Virtual Transport Network Services Specification 1.0

IA OIF-VTNS-01.0

April 28, 2017

Implementation Agreement created and approved
by the Optical Internetworking Forum
www.oiforum.com

The OIF is an international non-profit organization with over 100 member companies, including the world's leading carriers and vendors. Being an industry group uniting representatives of the data and optical worlds, OIF's purpose is to accelerate the deployment of interoperable, cost-effective and robust optical internetworks and their associated technologies. Optical internetworks are data networks composed of routers and data switches interconnected by optical networking elements.

With the goal of promoting worldwide compatibility of optical internetworking products, the OIF actively supports and extends the work of national and international standards bodies. Working relationships or formal liaisons have been established with CFP-MSA, COBO, EA, ETSI NFV, IEEE 802.3, IETF, INCITS T11, ITU SG-15, MEF, ONF.

For additional information contact:
The Optical Internetworking Forum
5177 Brandin Ct, Fremont, CA 94538
510-492-4040, info@oiforum.com

www.oiforum.com

Working Group: Networking and Operations WG

TITLE: **Virtual Transport Network Services Specification 1.0**

SOURCE: **TECHNICAL EDITORS**

Jia He, Maarten Vissers

Huawei Technologies Co., Ltd.
Email: hejia@huawei.com, maarten.vissers@huawei.com

Junjie Li, Ruiquan Jing
China Telecom Beijing Research Institute
Email: lijj@ctbri.com.cn, jingrq@ctbri.com.cn

WORKING GROUP CHAIR

Peter Landon

Notice: This Technical Document has been created by the Optical Internetworking Forum (OIF). This document is offered to the OIF Membership solely as a basis for agreement and is not a binding proposal on the companies listed as resources above. The OIF reserves the rights to at any time to add, amend, or withdraw statements contained herein. Nothing in this document is in any way binding on the OIF or any of its members.

The user's attention is called to the possibility that implementation of the OIF implementation agreement contained herein may require the use of inventions covered by the patent rights held by third parties. By publication of this OIF implementation agreement, the OIF makes no representation or warranty whatsoever, whether expressed or implied, that implementation of the specification will not infringe any third party rights, nor does the OIF make any representation or warranty whatsoever, whether expressed or implied, with respect to any claim that has been or may be asserted by any third party, the validity of any patent rights related to any such claim, or the extent to which a license to use any such rights may or may not be available or the terms hereof.

This document and the information contained herein is provided on an "AS IS" basis and THE OIF DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE OR FITNESS FOR A PARTICULAR PURPOSE.

1 Table of Contents

2 List of Figures

3 List of Tables

4 Introduction

4.1 Problem Statement

As new services emerge with the development of transport Software Defined Networking (SDN) technologies, new requirements and characteristics for transport networks have been identified. For example, Bandwidth on Demand (BoD) is a service that requires dynamic bandwidth provisioning to provide users with instantly created connectivity. Network as a Service (NaaS) is another example of new service that requires a network as a whole (often including network virtualization) provided to users and allows users with more management and control capabilities to achieve for example optimization of resource allocation. 5G slicing is yet another example, which requires slicing of network resources for different purposes, e.g. low latency, reliability. Third-party entities can be given permission to control certain aspects of slicing via a suitable API, in order to provide tailored services.

The existing fixed connection services, e.g. MEF E-Line, E-Tree, E-LAN services [MEF 6.2] provided by operators with signed contract cannot be changed automatically by customers. Therefore, this IA will define Virtual Transport Network Services (VTNS) to meet those new requirements.

4.2 Scope

By specifying VTNS, the requirements and characteristics of those new services will be identified and classified and the new service types and their attributes will be defined. It aims to become a main driver for the deployment of SDN in transport networks from a service perspective and help to identify transport APIs and requirements, which will complement the other standard organizations' work on developing enabling technologies for transport SDN.

Detailed technical specifications of how specific performance characteristics corresponding to a certain attribute or type of VTNS may be implemented are outside the scope of this specification.

4.3 Merits to OIF

The work on VTNS will help to establish a service specification working area in OIF.

4.4 Working Groups

Networking & Operations WG

Carrier Working Group

Interoperability (Networking) Working Group

4.5 Relationship to Other Standards Bodies

This VTNS IA follows the definition of virtualization and SDN architecture defined by [ONF SDN Architecture 1.0]and [ONF SDN Architecture 1.1].

This VTNS IA defines the requirements and characteristics of new types of services, but the implementation of a specific type of VTNS is not in the scope of this IA, which could be developed by other standards or other standard organizations' work (e.g. ONF, IETF). One example is the on-going [ONF T-API] work, which takes the defined service types in this VTNS IA as an input for the design of related APIs to meet the service attributes and capability requirements defined in VTNS IA.

4.6 Document Organization

This document is organized as follows:

- Section 4: Introduction
- Section 5: Abbreviations
- Section 6: Virtual Transport Network Service Definition
- Section 7: Virtual Transport Network Service Classification
- Section 8: Attribute and Parameter Definition
- Section 9: Virtual Transport Network Service types (attributes, parameters)
- Section 10: Requirements for Identifiers in VTNS
- Section 11: Virtual Transport Network Service recovery
- Section 12: Virtual Transport Network Service OAM
- Section 13: Summary
- Section 14: References
- Appendices

5 Abbreviations

BoD	Bandwidth on Demand
CTP	Connection Termination Point [ITU-T M.3100]
GUI	Graphical User Interfaces
IA	Implementation Agreement
ID	Identifier
IETF	Internet Engineering Task Force
MEF	Metro Ethernet Forum
MEP	MEG (Maintenance Entity Group) End Point

NaaS	Network as a Service
NE	Network Element
OAM	Operation, Administration, and Maintenance
OIF	Optical Internetworking Forum
ONF	Open Networking Foundation
OTT	over-the-top
PCE	Path Computation Element
SDN	Software Defined Networking
SLA	Service Level Agreement
SNPP	Subnetwork Point Pool [ITU-T G.7701]
T-API	Transport Application Programming Interface
TE	Traffic Engineering
TNA	Transport Network Assigned
TTP	Trail Termination Point [ITU-T M.3100]
UNI	User-network interface
UNI-N	Network side of a UNI
vLink	virtual Link
VN	Virtual Network
vNE	virtual NE
VTNS	Virtual Transport Network Services

6 Virtual Transport Network Service Definition

A Virtual Transport Network Service (VTNS) is the creation and offering of a Virtual Network (VN) by a provider to a user in accordance with agreements reached between them (e.g., satisfying the users' objectives). Such agreements may be negotiated statically or dynamically; in the latter case VNs may be dynamically created, deleted, or modified in response to requests from the user. This implies dynamic provider modification of resources reserved for the user. The user may then act upon the Virtual Network resources to perform connection management (set-up/release/modify connections), connection monitoring (activate/deactivate MEP functions and activate/configure/deactivate OAM flows) and connection protection (activate/configure/deactivate protection switch processes).

