RTGWG Working Group
Internet Draft
Intended status: Informational

Daniel King
Lancaster University

Young Lee (Editor)
Huawei

Expires: December 29, 2018

Jeff Tansura
Nuage

Qin Wu
Huawei

Daniele Ceccarelli
Ericsson

June 29, 2018

Applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to Enhanced VPN

draft-lee-rtgwg-actn-applicability-enhanced-vpn-02

Abstract

The Abstraction and Control of Traffic Engineered Networks (ACTN) defines an SDN-based architecture that relies on the concepts of network and service abstraction to detach network and service control from the underlying data plane.

This document outlines the overview of ACTN capability and the applicability of ACTN to Enhanced VPN. In particular, this document also discusses how ACTN features can fulfill some of the requirements of the enhanced VPN, which is also known as VPN+ [VPN+].

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction..3
2. ACTN Overview...3
   2.1. ACTN Virtual Network.......................................4
   2.2. Examples of ACTN Delivering Types of Virtual Networks.....5
      2.2.1. ACTN Used for Virtual Private Line Model............6
      2.2.2. ACTN Used for VPN Delivery Model....................7
      2.2.3. ACTN Used to Deliver a Virtual Customer Network......8
   2.3. Service Mapping from TE to ACTN VN Models.................9
   2.4. ACTN VN KPI telemetry Models..............................10
3. Enhanced VPN and ACTN..10
   3.1. Isolation between VPNs....................................11
   3.2. Guaranteed Performance....................................11
   3.3. Integration...13
   3.4. Dynamic Configuration.....................................13
   3.5. Customized Control Plane..................................14
   3.6. The Gaps..15
4. Security Considerations..16
5. IANA Considerations..17
6. Acknowledgements...17

7. References..17
   7.1. Informative References....................................17
8. Contributors..18
Authors' Addresses...18

1. Introduction

The Abstraction and Control of Traffic Engineered Networks (ACTN) defines an SDN-based architecture that relies on the concepts of network and service abstraction to detach network and service control from the underlying data plane.

This document outlines the overview of ACTN capability and the applicability of ACTN to Enhanced VPN. In particular, this document also discusses how ACTN features can fulfill some of the key requirements of the enhanced VPN, which is also known as VPN+ [VPN+].

2. ACTN Overview

The framework for ACTN [actn-framework] includes a reference architecture that has been adapted for Figure 1 in this document, it describes the functional entities and methods for the coordination of resources across multiple domains, to provide end-to-end services, components include:

- o Customer Network Controller (CNC);
- o Multi-domain Service Coordinator (MDSC);
- o Provisioning Network Controller (PNC).

```
         ---------                 ---------                  ---------
         | CNC-A |                 | CNC-B |                  | CNC-C |
         ---------                 ---------                  ---------
               \                       |                        /
                \__________            |-CMI I/F     __________/
                           \           |            /
                            -------------------------
                            |         MDSC          |
                            -------------------------
                             /      /    |         \
                            /      /     |-MPI I/F  \
                           /      /      |           \
                     -------   -------  -------       -------
```

```
                     | PNC |    | PNC |   | PNC |       | PNC |
                     -------    -------   -------       -------

      CMI - (CNC-MDSC Interface)
      MPI - (MDSC-PNC Interface)
```

Figure 1: ACTN Hierarchy

ACTN facilitates end-to-end connections and provides them to the user. The ACTN framework highlights how:

- o Abstraction of the underlying network resources are provided to higher-layer applications and customers;

- o Virtualization of underlying resources, whose selection criterion is the allocation of those resources for the customer, application, or service;

- o Creation of a virtualized environment allowing operators to view and control multi-domain networks as a single virtualized network;

- o The presentation to customers of networks as a virtual network via open and programmable interfaces.

The ACTN managed infrastructure are traffic engineered network resources, which may include:

- o Statistical packet bandwidth;

- o Physical forwarding plane sources, such as: wavelengths and time slots;

- o Forwarding and cross connect capabilities.

