Applicability of ACTN to Support Packet and Optical Integration

draft-lee-teas-actn-poi-applicability-00

Abstract

This document outlines the applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to Packet & Optical Integration (POI). It also identifies a number of deployment scenarios to support L3VPN and L2VPN in operator’s networks and provides implementation guidelines.

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/1id-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 20, 2019.

Copyright Notice

Copyright (c) 2019 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 3](#_Toc11939769)

[1.1. Requirements Language 3](#_Toc11939770)

[2. POI with L2/L3VPN Service Under Single Network Operator Control 3](#_Toc11939771)

[2.1. L2/L3VPN/VN Service Request by the Customer 5](#_Toc11939772)

[2.2. Service and Network Orchestration 7](#_Toc11939773)

[2.3. IP/MPLS Domain Controller and NE Functions 10](#_Toc11939774)

[2.3.1. Scenario A: Shared Tunnel Selection 10](#_Toc11939775)

[2.3.1.1. Domain Tunnel Selection 11](#_Toc11939776)

[2.3.1.2. VPN/VRF Provisioning for L3VPN 12](#_Toc11939777)

[2.3.1.3. VSI Provisioning for L2VPN 13](#_Toc11939778)

[2.3.1.4. Inter-domain Links Update 13](#_Toc11939779)

[2.3.1.5. End-to-end Tunnel Management 13](#_Toc11939780)

[2.3.2. Scenario B: Isolated VN/Tunnel Establishment 14](#_Toc11939781)

[2.4. Optical Domain Controller and NE Functions 14](#_Toc11939782)

[2.5. Orchestrator-Controllers-NEs Communication Protocol Flows 16](#_Toc11939783)

[3. POI with VN Recursion Under Multiple Network Operators Control 17](#_Toc11939784)

[3.1. Service Request Process between Multiple Operators 19](#_Toc11939785)

[3.2. Service/network Orchestration of Operator 2 19](#_Toc11939786)

[4. Security Considerations 20](#_Toc11939787)

[5. IANA Considerations 21](#_Toc11939788)

[6. Acknowledgements 21](#_Toc11939789)

[7. References 21](#_Toc11939790)

[7.1. Normative References 21](#_Toc11939791)

[7.2. Informative References 21](#_Toc11939792)

[8. Contributors 22](#_Toc11939793)

[Authors' Addresses 22](#_Toc11939794)

# Introduction

Abstraction and Control of Traffic Engineered Networks (ACTN) describes a set of management and control functions used to operate one or more TE networks to construct virtual networks that can be represented to customers and that are built from abstractions of the underlying TE networks so that, for example, a link in the customer's network is constructed from a path or collection of paths in the underlying networks [RFC8453].

This document outlines the applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to Packet and Optical Integration. It also identifies a number of deployment scenarios to support POI in operator’s networks and provides implementation guidelines.

## 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].

# POI with L2/L3VPN Service Under Single Network Operator Control

This section provides a number of deployment scenarios for packet and optical integration (POI). Specifically, this section provides a deployment scenario in which ACTN hierarchy is deployed to control a multi-layer and multi-domain network via two IP/MPLS PNCs and two Optical PNCs with coordination with L-MDSC. This scenario is in the context of an upper layer service configuration (e.g. L3VPN) across two AS domains which are transported by two transport underlay domains (e.g. OTN).

The provisioning of the L3VPN service is outside ACTN scope but it is worth showing how the L3VPN service provisioning is integrated for the end-to-end service fulfilment in ACTN context. An example of service configuration function in the Service/Network Orchestrator is discussed in [bess-l3vpn].

Figure 1 shows an ACTN POI Reference Architecture where it shows ACTN components as well as non-ACTN components that are necessary for the end-to-end service fulfilment. Both IP/MPLS and Optical Networks are multi-domain. Each IP/MPLS domain network is controlled by its’ domain controller and all the optical domains are controlled by a hierarchy of optical domain controllers. The L-MDSC function of the optical domain controllers provides an abstract view of the whole optical network to the Service/Network Orchestrator. It is assumed that all these components of the network belong to one single network operator domain under the control of the service/network orchestrator.

