed to be initiated (step 1 in Figure 2) at the CMI from CNC to MDSC, using XXX(LxSM, transport-service, VN, TBD) service models. The MDSC will understand this configure as as a request to setup a service from node A to node Z. Analysis of the CMI models is for further study.

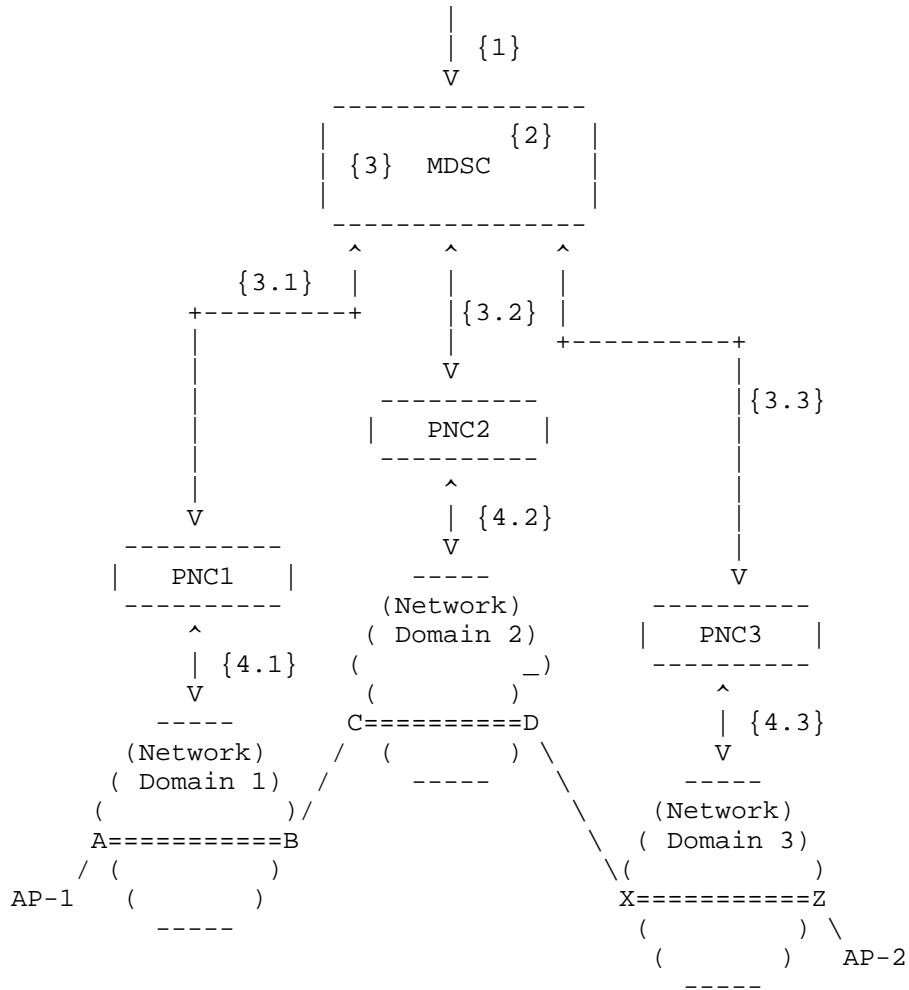


Figure 2 Multi-domain Service Setup

After receiving such request, MDSC determines the domain sequence, i.e., domain 1 <-> domain 2 <-> domain 3, with corresponding PNCs and inter-domain links (step 1 in Figure 2).

As described in [PATH-COMPUTE], the domain sequence can be determined by running the MDSC own path computation on the MDSC internal topology, defined in section 3.1.2, if and only if the MDSC has enough topology information. Otherwise the MDSC can send path computation requests to the different PNCs (steps 2.1, 2.2 and 2.3 in

Figure 2) and use this information to determine the optimal path on its internal topology and therefore the domain sequence.

The MDSC will then decompose the tunnel request into a few tunnel segments via tunnel model (including both TE tunnel model and OTN tunnel model), and request different PNCs to setup each intra-domain tunnel segment (steps 3, 3.1, 3.2 and 3.3 in Figure 2).

Assume that each intra-domain tunnel segment can be set up successfully, and each PNC response to the MDSC respectively. Based on each segment, MDSC will take care of the configuration of both the intra-domain tunnel segment and inter-domain tunnel via corresponding MPI (via TE tunnel model and OTN tunnel model). More specifically, for the inter-domain configuration, the ts bitmap and tpn information need to be configured via OTN tunnel model. . Then the end-to-end OTN tunnel will be ready.

In any case, the access link configuration is done only on the PNCs that control the access links (e.g., PNC-1 and PNC-3 in our example) and not on the PNCs of transit domain (e.g., PNC-2 in our example). Access link will be configured by MDSC after the OTN tunnel is set up. Access configuration is different and dependent on the different type of service. More details can be found in the following sections.

#### 3.2.2. ODU Transit Service

To be added

#### 3.2.3. EPL over ODU Service

To be added

#### 3.2.4. Other OTN Client Services

To be added

### 3.3. Protection Scenarios

#### 3.3.1. Linear Protection (end-to-end)

To be added

#### 3.3.2. Segmented Protection

To be added

#### 4. Topology Abstraction: detailed JSON examples

To be added

#### 5. Service Configuration: detailed JSON examples

##### 5.1. ODU Transit Service

To be added

#### 6. Security Considerations

This section is for further study

#### 7. IANA Considerations

This document requires no IANA actions.

#### 8. Conclusions

This section is for further study

#### 9. References

##### 9.1. Normative References

[ACTN-Fwk] Ceccarelli, D., Lee, Y. et al., "Framework for Abstraction and Control of Transport Networks", draft-ietf-teas-actn-framework, work in progress.

[TNBI-UseCases] Busi, I., King, D. et al, "Transport Northbound Interface Use Cases", draft-ietf-ccamp-transport-nbi-use-cases, work in progress.

[TNBI-UseCase-1] Busi, I., King, D. et al, "Analysis of Transport North Bound Interface Use Case 1", draft-tnbidt-ccamp-transport-nbi-analysis-uc1, work in progress.

[TE-TOPO] Liu, X. et al., "YANG Data Model for TE Topologies", draft-ietf-teas-yang-te-topo, work in progress.

[OTN-TOPO] Zheng, H. et al., "A YANG Data Model for Optical Transport Network Topology", draft-ietf-ccamp-otn-topo-yang, work in progress.

[TE-TUNNEL] Saad, T. et al., "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te, work in progress.

[PATH-COMPUTE] Busi, I., Belotti, S. et al, "Yang model for requesting Path Computation", draft-busibel-teas-yang-path-computation, work in progress.

[OTN-TUNNEL] Zheng, H. et al., "OTN Tunnel YANG Model", draft-sharma-ccamp-otn-tunnel-model, work in progress.

## 9.2. Informative References

[RFC6898] Li, D. et al., "Link Management Protocol Behavior Negotiation and Configuration Modifications", RFC 6898, March 2013.

[ACTN-YANG] Zhang, X. et al., "Applicability of YANG models for Abstraction and Control of Traffic Engineered Networks", draft-zhang-teas-actn-yang, work in progress.

[I2RS-TOPO] Clemm, A. et al., "A Data Model for Network Topologies", draft-ietf-i2rs-yang-network-topo, work in progress.

## 10. Acknowledgments

The authors would like to thank all members of the Transport NBI Design Team involved in the definition of use cases, gap analysis and guidelines for using the IETF YANG models at the Northbound Interface (NBI) of a Transport SDN Controller.

The authors would like to thank Xian Zhang, Anurag Sharma, Sergio Belotti, Tara Cummings, Michael Scharf, Karthik Sethuraman, Oscar Gonzalez de Dios, Hans Bjursrom and Italo Busi for having initiated the work on gap analysis for transport NBI and having provided foundations work for the development of this document.

The authors would like to thank the authors of the TE Topology and Tunnel YANG models [TE-TOPO] and [TE-TUNNEL], in particular Igor Bryskin, Vishnu Pavan Beeram, Tarek Saad and Xufeng Liu, for their support in addressing any gap identified during the analysis work.

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Haomian Zheng (Editor)  
Huawei  
Email: zhenghaomian@huawei.com

Italo Busi  
Huawei  
Email: italo.busi@huawei.com

Yunbin Xu (Editor)  
CAICT  
Email: xuyunbin@ritt.cn mailto:d.king@lancaster.ac.uk

Ricard Vilalta  
CTTC  
Email: ricard.vilalta@cttc.es

Carlo Perocchio  
Ericsson  
Email: carlo.perocchio@ericsson.com

Gianmarco Bruno  
Ericsson  
Email: gianmarco.bruno@ericsson.com



Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2018

S. Vallin  
Stefan Vallin AB  
M. Bjorklund  
Cisco  
October 30, 2017

YANG Alarm Module  
draft-vallin-ccamp-alarm-module-01

Abstract

This document defines a YANG module for alarm management. It includes functions for alarm list management, alarm shelving and notifications to inform management systems. There are also RPCs to manage the operator state of an alarm and administrative alarm procedures. The module carefully maps to relevant alarm standards.

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 <http://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 May 3, 2018.

Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of



the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Requirements notation . . . . .	3
2. Introduction . . . . .	3
2.1. Terminology . . . . .	3
3. Objectives . . . . .	4
4. Alarm Module Concepts . . . . .	5
4.1. Alarm Definition . . . . .	5
4.2. Alarm Type . . . . .	5
4.3. Identifying Resource . . . . .	7
4.4. Identifying Alarm Instances . . . . .	7
4.5. Alarm Life-Cycle . . . . .	8
4.5.1. Resource Alarm Life-Cycle . . . . .	8
4.5.2. Operator Alarm Life-cycle . . . . .	9
4.5.3. Administrative Alarm Life-Cycle . . . . .	9
4.6. Root Cause and Impacted Resources . . . . .	10
4.7. Alarm Shelving . . . . .	10
5. Alarm Data Model . . . . .	10
5.1. Alarm Control . . . . .	11
5.1.1. Alarm Shelving . . . . .	11
5.2. Alarm Inventory . . . . .	12
5.3. Alarm Summary . . . . .	13
5.4. The Alarm List . . . . .	13
5.5. The Shelved Alarms List . . . . .	15
5.6. RPCs and Actions . . . . .	15
5.7. Notifications . . . . .	15
6. Alarm YANG Module . . . . .	15
7. X.733 Alarm Mapping Data Model . . . . .	40
8. X.733 Alarm Mapping YANG Module . . . . .	41
9. Security Considerations . . . . .	47
10. Acknowledgements . . . . .	47
11. References . . . . .	47
11.1. Normative References . . . . .	47
11.2. Informative References . . . . .	47
Appendix A. Vendor-specific Alarm-Types Example . . . . .	48
Appendix B. Alarm Inventory Example . . . . .	49
Appendix C. Alarm List Example . . . . .	50
Appendix D. Alarm Shelving Example . . . . .	51
Appendix E. X.733 Mapping Example . . . . .	52
Appendix F. Background and Usability Requirements . . . . .	52
F.1. Alarm Concepts . . . . .	53
F.1.1. Alarm type . . . . .	53
F.2. Usability Requirements . . . . .	54
Authors' Addresses . . . . .	57

## 1. Requirements notation

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. Introduction

This document defines a YANG [RFC7950] module for alarm management. The purpose is to define a standardised alarm interface for network devices that can be easily integrated into management applications. The model is also applicable as a northbound alarm interface in the management applications.

Alarm monitoring is a fundamental part of monitoring the network. Raw alarms from devices do not always tell the status of the network services or necessarily point to the root cause. However, being able to feed alarms to the network management system in a standardised format is a starting point for performing higher level network assurance tasks.

This document defines a standardised YANG module for alarm management. The design of the module is based on experience from using and implementing available alarm standards.

### 2.1. Terminology

The following terms are defined in [RFC7950]:

- o action
- o client
- o data tree
- o RPC
- o server

The following terms are used within this document:

- o Alarm (the general concept): An alarm signifies an undesirable state in a resource that requires corrective action.

- o Alarm Instance: The alarm state for a specific resource and alarm type. For example (GigabitEthernet0/15, link-alarm). An entry in the alarm list.
- o Alarm Inventory: A list of all possible alarm types on a system.
- o Alarm Shelving: Blocking alarms according to specific criteria.
- o Alarm Type: An alarm type identifies a possible unique alarm state for a resource. Alarm types are names to identify the state like "link-alarm", "jitter-violation", "high-disk-utilization".
- o Management System: The alarm management application that consumes the alarms, i.e., acts as a client.
- o Resource: A fine-grained identification of the alarming resource, for example: an interface, a process.
- o System: The system that implements this YANG alarm module, i.e., acts as a server. This corresponds to a network device or a management application that provides a north-bound alarm interface.

Tree diagrams used in this document follow the notation defined in [I-D.ietf-netmod-yang-tree-diagrams].

### 3. Objectives

The objectives for the design of the Alarm Module are:

- o Simple to use. If a system supports this module, it shall be straight-forward to integrate this into a YANG based alarm manager.
- o View alarms as states on resources and not as discrete notifications.
- o Clear definition of "alarm" in order to exclude general events that should not be forwarded as alarm notifications.
- o Clear and precise identification of alarm types and alarm instances.
- o A management system should be able to pull all available alarm types from a system, i.e., read the alarm inventory from a system. This makes it possible to prepare alarm operators with corresponding alarm instructions.

- o Address alarm usability requirements. While IETF has not really addressed alarm management, telecom standards has addressed it purely from a protocol perspective. The process industry has published several relevant standards addressing requirements for a useful alarm interface; [EEMUA], [ISA182]. This alarm module defines usability requirements as well as a YANG data model.
- o Mapping to X.733, which is a requirement for many alarm systems. Still, keep some of the X.733 concepts out of the core model in order to make the model small and easy to understand.

#### 4. Alarm Module Concepts

This section defines the fundamental concepts behind the data model. This section is rooted in the works of Vallin et. al [ALARMSEM].

##### 4.1. Alarm Definition

An alarm signifies an undesirable state in a resource that requires corrective action.

See Appendix F for more motivation and consequences around this definition.

##### 4.2. Alarm Type

This document defines an alarm type with an alarm type id and an alarm type qualifier.

The alarm type id is modeled as a YANG identity. With YANG identities, new alarm types can be defined in a distributed fashion. YANG identities are hierarchical, which means that an hierarchy of alarm types can be defined.

Standards and vendors should define their own alarm type identities based on this definition.

The use of YANG identities means that all possible alarms are identified at design time. This explicit declaration of alarm types makes it easier to allow for alarm qualification reviews and preparation of alarm actions and documentation.

There are occasions where the alarm types are not known at design time. For example, a system with digital inputs that allows users to connect detectors (e.g., smoke detector) to the inputs. In this case it is a configuration action that says that certain connectors are fire alarms for example. The drawback of this is that there is a big risk that alarm operators will receive alarm types as a surprise,

they do not know how to resolve the problem since a defined alarm procedure does not necessarily exist.

In order to allow for dynamic addition of alarm types the alarm module also allows for further qualification of the identity based alarm type using a string.

A vendor or standard can then define their own alarm-type hierarchy. The example below shows a hierarchy based on X.733 event types:

```
import ietf-alarms {  
  prefix al;  
}  
identity vendor-alarms {  
  base al:alarm-type;  
}  
identity communications-alarm {  
  base vendor-alarms;  
}  
identity link-alarm {  
  base communications-alarm;  
}
```

Alarm types can be abstract. An abstract alarm type is used as a base for defining hierarchical alarm types. Concrete alarm types are used for alarm states and appear in the alarm inventory. There are two kinds of concrete alarm types:

1. The last subordinate identity in the "alarm-type-id" hierarchy is concrete, for example: "alarm-identity.environmental-alarm.smoke". In this example "alarm-identity" and "environmental-alarm" are abstract YANG identities, whereas "smoke" is a concrete YANG identity.
2. The YANG identity hierarchy is abstract and the concrete alarm type is defined by the dynamic alarm qualifier string, for example: "alarm-identity.environmental-alarm.external-detector" with alarm-type-qualifier "smoke".

For example:

```
// Alternative 1: concrete alarm type identity
import ietf-alarms {
  prefix al;
}
identity environmental-alarm {
  base al:alarm-type;
  description "Abstract alarm type";
}
identity smoke {
  base environmental-alarm;
  description "Concrete alarm type";
}

// Alternative 2: concrete alarm type qualifier
import ietf-alarms {
  prefix al;
}
identity environmental-alarm {
  base al:alarm-type;
  description "Abstract alarm type";
}
identity external-detector {
  base environmental-alarm;
  description
    "Abstract alarm type, a run-time configuration
    procedure sets the type of alarm detected. This will
    be reported in the alarm-type-qualifier.";
}
```

#### 4.3. Identifying Resource

It is of vital importance to be able to refer to the alarming resource. This reference must be as fine-grained as possible. If the alarming resource exists in the data tree then an instance-identifier MUST be used with the full path to the object.

This module also allows for alternate naming of the alarming resource if it is not available in the data tree.

#### 4.4. Identifying Alarm Instances

A primary goal of this alarm module is to remove any ambiguity in how alarm notifications are mapped to an update of an alarm instance. X.733 and especially 3GPP were not really clear on this point. This YANG alarm module states that the tuple (resource, alarm type identifier, alarm type qualifier) corresponds to a single alarm instance. This means that alarm notifications for the same resource

and same alarm type are matched to update the same alarm instance. These three leafs are therefore used as the key in the alarm list:

```
list alarm {  
    key "resource alarm-type-id alarm-type-qualifier";  
    ...  
}
```

#### 4.5. Alarm Life-Cycle

The alarm model clearly separates the resource alarm life-cycle from the operator and administrative life-cycles of an alarm.

- o resource alarm life-cycle: the alarm instrumentation that controls alarm raise, clearance, and severity changes.
- o operator alarm life-cycle: operators acting upon alarms with actions like acknowledgment and closing. Closing an alarm implies that the operator considers the corrective action performed. Operators can also shelf alarms in order to avoid nuisance alarms.
- o administrative alarm life-cycle: deleting (purging) alarms and compressing the alarm status change list. This module exposes operations to manage the administrative life-cycle. The server may also perform these operations based on other policies, but how that is done is out of scope for this document.

##### 4.5.1. Resource Alarm Life-Cycle

From a resource perspective, an alarm can have the following life-cycle: raise, change severity, change severity, clear, being raised again etc. All of these status changes can have different alarm texts generated by the instrumentation. Two important things to note:

1. Alarms are not deleted when they are cleared. Deleting alarms is an administrative process. The alarm module defines an rpc "purge" that deletes alarms.
2. Alarms are not cleared by operators, only the underlying instrumentation can clear an alarm. Operators can close alarms.

The YANG tree representation below illustrates the resource oriented life-cycle:

```

+--ro alarm* [resource alarm-type-id alarm-type-qualifier]
  ...
  +--ro is-cleared                boolean
  +--ro last-changed              yang:date-and-time
  +--ro perceived-severity        severity
  +--ro alarm-text                alarm-text
  +--ro status-change* [time]
    +--ro time                    yang:date-and-time
    +--ro perceived-severity      severity
    +--ro alarm-text              alarm-text

```

For every status change from the resource perspective a row is added to the "status-change" list. The last status values are also represented at leafs for the alarm. Note well that the alarm severity does not include "cleared", alarm clearance is a flag.

An alarm can therefore look like this: ((GigabitEthernet0/25, link-alarm,""), false, T, major, "Interface GigabitEthernet0/25 down")

#### 4.5.2. Operator Alarm Life-cycle

Operators can also act upon alarms using the set-operator-state action:

```

+--ro alarm* [resource alarm-type-id alarm-type-qualifier]
  ...
  +--ro operator-state-change* [time] {operator-actions}?
    | +--ro time          yang:date-and-time
    | +--ro operator      string
    | +--ro state          operator-state
    | +--ro text?         string
  +---x set-operator-state {operator-actions}?
    +---w input
      +---w state          operator-state
      +---w text?         string

```

The operator state for an alarm can be: "none", "ack", "shelved", and "closed". Alarm deletion (using the rpc "purge-alarms"), can use this state as a criteria. A closed alarm is an alarm where the operator has performed any required corrective actions. Closed alarms are good candidates for being deleted.

#### 4.5.3. Administrative Alarm Life-Cycle

Deleting alarms from the alarm list is considered an administrative action. This is supported by the "purge-alarms" rpc. The "purge-alarms" rpc takes a filter as input. The filter selects alarms based on the operator and resource life-cycle such as "all closed cleared



alarms older than a time specification". The server may also perform these operations based on other policies, but how that is done is out of scope for this document.

Alarms can be compressed. Compressing an alarm deletes all entries in the alarm's "status-change" list except for the last status change. A client can perform this using the "compress-alarms" rpc. The server may also perform these operations based on other policies, but how that is done is out of scope for this document.

#### 4.6. Root Cause and Impacted Resources

The general principle of this alarm module is to limit the amount of alarms. The alarm has two leaf-lists to identify possible impacted resources and possible root-cause resources. The system should not send individual alarms for the possible root-cause resources and impacted resources. These serves as hints only. It is up to the client application to use this information to present the overall status.

#### 4.7. Alarm Shelving

Alarm shelving is an important function in order for alarm management applications and operators to stop superfluous alarms. A shelved alarm implies that any alarms fulfilling this criteria are ignored. Shelved alarms appear in a dedicated shelved alarm list in order not to disturb the relevant alarms. Shelved alarms do not generate notifications.

### 5. Alarm Data Model

Alarm shelving and operator actions are YANG features so that a server can select not to support these.

The data model has the following overall structure:

```

+--rw alarms
  +--rw control
    |   +--rw max-alarm-status-changes?    union
    |   +--rw notify-status-changes?      boolean
    |   +--rw alarm-shelving {alarm-shelving}?
    |   ...
  +--ro alarm-inventory
    |   +--ro alarm-type* [alarm-type-id alarm-type-qualifier]
    |   ...
  +--ro summary
    |   +--ro alarm-summary* [severity]
    |   |   ...
    |   +--ro shelves-active?    empty {alarm-shelving}?
  +--ro alarm-list
    |   +--ro number-of-alarms?    yang:gauge32
    |   +--ro last-changed?       yang:date-and-time
    |   +--ro alarm* [resource alarm-type-id alarm-type-qualifier]
    |   ...
  +--ro shelved-alarms {alarm-shelving}?
    |   +--ro number-of-shelved-alarms?    yang:gauge32
    |   +--ro alarm-shelf-last-changed?    yang:date-and-time
    |   +--ro shelved-alarm*
    |       [resource alarm-type-id alarm-type-qualifier]
    |   ...

```

## 5.1. Alarm Control

The `"/alarms/control/notify-status-changes"` leaf controls if notifications are sent for all state changes, severity change and alarm text change, or just for new and cleared alarms.

Every alarm has a list of status changes, this is a circular list. The length of this list is controlled by `"/alarms/control/max-alarm-status-changes"`.

### 5.1.1. Alarm Shelving

The shelving control tree is shown below:

```
+--rw alarms
  +--rw control
    +--rw alarm-shelving {alarm-shelving}?
      +--rw shelf* [shelf-name]
        +--rw shelf-name          string
        +--rw resource?           resource
        +--rw alarm-type-id?      alarm-type-id
        +--rw alarm-type-qualifier? alarm-type-qualifier
        +--rw description?        string
```

Shelved alarms are shown in a dedicated shelved alarm list. The instrumentation MUST move shelved alarms from the alarm list (/alarms/alarm-list) to the shelved alarm list (/alarms/shelved-alarms/). Shelved alarms do not generate any notifications. When the shelving criteria is removed or changed the alarm list MUST be updated to the correct actual state of the alarms.

A leaf (/alarms/summary/shelfs-active) in the alarm summary indicates if there are shelved alarms.

A system can select to not support the shelving feature.

## 5.2. Alarm Inventory

The alarm inventory represents all possible alarm types that may occur in the system. A management system may use this to build alarm procedures. The alarm inventory is relevant for several reasons:

The system might not instrument all alarm type identities.

The system has configured dynamic alarm types using the alarm qualifier. The inventory makes it possible for the management system to discover these.

Note that the mechanism whereby dynamic alarm types are added using the alarm type qualifier MUST populate this list.

The optional leaf-list "resource" in the alarm inventory enables the system to publish for which resources a given alarm type may appear.

The alarm inventory tree is shown below:

```

+--rw alarms
  +--ro alarm-inventory
    +--ro alarm-type* [alarm-type-id alarm-type-qualifier]
      +--ro alarm-type-id          alarm-type-id
      +--ro alarm-type-qualifier    alarm-type-qualifier
      +--ro resource*              string
      +--ro has-clear               boolean
      +--ro severity-levels*        severity
      +--ro description             string

```

### 5.3. Alarm Summary

The alarm summary list summarises alarms per severity; how many cleared, cleared and closed, and closed. It also gives an indication if there are shelved alarms.