The ACTN type of network virtualization provides customers and applications (tenants) to utilize and independently control allocated virtual network resources as if resources as if they were physically their own resource.

2.1. ACTN Virtual Network

To support multiple clients each with its own view of and control of the server network, a network operator needs to partition the network resources. The resulting partition can be assigned to each client for guaranteed usage which is a step further than shared use of common network resources. See [actn-vn] for detailed ACTN VN and VNS.

An ACTN Virtual Network (VN) is a client view of the ACTN managed infrastructure, and is presented by the ACTN provider as a set of abstracted resources.

Depending on the agreement between client and provider various VN operations and VN views are possible.

- Virtual Network Creation: A VN could be pre-configured and created via static or dynamic request and negotiation between customer and provider. It must meet the specified SLA attributes which satisfy the customer's objectives.

- Virtual Network Operations: The virtual network may be further modified and deleted based on customer request to request changes in the network resources reserved for the customer, and used to construct the network slice. The customer can further act upon the virtual network to manage traffic flow across the virtual network.

- Virtual Network View: The VN topology from a customer point of view. These may be a variety of tunnels, or an entire VN topology. Such connections may comprise of customer end points, access links, intra domain paths and inter-domain links.

Dynamic VN Operations allow a customer to modify or delete the VN. The customer can further act upon the virtual network to create/modify/delete virtual links and nodes. These changes will result in subsequent tunnel management in the operator's networks.

Primitives (capabilities and messages) have been provided to support the different ACTN network control functions that will enable virtual network. These include: topology request/query, VN service request, path computation and connection control, VN service policy negotiation, enforcement, routing options. [actn-info]

2.2. Examples of ACTN Delivering Types of Virtual Networks

In examples below the ACTN framework is used to provide control, management and orchestration for the virtual network life-cycle, and the connectivity. These dynamic and highly flexible, end-to-end and

dedicated virtual network utilizing common physical infrastructure, and according to vertical-specific requirements.

The rest of this section provides three examples of using ACTN to achieve different scenarios of ACTN for virtual network. All three scenarios can be scaled up in capacity or be subject to topology changes as well as changes from customer requirements perspective.

2.2.1. ACTN Used for Virtual Private Line Model

ACTN provides virtual connections between multiple customer locations, requested via Virtual Private Line (VPL) requester (CNC-A). Benefits of this model include:

- o Automated: the service set-up and operation is network provider managed;
- o Virtual: the private line is seamlessly extended from customers Site A (vCE1 to vCE3) and Site B (vCE2 to vCE3) across the ACTN-managed WAN to Site C;
- o Agile: on-demand where the customer needs connectivity and fully adjustable bandwidth.

```
                        (Customer VPL Request)
                                   |
                               ---------
                               | CNC-A |
      Boundary                 ---------
      Between  ====================|====================
      Customer &                   |
      Network Operator          --------
                                | MDSC |
                                --------
                                 __|__
           Site A               ( PNC )              Site B
            ------             (       )             ------
            |vCE1|=============( Phys. )=============|vCE2|
            ------              ( Net )              ------
                  \              -----               /
                   \               ||               /
                    \              ||              /
               VPL 1 \__           ||           __/ VPL 2
                        \          ||          /
                         \         ||         /
```

```
                          \      ------     /
                           ------|vCE3|-----
                                 ------
                                 Site C
```

Figure 2: Virtual Private Line Model

2.2.2. ACTN Used for VPN Delivery Model

ACTN provides VPN connections between multiple sites, requested Via a VPN requestor (CNC-A), which is managed by the customer themselves. The CNC will then interact with the network provider's MDSC. Benefits of this model include:

- Provides edge-to-edge VPN multi-access connection;