Customer

+-------------------------------+

| +-----+ +------------+ |

| | CNC |----| Service Op.| |

| +-----+ +------------+ |

+-------|------------------|----+

| ACTN interface | Non-ACTN interface

| CMI | (Customer Service model)

Service/Network| +-----------------+

Orchestrator | |

+-----|------------------------------------|-----------+

| +----------------------------------+ | |

| |MDSC TE & Service Mapping Function| | |

| +----------------------------------+ | |

| | | | |

| +------------------+ +---------------------+ |

| | MDSC NP Function |-------|Service Config. Func.| |

| +------------------+ +---------------------+ |

+------|---------------------------|-------------------+

MPI | +---------------------+--+

| / Non-ACTN interface \

+-------+---/-------+------------+ \

IP/MPLS | / |Optical | \ IP/MPLS

Domain 1 | / |Domain | \ Domain 2

Controller| / |Controller | \ Controller

+------|-------/--+ +---|-----+ +--|-----------\----+

| +-----+ +-----+| | +-----+ | |+------+ +------+|

| |PNC1 | |Serv.|| | |PNC | | || PNC2 | | Serv.||

| +-----+ +----- | | +-----+ | |+------+ +------+|

+-----------------+ +---------+ +-------------------+

SBI | | | SBI

v | V

+------------------+ | +------------------+

/ IP/MPLS Network \ | / IP/MPLS Network \

+----------------------+ | SBI +----------------------+

v

+-------------------------------+

/ Optical Network \

+-----------------------------------+

Figure 1. ACTN POI Reference Architecture

Figure 1 shows ACTN POI Reference Architecture where it depicts:

* CMI (CNC-MDSC Interface) interfacing CNC with MDSC function in the Service/Network Orchestrator. This is where TE & Service Mapping [TSM] and either ACTN VN [ACTN-VN] or TE-topology [TE-Topo]model is exchanged over CMI.
* Customer Service Model Interface: Non-ACTN interface in the Customer Portal interfacing Service/Network Orchestrator’s Service Configuration Function. This is the interface where L3SM information is exchanged.
* MPI (MDSC-PNC Interface) interfacing IP/MPLS Domain Controllers and Optical Domain Controllers.
* Service Configuration Interface: Non-ACTN interface in Service/Network Orchestrator interfacing with the IP/MPLS Domain Controllers to coordinate L2/L3VPN multi-domain service configuration. This is where service specific information such as VPN, VPN binding policy (e.g., new underlay tunnel creation for isolation), etc. are conveyed.
* SBI (South Bound Interface): Non-ACTN interface in the domain controller interfacing network elements in the domain.

Please note that MPI and Service Configuration Interface can be implemented as the same interface with the two different capabilities. The split is just functional but doesn’t have to be also logical.

The following sections are provided to describe key functions that are necessary for the vertical as well as horizontal end-to-end service fulfilment of POI.

## L2/L3VPN/VN Service Request by the Customer

A customer can request L3VPN services with TE requirements using ACTN CMI models (i.e., ACTN VN YANG, TE & Service Mapping YANG) and non-ACTN customer service models such as L2SM/L3SM YANG together. Figure 2 shows detailed control flow between customer and service/network orchestrator to instantiate L2/L3VPN/VN service request.

Customer

+-------------------------------------------+

| +-----+ +------------+ |

| | CNC |--------------| Service Op.| |

| +-----+ +------------+ |

+-------|------------------------|----------+

2. VN & TE/Svc | | 1.L2/3SM

Mapping | | |

| | ^ | |

| | | | |

v | | 3. Update VN | v

| & TE/Svc |

Service/Network | mapping |

Orchestrator | |

+------------------|------------------------|-----------+

| +----------------------------------+ | |

| |MDSC TE & Service Mapping Function| | |

| +----------------------------------+ | |

| | | | |

| +------------------+ +---------------------+ |

| | MDSC NP Function |-------|Service Config. Func.| |

| +------------------+ +---------------------+ |

+-------|-----------------------------------|-----------+

NP: Network Provisioning

Figure 2. Service Request Process

* ACTN VN YANG provides VN Service configuration, as specified in [ACTN-VN].
  + It provides the profile of VN in terms of VN members, each of which corresponds to an edge-to-edge link between customer end-points (VNAPs). It also provides the mappings between the VNAPs with the LTPs and between the connectivity matrix with the VN member from which the associated traffic matrix (e.g., bandwidth, latency, protection level, etc.) of VN member is expressed (i.e., via the TE-topology’s connectivity matrix).
  + The model also provides VN-level preference information (e.g., VN member diversity) and VN-level admin-status and operational-status.
* L2SM YANG [RFC8466] provides all L2VPN service configuration and site information from a customer/service point of view.
* L3SM YANG [RFC8299] provides all L3VPN service configuration and site information from a customer/service point of view.
* The TE & Service Mapping YANG model [TE & Service] provides TE-service mapping as well as site mapping.
  + TE-service mapping provides the mapping of L3VPN instance from [RFC8299] with the corresponding ACTN VN instance.
  + The TE-service mapping also provides the service mapping requirement type as to how each L2/L3VPN/VN instance is created with respect to the underlay TE tunnels (e.g., whether the L3VPN requires a new and isolated set of TE underlay tunnels or not, etc.). See Section 2.2 for detailed discussion on the mapping requirement types.
  + Site mapping provides the site reference information across L2/L3VPN Site ID, ACTN VN Access Point ID, and the LTP of the access link.