The alarm summary tree is shown below:

```

+--rw alarms
  +--ro summary
    +--ro alarm-summary* [severity]
      | +--ro severity          severity
      | +--ro total?            yang:gauge32
      | +--ro cleared?          yang:gauge32
      | +--ro cleared-not-closed? yang:gauge32
      | | {operator-actions}?
      | +--ro cleared-closed?    yang:gauge32
      | | {operator-actions}?
      | +--ro not-cleared-closed? yang:gauge32
      | | {operator-actions}?
      | +--ro not-cleared-not-closed? yang:gauge32
      | | {operator-actions}?
      +--ro shelves-active?      empty {alarm-shelving}?

```

### 5.4. The Alarm List

The alarm list (/alarms/alarm-list) is a function from (resource, alarm type, alarm type qualifier) to the current alarm state.

```

+--ro alarm-list
  +--ro number-of-alarms?   yang:gauge32
  +--ro last-changed?       yang:date-and-time
  +--ro alarm* [resource alarm-type-id alarm-type-qualifier]
    +--ro time-created       yang:date-and-time
    +--ro resource           resource
    +--ro alarm-type-id      alarm-type-id
    +--ro alarm-type-qualifier alarm-type-qualifier
    +--ro alt-resource*      resource
    +--ro related-alarm*
      | [resource alarm-type-id alarm-type-qualifier]
      | +--ro resource
      | | -> /alarms/alarm-list/alarm/resource
      | +--ro alarm-type-id      leafref
      | +--ro alarm-type-qualifier leafref
    +--ro impacted-resource*  resource
    +--ro root-cause-resource* resource
    +--ro is-cleared          boolean
    +--ro last-changed        yang:date-and-time
    +--ro perceived-severity  severity
    +--ro alarm-text          alarm-text
    +--ro status-change* [time] {alarm-history}?
      | +--ro time              yang:date-and-time
      | +--ro perceived-severity severity-with-clear
      | +--ro alarm-text        alarm-text
    +--ro operator-state-change* [time] {operator-actions}?
      | +--ro time              yang:date-and-time
      | +--ro operator          string
      | +--ro state              operator-state
      | +--ro text?             string
    +---x set-operator-state {operator-actions}?
      +---w input
        +---w state              operator-state
        +---w text?             string

```

Every alarm has three important states, the resource clearance state "is-cleared", the severity "perceived-severity" and the operator state available in the operator state change list.

In order to see the alarm history the resource state changes are available in the "status-change" list and the operator history is available in the "operator-state-change" list.

### 5.5. The Shelved Alarms List

The shelved alarm list has the same structure as the alarm list above. It shows all the alarms that matches the shelving criteria (/alarms/control/alarm-shelving).

### 5.6. RPCs and Actions

The alarm module supports rpcs and actions to manage the alarms:

"purge-alarms" (rpc): delete alarms according to specific criteria, for example all cleared alarms older then a specific date.

"compress-alarms" (rpc): compress the status-change list for the alarms.

"set-operator-state" (action): change the operator state for an alarm: for example acknowledge.

### 5.7. Notifications

The alarm module supports a general notification to report alarm state changes. It carries all relevant parameters for the alarm management application.

There is also a notification to report that an operator changed the operator state on an alarm, like acknowledge.

If the alarm inventory is changed, for example a new card type is inserted, a notification will tell the management application that new alarm types are available.

## 6. Alarm YANG Module

```
<CODE BEGINS> file "ietf-alarms@2017-10-30.yang"
module ietf-alarms {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-alarms";
  prefix al;

  import ietf-yang-types {
    prefix yang;
  }

  organization
```

"IETF CCAMP Working Group";

contact

"WG Web: <<http://tools.ietf.org/wg/ccamp>>  
WG List: <<mailto:ccamp@ietf.org>>

Editor: Stefan Vallin  
<<mailto:stefan@wallan.se>>

Editor: Martin Bjorklund  
<<mailto:mbj@tail-f.com>>";

description

"This module defines an interface for managing alarms. Main inputs to the module design are the 3GPP Alarm IRP, ITU-T X.733 and ANSI/ISA-18.2 alarm standards.

Main features of this module include:

- \* Alarm list:  
A list of all alarms. Cleared alarms stay in the list until explicitly removed.
- \* Operator actions on alarms:  
Acknowledging and closing alarms.
- \* Administrative actions on alarms:  
Purging alarms from the list according to specific criteria.
- \* Alarm inventory:  
A management application can read all alarm types implemented by the system.
- \* Alarm shelving:  
Shelving (blocking) alarms according to specific criteria.

This module uses a stateful view on alarms. An alarm is a state for a specific resource (note that an alarm is not a notification). An alarm type is a possible alarm state for a resource. For example, the tuple:

('link-alarm', 'GigabitEthernet0/25')

is an alarm of type 'link-alarm' on the resource 'GigabitEthernet0/25'.

Alarm types are identified using YANG identities and an optional string-based qualifier. The string-based qualifier allows for dynamic extension of the statically defined alarm types. Alarm types identify a possible alarm state and not the individual notifications. For example, the traditional 'link-down' and 'link-up' notifications are two notifications referring to the same alarm type 'link-alarm'.

With this design there is no ambiguity about how alarm and alarm clear correlation should be performed: notifications that report the same resource and alarm type are considered updates of the same alarm, such as clearing an active alarm or changing the severity of an alarm.

The instrumentation can update 'severity' and 'alarm-text' on an existing alarm. The above alarm example can therefore look like:

```
((('link-alarm', 'GigabitEthernet0/25'),
  warning,
  'interface down while interface admin state is up'))
```

There is a clear separation between updates on the alarm from the underlying resource, like clear, and updates from an operator like acknowledge or closing an alarm:

```
((('link-alarm', 'GigabitEthernet0/25'),
  warning,
  'interface down while interface admin state is up',
  cleared,
  closed))
```

Administrative actions like removing closed alarms older than a given time is supported."

```
revision 2017-10-30 {
  description
    "Initial revision.";
  reference
    "RFC XXXX: YANG Alarm Module";
}

/*
 * Features
 */

feature operator-actions {
  description
```



```
    "This feature means that the systems supports operator states
    on alarms.";
}

feature alarm-shelving {
    description
        "This feature means that the system supports shelving
        (blocking) alarms.";
}

feature alarm-history {
    description
        "This feature means that the alarm list also maintains a
        history of state changes for each alarm.  For example, if an
        alarm toggles between cleared and active 10 times, a list for
        that alarm will show those state changes with time-stamps.";
}
/*
 * Identities
 */

identity alarm-identity {
    description
        "Base identity for alarm types.  A unique identification of the
        alarm, not including the resource.  Different resources can
        share alarm types.  If the resource reports the same alarm
        type, it is to be considered to be the same alarm.  The alarm
        type is a simplification of the different X.733 and 3GPP alarm
        IRP alarm correlation mechanisms and it allows for
        hierarchical extensions.

        A string-based qualifier can be used in addition to the
        identity in order to have different alarm types based on
        information not known at design-time, such as values in
        textual SNMP Notification var-binds.

        Standards and vendors can define sub-identities to clearly
        identify specific alarm types.

        This identity is abstract and shall not be used for alarms.";
}

/*
 * Common types
 */

typedef resource {
    type union {
```

```
    type instance-identifier {
        require-instance false;
    }
    type yang:object-identifier;
    type string;
}
description
    "This is an identification of the alarming resource, such as an
    interface. It should be as fine-grained as possible both to
    guide the operator and to guarantee uniqueness of the
    alarms. If a resource has both a config and a state tree
    normally this should identify the state tree,
    (e.g., /interfaces-state/interface/name).
    But if the instrumentation can detect a broken config, this
    should be identified as the resource.
    If the alarming resource is modelled in YANG, this
    type will be an instance-identifier. If the resource is an
    SNMP object, the type will be an object-identifier. If the
    resource is anything else, for example a distinguished name or
    a CIM path, this type will be a string."
}

typedef alarm-text {
    type string;
    description
        "The string used to inform operators about the alarm. This
        MUST contain enough information for an operator to be able
        to understand the problem and how to resolve it. If this
        string contains structure, this format should be clearly
        documented for programs to be able to parse that
        information."
}

typedef severity {
    type enumeration {
        enum indeterminate {
            value 2;
            description
                "Indicates that the severity level could not be
                determined. This level SHOULD be avoided."
        }
        enum minor {
            value 3;
            description
                "The 'minor' severity level indicates the existence of a
                non-service affecting fault condition and that corrective
                action should be taken in order to prevent a more serious
                (for example, service affecting) fault. Such a severity
```

```
        can be reported, for example, when the detected alarm
        condition is not currently degrading the capacity of the
        resource.";
    }
    enum warning {
        value 4;
        description
            "The 'warning' severity level indicates the detection of
            a potential or impending service affecting fault, before
            any significant effects have been felt. Action should be
            taken to further diagnose (if necessary) and correct the
            problem in order to prevent it from becoming a more
            serious service affecting fault.";
    }
    enum major {
        value 5;
        description
            "The 'major' severity level indicates that a service
            affecting condition has developed and an urgent
            corrective action is required. Such a severity can be
            reported, for example, when there is a severe
            degradation in the capability of the resource
            and its full capability must be restored.";
    }
    enum critical {
        value 6;
        description
            "The 'critical' severity level indicates that a service
            affecting condition has occurred and an immediate
            corrective action is required. Such a severity can be
            reported, for example, when a resource becomes totally
            out of service and its capability must be restored.";
    }
}
description
    "The severity level of the alarm. Note well that value 'clear'
    is not included. If an alarm is cleared or not is a separate
    boolean flag.";
reference
    "ITU Recommendation X.733: Information Technology
    - Open Systems Interconnection
    - System Management: Alarm Reporting Function";
}

typedef severity-with-clear {
    type union {
        type enumeration {
            enum cleared {
```

```
        value 1;
        description
            "The alarm is cleared by the instrumentation.";
    }
}
type severity;
}
description
    "The severity level of the alarm including clear.
    This is used *only* in notifications reporting state changes
    for an alarm.";
}

typedef operator-state {
    type enumeration {
        enum none {
            value 1;
            description
                "The alarm is not being taken care of.";
        }
        enum ack {
            value 2;
            description
                "The alarm is being taken care of.  Corrective action not
                taken yet, or failed";
        }
        enum closed {
            value 3;
            description
                "Corrective action taken successfully.";
        }
        enum shelved {
            value 4;
            description
                "Alarm shelved.  Alarms in alarms/shelved-alarms/
                MUST be assigned this operator state by the server as
                the last entry in the operator-state-change list.";
        }
        enum un-shelved {
            value 5;
            description
                "Alarm moved back to alarm-list from shelf.
                Alarms 'moved' from /alarms/shelved-alarms/
                to /alarms/alarm-list MUST be assigned this
                state by the server as the last entry in the
                operator-state-change list.";
        }
    }
}
```

```
    }
    description
        "Operator states on an alarm. The 'closed' state indicates
        that an operator considers the alarm being resolved. This
        is separate from the resource alarm clear flag.";
}

/* Alarm type */

typedef alarm-type-id {
    type identityref {
        base alarm-identity;
    }
    description
        "Identifies an alarm type. The description of the alarm type
        id MUST indicate if the alarm type is abstract or not. An
        abstract alarm type is used as a base for other alarm type ids
        and will not be used as a value for an alarm or be present in
        the alarm inventory.";
}

typedef alarm-type-qualifier {
    type string;
    description
        "If an alarm type can not be fully specified at design time by
        alarm-type-id, this string qualifier is used in addition to
        fully define a unique alarm type.

        The definition of alarm qualifiers is considered being part
        of the instrumentation and out of scope for this module.
        An empty string is used when this is part of a key.";
}

/*
 * Groupings
 */

grouping common-alarm-parameters {
    description
        "Common parameters for an alarm.

        This grouping is used both in the alarm list and in the
        notification representing an alarm state change.";

    leaf resource {
        type resource;
        mandatory true;
        description
```

```
        "The alarming resource.  See also 'alt-resource'.
        This could for example be a reference to the alarming
        interface";
    }

    leaf alarm-type-id {
        type alarm-type-id;
        mandatory true;
        description
            "This leaf and the leaf 'alarm-type-qualifier' together
            provides a unique identification of the alarm type.";
    }

    leaf alarm-type-qualifier {
        type alarm-type-qualifier;
        description
            "This leaf is used when the 'alarm-type-id' leaf cannot
            uniquely identify the alarm type.  Normally, this is not
            the case, and this leaf is the empty string.";
    }

    leaf-list alt-resource {
        type resource;
        description
            "Used if the alarming resource is available over other
            interfaces.  This field can contain SNMP OID's, CIM paths or
            3GPP Distinguished names for example.";
    }

    list related-alarm {
        key "resource alarm-type-id alarm-type-qualifier";

        description
            "References to related alarms.  Note that the related alarm
            might have been removed from the alarm list.";

        leaf resource {
            type leafref {
                path "/alarms/alarm-list/alarm/resource";
                require-instance false;
            }
            description
                "The alarming resource for the related alarm.";
        }

        leaf alarm-type-id {
            type leafref {
                path "/alarms/alarm-list/alarm"
                    + "[resource=current()/../resource]"
            }
        }
    }
}
```

```

        + "/alarm-type-id";
        require-instance false;
    }
    description
        "The alarm type identifier for the related alarm.";
}
leaf alarm-type-qualifier {
    type leafref {
        path "/alarms/alarm-list/alarm"
        + "[resource=current()/../resource]"
        + "[alarm-type-id=current()/../alarm-type-id]"
        + "/alarm-type-qualifier";
        require-instance false;
    }
    description
        "The alarm qualifier for the related alarm.";
}
}
leaf-list impacted-resource {
    type resource;
    description
        "Resources that might be affected by this alarm. If the
        system creates an alarm on a resource and also has a mapping
        to other resources that might be impacted, these resources
        can be listed in this leaf-list. In this way the system can
        create one alarm instead of several. For example, if an
        interface has an alarm, the 'impacted-resource' can
        reference the aggregated port channels.";
}
leaf-list root-cause-resource {
    type resource;
    description
        "Resources that are candidates for causing the alarm. If the
        system has a mechanism to understand the candidate root
        causes of an alarm, this leaf-list can be used to list the
        root cause candidate resources. In this way the system can
        create one alarm instead of several. An example might be a
        logging system (alarm resource) that fails, the alarm can
        reference the file-system in the 'root-cause-resource'
        leaf-list. Note that the intended use is not to also send an
        an alarm with the root-cause-resource as alarming resource.
        The root-cause-resource leaf list is a hint and should not
        also generate an alarm for the same problem.";
}
}

grouping alarm-state-change-parameters {
    description

```

"Parameters for an alarm state change.

This grouping is used both in the alarm list's status-change list and in the notification representing an alarm state change.";

```
leaf time {
  type yang:date-and-time;
  mandatory true;
  description
    "The time the status of the alarm changed. The value
    represents the time the real alarm state change appeared
    in the resource and not when it was added to the
    alarm list. The /alarm-list/alarm/last-changed MUST be
    set to the same value.";
}
leaf perceived-severity {
  type severity-with-clear;
  mandatory true;
  description
    "The severity of the alarm as defined by X.733. Note
    that this may not be the original severity since the alarm
    may have changed severity.";
  reference
    "ITU Recommendation X.733: Information Technology
    - Open Systems Interconnection
    - System Management: Alarm Reporting Function";
}
leaf alarm-text {
  type alarm-text;
  mandatory true;
  description
    "A user friendly text describing the alarm state change.";
  reference
    "ITU Recommendation X.733: Information Technology
    - Open Systems Interconnection
    - System Management: Alarm Reporting Function";
}
}

grouping operator-parameters {
  description
    "This grouping defines parameters that can
    be changed by an operator";
  leaf time {
    type yang:date-and-time;
    mandatory true;
    description
```



```
        "Timestamp for operator action on alarm.";
    }
    leaf operator {
        type string;
        mandatory true;
        description
            "The name of the operator that has acted on this
            alarm.";
    }
    leaf state {
        type operator-state;
        mandatory true;
        description
            "The operator's view of the alarm state.";
    }
    leaf text {
        type string;
        description
            "Additional optional textual information provided by
            the operator.";
    }
}

grouping resource-alarm-parameters {
    description
        "Alarm parameters that originates from the resource view.";
    leaf is-cleared {
        type boolean;
        mandatory true;
        description
            "Indicates the current clearance state of the alarm. An
            alarm might toggle from active alarm to cleared alarm and
            back to active again.";
    }

    leaf last-changed {
        type yang:date-and-time;
        mandatory true;
        description
            "A timestamp when the alarm status was last changed. Status
            changes are changes to 'is-cleared', 'perceived-severity',
            and 'alarm-text'.";
    }

    leaf perceived-severity {
        type severity;
        mandatory true;
        description
```

```
    "The last severity of the alarm.

    If an alarm was raised with severity 'warning', but later
    changed to 'major', this leaf will show 'major'.";
}

leaf alarm-text {
    type alarm-text;
    mandatory true;
    description
        "The last reported alarm text. This text should contain
        information for an operator to be able to understand
        the problem and how to resolve it.";
}

list status-change {
    if-feature alarm-history;
    key time;
    min-elements 1;
    description
        "A list of status change events for this alarm.

        The entry with latest time-stamp in this list MUST
        correspond to the leafs 'is-cleared', 'perceived-severity'
        and 'alarm-text' for the alarm. The time-stamp for that
        entry MUST be equal to the 'last-changed' leaf.

        This list is ordered according to the timestamps of
        alarm state changes. The last item corresponds to the
        latest state change.

        The following state changes creates an entry in this
        list:
        - changed severity (warning, minor, major, critical)
        - clearance status, this also updates the 'is-cleared'
          leaf
        - alarm text update";

    uses alarm-state-change-parameters;
}

/*
 * The /alarms data tree
 */

container alarms {
```

```
description
  "The top container for this module";
container control {
  description
    "Configuration to control the alarm behaviour.";
  leaf max-alarm-status-changes {
    type union {
      type uint16;
      type enumeration {
        enum infinite {
          description
            "The status change entries are accumulated
            infinitely.";
        }
      }
    }
  }
  default 32;
  description
    "The status-change entries are kept in a circular list
    per alarm.  When this number is exceeded, the oldest
    status change entry is automatically removed.  If the
    value is 'infinite', the status change entries are
    accumulated infinitely.";
}

leaf notify-status-changes {
  type boolean;
  default false;
  description
    "This leaf controls whether notifications are sent on all
    alarm status updates, e.g., updated perceived-severity or
    alarm-text.  By default the notifications are only sent
    when a new alarm is raised, re-raised after being cleared
    and when an alarm is cleared.";
}

container alarm-shelving {
  if-feature alarm-shelving;
  description
    "This list is used to shelve alarms.  The server will move
    any alarms corresponding to the shelving criteria from the
    alarms/alarm-list/alarm list to the
    alarms/shelved-alarms/shelved-alarm list.  It will also
    stop sending notifications for the shelved alarms.  The
    conditions in the shelf criteria are logically ANDed.
    When the shelving criteria is deleted or changed, the
    non-matching alarms MUST appear in the
    alarms/alarm-list/alarm list according to the real state.
    This means that the instrumentation MUST maintain states
```

```
        for the shelved alarms. Alarms that match the criteria
        shall have an operator-state 'shelved'.";
list shelf {
  key shelf-name;
  leaf shelf-name {
    type string;
    description
      "An arbitrary name for the alarm shelf.";
  }
  description
    "Each entry defines the criteria for shelving alarms.
    Criterias are ANDed.";

  leaf resource {
    type resource;
    description
      "Shelve alarms for this resource.";
  }
  leaf alarm-type-id {
    type alarm-type-id;
    description
      "Shelve alarms for this alarm type identifier.";
  }
  leaf alarm-type-qualifier {
    type alarm-type-qualifier;
    description
      "Shelve alarms for this alarm type qualifier.";
  }
  leaf description {
    type string;
    description
      "An optional textual description of the shelf. This
      description should include the reason for shelving
      these alarms.";
  }
}
}
}

container alarm-inventory {
  config false;
  description
    "This list contains all possible alarm types for the system.
    If the system knows for which resources a a specific alarm
    type can appear, this is also identified in the inventory.
    The list also tells if each alarm type has a corresponding
    clear state. The inventory shall only contain concrete
    alarm types."
```