VTNS is built on the virtualization of transport network resources. The physical transport network resources are sliced and assigned usually with an abstract view to different users. The user request may include traffic matrix, Service Level Agreement (SLA), topology, Operation, Administration, and Maintenance (OAM), recovery requirements etc. Users of VTNS may own the right to control and manage the assigned virtual network as if they were operating a physical transport network, more than just get managed connectivity. For example, users may choose their preferred routing algorithm to select the route and set up a virtual connection by configuring each virtual cross connect. Users may also choose to add OAM and protection to the virtual connections they have set up. From the user of a VTNS perspective, virtual nodes and virtual links will not appear to be virtual.

The virtual network can be reconfigured based on the request from the user, e.g. capacity expansion, topology change, without adding/removing the physical network resources.

VTNS may also require topology recovery in case of failures in the physical network to guarantee the consistent virtual network topology that is committed to users. This is different from connection recovery since there might be no connection set up yet on the virtual network topology.

For security reasons, the VTNS provider's resources outside a particular VTNS customer's virtual network should be invisible to that customer.

[Note: "User", "customer", and "client" are used interchangeably in this document to indicate any entity (e.g. a client controller) which requests virtual transport network services defined in this document.]

7 Virtual Transport Network Service Classification

Virtual transport network services are classified as below:

[Note: Customer access to Management and Management Graphical User Interfaces (GUI) are expected to be supported in the following types of services.]

Type A: Dynamic connection service with limited customer control

Type A service defines dynamic connection service that is provided to customers based on their request. As defined in Figure 1, Type A service makes available to the user a single virtual NE (vNE) with two or more interface ports that are interconnected via a switch function in the vNE and that are connected with client sites via links. The user has control over the configuration of the interface ports and over the cross connections between these interface ports.

For example, if a SDN approach is used, a Type A service request from the user SDN controller could result in the creation of such vNE by the provider's SDN controller and handing over configuration control of this vNE to the user SDN controller. The user SDN controller will add this vNE to its resource data base that may also contain its own physical NEs. The user SDN controller, or component that holds topology in the user context, can now extend its layer network topology models or multi-layer network topology model with a subnetwork that represents the vNE's switching function or functions, a set of links that terminate on the vNE's interface ports and TTP/CTP resource groups that represent the capabilities of its interface ports. The interface ports may be single cross connections in its physical NEs.

Once the user SDN controller has been given configuration control over the vNE, it can configure the interface ports and cross connections in this vNE. Interface port configuration and cross connection configuration in this vNE can be configured via a SDN control interface. For the case that such vNE supports GMPLS/ASON on its interfaces, OIF UNI [OIF UNI 2.0] may be used to configure a cross connection in this vNE. A cross connection in the vNE may exist for months/days/hours/minutes. The configuration can be done as scheduled with known duration.

Typical application of Type A service is Bandwidth on Demand (BoD). The time to provision these services is also expected to be shortened from days/months to hours/days or even less.

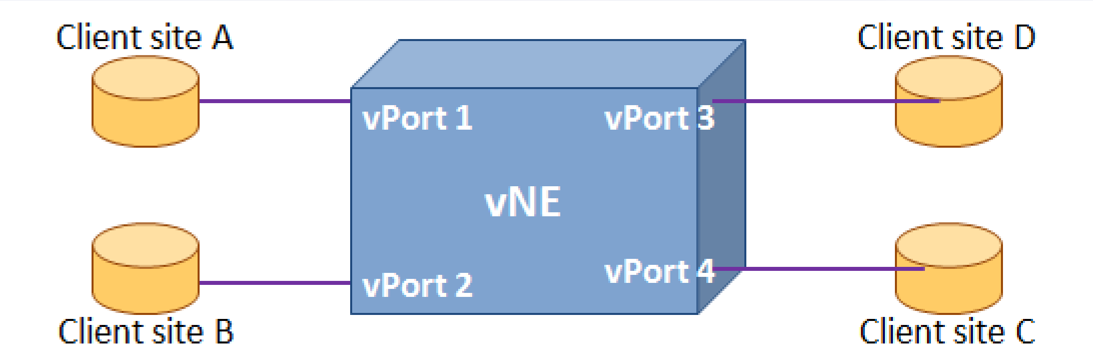

Figure 1: VTNS Type A

Type B: Fixed virtual network with customer connection control

Type B service as defined in Figure 2 makes available to the user a set of vNEs which are interconnected within the VN by a set of virtual links (vLink), and are connected with client sites via links. The user has control over the configuration of the interface ports and cross connections between these interfaces ports in every vNE within the VN, in a similar manner as it can configure interface ports and cross connections in its physical NEs. Type B service can be regarded as a super set of Type A.

For example, if a SDN approach is used, the user's Type B service request could result in the creation of such set of vNEs and vLinks by the provider's SDN controller and handing over configuration control of these vNEs to the user SDN controller. The user SDN controller will add the set of vNEs to its resource data base that may also contain its own physical NEs. The user SDN controller , or component that holds topology in the user context, can now extend its layer network topology models or multi-layer network topology model with a set of subnetworks that represents each vNE's switching function or functions, a set of links that terminate on the interface ports of each vNE and TTP/CTP resource groups (or transitional links) that represent the capabilities of each interface port. The interface ports may be single layer or multi-layer ports, as (implicitly or explicitly) requested within the Type B service request.

Once the user SDN controller has been given configuration control over these vNEs, it can configure the interface ports and cross connections in each of these vNEs. Interface port configuration and cross connection configuration in a vNE can be configured via a SDN control interface. For the case that such vNEs support GMPLS/ASON on its interfaces, OIF UNI [OIF UNI 2.0] may be used to configure a cross connection in these vNEs (e.g. via explicit routing). A cross connection in the vNE may exist for months/days/hours/minutes. Path computation is done in the user SDN controller's PCE application within the context of the user's hybrid physical/virtual network; i.e. not just in the context of the virtual network, or by obtaining the network topology in a distributed way (e,g., using OIF ENNI [OIF ENNI]) and locally computing the path. For the case that a vNE represents a larger subnetwork within the provider network, configuration of a cross connection in such vNE may trigger a path computation action within the provider SDN controller. But this is not required when potential paths through such provider subnetwork are precomputed.