## Service and Network Orchestration

The Service/Network orchestrator shown in Figure 1 interfaces the customer and decouples the ACTN MDSC functions from the customer service configuration functions.

An implementation can choose to split the Service/Network orchestration functions, as described in [RFC8309] and in section 4.2 of [RFC8453], between a top-level Service Orchestrator interfacing the customer and two low-level Network Orchestrators, one controlling a multi-domain IP/MPLS network and the other controlling the Optical networks.

Another implementation can choose to combine the L-MDSC functions of the Optical hierarchical controller, providing multi-domain coordination of the Optical network together with the MDSC functions in the Service/Network orchestrator.

Without loss of generality, this assumes that the service/network orchestrator as depicted in Figure 1 would include all the required functionalities as in a hierarchical orchestration case.

One of the important service functions the Service/Network orchestrator performs is to identify which TE Tunnels should carry the L3VPN traffic (from TE & Service Mapping Model) and to relay this information to the IP/MPLS domain controllers, via non-ACTN interface, to ensure proper IP/VRF forwarding table be populated according to the TE binding requirement for the L3VPN.

[Editor’s Note: What mechanism would convey on the interface to the IP/MPLS domain controllers as well as on the SBI (between IP/MPLS domain controllers and IP/MPLS PE routers) the TE binding policy dynamically for the L3VPN? Typically, VRF is the function of the device that participate MP-BGP in MPLS VPN. With current MP-BGP implementation in MPLS VPN, the VRF’s BGP next hop is the destination PE and the mapping to a tunnel (either an LDP or a BGP tunnel) toward the destination PE is done by automatically without any configuration. It is to be determined the impact on the PE VRF operation when the tunnel is an optical bypass tunnel which does not participate either LDP or BGP.

Figure 3 shows service/network orchestrator interactions with various domain controllers to instantiate tunnel provisioning as well as service configuration.

+-------|----------------------------------|-----------+

| +----------------------------------+ | |

| |MDSC TE & Service Mapping Function| | |

| +----------------------------------+ | |

| | | | |

| +------------------+ +---------------------+ |

| | MDSC NP Function |-------|Service Config. Func.| |

| +------------------+ +---------------------+ |

+-------|------------------------------|---------------+

| |

| +-------------------+------+ 3.

2. Inter-layer | / \ VPN Serv.

tunnel +-----+--------/-------+-----------------+ \provision

binding| / | 1. Optical | \

| / | tunnel creation | \

+----|-----------/-+ +---|------+ +-----|-------\---+

| +-----+ +-----+ | | +------+ | | +-----+ +-----+|

| |PNC1 | |Serv.| | | | PNC | | | |PNC2 | |Serv.||

| +-----+ +-----+ | | +------+ | | +-----+ +-----+|

+------------------+ +----------+ +-----------------+

Figure 3. Service and Network Orchestration Process

* TE binding requirement types [TE-service mapping] are:
  1. Hard Isolation with deterministic latency: Customer would request an L3VPN service [RFC8299] using a set of TE Tunnels with a deterministic latency requirement and that cannot be not shared with other L3VPN services nor compete for bandwidth with other Tunnels.
  2. Hard Isolation: This is similar to the above case without deterministic latency requirements.
  3. Soft Isolation: Customer would request an L3VPN service using a set of MPLS-TE tunnel which cannot be shared with other L3VPN services.
  4. Sharing: Customer would accept sharing the MPLS-TE Tunnels supporting its L3VPN service with other services.

For the first three types, there could be additional TE binding requirements with respect to different VN members of the same VN associated with an L3VPN service. For the first two cases, VN members can be hard-isolated, soft-isolated, or shared. For the third case, VN members can be soft-isolated or shared.