The alarm inventory MUST be updated by the system when new alarms can appear. This can be the case when installing new software modules or inserting new card types. A notification 'alarm-inventory-changed' is sent when the inventory is changed.";

```
list alarm-type {
  key "alarm-type-id alarm-type-qualifier";
  description
    "An entry in this list defines a possible alarm.";
  leaf alarm-type-id {
    type alarm-type-id;
    mandatory true;
    description
      "The statically defined alarm type identifier for this
       possible alarm.";
  }
  leaf alarm-type-qualifier {
    type alarm-type-qualifier;
    description
      "The optionally dynamically defined alarm type identifier
       for this possible alarm.";
  }
  leaf-list resource {
    type string;
    description
      "Optionally, specifies for which resources the alarm type
       is valid. This string is for human consumption but
       SHOULD refer to paths in the model.";
  }
  leaf has-clear {
    type boolean;
    mandatory true;
    description
      "This leaf tells the operator if the alarm will be
       cleared when the correct corrective action has been
       taken. Implementations SHOULD strive for detecting the
       cleared state for all alarm types. If this leaf is
       true, the operator can monitor the alarm until it
       becomes cleared after the corrective action has been
       taken. If this leaf is false the operator needs to
       validate that the alarm is not longer active using other
       mechanisms. Alarms can lack a corresponding clear due
       to missing instrumentation or that there is no logical
       corresponding clear state.";
  }
  leaf-list severity-levels {
    type severity;
  }
}
```

```
        description
            "This leaf-list indicates the possible severity levels of
            this alarm type. Note well that 'clear' is not part of
            the severity type. In general, the severity level should
            be defined by the instrumentation based on dynamic state
            and not defined statically by the alarm type in order to
            provide relevant severity level based on dynamic state
            and context. However most alarm types have a defined set
            of possible severity levels and this should be provided
            here.";
    }
    leaf description {
        type string;
        mandatory true;
        description
            "A description of the possible alarm. It SHOULD include
            information on possible underlying root causes and
            corrective actions.";
    }
}

container summary {
    config false;
    description
        "This container gives a summary of number of alarms
        and shelved alarms";
    list alarm-summary {
        key severity;
        description
            "A global summary of all alarms in the system.";
        leaf severity {
            type severity;
            description
                "Alarm summary for this severity level.";
        }
        leaf total {
            type yang:gauge32;
            description
                "Total number of alarms of this severity level.";
        }
        leaf cleared {
            type yang:gauge32;
            description
                "For this severity level, the number of alarms that are
                cleared.";
        }
        leaf cleared-not-closed {
```

```
        if-feature operator-actions;
        type yang:gauge32;
        description
            "For this severity level, the number of alarms that are
            cleared but not closed.";
    }
    leaf cleared-closed {
        if-feature operator-actions;
        type yang:gauge32;
        description
            "For this severity level, the number of alarms that are
            cleared and closed.";
    }
    leaf not-cleared-closed {
        if-feature operator-actions;
        type yang:gauge32;
        description
            "For this severity level, the number of alarms that are
            not cleared but closed.";
    }
    leaf not-cleared-not-closed {
        if-feature operator-actions;
        type yang:gauge32;
        description
            "For this severity level, the number of alarms that are
            not cleared and not closed.";
    }
}
leaf shelves-active {
    if-feature alarm-shelving;
    type empty;
    description
        "This is a hint to the operator that there are active
        alarm shelves. This leaf MUST exist if the
        alarms/shelved-alarms/number-of-shelved-alarms is > 0.";
}
}

container alarm-list {
    config false;
    description
        "The alarms in the system.";
    leaf number-of-alarms {
        type yang:gauge32;
        description
            "This object shows the total number of
            alarms in the system, i.e., the total number
            of entries in the alarm list.";
    }
}
```

```
}

leaf last-changed {
  type yang:date-and-time;
  description
    "A timestamp when the alarm list was last
    changed. The value can be used by a manager to
    initiate an alarm resynchronization procedure.";
}

list alarm {
  key "resource alarm-type-id alarm-type-qualifier";

  description
    "The list of alarms. Each entry in the list holds one
    alarm for a given alarm type and resource.
    An alarm can be updated from the underlying resource or
    by the user. The following leafs are maintained by the
    resource: is-cleared, last-change, perceived-severity,
    and alarm-text. An operator can change: operator-state
    and operator-text.

    Entries appear in the alarm list the first time an
    alarm becomes active for a given alarm-type and resource.
    Entries do not get deleted when the alarm is cleared, this
    is a boolean state in the alarm.

    Alarm entries are removed, purged, from the list by an
    explicit purge action. For example, delete all alarms
    that are cleared and in closed operator-state that are
    older than 24 hours. Systems may also remove alarms based
    on locally configured policies which is out of scope for
    this module.";

  leaf time-created {
    type yang:date-and-time;
    mandatory true;
    description
      "The time-stamp when this alarm entry was created. This
      represents the first time the alarm appeared, it can
      also represent that the alarm re-appeared after a purge.
      Further state-changes of the same alarm does not change
      this leaf, these changes will update the 'last-changed'
      leaf.";
  }

  uses common-alarm-parameters;
  uses resource-alarm-parameters;
  list operator-state-change {
```



```
    if-feature operator-actions;
    key time;
    description
        "This list is used by operators to indicate
        the state of human intervention on an alarm.
        For example, if an operator has seen an alarm,
        the operator can add a new item to this list indicating
        that the alarm is acknowledged.";
    uses operator-parameters;
}

action set-operator-state {
    if-feature operator-actions;
    description
        "This is a means for the operator to indicate
        the level of human intervention on an alarm.";
    input {
        leaf state {
            type operator-state;
            mandatory true;
            description
                "Set this operator state.";
        }
        leaf text {
            type string;
            description
                "Additional optional textual information.";
        }
    }
}

container shelved-alarms {
    if-feature alarm-shelving;
    config false;
    description
        "The shelved alarms. Alarms appear here if they match the
        criterias in /alarms/control/alarm-shelving. This list does
        not generate any notifications. The list represents alarms
        that are considered not relevant by the operator. Alarms in
        this list have an operator-state of 'shelved'. This can not
        be changed.";
    leaf number-of-shelved-alarms {
        type yang:gauge32;
        description
            "This object shows the total number of currently
            alarms, i.e., the total number of entries";
    }
}
```

```
        in the alarm list.";
    }

    leaf alarm-shelf-last-changed {
        type yang:date-and-time;
        description
            "A timestamp when the shelved alarm list was last
            changed. The value can be used by a manager to
            initiate an alarm resynchronization procedure.";
    }

    list shelved-alarm {
        key "resource alarm-type-id alarm-type-qualifier";

        description
            "The list of shelved alarms. Each entry in the list holds
            one alarm for a given alarm type and resource. An alarm
            can be updated from the underlying resource or by the
            user. These changes are reflected in different lists
            below the corresponding alarm.";

        uses common-alarm-parameters;
        uses resource-alarm-parameters;

        list operator-state-change {
            if-feature operator-actions;
            key time;
            description
                "This list is used by operators to indicate
                the state of human intervention on an alarm.
                For example, if an operator has seen an alarm,
                the operator can add a new item to this list indicating
                that the alarm is acknowledged.";
            uses operator-parameters;
        }
    }
}

/*
 * Operations
 */

rpc compress-alarms {
    if-feature alarm-history;
    description
        "This operation requests the server to compress entries in the
        alarm list by removing all but the latest state change for all
```

```
    alarms. Conditions in the input are logically ANDed. If no
    input condition is given, all alarms are compressed.";
input {
  leaf resource {
    type leafref {
      path "/alarms/alarm-list/alarm/resource";
      require-instance false;
    }
    description
      "Compress the alarms with this resource.";
  }
  leaf alarm-type-id {
    type leafref {
      path "/alarms/alarm-list/alarm/alarm-type-id";
    }
    description
      "Compress alarms with this alarm-type-id.";
  }
  leaf alarm-type-qualifier {
    type leafref {
      path "/alarms/alarm-list/alarm/alarm-type-qualifier";
    }
    description
      "Compress the alarms with this alarm-type-qualifier.";
  }
}
output {
  leaf compressed-alarms {
    type uint32;
    description
      "Number of compressed alarm entries.";
  }
}
}

grouping filter-input {
  description
    "Grouping to specify a filter construct on alarm information.";
  leaf alarm-status {
    type enumeration {
      enum any {
        description
          "Ignore alarm clearance status.";
      }
      enum cleared {
        description
          "Filter cleared alarms.";
      }
    }
  }
}
```

```
    enum not-cleared {
      description
        "Filter not cleared alarms.";
    }
  }
  mandatory true;
  description
    "The clearance status of the alarm.";
}

container older-than {
  presence "Age specification";
  description
    "Matches the 'last-status-change' leaf in the alarm.";
  choice age-spec {
    description
      "Filter using date and time age.";
    case seconds {
      leaf seconds {
        type uint16;
        description
          "Seconds part";
      }
    }
    case minutes {
      leaf minutes {
        type uint16;
        description
          "Minute part";
      }
    }
    case hours {
      leaf hours {
        type uint16;
        description
          "Hours part.";
      }
    }
    case days {
      leaf days {
        type uint16;
        description
          "Day part";
      }
    }
    case weeks {
      leaf weeks {
        type uint16;
      }
    }
  }
}
```

```
        description
            "Week part";
    }
}
}
container severity {
    presence "Severity filter";
    choice sev-spec {
        description
            "Filter based on severity level.";
        leaf below {
            type severity;
            description
                "Severity less than this leaf.";
        }
        leaf is {
            type severity;
            description
                "Severity level equal this leaf.";
        }
        leaf above {
            type severity;
            description
                "Severity level higher than this leaf.";
        }
    }
    description
        "Filter based on severity.";
}
container operator-state-filter {
    if-feature operator-actions;
    presence "Operator state filter";
    leaf state {
        type operator-state;
        description
            "Filter on operator state.";
    }
    leaf user {
        type string;
        description
            "Filter based on which operator.";
    }
    description
        "Filter based on operator state.";
}
}
```

```
rpc purge-alarms {
  description
    "This operation requests the server to delete entries from the
    alarm list according to the supplied criteria. Typically it
    can be used to delete alarms that are in closed operator state
    and older than a specified time. The number of purged alarms
    is returned as an output parameter";
  input {
    uses filter-input;
  }
  output {
    leaf purged-alarms {
      type uint32;
      description
        "Number of purged alarms.";
    }
  }
}

/*
 * Notifications
 */

notification alarm-notification {
  description
    "This notification is used to report a state change for an
    alarm. The same notification is used for reporting a newly
    raised alarm, a cleared alarm or changing the text and/or
    severity of an existing alarm.";

  uses common-alarm-parameters;
  uses alarm-state-change-parameters;
}

notification alarm-inventory-changed {
  description
    "This notification is used to report that the list of possible
    alarms has changed. This can happen when for example if a new
    software module is installed, or a new physical card is
    inserted";
}

notification operator-action {
  if-feature operator-actions;
  description
    "This notification is used to report that an operator
    acted upon an alarm.";
```

```
leaf resource {
  type leafref {
    path "/alarms/alarm-list/alarm/resource";
    require-instance false;
  }
  description
    "The alarming resource.";
}
leaf alarm-type-id {
  type leafref {
    path "/alarms/alarm-list/alarm"
      + "[resource=current()/../resource]"
      + "/alarm-type-id";
    require-instance false;
  }
  description
    "The alarm type identifier for the alarm.";
}
leaf alarm-type-qualifier {
  type leafref {
    path "/alarms/alarm-list/alarm"
      + "[resource=current()/../resource]"
      + "[alarm-type-id=current()/../alarm-type-id]"
      + "/alarm-type-qualifier";
    require-instance false;
  }
  description
    "The alarm qualifier for the alarm.";
}
uses operator-parameters;
}
```

<CODE ENDS>

## 7. X.733 Alarm Mapping Data Model

Many alarm management systems are based on the X.733 alarm standard. This YANG module allows a mapping from alarm types to X.733 event-type and probable-cause.

The module augments the alarm inventory, the alarm list and the alarm notification with X.733 parameters.

The module also supports a feature whereby the alarm manager can configure the mapping. This might be needed when the default mapping provided by the system is in conflict with other systems or not considered good.

## 8. X.733 Alarm Mapping YANG Module

This YANG module references [X.733].

```
<CODE BEGINS> file "ietf-alarms-x733@2017-10-30.yang"
module ietf-alarms-x733 {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-alarms-x733";
  prefix x733;

  import ietf-alarms {
    prefix al;
  }

  organization
    "IETF CCAMP Working Group";

  contact
    "WG Web:    <http://tools.ietf.org/wg/ccamp>
    WG List:    <mailto:ccamp@ietf.org>

    Editor:     Stefan Vallin
                <mailto:stefan@wallan.se>

    Editor:     Martin Bjorklund
                <mailto:mbj@tail-f.com>";

  description
    "This module augments the ietf-alarms module with X.733 mapping
    information.  The following structures are augmented with
    event type and probable cause:

    1) alarm inventory: all possible alarms.
    2) alarm: every alarm in the system.
    3) alarm notification: notifications indicating alarm state
       changes.

    The module also optionally allows the alarm management system
    to configure the mapping.  The mapping does not include a
    a corresponding specific problem value.  The recommendation is
    to use alarm-type-qualifier which serves the same purpose.";

  reference
    "ITU Recommendation X.733: Information Technology
    - Open Systems Interconnection
    - System Management: Alarm Reporting Function";

  revision 2017-10-30 {
    description
```



```
    "Initial revision.";
  reference
    "RFC XXXX: YANG Alarm Module";
}

/*
 * Features
 */

feature configure-x733-mapping {
  description
    "The system supports configurable X733 mapping from
    alarm type to event type and probable cause.";
}

/*
 * Typedefs
 */

typedef event-type {
  type enumeration {
    enum other {
      value 1;
      description
        "None of the below.";
    }
    enum communications-alarm {
      value 2;
      description
        "An alarm of this type is principally associated with the
        procedures and/or processes required to convey
        information from one point to another.";
      reference
        "ITU Recommendation X.733: Information Technology
        - Open Systems Interconnection
        - System Management: Alarm Reporting Function";
    }
    enum quality-of-service-alarm {
      value 3;
      description
        "An alarm of this type is principally associated with a
        degradation in the quality of a service.";
      reference
        "ITU Recommendation X.733: Information Technology
        - Open Systems Interconnection
        - System Management: Alarm Reporting Function";
    }
    enum processing-error-alarm {
```

```
    value 4;
    description
        "An alarm of this type is principally associated with a
        software or processing fault.";
    reference
        "ITU Recommendation X.733: Information Technology
        - Open Systems Interconnection
        - System Management: Alarm Reporting Function";
}
enum equipment-alarm {
    value 5;
    description
        "An alarm of this type is principally associated with an
        equipment fault.";
    reference
        "ITU Recommendation X.733: Information Technology
        - Open Systems Interconnection
        - System Management: Alarm Reporting Function";
}
enum environmental-alarm {
    value 6;
    description
        "An alarm of this type is principally associated with a
        condition relating to an enclosure in which the equipment
        resides.";
    reference
        "ITU Recommendation X.733: Information Technology
        - Open Systems Interconnection
        - System Management: Alarm Reporting Function";
}
enum integrity-violation {
    value 7;
    description
        "An indication that information may have been illegally
        modified, inserted or deleted.";
    reference
        "ITU Recommendation X.736: Information Technology
        - Open Systems Interconnection
        - System Management: Security Alarm Reporting Function";
}
enum operational-violation {
    value 8;
    description
        "An indication that the provision of the requested service
        was not possible due to the unavailability, malfunction or
        incorrect invocation of the service.";
    reference
        "ITU Recommendation X.736: Information Technology
```

```
        - Open Systems Interconnection
        - System Management: Security Alarm Reporting Function";
    }
    enum physical-violation {
        value 9;
        description
            "An indication that a physical resource has been violated
            in a way that suggests a security attack.";
        reference
            "ITU Recommendation X.736: Information Technology
            - Open Systems Interconnection
            - System Management: Security Alarm Reporting Function";
    }
    enum security-service-or-mechanism-violation {
        value 10;
        description
            "An indication that a security attack has been detected by
            a security service or mechanism.";
        reference
            "ITU Recommendation X.736: Information Technology
            - Open Systems Interconnection
            - System Management: Security Alarm Reporting Function";
    }
    enum time-domain-violation {
        value 11;
        description
            "An indication that an event has occurred at an unexpected
            or prohibited time.";
        reference
            "ITU Recommendation X.736: Information Technology
            - Open Systems Interconnection
            - System Management: Security Alarm Reporting Function";
    }
}
description
    "The event types as defined by X.733 and X.736. The use of the
    term 'event' is a bit confusing. In an alarm context these
    are top level alarm types.";
}

/*
 * Groupings
 */

grouping x733-alarm-parameters {
    description
        "Common X.733 parameters for alarms.";
```

```
    leaf event-type {
        type event-type;
        description
            "The X.733/X.736 event type for this alarm.";
    }
    leaf probable-cause {
        type uint32;
        description
            "The X.733 probable cause for this alarm.";
    }
}

grouping x733-alarm-definition-parameters {
    description
        "Common X.733 parameters for alarm definitions.";

    leaf event-type {
        type event-type;
        description
            "The alarm type has this X.733/X.736 event type.";
    }
    leaf probable-cause {
        type uint32;
        description
            "The alarm type has this X.733 probable cause value.
            This module defines probable cause as an integer
            and not as an enumeration. The reason being that the
            primary use of probable cause is in the management
            application if it is based on the X.733 standard.
            However, most management applications have their own
            defined enum definitions and merging enums from
            different systems might create conflicts. By using
            a configurable uint32 the system can be configured
            to match the enum values in the manager.";
    }
}

/*
 * Add X.733 parameters to the alarm definitions, alarms,
 * and notification.
 */

augment "/al:alarms/al:alarm-inventory/al:alarm-type" {
    description
        "Augment X.733 mapping information to the alarm inventory.";

    uses x733-alarm-definition-parameters;
}
```

```
augment "/al:alarms/al:control" {
  description
    "Add X.733 mapping capabilities. ";
  list x733-mapping {
    if-feature configure-x733-mapping;
    key "alarm-type-id alarm-type-qualifier-match";
    description
      "This list allows a management application to control the
      X.733 mapping for all alarm types in the system. Any entry
      in this list will allow the alarm manager to over-ride the
      default X.733 mapping in the system and the final mapping
      will be shown in the alarm-inventory";

    leaf alarm-type-id {
      type al:alarm-type-id;
      description
        "Map the alarm type with this alarm type identifier.";
    }
    leaf alarm-type-qualifier-match {
      type string;
      description
        "A W3C regular expression that is used when mapping an
        alarm type and alarm-type-qualifier to X.733 parameters.";
    }

    uses x733-alarm-definition-parameters;
  }
}

augment "/al:alarms/al:alarm-list/al:alarm" {
  description
    "Augment X.733 information to the alarm.";

  uses x733-alarm-parameters;
}

augment "/al:alarms/al:shelved-alarms/al:shelved-alarm" {
  description
    "Augment X.733 information to the alarm.";

  uses x733-alarm-parameters;
}

augment "/al:alarm-notification" {
  description
    "Augment X.733 information to the alarm notification.";

  uses x733-alarm-parameters;
}
```

```
}  
}
```

<CODE ENDS>

## 9. Security Considerations

None.

## 10. Acknowledgements

The author wishes to thank Viktor Leijon and Johan Nordlander for their valuable input on forming the alarm model.

## 11. References

### 11.1. 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>>.
- [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>>.
- [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>>.
- [X.733] International Telecommunications Union, "Information Technology - Open Systems Interconnection - Systems Management: Alarm Reporting Function", ITU-T Recommendation X.733, 1992.

### 11.2. Informative References

- [ALARMIRP] 3GPP, "Telecommunication management; Fault Management; Part 2: Alarm Integration Reference Point (IRP): Information Service (IS)", 3GPP TS 32.111-2 3.4.0, March 2005.

- [ALARMSEM] Wallin, S., Leijon, V., Nordlander, J., and N. Bystedt, "The semantics of alarm definitions: enabling systematic reasoning about alarms. International Journal of Network Management, Volume 22, Issue 3, John Wiley and Sons, Ltd, <http://dx.doi.org/10.1002/nem.800>", March 2012.
- [EEMUA] EEMUA Publication No. 191 Engineering Equipment and Materials Users Association, London, 2 edition., "Alarm Systems: A Guide to Design, Management and Procurement.", 2007.
- [I-D.ietf-netmod-yang-tree-diagrams] Bjorklund, M. and L. Berger, "YANG Tree Diagrams", draft-ietf-netmod-yang-tree-diagrams-02 (work in progress), October 2017.
- [ISA182] International Society of Automation, ISA, "ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries", 2009.
- [RFC3877] Chisholm, S. and D. Romascanu, "Alarm Management Information Base (MIB)", RFC 3877, DOI 10.17487/RFC3877, September 2004, <<https://www.rfc-editor.org/info/rfc3877>>.
- [X.736] International Telecommunications Union, "Information Technology - Open Systems Interconnection - Systems Management: Security alarm reporting function", ITU-T Recommendation X.736, 1992.

#### Appendix A. Vendor-specific Alarm-Types Example

This example shows how to define alarm-types in a vendor-specific module. In this case the vendor "xyz" has chosen to define top level identities according to X.733 event types.

```
module example-xyz-alarms {
  namespace "urn:example:xyz-alarms";
  prefix xyz-al;

  import ietf-alarms {
    prefix al;
  }

  identity xyz-alarms {
    base al:alarm-identity;
  }

  identity communications-alarm {
    base xyz-alarms;
  }
  identity quality-of-service-alarm {
    base xyz-alarms;
  }
  identity processing-error-alarm {
    base xyz-alarms;
  }
  identity equipment-alarm {
    base xyz-alarms;
  }
  identity environmental-alarm {
    base xyz-alarms;
  }

  // communications alarms
  identity link-alarm {
    base communications-alarm;
  }

  // QoS alarms
  identity high-jitter-alarm {
    base quality-of-service-alarm;
  }
}
```

#### Appendix B. Alarm Inventory Example

This shows an alarm inventory, it shows one alarm type defined only with the identifier, and another dynamically configured. In the latter case a digital input has been connected to a smoke-detector, therefore the 'alarm-type-qualifier' is set to "smoke-detector" and the 'alarm-type-identity' to "environmental-alarm".



```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
  xmlns:xyz-al="urn:example:xyz-alarms">
  <alarm-inventory>
    <alarm-type>
      <alarm-type-id>xyz-al:link-alarm</alarm-type-id>
      <alarm-type-qualifier/>
      <has-clear>true</has-clear>
      <description>
        Link failure, operational state down but admin state up
      </description>
    </alarm-type>
    <alarm-type>
      <alarm-type-id>xyz-al:environmental-alarm</alarm-type-id>
      <alarm-type-qualifier>smoke-alarm</alarm-type-qualifier>
      <has-clear>true</has-clear>
      <description>
        Connected smoke detector to digital input
      </description>
    </alarm-type>
  </alarm-inventory>
</alarms>
```

#### Appendix C. Alarm List Example

In this example we show an alarm that has toggled [major, clear, major]. An operator has acknowledged the alarm.

```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
  xmlns:xyz-al="urn:example:xyz-alarms"
  xmlns:dev="urn:example:device">
  <alarm-list>
    <number-of-alarms>1</number-of-alarms>
    <last-changed>2015-04-08T08:39:50.00Z</last-changed>

    <alarm>
      <resource>
        /dev:interfaces/dev:interface[name='FastEthernet1/0']
      </resource>
      <alarm-type-id>xyz-al:link-alarm</alarm-type-id>
      <alarm-type-qualifier></alarm-type-qualifier>

      <time-created>2015-04-08T08:39:50.00Z</time-created>
      <is-cleared>false</is-cleared>
      <alt-resource>1.3.6.1.2.1.2.2.1.1.17</alt-resource>
      <last-changed>2015-04-08T08:39:40.00Z</last-changed>
      <perceived-severity>major</perceived-severity>
      <alarm-text>
```

```
    Link operationally down but administratively up
  </alarm-text>
  <status-change>
    <time>2015-04-08T08:39:40.00Z</time>
    <perceived-severity>major</perceived-severity>
    <alarm-text>
      Link operationally down but administratively up
    </alarm-text>
  </status-change>
  <status-change>
    <time>2015-04-08T08:30:00.00+00:00</time>
    <perceived-severity>cleared</perceived-severity>
    <alarm-text>
      Link operationally up and administratively up
    </alarm-text>
  </status-change>
  <status-change>
    <time>2015-04-08T08:20:10.00+00:00</time>
    <perceived-severity>major</perceived-severity>
    <alarm-text>
      Link operationally down but administratively up
    </alarm-text>
  </status-change>
  <operator-state-change>
    <time>2015-04-08T08:39:50.00Z</time>
    <state>ack</state>
    <operator>joe</operator>
    <text>Will investigate, ticket TR764999</text>
  </operator-state-change>
</alarm>
</alarm-list>
</alarms>
```

#### Appendix D. Alarm Shelving Example

This example shows how to shelf alarms. We shelf alarms related to the smoke-detectors since they are being installed and tested. We also shelf all alarms from FastEthernet1/0.

```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
  xmlns:xyz-al="urn:example:xyz-alarms"
  xmlns:dev="urn:example:device">
  <control>
    <alarm-shelving>
      <shelf>
        <shelf-name>FE10</shelf-name>
        <resource>
          /dev:interfaces/dev:interface[name='FastEthernet1/0']
        </resource>
      </shelf>
      <shelf>
        <shelf-name>detectortest</shelf-name>
        <alarm-type-id>xyz-al:environmental-alarm</alarm-type-id>
        <alarm-type-qualifier>smoke-alarm</alarm-type-qualifier>
      </shelf>
    </alarm-shelving>
  </control>
</alarms>
```

#### Appendix E. X.733 Mapping Example

This example shows how to map a dynamic alarm type (alarm-type-identity=environmental-alarm, alarm-type-qualifier=smoke-alarm) to the corresponding X.733 event-type and probable cause parameters.

```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
  xmlns:xyz-al="urn:example:xyz-alarms">
  <control>
    <x733-mapping
      xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms-x733">
      <alarm-type-id>xyz-al:environmental-alarm</alarm-type-id>
      <alarm-type-qualifier-match>
        smoke-alarm
      </alarm-type-qualifier-match>
      <event-type>quality-of-service-alarm</event-type>
      <probable-cause>777</probable-cause>
    </x733-mapping>
  </control>
</alarms>
```

#### Appendix F. Background and Usability Requirements

This section gives background information regarding design choices in the alarm module. It also defines usability requirements for alarms. Alarm usability is important for an alarm interface. A data-model

will help in defining the format but if the actual alarms is of low value we have not gained the goal of alarm management.

The telecommunication domain has standardised an alarm interface in ITU-T X.733 [X.733]. This continued in mobile networks within the 3GPP organisation [ALARMIRP]. Although SNMP is the dominant mechanism for monitoring devices, IETF did not early on standardise an alarm MIB. Instead, management systems interpreted the enterprise specific traps per MIB and device to build an alarm list. When finally The Alarm MIB [RFC3877] was published, it had to address the existence of enterprise traps and map these into alarms. This requirement led to a MIB that is not always easy to use.

#### F.1. Alarm Concepts

There are two misconceptions regarding alarms and alarm interfaces that are important to sort out. The first problem is that alarms are mixed with events in general. Alarms MUST correspond to an undesirable state that needs corrective action. Many implementations of alarm interfaces do not adhere to this principle and just send events in general. In order to qualify as an alarm, there must exist a corrective action. If that is not true, it is an event that can go into logs.

The other misconception is that the term "alarm" refers to the notification itself. Rather, an alarm is a state of a resource in the system. The alarm notifications report state changes of the alarm, such as alarm raise and alarm clear.

"One of the most important principles of alarm management is that an alarm requires an action. This means that if the operator does not need to respond to an alarm (because unacceptable consequences do not occur), then it is not an alarm. Following this cardinal rule will help eliminate many potential alarm management issues." [ISA182]

##### F.1.1. Alarm type

Since every alarm has a corresponding corrective action, a vendor can to prepare a list of available alarms and their corrective actions. We use the term "alarm type" to refer to every possible alarm that could be active in the system.

Alarm types are also fundamental in order to provide a state-based alarm list. The alarm list correlates alarm state changes for the same alarm type and the same resource into one alarm.

Different alarm interfaces use different mechanisms to define alarm types, ranging from simple error numbers to more advanced mechanisms

like the X.733 triplet of event type, probable cause and specific problem.

A common misunderstanding is that individual alarm notifications are alarm types. This is not correct; e.g., "link-up" and "link-down" are two notifications reporting different states for the same alarm type, "link-alarm".

## F.2. Usability Requirements

Common alarm problems and the cause of the problems are summarised in Table 1. This summary is adopted to networking based on the ISA [ISA182] and EEMUA [EEMUA] standards.