The virtual network topology is pre-configured between customer and owner of the network. The operator stays in full control and has responsibility for configuring resources for the virtual network. In this type of service, customers have knowledge of the virtual network topology, including virtual nodes and virtual links. See Figure 2.

Typical application of Type B service is with virtual providers or over-the-tops (OTTs).

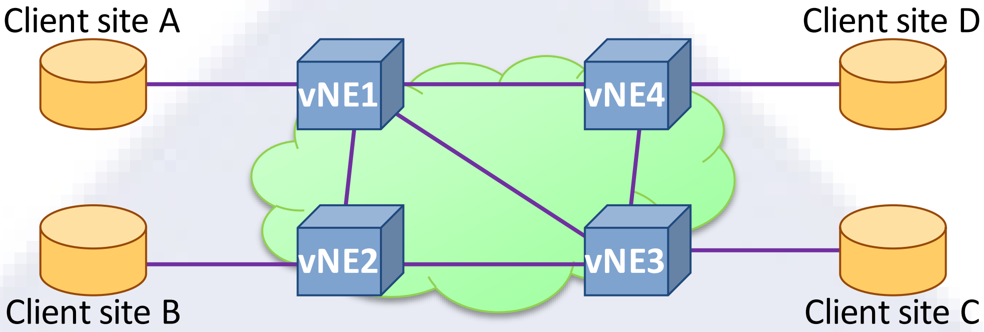

Figure 2: VTNS Type B

Type C: Dynamic virtual network with customer connection control

Type C service includes Type B service with additional capability that customers of a Type C service instance may request dynamic creation/modification/deletion of virtual networks provided by the operator.

The virtual network is not pre-configured between customer and owner of the physical network. The operator stays in full control and has responsibility for configuring resources for the virtual network. In this type of service, customers have knowledge of the virtual network topology and are able to change the virtual network topology, for example by adding or removing virtual nodes and virtual links. See Figure 8-3. [Note: Operator policies may limit the modifications for example to the addition/removal of virtual links as opposed to the addition/removal of virtual NEs.]

To establish connections, customers of a Type C service instance would need to request a virtual topology that connects customers of the service instance, followed by Type B connection requests over that topology.

Typical application of Type C service is also with virtual providers or OTTs.

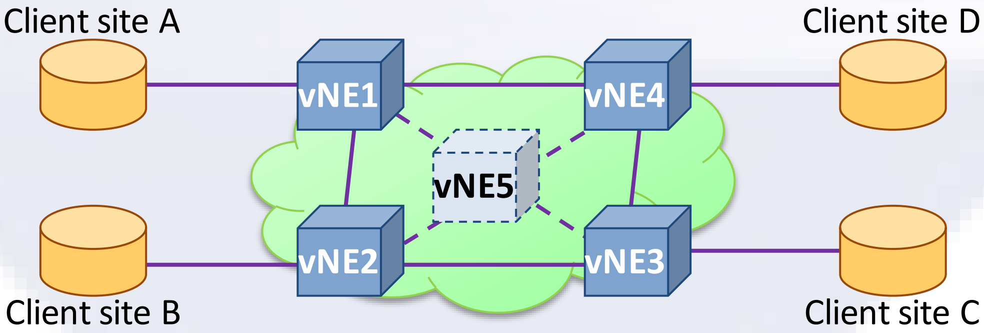

Figure 3: VTNS Type C

8 Attribute and Parameter Definition

Two dimensions are used to describe the characteristics of Virtual Transport Network Services:

- Attribute
- Capability

"Attribute" is used to describe those "static" characteristics of the service, e.g. bandwidth, SLA, etc, similar to what is used in the existing service definition, except for some new attributes correlated to the new types of services. For example, scheduled services might add time attributes (e.g. start/end time) to indicate that those services usually happen within an expected time frame or at a known frequency.

"Capability" is used to describe the added control and management (behavior) merits of the new types of services. It can be further divided into topology level and connection level. At each level, those capabilities like create/modify/delete/inquire can be authorized to clients based on their requested service types in the contract.

8.1 Attributes

The following Table 1 includes the description of service attributes and correlated parameters and values, which provides a necessary (may not be comprehensive) set of attributes to describe and distinguish the different types of services.

Table 1: VTNS - Service attributes

Service Attribute	Service Attribute Parameters and Values
Service ID	A string name to uniquely identify a VTNS service provided to a client. Refer to Section 11 "Requirements for Identifiers in VTNS"
Service Endpoint(s)	A list of endpoints. Each service endpoint from the provider's record will include customer endpoint name plus a network endpoint name (exposed to the customer by the provider) for the service; Each service endpoint from the customer's point of view includes only the customer's endpoint name. See Appendix A.
Service Type	As described in Section 8.
Call ID	To uniquely indentify a traffic flow within VTNS. Refer to Section 11 "Requirements for Identifiers in VTNS"
Connection ID	A connection identifier which is unique in the scope of a VTNS service. Refer to Section 11 "Requirements for Identifiers in VTNS"

Topology ID	A virtual network topology identifier which is unique in the scope of a VTNS service. Multiple topologies may exist for the same VTNS service instance. The topology is referenced by the Topology ID. Refer to Section 11 “Requirements for Identifiers in VTNS”
Connection Type	Point-to-Point connection or Point-to-MultiPoint connection.
Connection TE Parameters	A technology-dependent traffic description of a connection to be created or modified, which may include parameters such as Switching Type, Encoding Type, Signal Type, Bandwidth, etc. Connection TE parameters exist for the life of a specific connection.
Traffic Matrix	One or more matrixes describing the traffic (e.g. bandwidth) between each pair of customer’s access points for specific instances in time. This Traffic Matrix is used for dimensioning when creating or modifying a virtual network topology.
Service Scheduling	The start time, end time and the duration of a connection.
Connection SLA	The service level agreement of a connection, e.g. the recovery capability requirements in case a connection fails. This is equivalent to the Service Level defined in the [OIF UNI 2.0].
Topology SLA	The service level agreement of a virtual network topology, e.g. the capability of recovery from topology level failures *[Note]:Virtual network topology recovery indicates recovery from a damaged topology in case e.g. some virtual link or virtual node failures happen.*

8.2 Capability

The following Table 2 includes the description of service capabilities. It may not be a comprehensive set of capabilities but necessary to distinguish the different types of services.