* When “Hard Isolation with or w/o deterministic latency” (i.e., the first and the second type) TE binding requirement is applied for a L3VPN, a new optical layer tunnel has to be created (Step 1 in Figure 3). This operation requires the following control level mechanisms as follows:
  + The MDSC function of the Service/Network Orchestrator identifies only the domains in the IP/MPLS layer in which the VPN needs to be forwarded.
  + Once the IP/MPLS layer domains are determined, the MDSC function of the Service/Network Orchestrator needs to identify the set of optical ingress and egress points of the underlay optical tunnels providing connectivity between the IP/MPLS layer domains.
  + Once both IP/MPLS layers and optical layer are determined, the MDSC needs to identify the inter-layer peering points in both IP/MPLS domains as well as the optical domain(s). This implies that the L3VPN traffic will be forwarded to an MPLS-TE tunnel that starts at the ingress PE (in one IP/MPLS domain) and terminates at the egress PE (in another IP/MPLS domain) via a dedicated underlay optical tunnel.
* The MDSC function of the Service/Network Orchestrator needs to first request the optical L-MDSC to instantiate an optical tunnel for the optical ingress and egress. This is referred to as optical tunnel creation (Step 1 in Figure 3). Note that it is L-MDSC responsibility to perform multi-domain optical coordination with its underlying optical PNCs, for setting up a multi-domain optical tunnel.
* Once the optical tunnel is established, then the MDSC function of the Service/Network Orchestrator needs to coordinate with the PNC functions of the IP/MPLS Domain Controllers (under which the ingress and egress PEs belong) the setup of a multi-domain MPLS-TE Tunnel, between the ingress and egress PEs. This setup is carried by the created underlay optical tunnel (Step 2 in Figure 3).
* It is the responsibility of the Service Configuration Function of the Service/Network Orchestrator to identify interfaces/labels on both ingress and egress PEs and to convey this information to both the IP/MPLS Domain Controllers (under which the ingress and egress PEs belong) for proper configuration of the L3VPN (BGP and VRF function of the PEs) in their domain networks (Step 3 in Figure 3).

## IP/MPLS Domain Controller and NE Functions

IP/MPLS networks are assumed to have multiple domains and each domain is controlled by IP/MPLS domain controller in which the ACTN PNC functions and non-ACTN service functions are performed by the IP/MPLS domain controller.

Among the functions of the IP/MPLS domain controller are VPN service aspect provisioning such as VRF control and management for VPN services, etc. It is assumed that BGP is running in the inter-domain IP/MPLS networks for L2/L3VPN and that the IP/MPLS domain controller is also responsible for configuring the BGP speakers within its control domain if necessary.

Depending on the TE binding requirement types discussed in Section 2.2., there are two possible deployment scenarios.

### Scenario A: Shared Tunnel Selection

When the L2/L3VPN does not require isolation (either hard or soft), it can select an existing MPLS-TE and Optical tunnel between ingress and egress PE, without creating any new TE tunnels. Figure 4 shows this scenario.

IP/MPLS Domain 1 IP/MPLS Domain 2

Controller Controller

+------------------+ +------------------+

| +-----+ +-----+ | | +-----+ +-----+ |

| |PNC1 | |Serv.| | | |PNC2 | |Serv.| |

| +-----+ +-----+ | | +-----+ +-----+ |

+--|-----------|---+ +--|-----------|---+

| 1.Tunnel | 2.VPN/VRF | 1.Tunnel | 2.VPN/VRF

| Selection | Provisioning | Selection | Provisioning

V V V V

+---------------------+ +---------------------+

CE / PE tunnel 1 ASBR\ /ASBR tunnel 2 PE \ CE

o--/---o..................o--\--------/--o..................o---\--o

\ / \ /

\ AS Domain 1 / \ AS Domain 2 /

+---------------------+ +---------------------+

End-to-end tunnel

<----------------------------------------------------->

Figure 4. IP/MPLS Domain Controller & NE Functions

How VPN is disseminated across the network is out of the scope of this document. We assume that MP-BGP is running in IP/MPLS networks and VPN is made known to ABSRs and PEs by each IP/MPLS domain controllers. See RFC 4364 [RFC4364] for detailed descriptions on how MP-BGP works.

There are several functions IP/MPLS domain controllers need to provide in order to facilitate tunnel selection for the VPN in both domain level and end-to-end level.

#### Domain Tunnel Selection

Each domain IP/MPLS controller is responsible for selecting its domain level tunnel for the L3VPN. First it needs to determine which existing tunnels would fit for the L2/L3VPN requirements allotted to the domain by the Service/Network Orchestrator (e.g., tunnel binding, bandwidth, latency, etc.). If there are existing tunnels that are feasible to satisfy the L3VPN requirements, the IP/MPLS domain controller selects the optimal tunnel from the candidate pool. Otherwise, an MPLS tunnel with modified bandwidth or a new MPLS Tunnel needs to be setup. Note that with no isolation requirement for the L3VPN, existing MPLS tunnel can be selected. With soft isolation requirement for the L3VPN, an optical tunnel can be shared with other L2/L3VPN services while with hard isolation requirement for the L2/L3VPN, a dedicated MPLS-TE and a dedicated optical tunnel MUST be provisioned for the L2/L3VPN.