- Mostly network provider managed, with some flexibility delegated to the customer managed CNC.

```
             ----------------                            ----------------
             | Site-A Users |___________     ____________| Site-B Users |
             ----------------           |   |            ----------------
                                       -------
                                       |CNC-A|
      Boundary                         -------
      Between   ==========================|==========================
      Customer &                          |
      Network Operator                    |
                                          |
                                   ---------------
                                   |     MDSC    |
                                   ---------------
                         _________/       |       \__________
                        /                 |                  \
                       /                  |                   \
                  ---------           ---------            ---------
                  |  PNC  |           |  PNC  |            |  PNC  |
                  ---------           ---------            ---------
                     |                    |                 /
                     |                    |                /
                   -----                ---          -----
                  (     )              (     )         (     )
     <Site A>----( Phys. )------------( Phys. )-------( Phys. )----<Site B>
                  ( Net )              ( Net )         ( Net )
```

```
                   -----                -----           -----
```

Figure 3: VPN Model

2.2.3. ACTN Used to Deliver a Virtual Customer Network

In this example ACTN provides a virtual network resource to the customer. This resource is customer managed. Empowering the tenant to control allocated VN (recursively). Benefits of this model include:

- The MDSC provides the topology as part of the customer view so that the customer can control their network slice to fit their needs;

- Resource isolation, each customer network slice is fixed and will not be affected by changes to other customer network slices;

- Applications can interact with their assigned network slice directly, the customer may implement their own network control method and traffic prioritization, manage their own addressing scheme, and further slice their assigned network resource;

- The network slice may also include specific capability nodes, delivered as Physical Network Functions (PNFs) or Virtual Network Functions (VNFs).

```
                                                ___________
                     ---------------           (  Virtual  )
                     |    CNC      |---------->( Network 2 )
                     ---------------          _(_________  )
                  ---------------            (  Virtual  )_)
                  |    CNC      |----------->( Network 2 ) ^
                  ---------------            (           ) :
                        ^                    (___________) :
                        |                        ^    ^    :
      Boundary          |                        :    :    :
      Between ==========|========================:====:====:========
      Customer &        |                        :    :    :
      Network Operator  |                        :    :    :
                        v                        :    :    :
                  ---------------                :    :....:
                  |    MDSC     |                :         :
                  ---------------                :         :
                        ^                     ---^------    ...
```

```
                        |                    (          )      .
                        v                   (  Physical  )      .
                    ----------------         ( Network  )        .
                    |     PNC      |<------>  (        )      ---^------
                  ---------------- |           --------      (          )
                  |              |--                        (  Physical  )
                  |    PNC       |<------------------------->( Network  )
                  ---------------                             (        )
                                                               --------
```

Figure 4: Virtual Customer Networks

2.3. Service Mapping from TE to ACTN VN Models

The role of TE-service mapping model [te-service-mapping] is to create a binding relationship across a Layer-3 Service Model [L3sm], Layer-2 Service Model [L2SM], Layer-1 Service Model [L1CSM], and TE Tunnel model [TE-tunnel], via a generic ACTN Virtual Network (VN) model [actn-vn].

The ACTN VN YANG model [actn-vn] is a generic virtual network service model that allows customers (internal or external) to create a VN that meets the customer's service objective with various constraints.

```
            +---------+          +-------------+         +----------+
            |  L3SM   | <------> |             | <-----> | ACTN VN  |
            +---------+          |             |         |  Model   |
                                 |             |         +-----^----+
                                 |             |               |
            +---------+          | TE-Service  |         +-----v----+
            |  L2SM   | <------> |Mapping Model| <-----> | TE-Topo  |
            +---------+          |             |         |   Model  |
                                 |             |         +----------+
                                 |             |
            +---------+          |             |         +----------+
            |  L1CSM  | <------> |             | <-----> | TE-Tunnel|
            +---------+          |             |         |   Model  |
                                 +-------------+         +----------+
```

Figure 5: TE-Service Mapping ([te-service-mapping])

The TE-service mapping model [te-service-map] is needed to bind L1/2/3 VPN specific service requirements and policies pertaining to TE-specific parameters. For example, the model can express the

isolation requirement for each VPN service instance. Some VPN service would require a strict hard isolation with deterministic characteristic. In such case the underlay TE networks has to find end-to-end tunnels/LSPs that satisfy this particular isolation requirement.