Table 2: VTNS - Service Capabilities

Level	Service Capability	Service Capability Description
Connection Level	Connection Creation Configuration	The capability to allow customer to create a connection on a virtual NE provided by the carrier, with consideration of the customer specified connection SLA if any.
	Connection Deletion	The capability to allow customer to delete a

	Configuration	connection on a virtual NE provided by the carrier that has been created by the customer.
	Connection Modification Configuration	The capability to allow customer to modify connection on a virtual NE provided by the carrier that has been created by the customer.
	Connection Information Inquiry	The capability to allow customer to retrieve the information of the connection that has been created by the customer.
	Connection Status Notification	The capability to learn the change of connection status. e.g., connection fails, or connection recovers.
Topology Level	Virtual Network Topology Creation	The capability to allow customer to request a virtual network topology in the carrier’s network, with consideration of the customer specified virtual network topology SLA if any.
	Virtual Network Topology Deletion	The capability to allow customer to request to delete the virtual network topology that has been created for the customer.
	Virtual Network Topology Modification	The capability to allow customer to request to modify the virtual network topology that has been created for the customer.
	Virtual Port Configuration	The capability to configure a virtual port which supports a single layer or multiple layer end points including one or more monitoring functions that can report status/performance and client/server adaptation possibly with client muxing/demuxing.
	Virtual Network Topology Information Inquiry	The capability to allow customer to inquire the topology information of the virtual network topology that has been created for the customer.
	Virtual Node Information Inquiry	The capability to allow customer to retrieve all the virtual nodes or a specific virtual node within the virtual network topology that has been created for the customer.
	Virtual Port Information Inquiry	The capability to allow customer to retrieve all the virtual ports or a specific virtual port information of a virtual node in the virtual network topology that has been created for the customer.

	Virtual Link Information Inquiry	The capability to allow customer to retrieve all the virtual links or a specific virtual link information of the virtual network topology that has been created for the customer.
	Virtual Network Topology Status Notification	The capability to learn the change of virtual network topology status. e.g., virtual node/link/port fails, or virtual node/link/port recovers.

9 Virtual Transport Network Service types (attributes, parameters)

The attributes and parameters for Service types A,B,C are described respectively in the following.

9.1 Service Type A

Table 3 provides the service attributes for service Type A. Table 4 provides the service capabilities for service Type A.

Table 3: Service Attributes for VTNS Type A

Service Attribute	Remark
Service ID	Mandatory
Service Endpoint(s)	Mandatory
Service Type	Mandatory, MUST be Type A
Call ID	Mandatory
Connection ID	Optional
Topology ID	N/A
Connection Type	Mandatory
Connection TE Parameters	Mandatory
Traffic Matrix	Optional
Service Scheduling	Optional
Connection SLA	Optional
Topology SLA	N/A

Table 4: Service Capabilities for VTNS Type A

Level	Service Capability	Remark

Connection Level	Connection Creation Configuration	Mandatory
	Connection Deletion Configuration	Mandatory
	Connection Modification Configuration	Optional. If supported, the customer can modify the attributes of the connection which has been created, e.g., TE parameters, start or end time of the connection. Service ID, Service Endpoints cannot be modified.
	Connection Information Inquiry	Mandatory
	Connection Status Notification	Mandatory
Topology Level	Virtual Network Topology Creation	Disabled
	Virtual Network Topology Deletion	Disabled
	Virtual Network Topology Modification	Disabled
	Virtual Network Topology Information Inquiry	Disabled
	Virtual Port Configuration	Enabled
	Virtual Node Information Inquiry	Disabled
	Virtual Port Information Inquiry	Disabled
	Virtual Link Information Inquiry	Disabled
	Virtual Network Topology Status Notification	Disabled

9.2 Service Type B

Table 5 provides the service attributes for service Type B. Table 6 provides the service capabilities for service Type B.

Table 5: Service Attributes for VTNS Type B

Service Attribute	Remark
Service ID	Mandatory
Service Endpoint(s)	Mandatory
Service Type	Mandatory, MUST be Type B
Call ID	Mandatory
Connection ID	Mandatory
Topology ID	Mandatory
Connection Type	Mandatory
Connection TE Parameters	Mandatory
Traffic Matrix	Optional
Service Scheduling	Optional
Connection SLA	Optional
Topology SLA	Optional

Table 6: Service Capabilities for VTNS Type B

Level	Service Capability	Remark
Connection Level	Connection Creation Configuration	Mandatory. The resource used by the connection MUST be limited to the virtual network topology that the customer owns.
	Connection Deletion Configuration	Mandatory
	Connection Modification Configuration	Optional. If supported, the customer can modify the attributes of the connection which has been created, e.g., TE parameters, start or end time of the connection. Service ID, Service Endpoints cannot be modified.
	Connection Information Inquiry	Mandatory
	Connection Status	Mandatory

	Notification	
Topology Level	Virtual Network Topology Creation	Disabled. The carrier needs to configure a virtual network topology and assign it to the customer manually at the beginning of the VTNS service.
	Virtual Network Topology Deletion	Disabled. The carrier needs to release the resource of the virtual network topology and delete it manually at the end of the VTNS service.
	Virtual Network Topology Modification	Disabled
	Virtual Port Configuration	Enabled
	Virtual Network Topology Information Inquiry	Mandatory if at least one of the “Virtual Node/Port/Link Information Inquiry” capabilities is not supported.
	Virtual Node Information Inquiry	Mandatory if the “Virtual Network Topology Information Inquiry” capability is not supported.
	Virtual Port Information Inquiry	Mandatory if the “Virtual Network Topology Information Inquiry” capability is not supported.
	Virtual Link Information Inquiry	Mandatory if the “Virtual Network Topology Information Inquiry” capability is not supported.
	Virtual Network Topology Status Notification	Mandatory

9.3 Service Type C

Table 7 provides the service attributes for service Type C. Table 8 provides the service capabilities for service Type C.

Table 7: Service Attributes for VTNS Type C

Service Attribute	Remark
Service ID	Mandatory
Service Endpoint(s)	Mandatory

Service Type	Mandatory, MUST be Type C
Call ID	Mandatory
Connection ID	Mandatory
Topology ID	Mandatory
Connection Type	Mandatory
Connection TE Parameters	Mandatory
Traffic Matrix	Mandatory
Service Scheduling	Optional
Connection SLA	Optional
Topology SLA	Optional

Table 8: Service Capabilities for VTNS Type C

Level	Service Capability	Remark
Connection Level	Connection Creation Configuration	Mandatory. The resource used by the connection MUST be limited to the virtual network topology that the customer owns.
	Connection Deletion Configuration	Mandatory
	Connection Modification Configuration	Optional. If supported, the customer can modify the attributes of the connection having been created, e.g., TE parameters, start or end time of the connection. Service ID, Service Endpoints cannot be modified.
	Connection Information Inquiry	Mandatory
	Connection Status Notification	Mandatory
Topology Level	Virtual Network Topology Creation	Mandatory
	Virtual Network Topology Deletion	Mandatory
	Virtual Network Topology Modification	Mandatory
	Virtual Port Configuration	Enabled
	Virtual Network Topology Information Inquiry	Mandatory if at least one of the “Virtual Node/Port/Link Information Inquiry” capabilities is not supported.
	Virtual Node Information Inquiry	Mandatory if the “Virtual Network Topology Information Inquiry” capability is not supported.