#### VPN/VRF Provisioning for L3VPN

Once the domain level tunnel is selected for a domain, the Service Function of the IP/MPLS domain controller maps the L3VPN to the selected MPLS-TE tunnel and assigns a label (e.g., MPLS label) with the PE. Then the PE creates a new entry for the VPN in the VRF forwarding table so that when the VPN packet arrives to the PE, it will be able to direct to the right interface and PUSH the label assigned for the VPN. When the PE forwards a VPN packet, it will push the VPN label signaled by BGP and, in case of option A and B [RFC4364], it will also push the LSP label assigned to the configured MPLS-TE Tunnel to reach the ASBR next hop and forwards the packet to the MPLS next-hop of this MPLS-TE Tunnel.

In case of option C [RFC4364], the PE will push one MPLS LSP label signaled by BGP to reach the destination PE and a second MPLS LSP label assigned to the configured MPLS-TE Tunnel to reach the ASBR next-hop and forward the packet to the MPLS next-hop of this MPLS-TE Tunnel.

With Option C, the ASBR of the first domain interfacing the next domain should keep the VPN label intact to the ASBR of the next domain so that the ASBR in the next domain sees the VPN packets as if they are coming from a CE. With Option B, the VPN label is swapped. With option A, the VPN label is removed.

With Option A and B, the ASBR of the second domain does the same procedure that includes VPN/VRF tunnel mapping and interface/label assignment with the IP/MPLS domain controller. With option A, the ASBR operations are the same as of the PEs. With option B, the ASBR operates with VPN labels so it can see the VPN the traffic belongs to. With option C, the ASBR operates with the end-to-end tunnel labels so it may be not aware of the VPN the traffic belongs to.

This process is repeated in each domain. The PE of the last domain interfacing the destination CE should recognize the VPN label when the VPN packets arrive and thus POP the VPN label and forward the packets to the CE.

#### VSI Provisioning for L2VPN

The VSI provisioning for L2VPN is similar to the VPN/VRF provision for L3VPN. L2VPN service types include:

o Point-to-point Virtual Private Wire Services (VPWSs) that use

LDP-signaled Pseudowires or L2TP-signaled Pseudowires [RFC6074];

o Multipoint Virtual Private LAN Services (VPLSs) that use LDP-

signaled Pseudowires or L2TP-signaled Pseudowires [RFC6074];

o Multipoint Virtual Private LAN Services (VPLSs) that use a Border

Gateway Protocol (BGP) control plane as described in [RFC4761]

And [RFC6624];

o IP-Only LAN-Like Services (IPLSs) that are a functional subset of

VPLS services [RFC7436];

o BGP MPLS-based Ethernet VPN Services as described in [RFC7432]

and [RFC7209];

o Ethernet VPN VPWS specified in [RFC8214] and [RFC7432].

#### Inter-domain Links Update

In order to facilitate inter-domain links for the VPN, we assume that the service/network orchestrator would know the inter-domain link status and its resource information (e.g., bandwidth available, protection/restoration policy, etc.) via some mechanisms (which are beyond the scope of this document). We also assume that the inter-domain links are pre-configured prior to service instantiation.

#### End-to-end Tunnel Management

It is foreseen that the Service/Network orchestrator should control and manage end-to-end tunnels for VPNs per VPN policy.

As discussed in [ACTN-PM], the Orchestrator is responsible to collect domain LSP-level performance monitoring data from domain controllers and to derive and report end-to-end tunnel performance monitoring information to the customer.

### Scenario B: Isolated VN/Tunnel Establishment

When the L3VPN requires hard-isolated Tunnel establishment, optical layer tunnel binding with IP/MPLS layer is necessary. As such, the following functions are necessary.

* The IP/MPLS Domain Controller of Domain 1 needs to send the VRF instruction to the PE:
  + To the Ingress PE of AS Domain 1: Configuration for each L3VPN destination IP address (in this case the remote CE’s IP address for the VPN or any customer’s IP addresses reachable through a remote CE) of the associated VPN label assigned by the Egress PE and of the MPLS-TE Tunnel to be used to reach the Egress PE: so that the proper VRF table is populated to forward the VPN traffic to the inter-layer optical interface with the VPN label.
* The Egress PE, upon the discovery of a new IP address, needs to send the mapping information (i.e., VPN to IP address) to its’ IP/MPLS Domain Controller of Domain 2 which sends, in turn, to the service orchestrator. The service orchestrator would then propagate this mapping information to the IP/MPLS Domain Controller of Domain 1 which sends it, in turn, to the ingress PE so that it may override the VPN/VRF forwarding or VSI forwarding, respectively for L3VPN and L2VPN. As a result, when packets arriving at the ingress PE with that IP destination address, the ingress PE would then forward this packet to the inter-layer optical interface.