Problem	Cause	How this module address the cause
Alarms are generated but they are ignored by the operator.	"Nuisance" alarms (chattering alarms and fleeting alarms), faulty hardware, redundant alarms, cascading alarms, incorrect alarm settings, alarms have not been rationalised, the alarms represent log information rather than true alarms.	Strict definition of alarms requiring corrective response. Alarm requirements in Table 2.
When alarms occur, operators do not know how to respond.	Insufficient alarm response procedures and not well defined alarm types.	The alarm inventory lists all alarm types and corrective actions. Alarm requirements in Table 2.
The alarm display is full of alarms, even when there is nothing wrong.	Nuisance alarms, stale alarms, alarms from equipment not in service.	The alarm definition and alarm shelving.
During a failure, operators are flooded with so many alarms that they do not know which ones are the most important.	Incorrect prioritization of alarms. Not using advanced alarm techniques (e.g. state-based alarming).	State-based alarm model, alarm rate requirements in Table 3 and Table 4

Table 1: Alarm Problems and Causes

Based upon the above problems EEMUA gives the following definition of a good alarm:

Characteristic	Explanation
Relevant	Not spurious or of low operational value.
Unique	Not duplicating another alarm.
Timely	Not long before any response is needed or too late to do anything.
Prioritised	Indicating the importance that the operator deals with the problem.
Understandable	Having a message which is clear and easy to understand.
Diagnostic	Identifying the problem that has occurred.
Advisory	Indicative of the action to be taken.
Focusing	Drawing attention to the most important issues.

Table 2: Definition of a Good Alarm

Vendors SHOULD rationalise all alarms according to above. Another crucial requirement is acceptable alarm rates. Vendors SHOULD make sure that they do not exceed the recommendations from EEMUA below:

Long Term Alarm Rate in Steady Operation	Acceptability
More than one per minute	Very likely to be unacceptable.
One per 2 minutes	Likely to be over-demanding.
One per 5 minutes	Manageable.
Less than one per 10 minutes	Very likely to be acceptable.

Table 3: Acceptable Alarm Rates, Steady State

Number of alarms displayed in 10 minutes following a major network problem	Acceptability
More than 100	Definitely excessive and very likely to lead to the operator to abandon the use of the alarm system.
20-100	Hard to cope with.
Under 10	Should be manageable - but may be difficult if several of the alarms require a complex operator response.

Table 4: Acceptable Alarm Rates, Burst

The numbers in Table 3 and Table 4 are the sum of all alarms for a network being managed from one alarm console. So every individual system or NMS contributes to these numbers.

Vendors SHOULD make sure that the following rules are used in designing the alarm interface:

1. Rationalize the alarms in the system to ensure that every alarm is necessary, has a purpose, and follows the cardinal rule - that it requires an operator response. Adheres to the rules of Table 2
2. Audit the quality of the alarms. Talk with the operators about how well the alarm information support them. Do they know what to do in the event of an alarm? Are they able to quickly diagnose the problem and determine the corrective action? Does the alarm text adhere to the requirements in Table 2?
3. Analyze and benchmark the performance of the system and compare it to the recommended metrics in Table 3 and Table 4. Start by identifying nuisance alarms, standing alarms at normal state and startup.

#### Authors' Addresses

Stefan Vallin  
Stefan Vallin AB

Email: stefan@wallan.se



Martin Bjorklund  
Cisco

Email: [mbj@tail-f.com](mailto:mbj@tail-f.com)

CCAMP Working Group  
Internet Draft  
Intended status: Standards Track  
Expires: January 3, 2018

J.E. Lopez de Vergara  
Universidad Autonoma de Madrid  
Daniel Perdices  
Naudit HPCN  
V. Lopez  
O. Gonzalez de Dios  
Telefonica I+D/GCTO  
D. King  
Lancaster University  
Y. Lee  
Huawei  
G. Galimberti  
Cisco Photonics Srl  
July 3, 2017

YANG data model for Flexi-Grid media-channels  
draft-vergara-ccamp-flexigrid-media-channel-yang-00.txt

#### Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, except to publish it as an RFC and to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on January 3, 2018

#### Copyright Notice

Copyright (c) 2017 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

Internet-Draft YANG data model for Flexi-Grid media-channels July 2017  
carefully, as they describe your rights and restrictions with  
respect to this document. Code Components extracted from this  
document must include Simplified BSD License text as described in  
Section 4.e of the Trust Legal Provisions and are provided without  
warranty as described in the Simplified BSD License.

## Abstract

This document defines a YANG model for managing flexi-grid optical  
media channels, complementing the information provided by the  
flexi-grid TED model.  
It is also grounded on other defined YANG abstract models.

## Table of Contents

1. Introduction .....	2
2. Conventions used in this document .....	3
3. Flexi-grid media-channel overview .....	3
4. Example of use .....	4
5. Media Channel YANG Model .....	5
5.1. YANG Model - Tree .....	5
5.2. YANG Model - Code .....	6
5.3. License .....	10
6. Security Considerations .....	10
7. IANA Considerations .....	10
8. References .....	11
8.1. Normative References .....	11
8.2. Informative References .....	11
9. Contributors .....	11
10. Acknowledgments .....	11
Authors' Addresses .....	12

## 1. Introduction

Transport networks are evolving from current DWDM systems towards  
elastic optical networks, based on flexi-grid transmission and  
switching technologies [RFC7698]. Such technology aims at increasing  
both transport network scalability and flexibility, allowing the  
optimization of bandwidth usage.

Internet-Draft YANG data model for Flexi-Grid media-channels July 2017  
While [I-D.draft-vergara-ccamp-flexigrid-yang] focuses on flexi-grid objects such as nodes, transponders and links, this document presents a YANG model for the flexi-grid media-channel. This YANG module defines the whole path from a source transponder or node to the destination through a number of intermediate nodes in the flexi-grid network.

This document identifies the flexi-grid media-channel components, parameters and their values, characterizes the features and the performances of the flexi-grid elements. An application example is provided towards the end of the document to better understand their utility.

## 2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

In this document, the characters ">>" preceding an indented line(s) indicates a compliance requirement statement using the key words listed above. This convention aids reviewers in quickly identifying or finding the explicit compliance requirements of this RFC.

## 3. Flexi-grid media-channel overview

The present model defines a flexi-grid media-channel mainly composed of:

- source address
- source flexi-grid port
- source flexi-grid transponder
- destination address
- destination flexi-grid port
- destination flexi-grid transponder
- A list of links that defines the path
- Other optical attributes

Each path can be a media-channel (only defined by source and destination node) or a network media-channel (additionally needs source and destination transponders). Therefore, all the attributes are optional to support both situations.

This is achieved by a combination of the traffic engineering tunnel attributes explained in [I-D.draft-ietf-teas-yang-te] and augments when necessary. For instance, source address, source flexi-grid transponder, destination address and destination flexi-grid transponder attributes are directly taken from tunnel, whereas other attributes such as source flexi-grid port, destination flexi-grid port are defined, as they are specific for flexi-grid.

#### 4. Example of use

In order to explain how this model is used, we provide the following example. An optical network usually has multiple transponders, switches (nodes) and links between them. Figure 1 shows a simple topology, where two physical paths interconnect two optical transponders.

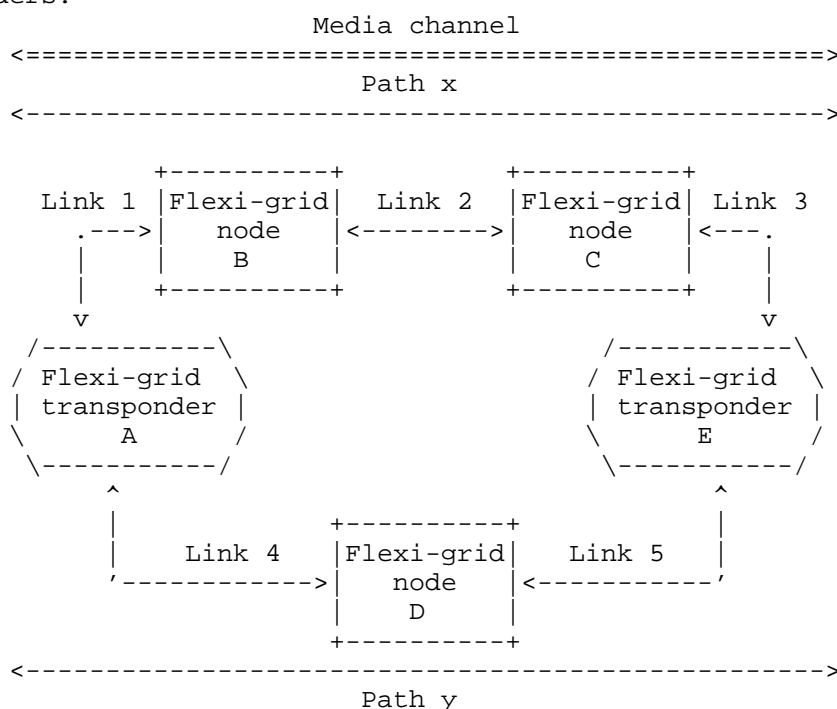


Figure 1. Topology example.

After the nodes, links and transponders have been defined using [I-D.draft-vergara-ccamp-flexigrid-yang], we can configure the media-channel from the information we have stored in the flexi-grid TED, by querying which elements are available, and planning the resources that have to be provided on each situation. Note that every element in the flexi-grid TED has a reference, and this is the way in which they are called in the media-channel.

1. Depending on the case, it is possible to define either the source and destination node ports, or the source and destination node and transponder. In our case, we would define a network media channel, with source transponder A and source node B, and destination transponder E and destination node C. Thus, we are going to follow path x.
2. Then, for each link in the path x, we indicate which channel we are going to use, providing information about the slots, and what nodes are connected.
3. Finally, the flexi-grid TED has to be updated with each element usage status each time a media channel is created or torn down.

## 5. Media Channel YANG Model

### 5.1. YANG Model - Tree

```
module: ietf-flexi-grid-media-channel
  augment /te:te/te:tunnels/te:tunnel/te:config:
    +--rw source-port?          fg-ted:flexi-grid-node-port-ref
    +--rw destination-port?     fg-ted:flexi-grid-node-port-ref
    +--rw effective-freq-slot
      +--rw N?   int32
      +--rw M?   int32
  augment /te:te/te:tunnels/te:tunnel/te:state:
    +--ro source-port?          fg-ted:flexi-grid-node-port-ref
    +--ro destination-port?     fg-ted:flexi-grid-node-port-ref
    +--ro effective-freq-slot
      +--ro N?   int32
      +--ro M?   int32
  augment /te:te/te:lsps-state/te:lsp:
    +--ro N?   int32
    +--ro M?   int32
    +--ro source-port?          fg-ted:flexi-grid-node-port-ref
    +--ro destination-port?     fg-ted:flexi-grid-node-port-ref
    +--ro link?                 fg-ted:flexi-grid-link-ref
    +--ro bidirectional?        boolean
```

```
<CODE BEGINS> file "ietf-flexi-grid-media-channel@2017-07-03.yang"
module ietf-flexi-grid-media-channel {
  yang-version 1.1;

  namespace
    "urn:ietf:params:xml:ns:yang:ietf-flexi-grid-media-channel";
  prefix "fg-mc";

  import ietf-flexi-grid-ted {
    prefix "fg-ted";
  }

  import ietf-te {
    prefix "te";
  }

  import ietf-network {
    prefix "nd";
  }
  organization
    "IETF CCAMP Working Group";
  contact
    "Editor: Jorge Lopez de Vergara
      <jorge.lopez_vergara@uam.es>";

  description
    "This module contains a collection of YANG definitions for
    a Flexi-Grid media channel.

    Copyright (c) 2017 IETF Trust and the persons identified as
    authors of the code. All rights reserved.

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

  revision 2017-07-03 {
    description
      "version 0.";

    reference
      "RFC XXX: A Yang Data Model for Flexi-Grid media-channels";
  }
}
```

```

grouping flexi-grid-media-channel {
  description
    "Media association that represents both the topology
    (i.e., path through the media) and the resource
    (frequency slot) that it occupies. As a topological
    construct, it represents a (effective) frequency slot
    supported by a concatenation of media elements (fibers,
    amplifiers, filters, switching matrices...). This term
    is used to identify the end-to-end physical layer entity
    with its corresponding (one or more) frequency slots
    local at each link filters.";
  reference "rfc7698";
  leaf source-port {
    type fg-ted:flexi-grid-node-port-ref;
    description "Source port";
  }
  leaf destination-port {
    type fg-ted:flexi-grid-node-port-ref;
    description "Destination port";
  }
  container effective-freq-slot {
    description "The effective frequency slot is an attribute
    of a media channel and, being a frequency slot, it is
    described by its nominal central frequency and slot
    width";
    reference "rfc7698";
    leaf N {
      type int32;
      description
        "Is used to determine the Nominal Central
        Frequency. The set of nominal central frequencies
        can be built using the following expression:
           $f = 193.1 \text{ THz} + n \times 0.00625 \text{ THz}$ ,
        where 193.1 THz is ITU-T ''anchor frequency'' for
        transmission over the C band, n is a positive or
        negative integer including 0.";
      reference "rfc7698";
    }
    leaf M {
      type int32;
      description
        "Is used to determine the slot width. A slot width
        is constrained to be M x SWG (that is, M x 12.5 GHz),
        where M is an integer greater than or equal to 1.";
      reference "rfc7698";
    }
  }
}

```



```

grouping link-channel-attributes {
  description
    "A link channel is one of the concatenated elements of
    the media channel.";
  leaf N {
    type int32;
    description
      "Is used to determine the Nominal Central Frequency.
      The set of nominal central frequencies can be built
      using the following expression:
       $f = 193.1 \text{ THz} + n \times 0.00625 \text{ THz}$ ,
      where 193.1 THz is ITU-T ''anchor frequency'' for
      transmission over the C band, n is a positive or
      negative integer including 0.";
    reference "rfc7698";
  }
  leaf M {
    type int32;
    description
      "Is used to determine the slot width. A slot
      width is constrained to be M x SWG (that is,
      M x 12.5 GHz), where M is an integer greater than
      or equal to 1.";
    reference "rfc7698";
  }
  leaf source-port {
    type fg-ted:flexi-grid-node-port-ref;
    description "Source port of the link channel";
  }
  leaf destination-port {
    type fg-ted:flexi-grid-node-port-ref;
    description "Destination port of the link channel";
  }
  leaf link {
    type fg-ted:flexi-grid-link-ref;
    description "Link of the link channel";
  }
  leaf bidirectional {
    type boolean;
    description
      "Determines whether the link is bidirectional or
      not";
  }
}

```

```
/* Augment for media-channel */
augment "/te:te/te:tunnels/te:tunnel/te:config" {
  when "/nd:networks/nd:network/nd:network-types/
fg-ted:flexi-grid-network"{
    description "Augment only for Flexigrid network.";
  }
  description "Augment tunnel with media-channel config";
  uses flexi-grid-media-channel;
}

augment "/te:te/te:tunnels/te:tunnel/te:state" {
  when "/nd:networks/nd:network/nd:network-types/
fg-ted:flexi-grid-network"{
    description "Augment only for Flexigrid network.";
  }
  uses flexi-grid-media-channel;
  description "Augment tunnel with media-channel state";
}

/* Augment for LSP */
augment "/te:te/te:lsps-state/te:lsp" {
  when "/nd:networks/nd:network/nd:network-types/
fg-ted:flexi-grid-network"{
    description "Augment only for Flexigrid network.";
  }
  uses link-channel-attributes;
  description "Augment LSP for paths";
}
}

<CODE ENDS>
```

Copyright (c) 2017 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, are permitted provided that the following conditions are met:

- o Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- o Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- o Neither the name of Internet Society, IETF or IETF Trust, nor the names of specific contributors, may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## 6. Security Considerations

The transport protocol used for sending the managed information MUST support authentication and SHOULD support encryption.

The defined data-model by itself does not create any security implications.

## 7. IANA Considerations

The namespace used in the defined models is currently based on the METRO-HAUL project URI. Future versions of this document could register a URI in the IETF XML registry [RFC3688], as well as in the YANG Module Names registry [RFC6020].

#### 8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.
- [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

#### 8.2. Informative References

- [RFC7698] Gonzalez de Dios, O., Casellas, R., Eds. "Framework and Requirements for GMPLS-Based Control of Flexi-Grid Dense Wavelength Division Multiplexing (DWDM) Networks", RFC7698, November 2015.
- [I-D.draft-vergara-ccamp-flexigrid-yang] Lopez de Vergara, J., Perdices, D., Lopez, V., Gonzalez de Dios, O., King, D., Lee, Y., Galimberti, G., "YANG data model for Flexi-Grid Optical Networks", Internet Draft, draft-vergara-ccamp-flexigrid-yang-04, 2017.
- [I-D.draft-ietf-teas-yang-te] Saad, T., Gandhi, R., Liu, X., Beeram, V., Shah, H., Bryskin, I., Chen, X., Jones, R., and B. Wen, "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te-08, 2017.

#### 9. Contributors

The model presented in this paper was contributed to by more people than can be listed on the author list. Additional contributors include:

- o Zafar Ali, Cisco Systems
- o Daniel Michaud Vallinoto, Universidad Autonoma de Madrid

#### 10. Acknowledgments

The work presented in this Internet-Draft has been partially funded by the European Commission under the project H2020 METRO-HAUL (Metro High bandwidth, 5G Application-aware optical network, with edge storage, compUte and low Latency), Grant Agreement number: 761727, and by the Spanish Ministry of Economy and Competitiveness under the project TRAFICA, MINECO/FEDER TEC2015-69417-C2-1-R.

Jorge E. Lopez de Vergara  
Universidad Autonoma de Madrid  
Escuela Politecnica Superior  
C/Francisco Tomas y Valiente, 11  
E-28049 Madrid, Spain

Email: [jorge.lopez\\_vergara@uam.es](mailto:jorge.lopez_vergara@uam.es)

Daniel Perdices Burrero  
Naudit High Performance Computing and Networking, S.L.  
C/Faraday, 7  
E-28049 Madrid, Spain

Email: [daniel.perdices@naudit.es](mailto:daniel.perdices@naudit.es)

Victor Lopez  
Telefonica I+D/GCTO  
Distrito Telefonica  
E-28050 Madrid, Spain

Email: [victor.lopezalvarez@telefonica.com](mailto:victor.lopezalvarez@telefonica.com)

Oscar Gonzalez de Dios  
Telefonica I+D/GCTO  
Distrito Telefonica  
E-28050 Madrid, Spain

Email: [oscar.gonzalezdedios@telefonica.com](mailto:oscar.gonzalezdedios@telefonica.com)

Daniel King  
Lancaster University

Email: [d.king@lancaster.ac.uk](mailto:d.king@lancaster.ac.uk)

Young Lee  
Huawei Technologies

Email: [leeyoung@huawei.com](mailto:leeyoung@huawei.com)

Gabriele Galimberti  
Cisco Photonics Srl

Email: [ggalimbe@cisco.com](mailto:ggalimbe@cisco.com)

CCAMP Working Group  
Internet Draft  
Intended status: Standards Track  
Expires: January 3, 2018

J.E. Lopez de Vergara  
Universidad Autonoma de Madrid  
Daniel Perdices  
Naudit HPCN  
V. Lopez  
O. Gonzalez de Dios  
Telefonica I+D/GCTO  
D. King  
Lancaster University  
Y. Lee  
Huawei  
G. Galimberti  
Cisco Photonics Srl  
July 3, 2017

YANG data model for Flexi-Grid Optical Networks  
draft-vergara-ccamp-flexigrid-yang-05.txt

#### Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, except to publish it as an RFC and to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on January 3, 2018.

#### Copyright Notice

Copyright (c) 2017 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

Internet-Draft    A YANG data model for Flexi-Grid    July 2017  
carefully, as they describe your rights and restrictions with  
respect to this document. Code Components extracted from this  
document must include Simplified BSD License text as described in  
Section 4.e of the Trust Legal Provisions and are provided without  
warranty as described in the Simplified BSD License.

## Abstract

This document defines a YANG model for managing flexi-grid optical Networks. The model described in this document defines a flexi-grid traffic engineering database. A complementary module is referenced to detail the flexi-grid media channels.

This module is grounded on other defined YANG abstract models.

## Table of Contents

1. Introduction .....	2
2. Conventions used in this document .....	3
3. Flexi-grid network topology model overview .....	3
4. Main building blocks of the Flexi-grid TED.....	4
4.1 Formal Syntax .....	7
5. Example of use .....	8
6. Flexi-grid TED YANG Model.....	9
6.1. YANG Model - Tree .....	9
6.2. YANG Model - Code .....	10
6.3. License .....	19
7. Security Considerations .....	20
8. IANA Considerations .....	20
9. References .....	20
9.1. Normative References .....	20
9.2. Informative References .....	21
10. Contributors .....	21
11. Acknowledgments .....	22
Authors' Addresses .....	22

## 1. Introduction

Internet-based traffic is dramatically increasing every year. Moreover, such traffic is also becoming more dynamic. Thus, transport networks need to evolve from current DWDM systems towards elastic optical networks, based on flexi-grid transmission and switching technologies [RFC7698]. This technology aims at increasing both transport network scalability and flexibility, allowing the optimization of bandwidth usage.

This document presents a YANG model for flexi-grid objects in the dynamic optical network, including the nodes, transponders and links between them, as well as how such links interconnect nodes and transponders.

The YANG model for flexi-grid networks allows the representation of the flexi-grid optical layer of a network, combined with the underlying physical layer.

This document identifies the flexi-grid components, parameters and their values, characterizes the features and the performances of the flexi-grid elements. An application example is provided towards the end of the document to better understand their utility.

## 2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

In this document, the characters ">>" preceding an indented line(s) indicates a compliance requirement statement using the key words listed above. This convention aids reviewers in quickly identifying or finding the explicit compliance requirements of this RFC.

## 3. Flexi-grid network topology model overview

YANG is a data modeling language used to model configuration data manipulated by the NETCONF protocol. Several YANG models have already been specified for network configurations. For instance, the work in [I-D.draft-ietf-i2rs-yang-network-topo] has proposed a generic YANG model for network/service topologies and inventories. The work in [I-D.draft-ietf-teas-yang-te-topo] presents a data model to represent, retrieve and manipulate Traffic Engineering (TE) Topologies. These models serve as base models that other technology specific models can augment. A YANG model has also been proposed in [I-D.draft-dharini-ccamp-dwdm-if-yang] to manage single channel optical interface parameters of DWDM applications, and in



Internet-Draft     A YANG data model for Flexi-Grid     July 2017  
[I-D.draft-ietf-ccamp-wson-yang] another model has been specified for the routing and wavelength assignment TE topology in wavelength switched optical networks (WSONs). None of them are specific for flexi-grid technology.

Then, as stated before, we propose a model to describe a flexi-grid topology that is split in two YANG sub-modules:

- o Flexi-grid-TED: In order to be compatible with existing proposals, we augment the definitions contained in [I-D.draft-ietf-i2rs-yang-network-topo] and [I-D.draft-ietf-teas-yang-te-topo], by defining the different elements we can find in a flexi-grid network: a node, a transponder and a link. For that, each of those elements is defined as a container that includes a group of attributes. References to the elements are provided to be later used in the definition of a media channel. It also includes the data types for the type of modulation, the flexi-grid technology, the FEC, etc.
- o Media-channel: This module defines the whole path from a source transponder to the destination through a number of intermediate nodes and links. For this, it takes the information defined before in the flexi-grid TED. This module is described in [ID.draft-vergara-ccamp-flexigrid-media-channel-yang]

The following section provides a detailed view of the first module.

#### 4. Main building blocks of the Flexi-grid TED

This section details the defined YANG module. It is listed below in section 6.

The description of the three main components, flexi-grid-node, flexi-grid-transponder and flexi-grid-link is provided below. flexi-grid-sliceable-transponders are also defined.

```
<flexi-grid-node> ::= <config> <state>
```

```
<flexi-grid-node>: This element designates a node in the network.
```

```
<config> ::= <flexi-grid-node-attributes-config>
```

```
<config>: Contains the configuration of a node.  
<flexi-grid-node-attributes-config> ::= <list-interface>  
<connectivity_matrix>
```

```
<flexi-grid-node-attributes-config>: Contains all the attributes related to the node configuration, such as its interfaces or its management addresses.
```

```
<list-interface> ::= <name> <port-number>
<input-port> <output-port> <description>
<interface-type>
[<numbered-interface> / <unnumbered-interface>]
```

<list-interface>: The list containing all the information of the interfaces.

<name>: Determines the interface name.

<port-number>: Port number of the interface.

<input-port>: Boolean value that defines whether the interface is input or not.

<output-port>: Boolean value that defines whether the interface is output or not.

<description>: Description of the usage of the interface.