	Virtual Port Information Inquiry	Mandatory if the "Virtual Network Topology Information Inquiry" capability is not supported.
	Virtual Link Information Inquiry	Mandatory if the "Virtual Network Topology Information Inquiry" capability is not supported.
	Virtual Network Topology Status Notification	Mandatory

10 Requirements for Identifiers in VTNS

The identification of entities in networks is a very important architectural and design aspect. Careful thought is required to ensure that the network can scale, can be re-organized, and can change one aspect without affecting other aspects. In order to describe the requirements for identifiers in VTNS, the following three categories are considered.

Resources (Data Plane)

R01. For a virtual network topology, a separate name space for its resources is supported. This name space is visible to the set of users of that virtual network topology. The name space is identified by the Topology ID.

R02. A resource may participate in multiple virtual network topologies and has identifiers in name spaces associated to each of the virtual network topologies.

R03. For the case of participation in multiple virtual network topologies, there may be overlapping address spaces, and distinction between them is maintained. That is, the address format for two address spaces may be identical and the range of values used in those spaces may be identical. The two address spaces may be applied to two virtual networks that overlap the same resources.

R04. Mappings exist between an address spaces for a virtual network topology and topology (or topologies) of the underlying resources. An example would be Subnetwork Point Pool (SNPP) to SNPP aliases.

R05. Optional. The user may provide the name space and identifiers in that space, for the virtual network.

R06. Connections created by the various VTNS types have identifiers. They are unique within the VTNS service instance. These are the Connection ID described in the VTNS specification.

Control/Management functions

R07. Users of a VTNS service are identified in an address space instance for that purpose. That address space could be shared by other VTNS services. In all cases the user identifier is unique within the VTNS service instance. Examples of such identifiers are OIF TNA names.

R08. A mapping exists between the VTNS identifier space and resource address spaces. In OIF IAs, this would be TNA name to SNPP mapping, and enables connection endpoints to be identified for the purpose of requesting a path in the topology.

R09. The set of VTNS services supported by a set of resources, is identified from a common address space. These are the Service IDs described in the VTNS specification.

R10. A call created for a VTNS user is identified by a Call ID, which is unique within the scope of the VTNS service. A global Call ID name space instance would satisfy this requirement for all VTNS service instances sharing the same underlying resources.

R11. Functional components that provide call/connection management, routing, discovery, directory service, VPN membership management, etc. have identifiers for the function and identifiers for distributed instances if they exist.

Communications Network for Control/Management functions

Functional components that serve VTNS services, communicate over a DCN. The identifier requirements from [ITU-T G.7712] are applied. If a common address space is used for multiple VTNS services that share the same underlying resources, the DCN address instances must disambiguate between functions for VTNS service instances.

11 Virtual Transport Network Service recovery

According to the definition of virtual transport network services, recovery of virtual transport network services falls into two categories: connection level recovery and topology level recovery.

11.1 Connection Level Recovery

Connection level recovery applies to all the three types of services listed in Section 8.

Type A service is a connection service directly set up by the VTNS provider. Connection level recovery for this type of service simply refers to the capability to recover those connections by VTNS provider when failures happen and impact the connections.

Type B and Type C services provide virtual network topologies with customer-geared connection control. Therefore, connection level recovery for Type B and Type C services refers to the capability to recover the virtual connections which have been set up by the customers in their requested virtual network topology from the VTNS provider. This operation might be performed by the VTNS provider, the customer or both. If both the VTNS provider and customer are allowed to perform the connection level recovery, some coordination is needed, for example by pre-configuration e.g. connection level recovery first, if not successful, topology level recovery is triggered,

Existing technologies, such as 1+1 or 1:1 linear protection or rerouting, can be applied to support the connection level recovery. Customers may request different types of connection level recovery according to their connection SLAs.

11.2 Topology Level Recovery

Topology level recovery only applies to Type B and Type C services.

Topology level recovery refers to the capability to recover a virtual network topology with all the virtual connections which have been set up inside when failures happen and impact the virtual network topology.

From the perspective of the customer, after the topology level recovery takes place, the customer's virtual network topology, as well as the virtual connections inside the virtual network topology, should stay the same as before the failures happen, although the failed physical resources have been replaced with new ones.

Customers may request different types of topology level recovery for their virtual network topology according to their topology SLAs. Two types of topology level recovery are defined: topology protection and topology restoration.

11.2.1 Virtual Network Topology Protection

The virtual network topology protection requires both working and protection resources reserved by VTNS provider in the physical network for the same virtual network topology, so that when failure happens to the working resources, the backup resources can be used to support the virtual network. More practically, this is done only on a few specific links not across all the links.

The customer may send a virtual network topology creation request to the VTNS provider with virtual network resource attributes (e.g. traffic matrix) and virtual network recovery (protection) types (e.g. topology SLA). After receiving the virtual network topology creation request, the VTNS provider should reserve both working and protection resources in the free physical network resources according to the required virtual network resources attributes and virtual network recovery types, and map both the working and protection resources to the same virtual network topology requested by customer and generate the virtual network for the customer. Preferably, the working and protection resources should be disjoint, which means each virtual link in the virtual network topology is mapped to two disjoint physical resources that are for working resources and protection resources respectively.

Topology protection can be typically categorized as 1+1 topology protection and 1:1 topology protection . When the customer requests to create a virtual connection in its virtual network, the provider should create two virtual links in the physical network using working and protection resources respectively, and make sure that the two paths map to the same virtual connection in the customer's virtual network.

- For 1+1 topology protection, traffic will be carried on both working link in the physical working topology and protection link in the physical protection topology, and will be received from the working link in the normal case. Once failures happen and impact the working link, the traffic will be received from the protection link.

- For 1:1 topology protection, traffic will only be carried on the working link in the physical working topology and received from the working link in the normal case. When failures happen and impact the working link, the traffic will be switched to the protection link in the physical protection topology, i.e. carried and received on the protection link.

11.2.2 Virtual Network Topology Restoration

The virtual network topology restoration refers to the capability to repair a broken virtual network topology automatically by the VTNS provider, after failures happen and impact the virtual network topology.