[Editor’s Note: in case of hard isolated tunnel required for the VPN, we need to create a separate MPLS TE tunnel and encapsulate the MPLS packets of the MPLS Tunnel into the ODU so that the optical NE would route this MPLS Tunnel to a separate optical tunnel from other tunnels.]

## Optical Domain Controller and NE Functions

Optical network provides the underlay connectivity services to IP/MPLS networks. The multi-domain optical network coordination is performed by the L-MDSC function shown in Figure 1 so that the whole multi-domain optical network appears to the service/network orchestrator as one optical network. The coordination of Packet/Optical multi-layer and IP/MPLS multi-domain is done by the service/network orchestrator where it interfaces two IP/MPLS domain controllers and one optical L-MDSC.

Figure 5 shows how the Optical Domain Controllers create a new optical tunnel and the related interaction with IP/MPLS domain controllers and the NEs to bind the optical tunnel with proper forwarding instruction so that the VPN requiring hard isolation can be fulfilled.

IP/MPLS Domain 1 Optical Domain IP/MPLS Domain 2

Controller Controller Controller

+------------------+ +---------+ +------------------+

| +-----+ +-----+ | | +-----+ | | +-----+ +-----+ |

| |PNC1 | |Serv.| | | |PNC | | | |PNC2 | |Serv.| |

| +-----+ +-----+ | | +-----+ | | +-----+ +-----+ |

+--|-----------|---+ +----|----+ +--|----------|----+

| 2.Tunnel | 3.VPN/VRF | |2.Tunnel | 3.VPN/VRF

| Binding | Provisioning| |Binding | Provisioning

V V | V V

+-------------------+ | +-------------------+

CE / PE ASBR\ | /ASBR PE \ CE

o--/---o o--\----|--/--o o---\--o

\ : / | \ : /

\ : AS Domain 1 / | \ AS Domain 2 : /

+-:-----------------+ | +-----------------:-+

: | :

: | 1. Optical :

: | Tunnel Creation :

: v :

+-:--------------------------------------------------:-+

/ : : \

/ o..................................................o \

| Optical Tunnel |

\ /

\ Optical Domain /

+------------------------------------------------------+

Figure 5. Domain Controller & NE Functions (Isolated Optical Tunnel)

* As discussed in 2.2., in case that VPN has requirement for hard-isolated tunnel establishment, the service/network orchestrator will coordinate across IP/MPLS domain controllers and Optical L-MDSC to ensure the creation of a new optical tunnel for the VPN in proper sequence. Figure 5 shows this scenario.
  + The MDSC of the service/network orchestrator requests the L-MDSC to setup and Optical tunnel providing connectivity between the inter-layer interfaces at the ingress and egress PEs and requests the two IP/MPLS domain controllers to setup an inter-domain IP link between these interfaces
  + The MDSC of the service/network orchestrator then should provide the ingress IP/MPLS domain controller with the routing instruction for the VPN so that the ingress IP/MPLS domain controller would help its ingress PE to populate forwarding table. The packet with the VPN label should be forwarded to the optical interface the MDSC provided.

The Ingress Optical Domain PE needs to recognize MPLS-TE label on its ingress interface from IP/MPLS domain PE and encapsulate the MPLS packets of this MPLS-TE Tunnel into the ODU.

[Editor’s Note: We assumed that the Optical PE is LSR.]

* The Egress Optical Domain PE needs to POP the ODU label before sending the packet (with MPLS-TE label kept intact at the top level) to the Egress PE in the IP/MPLS Domain to which the packet is destined.

[Editor’s Note: If there are two VPNs having the same destination CE requiring non-shared optical tunnels from each other, we need to explain this case with a need for additional Label to differentiate the VPNs]

## Orchestrator-Controllers-NEs Communication Protocol Flows

This section provides generic communication protocol flows across orchestrator, controllers and NEs in order to facilitate the POI scenarios discussed in Section 2.3.2 for dynamic optical Tunnel establishment. Figure 6 shows the communication flows.