<interface-type>: Determines if the interface is numbered or unnumbered.

```
<numbered-interface> ::= <n-i-ip-address>
<numbered-interface>: An interface with its own IP address.
```

<n-i-ip-address>: Only available if <interface-type> is "numbered-interface". Determines the IP address of the interface.

```
<unnumbered-interface> ::= <u-i-ip-address>
<label>
```

<unnumbered-interface>: A interface that needs a label to be unique.

<u-i-ip-address>: Only available if <interface-type> is "unnumbered-interface". Determines the node IP address, which with the label defines the interface.

<label>: Label that determines the interface, joint with the node IP address.

```
<connectivity-matrix> ::= <connections>
```

<connectivity-matrix>: Determines whether a connection port in/port out exists.

```
<connections> ::= <input-port-id>
<output-port-id>
```

<flexi-grid-transponder>: This item designates a transponder of a node.

<config> ::= <flexi-grid-transponder-attributes-config>

<config>: Contains the configuration of a transponder.

<flexi-grid-transponder-attributes-config> ::=  
<available-operational-mode> <operational-mode>

<flexi-grid-transponder-attributes>: Contains all the attributes related to the transponder.

<available-operational-mode>: It provides a list of the operational modes available at this transponder.

<operational-mode>: Determines the type of operational mode in use.

<state> ::= <flexi-grid-transponder-attributes-config>  
<flexi-grid-transponder-attributes-state>

<state>: Contains the state of a transponder.

<flexi-grid-transponder-attributes-config>: See above.

<flexi-grid-transponder-attributes-state>: Contains the state of a transponder.

<link> ::= <config> <state>

<link>: This element describes all the information of a link.

<config> ::= <flexi-grid-link-attributes-config>

<config>: Contains the configuration of a link.

Internet-Draft    A YANG data model for Flexi-Grid    July 2017  
    <flexi-grid-link-attributes-config> ::= <technology-type>  
    <available-label-flexi-grid> <N-max> <base-frequency>  
    <nominal-central-frequency-granularity>  
    <slot-width-granularity>

    <flexi-grid-link-attributes>: Contains all the attributes related to the link, such as its unique id, its N value, its latency, etc.

    <link-id>: Unique id of the link.

    <available-label-flexi-grid>: Array of bits that determines, with each bit, the availability of each interface for flexi-grid technology.

    <N-max>: The max value of N in this link, being N the number of slots.

    <base-frequency>: The default central frequency used in the link.

    <nominal-central-frequency-granularity>: It is the spacing between allowed nominal central frequencies and it is set to 6.25 GHz (note: sometimes referred to as 0.00625 THz).

    <slot-width-granularity>: 12.5 GHz, as defined in G.694.1.

<state> ::= <flexi-grid-link-attributes-config>  
<flexi-grid-link-attributes-state>

    <state>: Contains the state of a link.

    <flexi-grid-link-attributes-config>: See above.

    <flexi-grid-link-attributes-state>: Contains all the the information related to the state of a link.

#### 4.1. Formal Syntax

The previous syntax specification uses the augmented Backus-Naur Form (BNF) as described in [RFC5234].

In order to explain how this model is used, we provide the following example. An optical network usually has multiple transponders, switches (nodes) and links between them. Figure 1 shows a simple topology, where two physical paths interconnect two optical transponders.

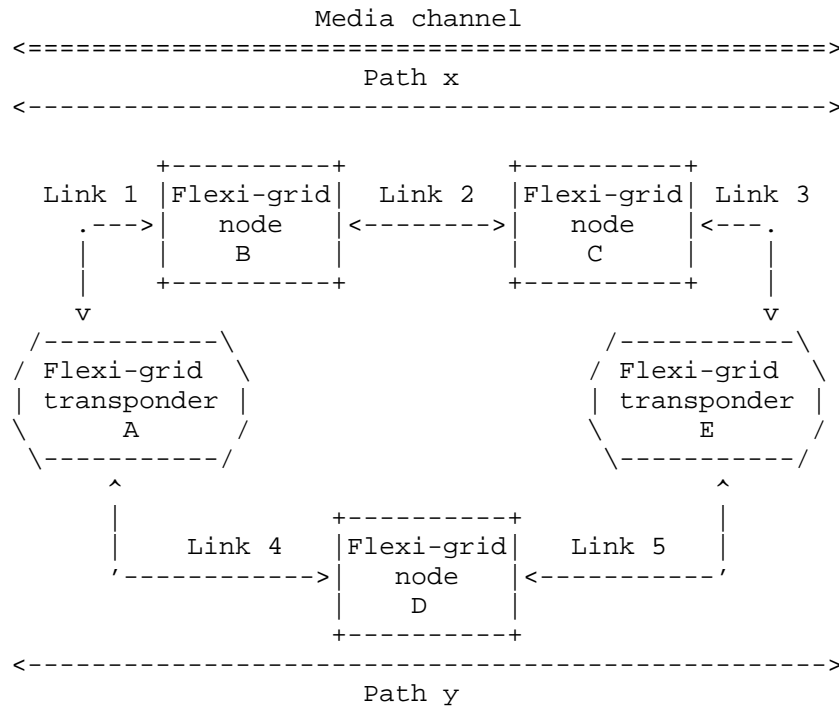


Figure 1. Topology example.

In order to configure a media channel to interconnect transponders A and E, first of all we have to populate the flexi-grid TED YANG model with all elements in the network:

1. We define the transponders A and E, including their FEC type, if enabled, and modulation type. We also provide node identifiers and addresses for the transponders, as well as interfaces included in the transponders. Sliceable transponders can also be defined if needed.
2. We do the same for the nodes B, C and D, providing their identifiers, addresses and interfaces, as well as the internal connectivity matrix between interfaces.
3. Then, we also define the links 1 to 5 that interconnect nodes and transponders, indicating which flexi-grid labels are available. Other information, such as the slot frequency and granularity are also provided.

Next, we can configure the media channel from the information we have stored in the flexi-grid TED, by querying which elements are available, and planning the resources that have to be provided on each situation. Note that every element in the flexi-grid TED has a reference, and this is the way in which they are called in the media channel. We refer to [I-D.draft-vergara-ccamp-flexigrid-media-channel-yang] to complete this example.

## 6. Flexi-grid TED YANG Model

### 6.1. Yang Model - Tree Structure

```

module: ietf-flexi-grid-topology
  augment /nd-s:networks/nd-s:network/nd-s:node/tet-s:te/
    tet-s:te-node-attributes:
      +--ro interfaces* [name]
        +--ro name                string
        +--ro port-number?        uint32
        +--ro input-port?         boolean
        +--ro output-port?        boolean
        +--ro description?        string
        +--ro type?               interface-type
        +--ro numbered-interface
          | +--ro n-i-ip-address?  inet:ip-address
        +--ro unnumbered-interface
          | +--ro u-i-ip-address?  inet:ip-address
          +--ro label?            uint32
  flexi-grid-connectivity-matrix-attributes
    augment /nd:networks/nd:network/nd:node/tet:te/
      tet:te-node-attributes/tet:connectivity-matrices/
      tet:connectivity-matrix:
        +--rw connections* [input-port-id]
          +--rw input-port-id      flexi-grid-node-port-ref
          +--rw output-port-id?    flexi-grid-node-port-ref
  flexi-grid-connectivity-matrix-attributes
    augment /nd-s:networks/nd-s:network/nd-s:node/tet-s:te/
      tet-s:te-node-attributes/tet-s:connectivity-matrices/
      tet-s:connectivity-matrix:
        +--ro connections* [input-port-id]
          +--ro input-port-id      flexi-grid-node-port-ref
          +--ro output-port-id?    flexi-grid-node-port-ref
  flexi-grid-transponder
    augment /nd:networks/nd:network/nd:node/tet:te/
      tet:tunnel-termination-point:
        +--rw available-operational-mode*  operational-mode
        +--rw operational-mode?            operational-mode
  flexi-grid-transponder
    augment /nd-s:networks/nd-s:network/nd-s:node/tet-s:te/
      tet-s:tunnel-termination-point:
        +--ro available-operational-mode*  operational-mode
        +--ro operational-mode?            operational-mode

```

```
<CODE BEGINS> file "ietf-flexi-grid-ted@2017-07-03.yang"
module ietf-flexi-grid-ted {
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-flexi-grid-ted";
  prefix "fg-ted";

  import ietf-network {
    prefix "nd";
  }
  import ietf-network-state {
    prefix "nd-s";
  }
  import ietf-network-topology {
    prefix "lnk";
  }
  import ietf-network-topology-state {
    prefix "lnk-s";
  }
  import ietf-te-topology {
    prefix "tet";
  }
  import ietf-te-topology-state {
    prefix "tet-s";
  }
  import ietf-inet-types {
    prefix "inet";
  }
}

organization
  "IETF CCAMP Working Group";

contact
  "Editor: Jorge Lopez de Vergara
    <jorge.lopez_vergara@uam.es>";

description
  "This module contains a collection of YANG definitions for
  a Flexi-Grid Traffic Engineering Database (TED).

  Copyright (c) 2017 IETF Trust and the persons identified as
  authors of the code. All rights reserved."
```

Internet-Draft    A YANG data model for Flexi-Grid    July 2017  
Redistribution and use in source and binary forms, with or  
without modification, is permitted pursuant to, and subject  
to the license terms contained in, the Simplified BSD  
License set forth in Section 4.c of the IETF Trust's Legal  
Provisions Relating to IETF Documents  
(<http://trustee.ietf.org/license-info>).";

```
revision 2017-07-03 {
  description
    "version 5.";

  reference
    "RFC XXX: A Yang Data Model for
    Flexi-Grid Optical Networks ";
}

/*
  Typedefs
*/

typedef operational-mode {
  type string;
  description
    "Vendor-specific mode that guarantees interoperability.
    It must be an string with the following format:
    B-DScW-ytz(v) where all these attributes are conformant
    to the ITU-T recomendation";
  reference "ITU-T G.698.2 (11/2009) Section 5.3";
}

typedef interface-type {
  type enumeration {
    enum numbered-interface {
      description "The interface is numbered";
    }
    enum unnumbered-interface {
      description "The interface is unnumbered";
    }
  }
  description
    "Enumeration that defines if an interface is numbered or
    unnumbered";
}
```



```
/*
  Typedef related to references
*/
typedef flexi-grid-link-ref {
  type leafref {
    path
      "/nd:networks/nd:network/lnk:link/lnk:link-id";
  }

  description
    "This type is used by data models that need to reference
    a flexi-grid optical link.";
}

typedef flexi-grid-node-port-ref {
  type leafref {
    path "/nd:networks/nd:network/nd:node/tet:te/"
      +"tet:te-node-attributes/fg-ted:interfaces/"
      +"fg-ted:port-number";
  }
  description
    "This type is used by data models that need to reference
    a flexi-grid port.";
}

typedef flexi-grid-transponder-ref {
  type leafref {
    path "/nd:networks/nd:network/nd:node/tet:te/"
      +"tet:tunnel-termination-point/tet:tunnel-tp-id";
  }
  description
    "This type is used by data models that need to reference
    a trasponder.";
}

/*
  Groupings of attributes
*/
grouping flexi-grid-network-type {
  container flexi-grid-network {
    presence "indicates a flexi-grid optical network";
    description "flexi-grid optical network";
  }
  description "If present, it indicates a flexi-grid
  optical TED network";
}
```

```
grouping flexi-grid-node-attributes {
  description "Set of attributes of an optical node.";

  list interfaces {
    key "name";
    unique "port-number"; // TODO Puerto y TP ID
    description "List of interfaces contained in the node";
    leaf name {
      type string;
      description "Interface name";
    }
    leaf port-number {
      type uint32;
      description "Number of the port used by the interface";
    }

    leaf input-port {
      type boolean;
      description "Determines if the port is an input port";
    }
    leaf output-port {
      type boolean;
      description
        "Determines if the port is an output port";
    }
    leaf description {
      type string;
      description "Description of the interface";
    }
    leaf type {
      type interface-type;
      description "Determines the type of the interface";
    }
    container numbered-interface {
      when "../fg-ted:type =
        'numbered-interface'" {
        description
          "If the interface is a numbered interface";
      }
      description "Container that defines an numbered
        interface with an ip-address";
      leaf n-i-ip-address {
        type inet:ip-address;
        description "IP address of the numbered interface";
      }
    }
  }
}
```

```

    container unnumbered-interface {
      when "../fg-ted:type =
        'unnumbered-interface'" {
        description
          "If the interface is an unnumbered interface";
      }
      description "Container that defines an unnumbered
        interface with an ip-address and a label";
      leaf u-i-ip-address{
        type inet:ip-address;
        description "IP address of the interface";
      }
      leaf label {
        type uint32;
        description "Number as label for the interface";
      }
    }
  }
}

grouping flexi-grid-link-attributes {
  description "Set of attributes of an optical link";
  leaf-list available-label-flexi-grid {
    type bits {
      bit is-available{
        description "Set to 1 when it is available";
      }
    }
    description
      "Array of bits that determines whether a spectral
        slot is available or not.";
  }

  leaf N-max {
    type int32;
    description "Maximum number of channels available.";
  }

  leaf base-frequency {
    type decimal64 {
      fraction-digits 5;
    }
    units THz;
    default 193.1;
    description "Default central frequency";
    reference "rfc7698";
  }
}

```

```
    leaf nominal-central-frequency-granularity {
      type decimal64 {
        fraction-digits 5;
      }
      units GHz;
      default 6.25;
      description
        "It is the spacing between allowed nominal central
        frequencies and it is set to 6.25 GHz";
      reference "rfc7698";
    }

    leaf slot-width-granularity {
      type decimal64 {
        fraction-digits 5;
      }
      units GHz;
      default 12.5;
      description "Minimum space between slot widths";
      reference "rfc7698";
    }
  }

  grouping flexi-grid-transponder-attributes {
    description "Configuration of an optical transponder";
    //TODO Validate attributes
    leaf-list available-operational-mode {
      type operational-mode;
      description "List of all vendor-specific supported
      mode identifiers";
    }

    leaf operational-mode {
      type operational-mode;
      description "Vendor-specific mode identifier";
    }
  }
}
```

```

    grouping flexi-grid-connectivity-matrix-attributes {
      description "Connectivity matrix between the input and
        output ports";
      list connections {
        key "input-port-id";
        leaf input-port-id {
          type flexi-grid-node-port-ref;
          description "Identifier of the input port";
        }
        leaf output-port-id {
          type flexi-grid-node-port-ref;
          description "Identifier of the output port";
        }
      }
      description "List of connections between input and
        output ports";
    }
  }
}

/*
  Augments
*/
augment "/nd:networks/nd:network/nd:network-types" {
  uses flexi-grid-network-type;
  description "Augment network-types including flexi-grid
    topology";
}
augment "/nd-s:networks/nd-s:network/nd-s:network-types" {
  uses flexi-grid-network-type;
  description "Augment network-types including flexi-grid
    topology";
}
augment "/nd:networks/nd:network/lnk:link/tet:te" +
  "/tet:te-link-attributes" {
  when "/nd:networks/nd:network/nd:network-types/
fg-ted:flexi-grid-network" {
    description "Augment only for Flexigrid network.";
  }
  description "Augment link configuration";
  uses flexi-grid-link-attributes;
}

augment "/nd-s:networks/nd-s:network/lnk-s:link/tet-s:te" +
  "/tet-s:te-link-attributes" {
  when "/nd-s:networks/nd-s:network/nd-s:network-types/
fg-ted:flexi-grid-network" {
    description "Augment only for Flexigrid network.";
  }

  description "Augment link state";
  uses flexi-grid-link-attributes;
}

```

```

Internet-Draft    A YANG data model for Flexi-Grid    July 2017
augment "/nd:networks/nd:network/nd:node/tet:te" +
  "/tet:te-node-attributes" {
    when "/nd:networks/nd:network/nd:network-types/
fg-ted:flexi-grid-network" {
      description "Augment only for Flexigrid network.";
    }
    uses flexi-grid-node-attributes;
    description "Augment node config with flexi-grid attributes";
  }

augment "/nd-s:networks/nd-s:network/nd-s:node/tet-s:te" +
  "/tet-s:te-node-attributes" {
    when "/nd-s:networks/nd-s:network/nd-s:network-types/
fg-ted:flexi-grid-network" {
      description "Augment only for Flexigrid network.";
    }

    uses flexi-grid-node-attributes;
    description "Augment node state with flexi-grid attributes";
  }
augment "/nd:networks/nd:network/nd:node/tet:te"+
  "/tet:te-node-attributes/tet:connectivity-matrices/" +
  "tet:connectivity-matrix" {
    when "/nd:networks/nd:network/nd:network-types/
fg-ted:flexi-grid-network" {
      description "Augment only for Flexigrid network.";
    }

    uses flexi-grid-connectivity-matrix-attributes;
    description "Augment node connectivity-matrix for node config";
  }

augment "/nd-s:networks/nd-s:network/nd-s:node/tet-s:te"+
  "/tet-s:te-node-attributes/tet-s:connectivity-matrices/" +
  "tet-s:connectivity-matrix" {
    when "/nd-s:networks/nd-s:network/nd-s:network-types/
fg-ted:flexi-grid-network" {
      description "Augment only for Flexigrid network.";
    }

    uses flexi-grid-connectivity-matrix-attributes;
    description "Augment node connectivity-matrix for node config";
  }

```

```

Internet-Draft    A YANG data model for Flexi-Grid    July 2017
augment "/nd:networks/nd:network/nd:node/tet:te"+
  "/tet:tunnel-termination-point" {
    when "/nd:networks/nd:network/nd:network-types/
fg-ted:flexi-grid-network"{
      description "Augment only for Flexigrid network.";
    }
    uses flexi-grid-transponder-attributes;
    description "Augment node state with transponder attributes";
  }

augment "/nd-s:networks/nd-s:network/nd-s:node/tet-s:te"+
  "/tet-s:tunnel-termination-point" {
    when "/nd-s:networks/nd-s:network/nd-s:network-types/
fg-ted:flexi-grid-network"{
      description "Augment only for Flexigrid network.";
    }

    uses flexi-grid-transponder-attributes;
    description "Augment node state with transponder attributes";
  }
}

<CODE ENDS>

```

Copyright (c) 2017 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, are permitted provided that the following conditions are met:

- o Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- o Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- o Neither the name of Internet Society, IETF or IETF Trust, nor the names of specific contributors, may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



The transport protocol used for sending the managed information MUST support authentication and SHOULD support encryption.

The defined data-model by itself does not create any security implications.

## 8. IANA Considerations

The namespace used in the defined models is currently based on the METRO-HAUL project URI. Future versions of this document could register a URI in the IETF XML registry [RFC3688], as well as in the YANG Module Names registry [RFC6020].

## 9. References

### 9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008, <<http://www.rfc-editor.org/info/rfc5234>>.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.
- [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

- [RFC7698] Gonzalez de Dios, O., Casellas, R., Eds. "Framework and Requirements for GMPLS-Based Control of Flexi-Grid Dense Wavelength Division Multiplexing (DWDM) Networks", RFC7698, November 2015.
- [I-D.draft-ietf-i2rs-yang-network-topo] Clemm, A., Medved, J., Varga, R., Bahadur, N., Ananthakrishnan, H., Liu, X., "A Data Model for Network Topologies", Internet Draft draft-ietf-i2rs-yang-network-topo-14.txt, 2017.
- [I-D.draft-ietf-teas-yang-te-topo] Liu, X., Bryskin, I., Pavan Beeram, V., Saad, T., Shah, H., Gonzalez De Dios, O., "YANG Data Model for TE Topologies", Internet Draft draft-ietf-teas-yang-te-topo-10.txt, 2017
- [I-D.draft-dharini-ccamp-dwdm-if-yang] Galimberti, G., Kunze, R., Lam, K., Hiremagalur, D., Grammel, G., Fang, L., Ratterree, G., Eds., "A YANG model to manage the optical interface parameters for an external transponder in a WDM network", Internet Draft, draft-dharini-ccamp-dwdm-if-param-yang-02.txt, 2016.
- [I-D.draft-ietf-ccamp-wson-yang] Lee, Y. Dhody, D., Zhang, X., Guo, A., Lopez, V., King, D., Yoon, B., "A Yang Data Model for WSON Optical Networks", Internet Draft, draft-ietf-ccamp-wson-yang-06.txt, 2017.
- [I-D.draft-vergara-ccamp-flexigrid-media-channel-yang] Lopez de Vergara, J., Perdices, D., Lopez, V., Gonzalez de Dios, O., King, D., Lee, Y., Galimberti, G., "YANG data model for Flexi-Grid media-channels", Internet Draft, draft-vergara-ccamp-flexigrid-media-channel-yang-00, 2017.

## 10. Contributors

The model presented in this paper was contributed to by more people than can be listed on the author list. Additional contributors include:

- o Zafar Ali, Cisco Systems
- o Daniel Michaud Vallinoto, Universidad Autonoma de Madrid

The work presented in this Internet-Draft has been partially funded by the European Commission under the project H2020 METRO-HAUL (Metro High bandwidth, 5G Application-aware optical network, with edge storage, compUte and low Latency), Grant Agreement number: 761727, and by the Spanish Ministry of Economy and Competitiveness under the project TRAFICA, MINECO/FEDER TEC2015-69417-C2-1-R.

#### Authors' Addresses

Jorge E. Lopez de Vergara  
Universidad Autonoma de Madrid  
Escuela Politecnica Superior  
C/Francisco Tomas y Valiente, 11  
E-28049 Madrid, Spain

Email: [jorge.lopez\\_vergara@uam.es](mailto:jorge.lopez_vergara@uam.es)

Daniel Perdices Burrero  
Naudit High Performance Computing and Networking, S.L.  
C/Faraday, 7  
E-28049 Madrid, Spain

Email: [daniel.perdices@naudit.es](mailto:daniel.perdices@naudit.es)

Victor Lopez  
Telefonica I+D/GCTO  
Distrito Telefonica  
E-28050 Madrid, Spain

Email: [victor.lopezalvarez@telefonica.com](mailto:victor.lopezalvarez@telefonica.com)

Oscar Gonzalez de Dios  
Telefonica I+D/GCTO  
Distrito Telefonica  
E-28050 Madrid, Spain

Email: [oscar.gonzalezdedios@telefonica.com](mailto:oscar.gonzalezdedios@telefonica.com)

Daniel King  
Lancaster University

Email: [d.king@lancaster.ac.uk](mailto:d.king@lancaster.ac.uk)

Young Lee  
Huawei Technologies

Email: [leeyoung@huawei.com](mailto:leeyoung@huawei.com)

Gabriele Galimberti  
Cisco Photonics Srl

Email: [ggalimbe@cisco.com](mailto:ggalimbe@cisco.com)

CCAMP Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2018

H. Zheng  
A. Guo  
I. Busi  
Huawei Technologies  
Y. Xu  
CAICT  
Y. Zhao  
China Mobile  
X. Liu  
Jabil  
G. Fioccola  
Telecom Italia  
October 30, 2017

A YANG Data Model for Client-layer Topology  
draft-zheng-ccamp-client-topo-yang-01

Abstract

A transport network is a server-layer network to provide connectivity services to its client. In this draft the topology of client is described.

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 May 3, 2018.

Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology and Notations . . . . .	3
3. YANG Model for Topology of Client Layer . . . . .	3
3.1. YANG Tree for Ethernet Topology . . . . .	3
3.2. YANG Tree for topology Model of other Client Layer . . . . .	4
4. YANG Code for Topology Client Layer . . . . .	4
4.1. The ETH Topology YANG Code . . . . .	4
4.2. Other OTN client signal YANG Code . . . . .	10
5. Considerations and Open Issue . . . . .	10
6. IANA Considerations . . . . .	10
7. Manageability Considerations . . . . .	10
8. Security Considerations . . . . .	10
9. Acknowledgements . . . . .	11
10. Contributors . . . . .	11
11. References . . . . .	11
11.1. Normative References . . . . .	11
11.2. Informative References . . . . .	12
Authors' Addresses . . . . .	13

## 1. Introduction

A transport network is a server-layer network designed to provide connectivity services for a client-layer network to carry the client traffic transparently across the server-layer network resources. The topology model in Traffic-Engineered network has been defined in both generic way and technology-specific way. The generic model, which is the base TE YANG model, can be found at [I-D.ietf-teas-yang-te-topo]. Technology-specific models, such as OTN/WSN topology model, have also been defined in [I-D.ietf-ccamp-otn-topo-yang] and [I-D.ietf-ccamp-wson-yang] respectively. Corresponding topology on client-layer is also required, to have a complete topology view from the perspective of network controllers.

This document defines a data model of all client-layer Topology, using YANG language defined in [RFC7950]. The model is augmenting the generic TE topology model, and can be used by applications exposing to a network controller via a REST interface. Furthermore,

it can be used by an application for topology description in client-layer network.

## 2. Terminology and Notations

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in the YANG data tree presented later in this document is defined in [I-D.ietf-netmod-yang-tree-diagrams]. They are provided below for reference.