The customer may send a virtual network topology creation request to the VTNS provider with virtual network resource attributes (e.g. traffic matrix) and virtual network recovery (restoration) types (e.g. topology SLA). After receiving the virtual network topology creation request, the VTNS provider should reserve resources in the free and available physical network resources according to the required virtual network resources and virtual network recovery types, and map the reserved resources to the virtual network topology requested by customer. When the VTNS provider detects failures in the physical network (e.g. physical link failure) which affect the customer's virtual network topology, i.e., one or more virtual links (corresponding to the failed physical link) in the virtual network topology fail, the provider should map the affected one or more virtual links to the failure-free and available resources in the physical network, so that the virtual links still have the same attributes (e.g., link capacity) as before failures happen.

Furthermore, if there are virtual connections in the virtual network topology traversing at least one affected virtual link (corresponding to the failed physical link), these virtual connections should be migrated to the failure-free and available resources in the physical network, i.e. new connections, which should have the same attributes (e.g., signal type, bandwidth) as the affected virtual connections, should be created using the free and available physical resources and those affected virtual connections should be remapped to the new physical connections. If revert mode is enabled, the resources of the failed virtual links should be kept and the virtual connections traversing the failed virtual links should remain. When network failures disappear, the virtual network and the virtual connections inside will return to the original working resources before network failures happen.

If revert mode is disabled (or non-revert mode is enabled), the virtual connections traversing the failed virtual links can be deleted, and the resources of the failed virtual links can be released from the virtual network, so that other services can use these resources once network failures are cleared.

11.2.3 Coordination between connection and topology level recovery

For Type B and Type C VTNS services, both connection level recovery and topology level recovery are applicable, but typically only one of them will be adopted. Coordination mechanism like hold-off timer may be applied when two level recovery methods co-exist.

12 Virtual Transport Network Service OAM

It is also expected to provide OAM capabilities for virtual transport network services in order to operate and maintain the network and service aspects. The basic OAM requirement for VTNS is done by VTNS provider, i.e. to monitor and troubleshoot the links, connections etc. over the physical networks using the existing standard OAM mechanisms, which is transparent to the customer. Further, customers of the virtual transport network may set up OAM mechanisms for specific virtual links, connections etc. according to their willingness over their own virtual network. This includes connection monitoring and configuration. This is for further study.

13 Summary

Three types (Type A,B,C) of virtual transport network services are identified and defined in this IA. With the specification of those services, it provides a driver for the deployment of SDN in transport networks from a service perspective and helps the industry to categorize the emerging new services with highlighted characteristics and requirements. On the other hand, this service specification can also be used as input to further identify enabling technologies to support these services.

14 References

14.1 Normative references

1. [ONF SDN Architecture 1.0] ONF SDN Architecture 1.0, “SDN Architecture Issue 1”, June 2014
2. [ONF SDN Architecture 1.1] ONF SDN Architecture 1.1, ONF TR-521, “SDN Architecture Issue 1.1”, February 2016

14.2 Informative references

1. [ITU-T M.3100] ITU-T Recommendation M.3100, “ Generic network information model”, April 2005

2. [ITU-T G.7701] ITU-T Recommendation G.7701, “Common Control Aspects”, November 2016

3. [OIF SDN API Framework] OIF-FD-Transport-SDN-01.0, “Framework for Transport SDN: Components and APIs”, May 2015
4. [ONF T-API] ONF TR-527, “Functional Requirements for Transport API”, June 2016
5. [MEF6.2] MEF 6.2, “EVC Ethernet Services Definition Phase 3”, August 2014
6. [OIF UNI 2.0] OIF UNI 2.0, “User Network Interface (UNI) 2.0 Signaling Specification”, February 2008
7. [OIF ENNI] OIF E-NNI 2.0, “ OIF E-NNI Signaling Specification”, April 2009

8. [ITU-T G.7712] ITU-T G.7712, “ Architecture and specification of data communication network”, September 2010

9. [ITU-T Y.1311] ITU-T Recommendation Y.1131 “Network-based VPNs – Generic architecture and service requirements”, March 2002

10. [ITU-T Y.1312] ITU-T Recommendation Y.1312, “Layer 1 Virtual Private Network generic requirements and architecture”, September 2003

Appendix A: Service endpoint vs. network endpoint

Service endpoints exist independent of network endpoints. A service endpoint represents a set of points (2 or more) that a service user wishes to connect. The network endpoint represents a point at the edge of the network used by a network connection. This independence is important as a network endpoint may be able to access multiple service endpoints. Likewise, it is possible for a service endpoint to be reached through multiple network endpoints. These relationships are shown in Figure A-1 below.

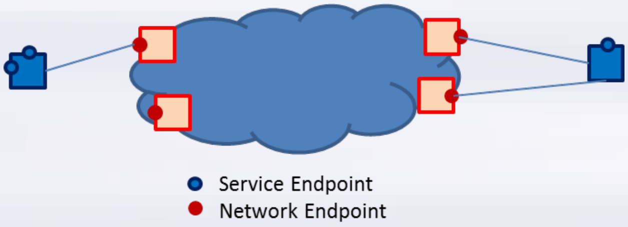

Figure A-4 Examples of multiple and dual-homed service endpoints

The relationship between service endpoint and network endpoint is not permanent. It is possible for the binding between these endpoints to change as the network changes or the service user changes. For example, a carrier may add additional switching equipment to their network and benefit from move a service endpoint from its original switch to a new switch. Likewise, a service user may move locations, causing the service endpoint to be reached via a different switch than prior to the move. See Figure A-2.

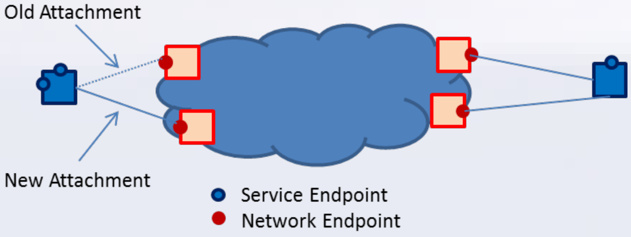

Figure A-5 Examples of moving service endpoint attachment points

Given the independence of service endpoint to network endpoint binding, it is possible for a service endpoint to exist but not be associated with a network endpoint. Likewise, it is possible for a network endpoint to exist without any associated service endpoints. See Figure A-3.