+---------+ +-------+ +------+ +------+ +------+ +------+

|Orchestr.| |Optical| |Packet| |Packet| |Ing.PE| |Egr.PE|

| | | Ctr. | |Ctr-D1| |Ctr-D2| | D1 | | D2 |

+---------+ +-------+ +------+ +------+ +------+ +------+

| | | | | |

| | | | |<--BGP--->|

| | | |VPN Update | |

| | | VPN Update|<---------------------|

|<--------------------------------------|(Dest, VPN)| |

| | |(Dest, VPN)| | |

| Tunnel Create | | | | |

|---------------->| | | | |

|(VPN,Ingr/Egr if)| | | | |

| | | | | |

| Tunnel Confirm | | | | |

|<----------------| | | | |

| (Tunnel ID) | | | | |

| | | | | |

| Tunnel Bind | | | | |

|-------------------------->| | | |

| (Tunnel ID, VPN, Ingr if) | Forward. Mapping | |

| | |---------------------->| (1) |

| Tunnel Bind Confirm | (Dest, VPN, Ingr if | |

|<--------------------------| | | |

| | | | | |

| Tunnel Bind | | | | |

|-------------------------------------->| | |

| (Tunnel ID, VPN, Egr if) | | | |

| | | | Forward. Mapping |

| | | |--------------------->|(2)

| | | | (Dest, VPN , Egr if) |

| | Tunnel Bind Confirm | | |

|<--------------------------------------| | |

| | | | | |

Figure 6. Communication Flows for Optical Tunnel Establishment

and binding.

When Domain Packet Controller 1 sends the forwarding mapping information as indicated in (1) in Figure 6, the Ingress PE in Domain 1 will need to provision the VRF forwarding table based on the information it receives. Please see the detailed procedure in Section 2.3.1.2. A similar procedure is to be done at the Egress PE in Domain 2.

# POI with VN Recursion Under Multiple Network Operators Control

[RFC8453] briefly introduces a case for the VN supplied to a customer may be built using resources from different technology layers operated by different operators. For example, one operator may run a packet TE network and use optical connectivity provided by another operator.

Figure 7 extracted from [RFC8453] shows the case where a customer asks for end-to-end connectivity between CE A and CE B, a virtual network. The customer's CNC makes a request to Operator 1's MDSC. The MDSC works out which network resources need to be configured and sends instructions to the appropriate PNCs. However, the link between Q and R is a virtual link supplied by Operator 2: Operator 1 is a customer of Operator 2.

To support this, Operator 1 has a CNC that communicates with Operator 2's MDSC. Note that Operator 1's CNC in Figure 10 is a functional component that does not dictate implementation: it may be embedded in a PNC.

Virtual CE A o===============================o CE B

Network

----- CNC wants to create

Customer | CNC | a VN between CE A

----- and CE B

:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* CMI

:

Operator 1 ---------------------------

| MDSC |

---------------------------

: : :

: : :

----- ------------- -----

| PNC | | PNC | | PNC |

----- ------------- -----

: : : : :

Higher v v : v v

Layer CE A o---P-----Q===========R-----S---o CE B

Network | : |

| : |

| ----- |

| | CNC | | CNC wants to create

| ----- | a VN between Q and R

| : |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* CMI

| : |

Operator 2 | ------ |

| | MDSC | |

| ------ |

| : |

| ------- |

| | PNC | |

| ------- |

\ : : : /

Lower \v v v/

Layer X--Y--Z

Network

Where

--- is a link

=== is a virtual link

Figure 7: VN Recursion with Network Layers

The CMI in Figure 7 interfaces Operator 1’s CNC with Operator 2’s MDSC. The functions to perform and the information carried over the inter-operator CMI are identical to those of the Customer’s CNC and Operator 1’s MDSC. In other words, the two CMIs depicted in Figure 7 are recursive in nature.

## Service Request Process between Multiple Operators

As discussed previously, the reclusiveness principle applies seamlessly over the two CMIs. This implies that Operator 1’s MDSC needs to pass all customer service requirements transparently to Operator 2’s MDSC so that Operator 2 should provision its underlay network tunnels to meet the service requirements of the original customer. The MDSC of Operator 1 should translate/map the original customer’s intent and service requirements and pass down to the corresponding PNC(s) which is(are) responsible for interfacing another operator (in this example, Operator 2) that provides transport services for the segment of the customer’s VN. The PNC in turn performs as a CNC when interfacing its southbound with Operator 2’s MDSC.

It is possible that additional recursive relationships may also exist between Operator 2 and other operators.

## Service/network Orchestration of Operator 2

Operator 2 that provides transport service for Operator 1 may also need to perform service/network orchestration function just as the case for Operator 1.

# Security Considerations

From a security and reliability perspective, ACTN may encounter many risks such as malicious attack and rogue elements attempting to connect to various ACTN components. Furthermore, some ACTN

components represent a single point of failure and threat vector and must also manage policy conflicts and eavesdropping of communication between different ACTN components.