- o Brackets "[" and "]" enclose list keys.
- o Abbreviations before data node names: "rw" means configuration (read-write) and "ro" state data (read-only).
- o Symbols after data node names: "?" means an optional node, "!" means a presence container, and "\*" denotes a list and leaf-list.
- o Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- o Ellipsis ("...") stands for contents of subtrees that are not shown.

## 3. YANG Model for Topology of Client Layer

### 3.1. YANG Tree for Ethernet Topology

```
module: ietf-eth-te-topology
  augment /nd:networks/nd:network/nd:network-types/tet:te-topology:
    +--rw eth-tran-topology!
  augment /nd:networks/nd:network:
    +--rw name?      string
  augment /nd:networks/nd:network/nd:node:
    +--rw name?      string
    +--rw node-mac-address? yang:mac-address
  augment /nd:networks/nd:network/lnk:link/tet:te/tet:config:
    +--rw max-bandwidth?      uint64
    +--rw available-bandwidth? uint64
    +--rw available-vlan-range? eth-types:vid-range-type
  augment /nd:networks/nd:network/lnk:link/tet:te/tet:state:
    +--ro max-bandwidth?      uint64
    +--ro available-bandwidth? uint64
    +--ro available-vlan-range? eth-types:vid-range-type
  augment /nd:networks/nd:network/nd:node/lnk:termination-point:
```

```

+--rw config
|   +--rw ltp-mac-address?          yang:mac-address
|   +--rw port-vlan-id?             etht-types:vlanid
|   +--rw access-link-bandwidth-profiles
|       +--rw bandwidth-profile-name? string
|       +--rw bandwidth-profile-type? etht-types:bandwidth-profile-type
|       +--rw CIR?                  uint64
|       +--rw CBS?                  uint64
|       +--rw EIR?                  uint64
|       +--rw EBS?                  uint64
|       +--rw color-aware?          boolean
|       +--rw coupling-flag?        boolean
+--ro state
|   +--ro ltp-mac-address?          yang:mac-address
|   +--ro port-vlan-id?             etht-types:vlanid
|   +--ro access-link-bandwidth-profiles
|       +--ro bandwidth-profile-name? string
|       +--ro bandwidth-profile-type? etht-types:bandwidth-profile-type
|       +--ro CIR?                  uint64
|       +--ro CBS?                  uint64
|       +--ro EIR?                  uint64
|       +--ro EBS?                  uint64
|       +--ro color-aware?          boolean
|       +--ro coupling-flag?        boolean
augment /nd:networks/nd:network/nd:node/lnk:termination-point/tet:te/tet:config:
    +--rw client-facing?            empty
    +--rw maximum-frame-size?       uint16
augment /nd:networks/nd:network/nd:node/lnk:termination-point/tet:te/tet:state:
    +--ro client-facing?            empty
    +--ro maximum-frame-size?       uint16

```

### 3.2. YANG Tree for topology Model of other Client Layer

This section will be completed later.

## 4. YANG Code for Topology Client Layer

### 4.1. The ETH Topology YANG Code

<CODE BEGINS> file "ietf-eth-te-topology@2017-09-12.yang"

```
module ietf-eth-te-topology {
```

```
/* TODO: FIXME */
yang-version 1.1;

namespace "urn:ietf:params:xml:ns:yang:ietf-eth-tran-topology";

prefix "ethtetopo";

import ietf-network {
    prefix "nd";
}

import ietf-network-topology {
    prefix "lnk";
}

import ietf-te-topology {
    prefix "tet";
}

import ietf-yang-types {
    prefix "yang";
}

import ietf-eth-tran-types {
    prefix "etht-types";
}

organization
    "Internet Engineering Task Force (IETF) CCAMP WG";
contact
    "
        WG List: <mailto:ccamp@ietf.org>

        ID-draft editor:
        Haomian Zheng (zhenghaomian@huawei.com);
        Italo Busi (italo.busi@huawei.com);
        Aihua Guo (aihuaguo@huawei.com);
        Yunbin Xu (xuyunbin@ritt.cn);
        Yang Zhao (zhaoyangyjy@chinamobile.com);
        Xufeng Liu (Xufeng_Liu@jabil.com);
        Giuseppe Fioccola (giuseppe.fioccola@telecomitalia.it);
        ";

description
    "This module defines a YANG data model for describing
    layer-2 Ethernet transport topologies.";

revision 2017-09-12 {
```



```
        description
            "Updated version:

                Moved eth-ltp-svc-attributes grouping to ietf-et
h-tran-svc module.

            ";
    }

    revision 2017-08-10 {
        description
            "Initial version";
    }

    /*
    Groupings
    */

    grouping eth-tran-topology-type {
        description
            "Identifies the Ethernet Transport topology type";

        container eth-tran-topology {
            presence "indicates a topology type of Ethernet
                Transport Network.";
            description "Eth transport topology type";
        }
    }

    grouping eth-topology-attributes {
        description "Ethernet transport topology attributes";

        leaf name {
            type string;
            description "the topology name";
        }
    }

    grouping eth-node-attributes {
        description "Ethernet transport node attributes";

        leaf name {
            type string;
            description "a name for this node.";
        }
        leaf node-mac-address {
            type yang:mac-address;
            description "the MAC address of the node.";
        }
    }
}
```

```

    grouping eth-link-te-attributes {
        description "Ethernet TE link attributes";

        leaf max-bandwidth {
            type uint64{
                range "0..100000000000";
            }
            units "Kbps";
            description "Maximum bandwidth value expressed in kilobit
s per second";
        }

        leaf available-bandwidth {
            type uint64{
                range "0..100000000000";
            }
            units "Kbps";
            description "Available bandwidth value expressed
in kilobits per second";
        }

        leaf available-vlan-range {
            type eth-types:vid-range-type;
            description
                "The range of the VLAN values that are available
.";
        }
    }

    grouping eth-ltp-attributes {
        description "Ethernet transport link termination point attribute
s";

        leaf ltp-mac-address {
            type yang:mac-address;
            description "the MAC address of the LTP.";
        }
        leaf port-vlan-id {
            type eth-types:vlanid;
            description "the port VLAN ID of the LTP.";
        }
    }

    grouping eth-ltp-te-attributes {
        description "Ethernet transport link termination point TE attrib
utes";

        /*
           Do we need the client-facing attribute?
           Cannot we use the svc container presence instead?
        */
        leaf client-facing {
            type empty;

```

```

        description
            "if present, it means this tp is a client-facing
ltp.";
    }
    leaf maximum-frame-size {
        type uint16 {
            range "64 .. 65535";
        }
        description
            "Maximum frame size";
    }
}

/*
Data nodes
*/

augment "/nd:networks/nd:network/nd:network-types/tet:te-topology" {
    description "Augment network types to include ETH transport newt
ork";

    uses eth-tran-topology-type;
}

augment "/nd:networks/nd:network" {
    when "nd:network-types/tet:te-topology/eth-tran-topology" {
        description "Augment only for ETH transport network";
    }
    description "Augment ETH transport network topology attributes";

    uses eth-topology-attributes;
}

augment "/nd:networks/nd:network/nd:node" {
    when "../nd:network-types/tet:te-topology/eth-tran-topology" {
        description "Augment only for ETH transport network";
    }
    description "Augment ETH transport node attributes";

    uses eth-node-attributes;
}

augment "/nd:networks/nd:network/lnk:link/tet:te/tet:config" {
    when "../../../nd:network-types/tet:te-topology/eth-tran-topolog
y" {
        description "Augment only for ETH transport network.";
    }
    description "Augment ETH transport link config attributes";

    uses eth-link-te-attributes;
}

```

```

    augment "/nd:networks/nd:network/lnk:link/tet:te/tet:state" {
y" {
        when "../..../nd:network-types/tet:te-topology/eth-tran-topolog

            description "Augment only for ETH transport network.";
        }
        description "Augment ETH transport link state attributes";

        uses eth-link-te-attributes;
    }

    augment "/nd:networks/nd:network/nd:node/lnk:termination-point" {
{
        when "../..../nd:network-types/tet:te-topology/eth-tran-topology"

            description "Augment only for ETH transport network";
        }
        description "Augment ETH LTP attributes";

        container config {
            description
                "ETH LTP configuration data.";
            uses eth-ltp-attributes;
            container access-link-bandwidth-profiles {
                uses eth-types:eth-bandwidth-profiles;
                description
                    "Bandwidth profiles for access link.";
            }
        }
        container state {
            config false;
            description
                "ETH LTP operational state data.";
            uses eth-ltp-attributes;
            container access-link-bandwidth-profiles {
                uses eth-types:eth-bandwidth-profiles;
                description
                    "Bandwidth profiles for access link.";
            }
        }
    }

    augment "/nd:networks/nd:network/nd:node/"
    + "lnk:termination-point/tet:te/tet:config" {
{
        when "../..../nd:network-types/tet:te-topology/eth-tran-topology"

            description "Augment only for ETH transport network";
        }
        description "Augment ETH transport LTP TE config attributes";

        uses eth-ltp-te-attributes;
    }

```

```
    augment "/nd:networks/nd:network/nd:node/"
      + "lnk:termination-point/tet:te/tet:state" {
        when "../nd:network-types/tet:te-topology/eth-tran-topology"
      {
        description "Augment only for ETH transport network";
      }
      description "Augment ETH transport LTP TE state attributes";
      uses eth-ltp-te-attributes;
    }
  }
```

<CODE ENDS>

#### 4.2. Other OTN client signal YANG Code

TBD.

#### 5. Considerations and Open Issue

Editor Notes: This section is used to note temporary discussion/conclusion that to be fixed in the future version, and will be removed before publication.

#### 6. IANA Considerations

TBD.

#### 7. Manageability Considerations

TBD.

#### 8. Security Considerations

The data following the model defined in this document is exchanged via, for example, the interface between an orchestrator and a transport network controller. The security concerns mentioned in [I-D.ietf-teas-yang-te-topo] for using ietf-te-topology.yang model also applies to this document.

The YANG module defined in this document can be accessed via the RESTCONF protocol defined in [RFC8040], or maybe via the NETCONF protocol [RFC6241].

There are a number of data nodes defined in the YANG module which are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable

in some network environments. Write operations (e.g., POST) to these data nodes without proper protection can have a negative effect on network operations.

Editors note: to list specific subtrees and data nodes and their sensitivity/vulnerability.

## 9. Acknowledgements

We would like to thank Igor Bryskin and Daniel King for their comments and discussions.

## 10. Contributors

Yanlei Zheng  
China Unicom  
Email: zhengyl@dimpt.com

Zhe Liu  
Huawei Technologies,  
Email: liuzhel23@huawei.com

Zheyu Fan  
Huawei Technologies,  
Email: fanzheyu2@huawei.com

Sergio Belotti  
Nokia,  
Email: sergio.belotti@nokia.com

Yingxi Yao  
Shanghai Bell,  
yingxi.yao@nokia-sbell.com

## 11. References

### 11.1. Normative References

[I-D.ietf-ccamp-otn-topo-yang]  
zhenghaomian@huawei.com, z., Fan, Z., Sharma, A., Liu, X.,  
Belotti, S., Xu, Y., Wang, L., and O. Dios, "A YANG Data  
Model for Optical Transport Network Topology", draft-ietf-  
ccamp-otn-topo-yang-01 (work in progress), September 2017.

- [I-D.ietf-ccamp-otn-tunnel-model]  
zhenghaomian@huawei.com, z., Fan, Z., Sharma, A., Rao, R., Belotti, S., Lopezalvarez, V., and Y. Li, "OTN Tunnel YANG Model", draft-ietf-ccamp-otn-tunnel-model-00 (work in progress), July 2017.
- [I-D.ietf-teas-yang-te-topo]  
Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Dios, "YANG Data Model for Traffic Engineering (TE) Topologies", draft-ietf-teas-yang-te-topo-13 (work in progress), October 2017.
- [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>>.
- [RFC7139] Zhang, F., Ed., Zhang, G., Belotti, S., Ceccarelli, D., and K. Pithewan, "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks", RFC 7139, DOI 10.17487/RFC7139, March 2014, <<https://www.rfc-editor.org/info/rfc7139>>.
- [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>>.
- [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>>.

## 11.2. Informative References

- [I-D.ietf-ccamp-wson-yang]  
Lee, Y., Dhody, D., Zhang, X., Guo, A., Lopezalvarez, V., King, D., Yoon, B., and R. Vilata, "A Yang Data Model for WSON Optical Networks", draft-ietf-ccamp-wson-yang-08 (work in progress), October 2017.
- [I-D.ietf-netmod-yang-tree-diagrams]  
Bjorklund, M. and L. Berger, "YANG Tree Diagrams", draft-ietf-netmod-yang-tree-diagrams-02 (work in progress), October 2017.

[I-D.zhang-teas-transport-service-model]

Zhang, X. and J. Ryoo, "A Service YANG Model for Connection-oriented Transport Networks", draft-zhang-teas-transport-service-model-01 (work in progress), October 2016.

[RFC7062] Zhang, F., Ed., Li, D., Li, H., Belotti, S., and D. Ceccarelli, "Framework for GMPLS and PCE Control of G.709 Optical Transport Networks", RFC 7062, DOI 10.17487/RFC7062, November 2013, <<https://www.rfc-editor.org/info/rfc7062>>.

#### Authors' Addresses

Haomian Zheng  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base, Bantian, Longgang District  
Shenzhen, Guangdong 518129  
P.R.China

Email: [zhenghaomian@huawei.com](mailto:zhenghaomian@huawei.com)

Aihua Guo  
Huawei Technologies

Email: [aihuaguo@huawei.com](mailto:aihuaguo@huawei.com)

Italo Busi  
Huawei Technologies

Email: [Italo.Busi@huawei.com](mailto:Italo.Busi@huawei.com)

Yunbin Xu  
CAICT

Email: [xuyunbin@ritr.cn](mailto:xuyunbin@ritr.cn)

Yang Zhao  
China Mobile

Email: [zhaoyangyjy@chinamobile.com](mailto:zhaoyangyjy@chinamobile.com)



Xufeng Liu  
Jabil

Email: Xufeng\_Liu@jabil.com

Giuseppe Fioccola  
Telecom Italia

Email: giuseppe.fioccola@telecomitalia.it

CCAMP Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2018

H. Zheng  
A. Guo  
I. Busi  
Huawei Technologies  
Y. Xu  
CAICT  
Y. Zhao  
China Mobile  
X. Liu  
Jabil  
G. Fioccola  
Telecom Italia  
October 30, 2017

A YANG Data Model for Client-layer Tunnel  
draft-zheng-ccamp-client-tunnel-yang-01

Abstract

A transport network is a server-layer network to provide connectivity services to its client. In this draft the tunnel of client is described, with the definition of client tunnel YANG model.

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 May 3, 2018.

Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology and Notations . . . . .	3
3. YANG Model for Client-layer Tunnel . . . . .	3
3.1. YANG Tree for Ethernet Tunnel . . . . .	3
3.2. YANG Tree for Tunnel of other Client Signal Model . . . . .	4
4. YANG Code for Client-layer Tunnel . . . . .	4
4.1. The ETH Tunnel YANG Code . . . . .	4
4.2. Other Client-layer Tunnel YANG Code . . . . .	7
5. Considerations and Open Issue . . . . .	7
6. IANA Considerations . . . . .	7
7. Manageability Considerations . . . . .	7
8. Security Considerations . . . . .	7
9. Acknowledgements . . . . .	8
10. Contributors . . . . .	8
11. References . . . . .	8
11.1. Normative References . . . . .	8
11.2. Informative References . . . . .	9
Authors' Addresses . . . . .	10

## 1. Introduction

A transport network is a server-layer network designed to provide connectivity services for a client-layer network to carry the client traffic transparently across the server-layer network resources. The tunnel model in Traffic-Engineered network has been defined in both generic way and technology-specific way. The generic model, which is the base TE tunnel YANG model, can be found at [I-D.ietf-teas-yang-te]. Technology-specific models, such as OTN/WSO tunnel model, have also been defined in [I-D.ietf-ccamp-otn-tunnel-model] and [I-D.lee-ccamp-wson-tunnel-model] respectively. Corresponding tunnel on client-layer is also required, to have a complete topology view from the perspective of network controllers.

This document defines a data model of all client-layer tunnel, using YANG language defined in [RFC7950]. The model is augmenting the generic TE tunnel model, and can be used by applications exposing to a network controller via a REST interface. Furthermore, it can be

used by an application to describe the client tunnel that constructed above the server-layer network.

## 2. Terminology and Notations

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in the YANG data tree presented later in this document is defined in [I-D.ietf-netmod-yang-tree-diagrams]. They are provided below for reference.

- o Brackets "[" and "]" enclose list keys.
- o Abbreviations before data node names: "rw" means configuration (read-write) and "ro" state data (read-only).
- o Symbols after data node names: "?" means an optional node, "!" means a presence container, and "\*" denotes a list and leaf-list.
- o Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- o Ellipsis ("...") stands for contents of subtrees that are not shown.

## 3. YANG Model for Client-layer Tunnel

### 3.1. YANG Tree for Ethernet Tunnel

```

module: ietf-eth-te-tunnel
  augment /te:te/te:tunnels/te:tunnel/te:config:
    +--rw src-eth-tunnel-endpoint
    |   +--rw vlanid?      etht-types:vlanid
    |   +--rw tag-type?   etht-types:eth-tag-type
    +--rw dst-eth-tunnel-endpoint
    |   +--rw vlanid?      etht-types:vlanid
    |   +--rw tag-type?   etht-types:eth-tag-type
    +--rw bandwidth-profile
    |   +--rw bandwidth-profile-name?  string
    |   +--rw bandwidth-profile-type?  etht-types:bandwidth-profile-type
    |   +--rw CIR?                     uint64
    |   +--rw CBS?                     uint64
    |   +--rw EIR?                     uint64
    |   +--rw EBS?                     uint64
    |   +--rw color-aware?             boolean
    |   +--rw coupling-flag?           boolean
  augment /te:te/te:tunnels/te:tunnel/te:state:
    +--ro src-eth-tunnel-endpoint
    |   +--ro vlanid?      etht-types:vlanid
    |   +--ro tag-type?   etht-types:eth-tag-type
    +--ro dst-eth-tunnel-endpoint
    |   +--ro vlanid?      etht-types:vlanid
    |   +--ro tag-type?   etht-types:eth-tag-type
    +--ro bandwidth-profile
    |   +--ro bandwidth-profile-name?  string
    |   +--ro bandwidth-profile-type?  etht-types:bandwidth-profile-type
    |   +--ro CIR?                     uint64
    |   +--ro CBS?                     uint64
    |   +--ro EIR?                     uint64
    |   +--ro EBS?                     uint64
    |   +--ro color-aware?             boolean
    |   +--ro coupling-flag?           boolean

```

### 3.2. YANG Tree for Tunnel of other Client Signal Model

This section will be completed later.

## 4. YANG Code for Client-layer Tunnel

### 4.1. The ETH Tunnel YANG Code

<CODE BEGINS> file "ietf-eth-te-tunnel@2017-09-04.yang"

```
module ietf-eth-te-tunnel {
  //TODO: FIXME
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-eth-tunnel";
  prefix "eth-tunnel";

  import ietf-te { prefix "te"; }
  import ietf-eth-tran-types { prefix "eth-t-types"; }

  organization
    "IETF CCAMP Working Group";

  contact
    "WG Web: <http://tools.ietf.org/wg/ccamp/>
    WG List: <mailto:ccamp@ietf.org>

    ID-draft editor:
      Haomian Zheng (zhenghaomian@huawei.com);
      Italo Busi (italo.busi@huawei.com);
      Aihua Guo (aihuaguo@huawei.com);
      Yunbin Xu (xuyunbin@ritt.cn);
      Yang Zhao (zhaoyangyjy@chinamobile.com);
      Xufeng Liu (Xufeng_Liu@jabil.com);
      Giuseppe Fioccola (giuseppe.fioccola@telecomitalia.it);

    ";

  description
    "This module defines a model for ETH transport tunnel";

  revision "2017-09-04" {
    description
      "Revision 0.1";
    reference "TBD";
  }

  grouping eth-tunnel-endpoint {
    description "Parameters for ETH tunnel.";

    leaf vlanid {
      type eth-t-types:vlanid;
      description
        "VLAN tag id.";
    }

    leaf tag-type {
      type eth-t-types:eth-tag-type;
      description "VLAN tag type.";
    }
  }
}
```

```
    }  
  }  
  
  augment "/te:te/te:tunnels/te:tunnel/te:config" {  
    description  
      "Augment with additional parameters required for ETH  
      service.";  
  
    container src-eth-tunnel-endpoint {  
      description  
        "Source ETH tunnel endpoint.";  
  
      uses eth-tunnel-endpoint;  
    }  
  
    container dst-eth-tunnel-endpoint {  
      description  
        "Destination ETH tunnel endpoint.";  
  
      uses eth-tunnel-endpoint;  
    }  
  
    container bandwidth-profile {  
      description  
        "ETH tunnel bandwidth profile specification.";  
  
      uses etht-types:etht-bandwidth-profiles;  
    }  
  }  
  
  augment "/te:te/te:tunnels/te:tunnel/te:state" {  
    description  
      "Augment with additional parameters required for ETH  
      service.";  
  
    container src-eth-tunnel-endpoint {  
      description  
        "Source ETH tunnel endpoint.";  
  
      uses eth-tunnel-endpoint;  
    }  
  
    container dst-eth-tunnel-endpoint {  
      description  
        "Destination ETH tunnel endpoint.";  
  
      uses eth-tunnel-endpoint;  
    }  
  }
```

```
        container bandwidth-profile {  
            description  
                "ETH tunnel bandwidth profile specification.";  
            uses etht-types:etht-bandwidth-profiles;  
        }  
    }  
}
```

<CODE ENDS>

#### 4.2. Other Client-layer Tunnel YANG Code

TBD.

#### 5. Considerations and Open Issue

Editor Notes: This section is used to note temporary discussion/conclusion that to be fixed in the future version, and will be removed before publication. This is a part of L2 work, need to discuss how to go with other L2 network models. The expectation is to include all potential L2 TE part in this work.

#### 6. IANA Considerations

TBD.

#### 7. Manageability Considerations

TBD.

#### 8. Security Considerations

The data following the model defined in this document is exchanged via, for example, the interface between an orchestrator and a transport network controller. The security concerns mentioned in [I-D.ietf-teas-yang-te] also applies to this document.

The YANG module defined in this document can be accessed via the RESTCONF protocol defined in [RFC8040], or maybe via the NETCONF protocol [RFC6241].



## 9. Acknowledgements

We would like to thank Igor Bryskin and Daniel King for their comments and discussions.

## 10. Contributors

Yanlei Zheng  
China Unicom  
Email: zhengyl@dimpt.com

Zhe Liu  
Huawei Technologies,  
Email: liuzhel23@huawei.com

Zheyu Fan  
Huawei Technologies,  
Email: fanzheyu2@huawei.com

Sergio Belotti  
Nokia,  
Email: sergio.belotti@nokia.com

Yingxi Yao  
Shanghai Bell,  
yingxi.yao@nokia-sbell.com

## 11. References

### 11.1. Normative References

[I-D.ietf-ccamp-otn-topo-yang]  
zhenghaomian@huawei.com, z., Fan, Z., Sharma, A., Liu, X., Belotti, S., Xu, Y., Wang, L., and O. Dios, "A YANG Data Model for Optical Transport Network Topology", draft-ietf-ccamp-otn-topo-yang-01 (work in progress), September 2017.

[I-D.ietf-ccamp-otn-tunnel-model]  
zhenghaomian@huawei.com, z., Fan, Z., Sharma, A., Rao, R., Belotti, S., Lopezalvarez, V., and Y. Li, "OTN Tunnel YANG Model", draft-ietf-ccamp-otn-tunnel-model-00 (work in progress), July 2017.

[I-D.ietf-teas-yang-te]  
Saad, T., Gandhi, R., Liu, X., Beeram, V., Shah, H., and I. Bryskin, "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te-09 (work in progress), October 2017.

- [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>>.
- [RFC7139] Zhang, F., Ed., Zhang, G., Belotti, S., Ceccarelli, D., and K. Pithewan, "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks", RFC 7139, DOI 10.17487/RFC7139, March 2014, <<https://www.rfc-editor.org/info/rfc7139>>.
- [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>>.
- [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>>.