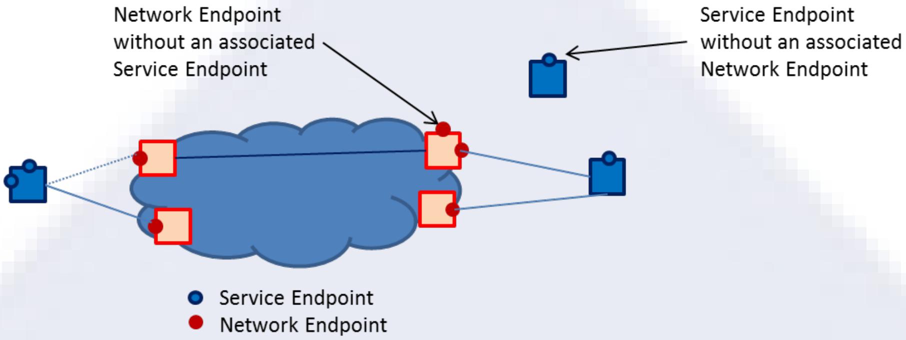
Network Endpoint without an associated Service Endpoint
Service Endpoint without an associated Network Endpoint
● Service Endpoint
● Network Endpoint

Figure A-6 Independence of Service and Network Endpoints

Appendix B: VTNS and ONF T-API

The [OIF SDN API Framework] specifies a set of APIs to be delivered by an SDN controller. The [ONF T-API] specification is an example implementation of these APIs. The following table shows which APIs are used to support the requirement and definition of each VTNS type.

Table B-1: VTNS and ONF T-APIs

ONF T-APIs	VTNS Type A	VTNS Type B	VTNS Type C
Topology Service APIs		√	√
Connectivity Service APIs	√	√	√
Path Computation Service APIs		√	√
Virtual Network Service APIs			√
Notification Service APIs	√	√	√

Appendix C: VTNS and Other Existing Standards

This appendix relates the descriptions of the three VTNS types to more detailed descriptions in published standards. The capabilities described in this section illustrate how detailed VTNS capabilities could be specified.

In the [ONF SDN Architecture 1.1] clients of an SDN controller are supported by individual client contexts. A client context is information such as identifiers and objects held by the SDN controller to support a particular client. One of the objects in the client context can be a representation of the virtual topology the controller is providing to the client. This virtual topology may have varying amount of detail (more or less abstraction). For VTNS Type A, the client has the most abstract virtual topology as it does not have visibility of the network around which its associated clients connect. In Types B and C, greater details of the virtual topology are presented to clients.

C.1 Type A: Dynamic connection service with limited customer control

The Type A service allows customers to request connectivity, but they do not have visibility of network topology. The transport infrastructure for this service can be done with:

- L0 – dynamic L0 service is not standardized with DWDM interfaces so these would need to be specified or remain proprietary
- L1 – dynamic services could be provided by an OIF UNI 2.0.
- A ITU-T Y.1312 L1 VPN. The CE (customer edge device) is connected to the PE (provider edge) with an L1 link. The L1 VPN is a "network formed by a set of CEs and network resources between CEs. A set of CEs is managed by the same authority. Network resources between CEs are provided by the service provider, and may include links, connections and C-plane functionalities". Resource and control combination for the VPN are: ITU-T Y.1312 "shared U-Plane" with "shared C-plane", or "dedicated U-Plane" with "shared C-Plane", or "dedicated U-Plane" with "dedicated C-Plane".
- L2 – MEF UNI type 1 (MEF13) and type 2 (MEF20) do not provide for a CE to request connections. MEF UNI type 3 "allows the UNI-C to request, signal and negotiate EVCs and its associated Service Attributes to the UNI-N" but has not been specified in the MEF. The OIF UNI 2.0 could provide for signaling of EPL and EVPL. GMPLS UNI is another alternative.
- A ITU-T Y.1311 L2 VPN. The CE (customer edge device) is connected to the PE (provider edge) with an L2 link. "Forwarding of user data packets is based on information in the packets' data link layer headers (e.g., DLCI, ATM VCI/VPI, or MAC addresses)." (from ITU-T Y.1314)
- Scheduled calls/connections are not included in ITU-T Y.1312 capabilities.

VPN management for customer and provider has the following services as listed in ITU-T Y.1312 table 7-1:

Item number	Service requirement	Customer	Provider
1	Basic layer 1 service features	Mandatory	Mandatory
2	Dynamic control of layer 1 connection	Mandatory	Mandatory
3	Notification of connection rejection	Mandatory	Mandatory
4	Subscription of multiple VPNs at the service interface		
5	Parallel connection with public network		
6	Authentication		Mandatory
7	Authorization		Mandatory
8	Accounting		

Item number	Service requirement	Customer	Provider
9	Connectivity restrictions		Mandatory
10	Explicit link selection (NOTE – Typically only for DUPN)		
11	Distribution of membership information	Optional	Optional
12	Distribution of member availability information		
13	Transfer of resource information (NOTE – Typically only for DUPN)		
14	Transfer of connectivity information		
15	Transparent transfer of control information between customer entities		
16	Network participation in customer domain routing		
17	Per-VPN policy		Mandatory
18	Selection of L1 class of service (e.g. availability level)	Optional	Optional
19	CNM		
20	Per-CE policy and its management		
21	Transfer of performance information		
22	Transfer of fault information		

C.2 Type B: Fixed virtual network topology with customer connection control

In a Type B service a fixed topology is visible by the customer CEs. Connection setup, modification, and deletion by the customer can be performed including specification of explicit routes. The transport infrastructure for this service can be done with:

- L0 – dynamic L0 service is not standardized with DWDM interfaces so these would need to be specified or remain proprietary
- L1 – dynamic services could be provided by an OIF UNI 2.0 Soft Permanent Connection (essentially the UNI-N) within the CE, with an OIF ENNI between CE and P nodes to provide network topology visibility.
- A ITU-T Y.1312 L1 VPN. The CE (customer edge device) is connected to the PE (provider edge) with an L1 link. The L1 VPN is a “network formed by a set of CEs and network resources between CEs. A set of CEs is managed by the same authority. Network resources between CEs are provided by the service provider,

and may include links, connections and C-plane functionalities". Resource and control combination for the VPN are: Y.1312 "shared U-Plane" with "shared C-plane", or "dedicated U-Plane" with "shared C-Plane", or "dedicated U-Plane" with "dedicated C-Plane".

- L2 –The OIF UNI 2.0 (the UNI-N) could provide for signaling of EPL and EVPL. GMPLS (the INNI) is another alternative.
- A ITU-T Y.1311 L2 VPN. The CE (customer edge device) is connected to the PE (provider edge) with an L2 link. "Forwarding of user data packets is based on information in the packets' data link layer headers (e.g., DLCI, ATM VCI/VPI, or MAC addresses)." (from ITU-T Y.1314)
- Scheduled calls/connections are not included in ITU-T Y.1312 capabilities.
- The [ONF T-API] specification includes capabilities for a client to request a connection between clients of the same the virtual network provided an SDN controller. Clients have visibility of the virtual network.