This binding will facilitate a seamless service operation with underlay-TE network visibility. The TE-service model developed in this document can also be extended to support other services including L2SM, and L1CSM.

2.4. ACTN VN KPI telemetry Models

The role of ACTN VN KPI telemetry model [actn-pm-telemetry] is to provide YANG models so that customer can define key performance monitoring data relevant for its VN via the YANG subscription model.

Key characteristics of [actn-pm-telemetry] include:

- o an ability to provide scalable VN-level telemetry aggregation based on customer-subscription model for key performance parameters defined by the customer;
- o an ability to facilitate proactive re-optimization and reconfiguration of VNs based on network autonomic traffic engineering scaling configuration mechanism.

3. Enhanced VPN and ACTN

This section discusses how the advanced features of ACTN discussed in Section 3 can fulfill the enhanced VPN requirements defined in [vpn+]. Key requirements of the enhanced VPN include:

1. Isolation between VPNs
2. Guaranteed Performance
3. Integration
4. Dynamic Configuration
5. Customized Control Plane

Simple creation, deletion and modification of the services.
Control over VPN Seamless integration of both physical and virtual network and service functions

In the subsequent sections, we discuss how each requirement can be fulfilled by the ACTN features and the gaps that remain to be solved if applicable.

3.1. Isolation between VPNs

The ACTN VN YANG model [actn-vn] and the TE-service mapping model [te-service-mapping] fulfill the isolation requirement by providing the features.

- o Each VN is identified with a unique identifier (vn-id and vn-name) and so is each VN member that belongs to the VN (vn-member-id).

- o Each instantiated VN is managed and controlled independent of other VNs in the network with proper protection level (protection)

- o Each VN is instantiated with proper isolation requirement mapping introduced by the TE-service mapping model [te-service-mapping]. This mapping can support:

  - o hard isolation with deterministic characteristics (e.g., this case may need optical bypass tunnel to guarantee latency with no jitter);
  - o hard isolation (i.e., dedicated TE resources in all layers (e.g., packet and optical));
  - o soft isolation (i.e., optical layer may be shared while packet layer is dedicated);
  - o no isolation (i.e., sharing with other VN).

3.2. Guaranteed Performance

Performance objectives of a VN need first to be expressed in order to assure the performance guarantee. [actn-vn] and [te-topo] allow configuration of several parameters that may affect the VN performance objectives. Among the performance-related parameters per a VN level provided by [actn-vn] and [te-topo] are as follows:

- o Bandwidth
- o Objective function (e.g., min cost path, min load path, etc.)

- Metric Types and their threshold:
  - TE cost, IGP cost, Hop count, or Unidirectional Delay (e.g., can set all path delay <= threshold)

See the below actn-vn tree structure for the pointer for the connectivity matrix identifier for each vn member in which the configuration parameters listed above is provisioned using [te-topo] model together with [te-tunnel] model in the network.

```
       +--rw vn
          +--rw vn-list* [vn-id]
             +--rw vn-id                 uint32
             +--rw vn-name?              string
             +--rw vn-topology-id?       te-types:te-topology-id
             +--rw abstract-node?        -> /nw:networks/network/node/tet:te-
node-id
             +--rw vn-member-list* [vn-member-id]
             |  +--rw vn-member-id             uint32
             |  +--rw src
             |  |  +--rw src?            -> /actn/ap/access-point-list/access-
point-id
             |  |  +--rw src-vn-ap-id?   -> /actn/ap/access-point-list/vn-ap/
vn-ap-id
             |  |  +--rw multi-src?      boolean {multi-src-dest}?
             |  +--rw dest
             |  |  +--rw dest?            -> /actn/ap/access-point-list/access-
point-
id
             |  |  +--rw dest-vn-ap-id?   -> /actn/ap/access-point-list/vn-ap/
vn-ap-id
             |  |  +--rw multi-dest?      boolean {multi-src-dest}?
             |  +--rw connetivity-matrix-id?   -> /nw:networks/network/node/
tet:te/te-
node-attributes/connectivity-matrices/connectivity-matrix/id
             |  +--ro oper-status?             identityref
             +--ro if-selected?          boolean {multi-src-dest}?
             +--rw admin-status?         identityref
             +--ro oper-status?          identityref
             +--rw vn-level-diversity?   vn-disjointness
```