## 11.2. Informative References

- [I-D.ietf-netmod-yang-tree-diagrams]  
Bjorklund, M. and L. Berger, "YANG Tree Diagrams", draft-ietf-netmod-yang-tree-diagrams-02 (work in progress), October 2017.
- [I-D.lee-ccamp-wson-tunnel-model]  
Lee, Y., Dhody, D., Lopezalvarez, V., King, D., Yoon, B., and R. Vilata, "A Yang Data Model for WSON Tunnel", draft-lee-ccamp-wson-tunnel-model-02 (work in progress), October 2017.
- [I-D.zhang-teas-transport-service-model]  
Zhang, X. and J. Ryoo, "A Service YANG Model for Connection-oriented Transport Networks", draft-zhang-teas-transport-service-model-01 (work in progress), October 2016.
- [RFC7062] Zhang, F., Ed., Li, D., Li, H., Belotti, S., and D. Ceccarelli, "Framework for GMPLS and PCE Control of G.709 Optical Transport Networks", RFC 7062, DOI 10.17487/RFC7062, November 2013, <<https://www.rfc-editor.org/info/rfc7062>>.

Authors' Addresses

Haomian Zheng  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base, Bantian, Longgang District  
Shenzhen, Guangdong 518129  
P.R.China

Email: zhenghaomian@huawei.com

Aihua Guo  
Huawei Technologies

Email: aihuaguo@huawei.com

Italo Busi  
Huawei Technologies

Email: Italo.Busi@huawei.com

Yunbin Xu  
CAICT

Email: xuyunbin@rict.cn

Yang Zhao  
China Mobile

Email: zhaoyangyjy@chinamobile.com

Xufeng Liu  
Jabil

Email: Xufeng\_Liu@jabil.com

Giuseppe Fioccola  
Telecom Italia

Email: giuseppe.fioccola@telecomitalia.it

CCAMP Working Group  
Internet Draft  
Category: Informational

Haomian Zheng  
Xianlong Luo  
Zheyu Fan  
Yi Lin  
Huawei Technologies  
October 30, 2017

Expires: April 30, 2018

## Interworking of GMPLS Control and Centralized Controller System

draft-zheng-ccamp-gmpls-controller-inter-work-00

### Abstract

Generalized Multi-Protocol Label Switching (GMPLS) control allows each network element (NE) to perform resource discovery, routing and signaling in a distributed manner. On the other hand, with the development of software-defined transport networking technology, central controllers are introduced to transport networks to control a set of NEs.

In transport networks, the GMPLS control has many mature mechanisms such as RSVP-TE, OSPF-TE, and LMP, so that GMPLS can be applied for the NE-level control in the centralized controller systems.

This document describes how GMPLS control interworks with centralized controller systems (e.g. ACTN) in transport network.

### Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 30, 2018.

#### Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

#### Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

#### Table of Contents

1. Introduction .....	3
2. Overview .....	3
2.1. Overview of GMPLS Control Plane .....	3
2.2. Overview of Centralized Controller System .....	4
2.3. GMPLS Control Interwork with Centralized Controller System .....	4
3. Link Management Protocol .....	5
4. Routing Options .....	6
4.1. OSPF-TE .....	6
4.2. ISIS-TE .....	6
5. Path Computation .....	6
5.1. Constraint-based Path Computing in GMPLS Control .....	6
5.2. Path Computation Element (PCE) .....	7
6. Signaling Options .....	7
6.1. RSVP-TE .....	8
6.2. CR-LDP .....	8
7. Recovery .....	8
8. Network Management .....	8
9. IANA Considerations .....	8

10. References .....	9
10.1. Normative References .....	9
10.2. Informative References .....	11
11. Authors' Addresses .....	11

## 1. Introduction

Generalized Multi-Protocol Label Switching (GMPLS) [RFC3945] extends MPLS to support different classes of interfaces and switching capabilities such as Time-Division Multiplex Capable (TDM), Lambda Switch Capable (LSC), and Fiber-Switch Capable (FSC). Each network element (NE) running a control plane collects network information from other NEs and provisions services through signaling in a distributed manner.

On the other hand, Software-Defined Networking (SDN) technologies have been introduced to control the transport network in a centralized manner. Central controllers, which can locate outside of the network, can collect network information from each node and provision services to corresponding nodes. One of the examples is the Abstraction and Control of Traffic Engineered Networks (ACTN) [I-D.ietf-teas-actn-framework], which defines a hierarchical architecture with PNC, MDSC and CNC as central controllers for different network abstraction levels.

In such centralized controller systems, GMPLS can be applied for the NE-level control. Introducing GMPLS in centralized controller system can reuse the mature mechanisms defined for GMPLS and be practical for legacy transport networks. This document describes how GMPLS control interworks with centralized controller system in transport network.

## 2. Overview

In this section, overviews of GMPLS control plane and centralized controller system are discussed as well as the cooperation between GMPLS control plane and centralized controller system.

### 2.1. Overview of GMPLS Control Plane

GMPLS separates the control plane and the data plane to support time-division, wavelength, and spatial switching, which are significant in transport networks. For the NE level control in GMPLS, each node has its controller to perform service provisioning,

protection, and restoration. At the same time, the controller can negotiate available link resources with controllers in adjacent nodes, and it can also collect node and link resources in the network to construct the network topology and compute routing paths for serving service requests.

Several protocols have been designed for GMPLS control [RFC3945] including link management [RFC4204], signaling [RFC3471], and routing [RFC4202] protocols. The controllers applying these protocols communicate with each other to exchange resource information and establish LSP. In this way, controllers in different nodes in the network have the same network topology and provision services by their local policies.

## 2.2. Overview of Centralized Controller System

With the development of SDN technologies, centralized controller system has been introduced to transport networks such as ACTN. In centralized controller system, a controller is aware of the network topology and is responsible for provisioning incoming service requests. In ACTN, multiple abstraction levels are designed and controllers at different levels implement different functions. This kind of abstraction enables multi-vendor, multi-domain, and multi-technology control.

For example in ACTN, an MDSC coordinates several PNCs controlling different domains. Each PNC reports its topology, which can be abstracted, to the MDSC, so that the MDSC learns the picture of multiple domains. When a multi-domain service arrives at the MDSC, the MDSC first computes an end-to-end routing path. Then the MDSC splits this path to multiple segment according to domain boundaries and allocate each segment to corresponding PNC for detailed path computation and LSP segment setup. After each PNC reporting the establishment of corresponding LSP segment, this multi-domain service is accommodated.

## 2.3. GMPLS Control Interwork with Centralized Controller System

Centralized controller system as ACTN provides the architecture and communication between central controllers of different abstraction levels to coordinate multiple domains. Within each domain, GMPLS control can be applied to each NE. The bottom-level central controller like PNC can act as a NE to collect network information and initiate LSP. Following figure shows an example of GMPLS interworking with ACTN.

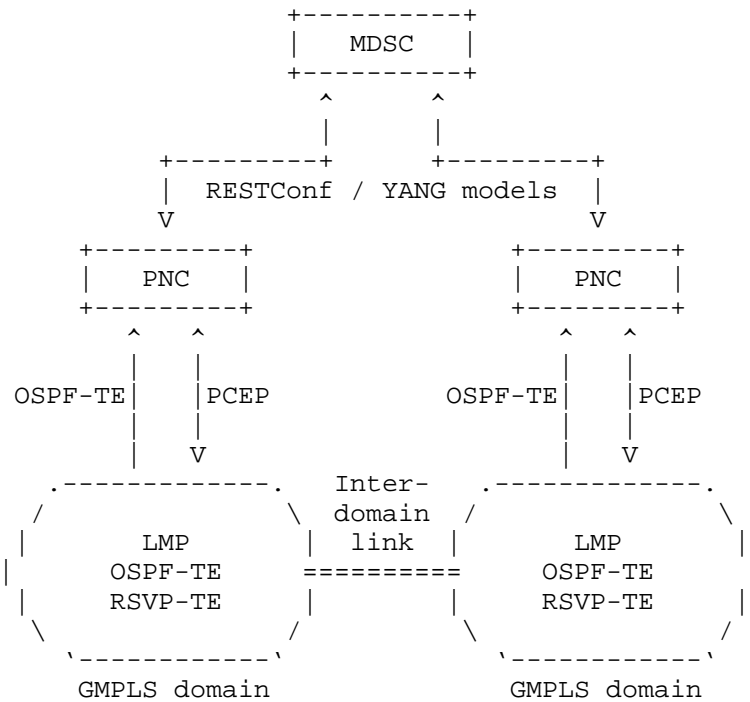


Figure 1: Example of GMPLS interworks with ACTN

In Figure 1, each domain runs GMPLS control. The PNC listens LSAs flooded in the domain and learns the topology. For path computation in the domain with PNC implementing a PCE, NEs use PCEP to ask the PNC for a path and get replies. The MDSC communicates with PNCs using RESTConf or YANG models. As a PNC has learned its domain topology, it can report the topology to the MDSC. When a service arrives, the MDSC computes the path and coordinates PNCs to establish the corresponding LSP segment.

### 3. Link Management Protocol

Link management protocol (LMP) [RFC4204] runs between a pair of nodes and is used to manage TE links. In addition to setup and maintain control channels, LMP can be used to verify the data link connectivity and correlate the link property. In this way, link



resources, which are fundamental resources in the network, are discovered by both ends of the link.

#### 4. Routing Options

In GMPLS control, link state information is flooded within the network as defined in [RFC4202]. Each node in the network can build the network topology according to the flooded link state information. Routing protocols such as OSPF-TE [RFC4203] and ISIS-TE [RFC5307] have been extended to support different interfaces in GMPLS.

In centralized controller system, central controller can be placed at the GMPLS network and passively receive the information flooded in the network. In this way, the central controller can construct and update the network topology.

##### 4.1. OSPF-TE

OSPF-TE is introduced for TE networks in [RFC3630]. OSPF extensions have been defined in [RFC4203] to enable the capability of link state information for GMPLS network. Based on this work, OSPF protocol has been extended to support technology-specific routing. The routing protocol for OTN, WSON and optical flexi-grid network are defined in [RFC7138], [RFC7688] and [I-D.ietf-ccamp-flexible-grid-ospf-ext], respectively.

##### 4.2. ISIS-TE

ISIS-TE is introduced for TE networks in [RFC5305] and is extended to support GMPLS routing functions [RFC5307], and has been updated to [RFC7074] to support the latest GMPLS switching capability and Types fields.

#### 5. Path Computation

Once a controller learn the network topology, it can utilize the available resources to serve service requests by performing path computation. Path computation is one of the key objectives in various types of controllers. In the given architecture, it is possible for different components that have the capability to compute the path.

##### 5.1. Constraint-based Path Computing in GMPLS Control

In GMPLS control, a routing path is computed by the ingress node [RFC3473] and is based on the ingress node TED. Constraint-based

path computation is performed according to the local policy of the ingress node.

## 5.2. Path Computation Element (PCE)

PCE has been introduced in [RFC4655] as a functional component that provides services to compute path in a network. In [RFC5440], the path computation is accomplished by using the Traffic Engineering Database (TED), which maintains the link resources in the network. The emergence of PCE efficiently improve the quality of network planning and offline computation, but there is a risk that the computed path may be infeasible if there is a diversity requirement, because stateless PCE has no knowledge about the former computed paths.

To address this issue, stateful PCE has been proposed in [RFC8231]. Besides the TED, an additional LSP Database (LSP-DB) is introduced to archive each LSP computed by the PCE. In this way, PCE can easily figure out the relationship between the computing path and former computed paths. In this approach, PCE provides computed paths to PCC, and then PCC decides which path is deployed and when to be established.

In PCE Initiation [I-D.ietf-pce-pce-initiated-lsp], PCE is allowed to trigger the PCC to setup, maintenance, and teardown of the PCE-initiated LSP under the stateful PCE model. This would allow a dynamic network that is centrally controlled and deployed.

In centralized controller system, the PCE can be implement in a central controller, and the central controller performs path computation according to its local policies. On the other hand, the PCE can also be placed outside of the central controller. In this case, the central controller acts as a PCC to request path computation to the PCE through PCEP.

## 6. Signaling Options

Signaling mechanism is used to setup LSPs in GMPLS control. Messages are sent hop by hop between the ingress node and the egress node of the LSP to allocate labels. Once the labels are allocated along the path, the LSP setup is accomplished. Signaling protocols such as RSVP-TE [RFC3473] and CR-LDP [RFC3472] have been extended to support different interfaces in GMPLS.

In centralized controller system, the central controller can manage LSPs by using PCE-initiation [I-D.ietf-pce-pce-initiated-lsp] to

notify the corresponding ingress node. The ingress node will maintain the LSP through GMPLS signaling.

#### 6.1. RSVP-TE

RSVP-TE is introduced in [RFC3209] and extended to support GMPLS signaling in [RFC3473]. Several label formats are defined for a generalized label request, a generalized label, suggested label and label sets. Based on [RFC3473], RSVP-TE has been extended to support technology-specific signaling. The RSVP-TE extensions for OTN, WSON, optical flexi-grid network are defined in [RFC7139], [RFC7689], and [RFC7792], respectively.

#### 6.2. CR-LDP

In order to support the label formats and signaling mechanism defined in [RFC3471], CR-LDP is extended in [RFC3472]. Several label formats are defined and bidirectional LSPs are supported.

#### 7. Recovery

The GMPLS recovery functions are described in [RFC4426]. Two models, span protection and end-to-end protection and restoration, are discussed with different protection schemes and message exchange requirements. Related RSVP-TE extensions to support end-to-end recovery is described in [RFC4872]. The extensions in [RFC4872] include protection, restoration, preemption, and rerouting mechanisms for an end-to-end LSP.

Besides end-to-end recovery, a GMPLS segment recovery mechanism is defined in [RFC4873]. By introducing secondary record route objects, LSP segment can be switched to another path like fast rereoute [RFC4090].

#### 8. Network Management

TBD.

#### 9. Security Considerations

TBD.

#### 10. IANA Considerations

This document requires no IANA actions.

## 11. References

### 11.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.
- [RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.
- [RFC3471] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, January 2003.
- [RFC3472] Ashwood-Smith, P., Ed. and L. Berger, Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions", RFC 3472, January 2003.
- [RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.
- [RFC3630] Katz, D., Kompella, K., and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, September 2003.
- [RFC3945] Mannie, E., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, October 2004.
- [RFC4090] Pan, P., Ed., Swallow, G., Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, May 2005.
- [RFC4202] Kompella, K., Ed. and Y. Rekhter, Ed., "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4202, October 2005.
- [RFC4203] Kompella, K., Ed. and Y. Rekhter, Ed., "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, October 2005.
- [RFC4204] Lang, J., Ed., "Link Management Protocol (LMP)", RFC 4204, October 2005.

- [RFC4426] Lang, J., Ed., Rajagopalan, B., Ed., and D. Papadimitriou, Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Recovery Functional Specification", RFC 4426, March 2006.
- [RFC4655] Farrel, A., Vasseur, J., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, August 2006.
- [RFC4872] Lang, J., Ed., Rekhter, Y., Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, May 2007.
- [RFC4873] Berger, L., Bryskin, I., Papadimitriou, D., and A. Farrel, "GMPLS Segment Recovery", RFC 4873, May 2007.
- [RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, October 2008.
- [RFC5307] Kompella, K., Ed. and Y. Rekhter, Ed., "IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 5307, October 2008.
- [RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, March 2009.
- [RFC7074] Berger, L. and J. Meuric, "Revised Definition of the GMPLS Switching Capability and Type Fields", RFC 7074, November 2013.
- [RFC7138] Ceccarelli, D., Ed., Zhang, F., Belotti, S., Rao, R., and J. Drake, "Traffic Engineering Extensions to OSPF for GMPLS Control of Evolving G.709 Optical Transport Networks", RFC 7138, March 2014.
- [RFC7139] Zhang, F., Ed., Zhang, G., Belotti, S., Ceccarelli, D., and K. Pithewan, "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks", RFC 7139, March 2014.
- [RFC7688] Lee, Y., Ed. and G. Bernstein, Ed., "GMPLS OSPF Enhancement for Signal and Network Element Compatibility for Wavelength Switched Optical Networks", RFC 7688, November 2015.

- [RFC7689] Bernstein, G., Ed., Xu, S., Lee, Y., Ed., Martinelli, G., and H. Harai, "Signaling Extensions for Wavelength Switched Optical Networks", RFC 7689, November 2015.
- [RFC7792] Zhang, F., Zhang, X., Farrel, A., Gonzalez de Dios, O., and D. Ceccarelli, "RSVP-TE Signaling Extensions in Support of Flexi-Grid Dense Wavelength Division Multiplexing (DWDM) Networks", RFC 7792, March 2016.
- [RFC8231] Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE", RFC 8231, September 2017.
- [I-D.ietf-ccamp-flexible-grid-ospf-ext] Zhang, X., Zheng, H., Casellas, R., Dios, O., and D. Ceccarelli, "GMPLS OSPF-TE Extensions in support of Flexi-grid DWDM networks", draft-ietf-ccamp-flexible-grid-ospf-ext-09 (work in progress), February 2017.
- [I-D.ietf-pce-pce-initiated-lsp] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model", draft-ietf-pce-pce-initiated-lsp-11 (work in progress), October 2017.
- [I-D.ietf-teas-actn-framework] Ceccarelli, D. and Y. Lee, "Framework for Abstraction and Control of Traffic Engineered Networks", draft-ietf-teas-actn-framework-11 (work in progress), October 2017.

## 11.2. Informative References

## 12. Authors' Addresses

Haomian Zheng  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base,  
Bantian, Longgang District,  
Shenzhen 518129 P.R.China  
Email: zhenghaomian@huawei.com

Xianlong Luo  
Huawei Technologies

F3 R&D Center, Huawei Industrial Base,  
Bantian, Longgang District,  
Shenzhen 518129 P.R.China  
Email: luoxianlong@huawei.com

Zheyu Fan  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base,  
Bantian, Longgang District,  
Shenzhen 518129 P.R.China  
Email: fanzheyu2@huawei.com

Yi Lin  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base,  
Bantian, Longgang District,  
Shenzhen 518129 P.R.China  
Email: yi.lin@huawei.com





CCAMP Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2018

H. Zheng  
A. Guo  
I. Busi  
Huawei Technologies  
Y. Xu  
CAICT  
Y. Zhao  
China Mobile  
X. Liu  
Jabil  
G. Fioccola  
Telecom Italia  
October 30, 2017

A YANG Data Model for Optical Transport Network Client Signals  
draft-zheng-ccamp-otn-client-signal-yang-01

Abstract

A transport network is a server-layer network to provide connectivity services to its client. The topology and tunnel information in the transport layer has already been defined by Traffic-engineered models and OTN models, however, the access to the network has not been described. These information is useful to both client and provider.

This draft describe how the client signals are carried over OTN and defined corresponding YANG data model which is required during configuration procedure. More specifically, several client signal (of OTN) models including ETH, STM-n, FC and so on, are defined in this draft.

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 May 3, 2018.

## Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology and Notations . . . . .	3
3. OTN Client Signal Overview . . . . .	4
4. YANG Model for OTN Client Signal . . . . .	4
4.1. YANG Tree for Ethernet Service . . . . .	4
4.2. YANG Tree for other OTN Client Signal Model . . . . .	8
5. YANG Code for OTN Client Signal . . . . .	8
5.1. The ETH Service YANG Code . . . . .	8
5.2. YANG Code for ETH transport type . . . . .	18
5.3. Other OTN client signal YANG Code . . . . .	24
6. Considerations and Open Issue . . . . .	24
7. IANA Considerations . . . . .	24
8. Manageability Considerations . . . . .	24
9. Security Considerations . . . . .	24
10. Acknowledgements . . . . .	25
11. Contributors . . . . .	25
12. References . . . . .	25
12.1. Normative References . . . . .	25
12.2. Informative References . . . . .	26
Authors' Addresses . . . . .	27

## 1. Introduction

A transport network is a server-layer network designed to provide connectivity services for a client-layer network to carry the client traffic transparently across the server-layer network resources. Currently there has been topology and tunnel model defined for transport network, such as [I-D.ietf-ccamp-otn-topo-yang] and [I-D.ietf-ccamp-otn-tunnel-model], which has described the network model between PEs. However, there is a missing piece between the PE and CE, which is expected to be solved in this document.

This document defines a data model of all OTN network client signals, using YANG language defined in [RFC7950]. The model can be used by applications exposing to a transport controller via a REST interface. Furthermore, it can be used by an application for the following purposes (but not limited to):

- o To request/update an end-to-end service by driving a new OTN tunnel to be set up to support this service;
- o To request/update an end-to-end service by using an existing OTN tunnel;
- o To receive notification with regard to the information change of the given service;

The YANG model defined in this document is independent of control plane protocols and captures topology related information pertaining to an Optical Transport Networks (OTN)-electrical layer, as the scope specified by [RFC7062] and [RFC7139]. Furthermore, it is not a stand-alone model, but augmenting from the TE topology YANG model defined in [I-D.ietf-teas-yang-te-topo].

## 2. Terminology and Notations

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in the YANG data tree presented later in this document is defined in [I-D.ietf-netmod-yang-tree-diagrams]. They are provided below for reference.

- o Brackets "[" and "]" enclose list keys.
- o Abbreviations before data node names: "rw" means configuration (read-write) and "ro" state data (read-only).
- o Symbols after data node names: "?" means an optional node, "!" means a presence container, and "\*" denotes a list and leaf-list.
- o Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- o Ellipsis ("...") stands for contents of subtrees that are not shown.

### 3. OTN Client Signal Overview

The OTN is usually a server-layer network designed to provide connectivity services for a client-layer network to carry the client traffic opaquely across the server-layer network resources. A transport network may be constructed from equipments utilizing any of a number of different transport technologies such as the evolving optical transport infrastructure (SONET/SDH and OTN) or packet transport as epitomized by the MPLS Transport Profile (MPLS-TP).

A full list of G-PID was summarized in [RFC7139], which can be divided into a few categories of OTN client signal. The first category of service type is Ethernet related, including GE, WAN/LAN to support EPL/EVPL service. Another category of service type would be client service which includes SDH/SONET, OTN service, SAN storage (FICON, Fiber Channel) and other applications such as video service (HD-SDI, 3G-SDI, etc.).