VPN management for customer and provider has the following services as listed in ITU-T Y.1312 table 7-1:

Item number	Service requirement	Customer	Provider
1	Basic layer 1 service features	Mandatory	Mandatory
2	Dynamic control of layer 1 connection	Mandatory	Mandatory
3	Notification of connection rejection	Mandatory	Mandatory
4	Subscription of multiple VPNs at the service interface		
5	Parallel connection with public network		
6	Authentication		Mandatory
7	Authorization		Mandatory
8	Accounting		
9	Connectivity restrictions		Mandatory
10	Explicit link selection (NOTE – Typically only for DUPN)	Optional	Optional
11	Distribution of membership information	Optional	Optional
12	Distribution of member availability information		
13	Transfer of resource information (NOTE – Typically only for DUPN)	Mandatory	Mandatory
14	Transfer of connectivity information		

Item number	Service requirement	Customer	Provider
15	Transparent transfer of control information between customer entities		
16	Network participation in customer domain routing		
17	Per-VPN policy		Mandatory
18	Selection of L1 class of service (e.g. availability level)	Optional	Optional
19	CNM		
20	Per-CE policy and its management		
21	Transfer of performance information	Optional	Optional
22	Transfer of fault information	Optional	Optional

C.3 Type C: Dynamic virtual network with customer connection control

In a Type C service the customer has a management interface that allows some control over the network topology it uses. Beyond the CE-P link, topology negotiation is possible. Connection setup, modification, and deletion by the customer can be performed including specification of explicit routes. The transport infrastructure for this service can be done with:

- L0 – dynamic L0 service is not standardized with DWDM interfaces so these would need to be specified or remain proprietary
- L1 – dynamic services could be provided by an OIF UNI 2.0 Soft Permanent Connection (essentially the UNI-N) within the CE, with an OIF ENNI between CE and P nodes to provide network topology visibility. There is not a standardized topology specification interface.
- A Y.1312 L1 VPN. The CE (customer edge device) is connected to the PE (provider edge) with an L1 link. The L1 VPN is a “network formed by a set of CEs and network resources between CEs. A set of CEs is managed by the same authority. Network resources between CEs are provided by the service provider, and may include links, connections and C-plane functionalities”. Resource and control combination for the VPN are: Y.1312 “shared U-Plane” with “shared C-plane”, or “dedicated U-Plane” with “shared C-Plane”, or “dedicated U-Plane” with “dedicated C-Plane”.
- L2 –The OIF UNI 2.0 (the UNI-N) could provide for signaling of EPL and EVPL. GMPLS (the INNI) is another alternative.
- A Y.1311 L2 VPN. The CE (customer edge device) is connected to the PE (provider edge) with an L2 link. “Forwarding of user data packets is based on information in the packets' data link layer headers (e.g., DLCI, ATM VCI/VPI, or MAC addresses).” (from Y.1314)

- Scheduled calls/connections are not included in Y.1312 capabilities.
- The draft ONF TAPI specification has support for creation, deletion and retrieval of a virtual network as in Type C, but not for virtual topology modification.

VPN management for customer and provider has the following services as listed in Y.1312 table 7-1:

Item number	Service requirement	Customer	Provider
1	Basic layer 1 service features	Mandatory	Mandatory
2	Dynamic control of layer 1 connection	Mandatory	Mandatory
3	Notification of connection rejection	Mandatory	Mandatory
4	Subscription of multiple VPNs at the service interface		
5	Parallel connection with public network		
6	Authentication		Mandatory
7	Authorization		Mandatory
8	Accounting		
9	Connectivity restrictions		Mandatory
10	Explicit link selection (NOTE – Typically only for DUPN)	Optional	Optional
11	Distribution of membership information	Optional	Optional
12	Distribution of member availability information		
13	Transfer of resource information (NOTE – Typically only for DUPN)	Mandatory	Mandatory
14	Transfer of connectivity information		
15	Transparent transfer of control information between customer entities		
16	Network participation in customer domain routing		
17	Per-VPN policy		Mandatory
18	Selection of L1 class of service (e.g. availability level)	Optional	Optional
19	CNM	Mandatory	

Item number	Service requirement	Customer	Provider
20	Per-CE policy and its management		
21	Transfer of performance information	Optional	Optional
22	Transfer of fault information	Optional	Optional

Appendix D: List of Contributors

We acknowledge the work from the following contributors.

Christoph Gerlach, Eve Varma, Evelyn Roch, Hans-Martin Foisel, Jia He, Jonathan Sadler, Junjie Li, Lyndon Ong, Maarten Vissers, Ruiquan Jin, Sergio Belotti, Stephen Shew, Vishnu Shukla, Yi Lin

Appendix E: List of OIF Members

Acacia Communications	Kandou Bus
ADVA Optical Networking	KDDI R&D Laboratories
Alibaba (China) Co., Ltd	Keysight Technologies, Inc.
AMCC	Lumentum
Amphenol Corp.	MACOM Technology Solutions
Anritsu	Marvell Technology
Broadcom Limited	Mellanox Technologies
Brocade	Microsemi Inc.
BRPhotonics	Microsoft Corporation
China Telecom	Mitsubishi Electric Corporation
Ciena Corporation	Molex
Cisco Systems	MoSys, Inc.
ClariPhy Communications	MRV
Coriant	NEC Corporation
Corning	NeoPhotonics
CPqD	Nokia
Credo Semiconductor (HK) LTD	NTT Corporation
Dell, Inc.	O-Net Communications (HK) Limited
ETRI	Oclaro
Fiberhome Technologies Group	Orange
Finisar Corporation	PETRA
Foxconn Interconnect Technology, Ltd.	QLogic Corporation
Fujikura	Qorvo
Fujitsu	Ranovus
Furukawa Electric Japan	Rianta Solutions, Inc.
Gigamon Inc.	Rockley Photonics
Global Foundries	Samsung Electronics Co. Ltd.
Google	Samtec Inc.
Hewlett Packard Enterprise (HPE)	Semtech
Hitachi	Socionext Inc.
Huawei Technologies Co., Ltd.	Spirent Communications
Infinera	Sumitomo Electric Industries
Inphi	Sumitomo Osaka Cement
Integrated Device Technology	TE Connectivity
Intel	Tektronix
Invecas	Teledyne LeCroy
Ixia	TELUS Communications, Inc.
Juniper Networks	UNH InterOperability Laboratory (UNH-IOL)