All protocols used to realize the ACTN framework should have rich security features, and customer, application and network data should be stored in encrypted data stores. Additional security risks may still exist. Therefore, discussion and applicability of specific security functions and protocols will be better described in documents that are use case and environment specific.

The CMI will likely be an external protocol interface. Suitable authentication and authorization of each CNC connecting to the MDSC will be required; especially, as these are likely to be implemented by different organizations and on separate functional nodes. Use of the AAA-based mechanisms would also provide role-based authorization methods so that only authorized CNC's may access the different functions of the MDSC.

Where the MDSC must interact with multiple (distributed) PNCs, a PKI-based mechanism is suggested, such as building a TLS or HTTPS connection between the MDSC and PNCs, to ensure trust between the

physical network layer control components and the MDSC. Trust anchors for the PKI can be configured to use a smaller (and potentially non-intersecting) set of trusted Certificate Authorities (CAs) than in the Web PKI. Which MDSC the PNC exports topology information to, and the level of detail (full or abstracted), should also be authenticated, and specific access restrictions and topology views should be configurable and/or policy based.

# IANA Considerations

This document has no IANA actions.

# Acknowledgements

The authors thank Adrian Farrel for useful discussions and their suggestions for this work.

# References

## Normative References

[RFC2119] S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels”, RFC 2119, March 1997.

[RFC8453] D. Ceccarelli and Y. Lee, “Framework for Abstraction and Control of Transport Networks”, RFC 8453, August 2018.

## Informative References

[bgp-l3vpn] D. Jain, et al. “Yang Data Model for BGP/MPLS L3 VPNs”, draft-ietf-bess-l3vpn-yang, work in progress.

[RFC4364] E. Rosen and Y. Rekhter, “BGP/MPLS IP Virtual Private Networks (VPNs)”, RFC 4364, February 2006.

[RFC4761] K. Kompella, Ed., Y. Rekhter, Ed., “Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling”, RFC 4761, January 2007.

[ACTN-VN] Y. Lee, et al., “A Yang Data Model for ACTN VN Operation”, draft-ietf-teas-actn-vn-yang, work in progress.

[TSM] Y. Lee, et al., “Traffic Engineering and Service Mapping Yang Model”, draft-ietf-teas-te-service-mapping-yang, work in progress.

[ACTN-PM] Y. Lee, et al., “YANG models for VN & TE Performance Monitoring Telemetry and Scaling Intent Autonomics”, draft-lee-teas-actn-pm-telemetry-autonomics, work in progress.

[TE-Topo] X. Liu, et al., “YANG Data Model for Traffic Engineering (TE) Topologies”, draft-ietf-teas-yang-te-topo, work in progress.

[RFC6074] E. Rosen, B. Davie, V. Radoaca, and W. Luo, “Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)”, RFC 6074, January 2011.

[RFC6624] K. Kompella, B. Kothari, and R. Cherukuri, “Layer 2 Virtual Private Networks Using BGP for Auto-Discovery and Signaling”, RFC 6624, May 2012.

[RFC7209] A. Sajassi, R. Aggarwal, J. Uttaro, N. Bitar, W. Henderickx, and A. Isaac, “Requirements for Ethernet VPN (EVPN)”, RFC 7209, May 2014.

[RFC7432] A. Sajassi, Ed., et al., “BGP MPLS-Based Ethernet VPN”, RFC 7432, February 2015.

[RFC7436] H. Shah, E. Rosen, F. Le Faucheur, and G. Heron, “IP-Only LAN Service (IPLS)”, RFC 7436, January 2015.

[RFC8214] S. Boutros, A. Sajassi, S. Salam, J. Drake, and J. Rabadan, “Virtual Private Wire Service Support in Ethernet VPN”, RFC 8214, August 2017.

[RFC8309] Q. Wu, W. Liu, and A. Farrel, “Service Model Explained”, RFC 8309, January 2018.

[RFC8299] Q. Wu, S. Litkowski, L. Tomotaki, and K. Ogaki, “YANG Data Model for L3VPN Service Delivery”, RFC 8299, January 2018.

[RFC8466] G. Fioccola, ed., “A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery”, RFC8466, October 2018.

# Contributors

Authors' Addresses

Y. Lee

Futurewei Technologies

Email: [younglee.tx@gmail.com](mailto:younglee.tx@gmail.com)

D. Ceccarelli

Ericsson

Email: [daniele.ceccarelli@ericsson.com](mailto:daniele.ceccarelli@ericsson.com)

J. Tantsura

Apstra

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