#### 4. YANG Model for OTN Client Signal

#### 4.1. YANG Tree for Ethernet Service

```
module: ietf-eth-tran-service
  +--rw etht-svc
    +--rw globals
      +--rw etht-svc-bandwidth-profiles* [bandwidth-profile-name]
        +--rw bandwidth-profile-name string
        +--rw bandwidth-profile-type? etht-types:bandwidth-profile-type
        +--rw CIR? uint64
        +--rw CBS? uint64
        +--rw EIR? uint64
        +--rw EBS? uint64
        +--rw color-aware? boolean
        +--rw coupling-flag? boolean
    +--rw etht-svc-instances* [etht-svc-name]
      +--rw etht-svc-name -> ../config/etht-svc-name
      +--rw config
        +--rw etht-svc-name? string
        +--rw access-provider-id? te-types:te-global-id
        +--rw access-client-id? te-types:te-global-id
        +--rw access-topology-id? te-types:te-topology-id
        +--rw admin-status? identityref
        +--rw etht-svc-access-ports* [access-port-id]
          +--rw access-port-id uint16
          +--rw access-node-id? te-types:te-node-id
          +--rw access-ltp-id? te-types:te-tp-id
```

```

+--rw service-classification-type?          identityref
+--rw (service-classification)?
|   +--:(port-classification)
|   +--:(vlan-classification)
|       +--rw outer-tag!
|           +--rw tag-type?          etht-types:eth-tag-classify
|           +--rw (individual-bundling-vlan)?
|               +--:(individual-vlan)
|                   +--rw vlan-value?  etht-types:vlanid
|               +--:(vlan-bundling)
|                   +--rw vlan-range?  etht-types:vid-range-type
|       +--rw second-tag!
|           +--rw tag-type?          etht-types:eth-tag-classify
|           +--rw (individual-bundling-vlan)?
|               +--:(individual-vlan)
|                   +--rw vlan-value?  etht-types:vlanid
|               +--:(vlan-bundling)
|                   +--rw vlan-range?  etht-types:vid-range-type
+--rw (direction)?
|   +--:(symmetrical)
|   |   +--rw ingress-egress-bandwidth-profile-name?  string
|   +--:(asymmetrical)
|       +--rw ingress-bandwidth-profile-name?        string
|       +--rw egress-bandwidth-profile-name?         string
+--rw vlan-operations
|   +--rw (direction)?
|       +--:(symmetrical)
|           +--rw symmetrical-operation
|               +--rw pop-tags?      uint8
|               +--rw push-tags
|                   +--rw outer-tag!
|                       +--rw tag-type?  etht-types:eth-tag-type
|                       +--rw vlan-value? etht-types:vlanid
|               +--rw second-tag!
|                   +--rw tag-type?  etht-types:eth-tag-type
|                   +--rw vlan-value? etht-types:vlanid
|       +--:(asymmetrical)
|           +--rw asymmetrical-operation
|               +--rw ingress
|                   +--rw pop-tags?      uint8
|                   +--rw push-tags
|                       +--rw outer-tag!
|                           +--rw tag-type?  etht-types:eth-tag-type
|                           +--rw vlan-value? etht-types:vlanid
|                   +--rw second-tag!
|                       +--rw tag-type?  etht-types:eth-tag-type
|                       +--rw vlan-value? etht-types:vlanid
|               +--rw egress

```

```

+---rw pop-tags?          uint8
+---rw push-tags
+---rw outer-tag!
+---rw tag-type?          etht-types:eth-tag-type
+---rw vlan-value?        etht-types:vlanid
+---rw second-tag!
+---rw tag-type?          etht-types:eth-tag-type
+---rw vlan-value?        etht-types:vlanid
+---rw etht-svc-tunnels* [tunnel-name]
+---rw tunnel-name        string
+---rw (svc-multiplexing-tag)?
+---:(other)
+---:(none)
+---:(vlan-tag)
+---:(pw)
+---ro state
+---ro etht-svc-name?      string
+---ro access-provider-id? te-types:te-global-id
+---ro access-client-id?  te-types:te-global-id
+---ro access-topology-id? te-types:te-topology-id
+---ro admin-status?      identityref
+---ro etht-svc-access-ports* [access-port-id]
+---ro access-port-id      uint16
+---ro access-node-id?     te-types:te-node-
id
+---ro access-ltp-id?      te-types:te-tp-id
+---ro service-classification-type? identityref
+---ro (service-classification)?
+---:(port-classification)
+---:(vlan-classification)
+---ro outer-tag!
+---ro tag-type?          etht-types:eth-tag-classify
+---ro (individual-bundling-vlan)?
+---:(individual-vlan)
+---ro vlan-value?        etht-types:vlanid
+---:(vlan-bundling)
+---ro vlan-range?        etht-types:vid-range-type
+---ro second-tag!
+---ro tag-type?          etht-types:eth-tag-classify
+---ro (individual-bundling-vlan)?
+---:(individual-vlan)
+---ro vlan-value?        etht-types:vlanid
+---:(vlan-bundling)
+---ro vlan-range?        etht-types:vid-range-type
+---ro (direction)?
+---:(symmetrical)
+---ro ingress-egress-bandwidth-profile-name? string
+---:(asymmetrical)
+---ro ingress-bandwidth-profile-name?      string

```

```

|         +--ro egress-bandwidth-profile-name?          string
+--ro vlan-operations
  +--ro (direction)?
    +--:(symmetrical)
      +--ro symmetrical-operation
        +--ro pop-tags?      uint8
        +--ro push-tags
          +--ro outer-tag!
            +--ro tag-type?    etht-types:eth-tag-type
            +--ro vlan-value?  etht-types:vlanid
          +--ro second-tag!
            +--ro tag-type?    etht-types:eth-tag-type
            +--ro vlan-value?  etht-types:vlanid
    +--:(asymmetrical)
      +--ro asymmetrical-operation
        +--ro ingress
          +--ro pop-tags?      uint8
          +--ro push-tags
            +--ro outer-tag!
              +--ro tag-type?    etht-types:eth-tag-type
              +--ro vlan-value?  etht-types:vlanid
            +--ro second-tag!
              +--ro tag-type?    etht-types:eth-tag-type
              +--ro vlan-value?  etht-types:vlanid
          +--ro egress
            +--ro pop-tags?      uint8
            +--ro push-tags
              +--ro outer-tag!
                +--ro tag-type?    etht-types:eth-tag-type
                +--ro vlan-value?  etht-types:vlanid
              +--ro second-tag!
                +--ro tag-type?    etht-types:eth-tag-type
                +--ro vlan-value?  etht-types:vlanid
+--ro etht-svc-tunnels* [tunnel-name]
  +--ro tunnel-name      string
  +--ro (svc-multiplexing-tag)?
    +--:(other)
    +--:(none)
    +--:(vlan-tag)
    +--:(pw)
+--ro operational-state?      identityref
+--ro provisioning-state?     identityref

```

#### 4.2. YANG Tree for other OTN Client Signal Model

This section will be completed later.

#### 5. YANG Code for OTN Client Signal

##### 5.1. The ETH Service YANG Code

```
<CODE BEGINS> file "ietf-eth-tran-service@2017-09-12.yang"

module ietf-eth-tran-service {
  /* TODO: FIXME */
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-eth-tran-svc";

  prefix "ethtsvc";

  /*
  import ietf-inet-types {
    prefix "inet";
  }
  */

  import ietf-te-types {
    prefix "te-types";
  }

  import ietf-eth-tran-types {
    prefix "eth-t-types";
  }

  organization
    "Internet Engineering Task Force (IETF) CCAMP WG";
  contact
    "
      WG List: <mailto:ccamp@ietf.org>

      ID-draft editor:
        Haomian Zheng (zhenghaomian@huawei.com);
        Italo Busi (italo.busi@huawei.com);
        Aihua Guo (aihuaguo@huawei.com);
        Yunbin Xu (xuyunbin@ritt.cn);
        Yang Zhao (zhaoyangyjy@chinamobile.com);
        Xufeng Liu (Xufeng_Liu@jabil.com);
        Giuseppe Fioccola (giuseppe.fioccola@telecomitalia.it);
    ";
```



```
description
  "This module defines a YANG data model for describing
  the Ethernet transport services.";

revision 2017-09-12 {
  description
    "Updated version:

    Changed s-tag to vlan-tag choice in svc-multiplexing-tag
    to support also services where the C-Tag is used
    as service multiplexing tag
    (assume proper coordination/configuration of C-Tag is adopted)

    Added support for bandwidth profiles.

    Split config and state data for Ethernet services.
  ";
}

revision 2017-08-10 {
  description
    "Initial version";
}

/*
Groupings
*/

grouping vlan-classification {
  description
    "A grouping which represents classification on an 802.1Q VLAN tag.";

  leaf tag-type {
    type eth-types:eth-tag-classify;
    description
      "The tag type used for VLAN classification.";
  }

  choice individual-bundling-vlan {
    description
      "VLAN based classification can be individual
      or bundling.";

    case individual-vlan {
      leaf vlan-value {
        type eth-types:vlanid;
        description
          "VLAN ID value.";
      }
    }
  }
}
```

```
    }

    case vlan-bundling {
      leaf vlan-range {
        type etht-types:vid-range-type;
        description
          "List of VLAN ID values.";
      }
    }
  }
}

grouping vlan-write {
  description
    "A grouping which represents push/pop operations
    of an 802.1Q VLAN tag.";

  leaf tag-type {
    type etht-types:eth-tag-type;
    description
      "The VLAN tag type to push/swap.";
  }
  leaf vlan-value {
    type etht-types:vlanid;
    description
      "The VLAN ID value to push/swap.";
  }
}

grouping vlan-operations {
  description
    "A grouping which represents VLAN operations.";

  leaf pop-tags {
    type uint8 {
      range "1..2";
    }
    description
      "The number of VLAN tags to pop (or swap if used in
      conjunction with push-tags)";
  }
  container push-tags {
    description
      "The VLAN tags to push (or swap if used in
      conjunction with pop-tags)";
  }
  container outer-tag {
    presence

```

```

        "Indicates existence of the outermost VLAN tag to
        push/swap";

    description
        "The outermost VLAN tag to push/swap.";

    uses vlan-write;
}
container second-tag {
    must
        '../outer-tag/write-tag-type = "s-vlan-tag-type" and ' +
        'write-tag-type = "c-vlan-tag-type"'
    {

        error-message
            "
                When pushing/swapping two tags, the outermost tag must
                be specified and of S-VLAN type and the second
                outermost tag must be of C-VLAN tag type.
            ";
        description
            "
                For IEEE 802.1Q interoperability, when pushing/swapping
                two tags, it is required that the outermost tag exists
                and is an S-VLAN, and the second outermost tag is a
                C-VLAN.
            ";
    }

    presence
        "Indicates existence of a second outermost VLAN tag to
        push/swap";

    description
        "The second outermost VLAN tag to push/swap.";

    uses vlan-write;
}
}

grouping bandwidth-profiles {
    description
        "A grouping which represent bandwidth profile configuration.";

    choice direction {
        description
            "Whether the bandwidth profiles are symmetrical or

```

```
        asymmetrical";
    case symmetrical {
        description
            "The same bandwidth profile is used to describe the ingress
            and the egress bandwidth profile.";

        leaf ingress-egress-bandwidth-profile-name {
            type "string";
            description
                "Name of the bandwidth profile.";
        }
    }
    case asymmetrical {
        description
            "Ingress and egress bandwidth profiles can be specified.";
        leaf ingress-bandwidth-profile-name {
            type "string";
            description
                "Name of the bandwidth profile used in
                the ingress direction.";
        }
        leaf egress-bandwidth-profile-name {
            type "string";
            description
                "Name of the bandwidth profile used in
                the egress direction.";
        }
    }
}

grouping etht-svc-access-parameters {
    description
        "ETH transport services access parameters";

    leaf access-node-id {
        type te-types:te-node-id;
        description
            "The identifier of the access node in
            the ETH transport topology.";
    }
    leaf access-ltp-id {
        type te-types:te-tp-id;
        description
            "The TE link termination point identifier, used
            together with access-node-id to identify the
            access LTP.";
    }
}
```

```
leaf service-classification-type {
  type identityref {
    base eth-types:service-classification-type;
  }
  description
    "Service classification type.";
}

choice service-classification {
  description
    "Access classification can be port-based or
    VLAN based.";

  case port-classification {
    /* no additional information */
  }

  case vlan-classification {
    container outer-tag {
      presence "The outermost VLAN tag exists";
      description
        "Classifies traffic using the outermost VLAN tag.";

      uses vlan-classification;
    }
    container second-tag {
      must
        '../outer-tag/access-tag-type = "classify-s-vlan" and ' +
        'access-tag-type = "classify-s-vlan"'
      {
        error-message
          "
            When matching two tags, the outermost tag must be
            specified and of S-VLAN type and the second
            outermost tag must be of C-VLAN tag type.
          ";
        description
          "
            For IEEE 802.1Q interoperability, when matching two
            tags, it is required that the outermost tag exists
            and is an S-VLAN, and the second outermost tag is a
            C-VLAN.
          ";
      }
      presence "The second outermost VLAN tag exists";

      description

```

```
        "Classifies traffic using the second outermost VLAN tag.";
    }
    uses vlan-classification;
}

uses bandwidth-profiles;

container vlan-operations {
    choice direction {
        description
            "Whether the VLAN operations are symmetrical or
            asymmetrical";
        case symmetrical {
            container symmetrical-operation {
                uses vlan-operations;
                description
                    "Symmetrical operations.
                    Expressed in the ingress direction, but
                    the reverse operation is applied to egress traffic";
            }
        }
        case asymmetrical {
            container asymmetrical-operation {
                description "Asymmetrical operations";
                container ingress {
                    uses vlan-operations;
                    description "Ingress operations";
                }
                container egress {
                    uses vlan-operations;
                    description "Egress operations";
                }
            }
        }
    }
}

grouping etht-svc-tunnel-parameters {
    description
        "ETH transport services tunnel parameters";

    leaf tunnel-name {
        type string;
        description
            "TE service tunnel instance name.";
    }
}
```

```
    }
    choice svc-multiplexing-tag {
      description
        "Service multiplexing is optional and flexible.";

      case other {
        /*
         * placeholder to support proprietary multiplexing
         * (for further discussion)
         */
      }

      case none {
        /* no additional information is needed */
      }

      case vlan-tag {
        /*
         * No additional information is needed
         * The C-Tag or S-Tag used for service multiplexing is defined
         * by the VLAN classification and operations configured in the
         * eth-t-svc-access-parameters grouping
         */
      }

      case pw {
        /* to be completed (for further discussion) */
      }
    }
  }

  grouping te-topology-identifier {
    leaf access-provider-id {
      type te-types:te-global-id;
      description
        "An identifier to uniquely identify a provider.";
    }
    leaf access-client-id {
      type te-types:te-global-id;
      description
        "An identifier to uniquely identify a client.";
    }
    leaf access-topology-id {
      type te-types:te-topology-id;
      description
        "Identifies the topology the
         service access ports belong to.";
    }
  }
```

```
}

grouping etht-svc-instance_config {
  description
    "Configuraiton parameters for Ethernet services.";

  leaf etht-svc-name {
    type string;
    description
      "Name of the p2p ETH transport service.";
  }

  uses te-topology-identifier;

  leaf admin-status {
    type identityref {
      base te-types:state-type;
    }
    default te-types:state-up;
    description "ETH service administrative state.";
  }

  list etht-svc-access-ports {
    key access-port-id;
    min-elements "1";
    /* to be updated if extended to mp services */
    max-elements "2";
    description
      "List of the ETH trasport services access port instances.";

    leaf access-port-id {
      type uint16;
      description
        "ID of the service access port instance";
    }
    uses etht-svc-access-parameters;
  }
  list etht-svc-tunnels {
    key tunnel-name;
    description
      "List of the TE Tunnels supporting the ETH
      transport service.";

    uses etht-svc-tunnel-parameters;
  }
}

grouping etht-svc-instance_state {
```



```
description
  "State parameters for Ethernet services.";

leaf operational-state {
  type identityref {
    base te-types:state-type;
  }
  description "ETH service operational state.";
}
leaf provisioning-state {
  type identityref {
    base te-types:prov-state-type;
  }
  description "ETH service provisioning state.";
}
}

/*
Data nodes
*/

container etht-svc {
  description
    "ETH transport services.";

  container globals {
    list etht-svc-bandwidth-profiles {
      key bandwidth-profile-name;
      description
        "List of bandwidth profile templates used by
        Ethernet services.";

      uses etht-types:etht-bandwidth-profiles;
    }
  }

  list etht-svc-instances {
    key etht-svc-name;
    description
      "The list of p2p ETH transport service instances";

    leaf etht-svc-name {
      type leafref {
        path "../config/etht-svc-name";
      }
      description
        "ID of the p2p ETH transport service instance.";
    }
  }
}
```

```

    container config {
      description
        "Configuration of intended parameters.";

      uses etht-svc-instance_config;
    }

    container state {
      config false;
      description
        "Configuration of applied parameters and states.";

      uses etht-svc-instance_config;
      uses etht-svc-instance_state;
    }
  }
}

```

<CODE ENDS>

## 5.2. YANG Code for ETH transport type

<CODE BEGINS> file "ietf-eth-tran-types@2017-09-12.yang"

```

module ietf-eth-tran-types {
  /* TODO: FIXME */
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-eth-tran-types";

  prefix "etht-types";

  organization
    "Internet Engineering Task Force (IETF) CCAMP WG";
  contact
    "
      WG List: <mailto:ccamp@ietf.org>

      ID-draft editor:
        Haomian Zheng (zhenghaomian@huawei.com);
        Italo Busi (italo.busi@huawei.com);
        Aihua Guo (aihuaguo@huawei.com);
        Yunbin Xu (xuyunbin@ritt.cn);
        Yang Zhao (zhaoyangyjy@chinamobile.com);
    "

```

```
        Xufeng Liu (Xufeng_Liu@jabil.com);
        Giuseppe Fioccola (giuseppe.fioccola@telecomitalia.it);
    ";

    description
        "This module defines the ETH transport types.";

    revision 2017-09-12 {
        description
            "Updated version:

            Added bandwidth-profile-type
        ";
    }

    revision 2017-08-10 {
        description
            "Initial version";
    }

    /*
    Identities
    */

    identity eth-vlan-tag-type {
        description
            "ETH VLAN tag type.";
    }

    identity c-vlan-tag-type {
        base eth-vlan-tag-type;
        description
            "802.1Q Customer VLAN";
    }

    identity s-vlan-tag-type {
        base eth-vlan-tag-type;
        description
            "802.1Q Service VLAN (QinQ)";
    }

    identity service-classification-type {
        description
            "Service classification.";
    }

    identity port-classification {
        base service-classification-type;
```

```
    description
      "Port classification.";
  }

  identity vlan-classification {
    base service-classification-type;
    description
      "VLAN classification.";
  }

  identity eth-vlan-tag-classify {
    description
      "VLAN tag classification.";
  }

  identity classify-c-vlan {
    base eth-vlan-tag-classify;
    description
      "Classify 802.1Q Customer VLAN tag.
       Only C-tag type is accepted";
  }

  identity classify-s-vlan {
    base eth-vlan-tag-classify;
    description
      "Classify 802.1Q Service VLAN (QinQ) tag.
       Only S-tag type is accepted";
  }

  identity classify-s-or-c-vlan {
    base eth-vlan-tag-classify;
    description
      "Classify S-VLAN or C-VLAN tag-classify.
       Either tag is accepted";
  }

  identity bandwidth-profile-type {
    description
      "Bandwidth Profile Types";
  }

  identity mef-10-bwp {
    base bandwidth-profile-type;
    description
      "MEF 10 Bandwidth Profile";
  }

  identity rfc-2697-bwp {
```

```
    base bandwidth-profile-type;
    description
        "RFC 2697 Bandwidth Profile";
}

identity rfc-2698-bwp {
    base bandwidth-profile-type;
    description
        "RFC 2698 Bandwidth Profile";
}

identity rfc-4115-bwp {
    base bandwidth-profile-type;
    description
        "RFC 4115 Bandwidth Profile";
}

/*
Type Definitions
*/

typedef eth-tag-type {
    type identityref {
        base eth-vlan-tag-type;
    }
    description
        "Identifies a specific ETH VLAN tag type.";
}

typedef eth-tag-classify {
    type identityref {
        base eth-vlan-tag-classify;
    }
    description
        "Identifies a specific VLAN tag classification.";
}

typedef vlanid {
    type uint16 {
        range "1..4094";
    }
    description
        "The 12-bit VLAN-ID used in the VLAN Tag header.";
}

typedef vid-range-type {
    type string {
        pattern "([1-9][0-9]{0,3}(-[1-9][0-9]{0,3}))?" +
```

```

        "([1-9][0-9]{0,3}(-[1-9][0-9]{0,3})?)*";
    }
    description
        "A list of VLAN Ids, or non overlapping VLAN ranges, in
        ascending order, between 1 and 4094.

        This type is used to match an ordered list of VLAN Ids, or
        contiguous ranges of VLAN Ids. Valid VLAN Ids must be in the
        range 1 to 4094, and included in the list in non overlapping
        ascending order.

        For example: 1,10-100,50,500-1000";
}

typedef bandwidth-profile-type {
    type identityref {
        base bandwidth-profile-type;
    }
    description
        "Identifies a specific Bandwidth Profile type.";
}

/*
Grouping Definitions
*/
grouping etht-bandwidth-profiles {
    description
        "Bandwidth profile configuration paramters.";

    leaf bandwidth-profile-name {
        type string;
        description
            "Name of the bandwidth profile.";
    }
    leaf bandwidth-profile-type {
        type etht-types:bandwidth-profile-type;
        description
            "The type of bandwidth profile.";
    }
    leaf CIR {
        type uint64;
        description
            "Committed Information Rate in Kbps";
    }
    leaf CBS {
        type uint64;
        description
            "Committed Burst Size in in KBytes";
    }
}

```

```
}
leaf EIR {
  type uint64;
  /*
    Need to indicate that EIR is not supported by RFC 2697

    must
      '../bw-profile-type = "mef-10-bwp" or ' +
      '../bw-profile-type = "rfc-2698-bwp" or ' +
      '../bw-profile-type = "rfc-4115-bwp"'

    must
      '../bw-profile-type != "rfc-2697-bwp"'
  */
  description
    "Excess Information Rate in Kbps
     In case of RFC 2698, PIR = CIR + EIR";
}
leaf EBS {
  type uint64;
  description
    "Excess Burst Size in KBytes.
     In case of RFC 2698, PBS = CBS + EBS";
}
leaf color-aware {
  type boolean;
  description
    "Indicates weather the color-mode is
     color-aware or color-blind.";
}
leaf coupling-flag {
  type boolean;
  /*
    Need to indicate Coupling Flag is defined only for MEF 10

    must
      '../bw-profile-type = "mef-10-bwp"'
  */
  description
    "Coupling Flag.";
}
}
```

<CODE ENDS>

### 5.3. Other OTN client signal YANG Code

TBD.

## 6. Considerations and Open Issue

Editor Notes: This section is used to note temporary discussion/conclusion that to be fixed in the future version, and will be removed before publication. Currently this work only covers the Ethernet related service model. Other client signals would be defined in later version. We currently assume that there won't be much common part between Ethernet service model and other client signals service model, therefore the two groups of models are defined independently.

It is possible that there can be something in common for Ethernet service and other client signal service. If there is any need to construct a base model, we will also work it out in this draft. It is worth noting that a previous ID draft [I-D.zhang-teas-transport-service-model] is also addressing the same problem by defining a base model. But unfortunately we have not found any chance to augment to that model. Need to determine how we should go depending on the discussion in WG.

## 7. IANA Considerations

TBD.

## 8. Manageability Considerations

TBD.

## 9. Security Considerations

The data following the model defined in this document is exchanged via, for example, the interface between an orchestrator and a transport network controller. The security concerns mentioned in [I-D.ietf-teas-yang-te-topo] for using ietf-te-topology.yang model also applies to this document.

The YANG module defined in this document can be accessed via the RESTCONF protocol defined in [RFC8040], or maybe via the NETCONF protocol [RFC6241].

There are a number of data nodes defined in the YANG module which are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., POST) to these



data nodes without proper protection can have a negative effect on network operations.

Editors note: to list specific subtrees and data nodes and their sensitivity/vulnerability.

## 10. Acknowledgements

We would like to thank Igor Bryskin and Daniel King for their comments and discussions.

## 11. Contributors

Yanlei Zheng  
China Unicom  
Email: zhengyl@dimpt.com

Zhe Liu  
Huawei Technologies,  
Email: liuzhel23@huawei.com

Zheyu Fan  
Huawei Technologies,  
Email: fanzheyu2@huawei.com

Sergio Belotti  
Nokia,  
Email: sergio.belotti@nokia.com

Yingxi Yao  
Shanghai Bell,  
yingxi.yao@nokia-sbell.com

## 12. References

### 12.1. Normative References

[I-D.ietf-ccamp-otn-topo-yang]  
zhenghaomian@huawei.com, z., Fan, Z., Sharma, A., Liu, X., Belotti, S., Xu, Y., Wang, L., and O. Dios, "A YANG Data Model for Optical Transport Network Topology", draft-ietf-ccamp-otn-topo-yang-01 (work in progress), September 2017.

[I-D.ietf-ccamp-otn-tunnel-model]  
zhenghaomian@huawei.com, z., Fan, Z., Sharma, A., Rao, R., Belotti, S., Lopezalvarez, V., and Y. Li, "OTN Tunnel YANG Model", draft-ietf-ccamp-otn-tunnel-model-00 (work in progress), July 2017.

- [I-D.ietf-teas-yang-te-topo]  
Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Dios, "YANG Data Model for Traffic Engineering (TE) Topologies", draft-ietf-teas-yang-te-topo-13 (work in progress), October 2017.
- [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>>.
- [RFC7139] Zhang, F., Ed., Zhang, G., Belotti, S., Ceccarelli, D., and K. Pithewan, "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks", RFC 7139, DOI 10.17487/RFC7139, March 2014, <<https://www.rfc-editor.org/info/rfc7139>>.
- [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>>.
- [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>>.

## 12.2. Informative References

- [I-D.ietf-netmod-yang-tree-diagrams]  
Bjorklund, M. and L. Berger, "YANG Tree Diagrams", draft-ietf-netmod-yang-tree-diagrams-02 (work in progress), October 2017.
- [I-D.zhang-teas-transport-service-model]  
Zhang, X. and J. Ryoo, "A Service YANG Model for Connection-oriented Transport Networks", draft-zhang-teas-transport-service-model-01 (work in progress), October 2016.
- [RFC7062] Zhang, F., Ed., Li, D., Li, H., Belotti, S., and D. Ceccarelli, "Framework for GMPLS and PCE Control of G.709 Optical Transport Networks", RFC 7062, DOI 10.17487/RFC7062, November 2013, <<https://www.rfc-editor.org/info/rfc7062>>.

Authors' Addresses

Haomian Zheng  
Huawei Technologies  
F3 R&D Center, Huawei Industrial Base, Bantian, Longgang District  
Shenzhen, Guangdong 518129  
P.R.China

Email: zhenghaomian@huawei.com

Aihua Guo  
Huawei Technologies

Email: aihuaguo@huawei.com

Italo Busi  
Huawei Technologies

Email: Italo.Busi@huawei.com

Yunbin Xu  
CAICT

Email: xuyunbin@rict.cn

Yang Zhao  
China Mobile

Email: zhaoyangyjy@chinamobile.com

Xufeng Liu  
Jabil

Email: Xufeng\_Liu@jabil.com

Giuseppe Fioccola  
Telecom Italia

Email: giuseppe.fioccola@telecomitalia.it