Once these requests are instantiated, the resources are committed and guaranteed through the life cycle of the VN.

[actn-pm-telemetry] provides models that allow for key performance telemetry configuration mechanisms per VN level, VN member level as well as path/link level.

The following tree structure from [actn-pm-telemetry] illustrates how performance data (e.g., delay, delay-variation, utilization, etc.) can be subscribed per VN need and monitored via YANG push streaming mechanism.

```
   module: ietf-actn-te-kpi-telemetry
     augment /actn-vn:actn/actn-vn:vn/actn-vn:vn-list/actn-vn:vn-member-list:
       +--ro vn-member-telemetry
          +--ro unidirectional-delay?                 uint32
          +--ro unidirectional-min-delay?             uint32
          +--ro unidirectional-max-delay?             uint32
          +--ro unidirectional-delay-variation?       uint32
          +--ro unidirectional-packet-loss?           decimal64
          +--ro unidirectional-residual-bandwidth?    rt-types:bandwidth-ieee-
float32
          +--ro unidirectional-available-bandwidth?   rt-types:bandwidth-ieee-
float32
          +--ro unidirectional-utilized-bandwidth?    rt-types:bandwidth-ieee-
float32
          +--ro bidirectional-delay?                  uint32
          +--ro bidirectional-min-delay?              uint32
          +--ro bidirectional-max-delay?              uint32
          +--ro bidirectional-delay-variation?        uint32
          +--ro bidirectional-packet-loss?            decimal64
          +--ro bidirectional-residual-bandwidth?     rt-types:bandwidth-ieee-
float32
          +--ro bidirectional-available-bandwidth?    rt-types:bandwidth-ieee-
float32
          +--ro bidirectional-utilized-bandwidth?     rt-types:bandwidth-ieee-
float32
          +--ro utilized-percentage?                  uint8
          +--ro vn-ref?                               -> /actn-vn:actn/vn/vn-
list/vn-
   id
          +--ro vn-member-ref?                        -> /actn-vn:actn/vn/vn-
list/vn-
   member-list/vn-member-id
          +--ro te-grouped-params*                    ->
   /te:te/tunnels/tunnel/state/te-kpi:te-telemetry/id
       ......
```

3.3. Integration

ACTN provides mechanisms to correlate customer's VN and the actual TE tunnels instantiated in the provider's network. Specifically,

- o Link each VN member to actual TE tunnel
- o Each VN can be monitored on a various level such as VN level, VN member level, TE-tunnel level, and link/node level.

Service function integration with network topology (L3 and TE topology) is in progress in [sf-topology]. Specifically, [sf-topology] addresses a number of use-cases that how TE topology supports various service functions.

3.4. Dynamic Configuration

ACTN provides an architecture that allows the customer network controller (CNC) interacts with the MDSC which is network provider's

SDN controller in such a way that customer is given the control of their VNs.

Specifically, the ACTN VN model [actn-vn] allows the following capabilities:

- o Dynamic control over VN the customer creates.
  - o Create, Modify, Delete

See the following tree structure from [actn-vn] as an example for the dynamic configuration capability (write) VN creation, modify and delete. VN can be dynamically created/modified/deleted with constraints such as metric types (e.g., delay), bandwidth, protection, etc.

```
   +--rw vn
       +--rw vn-list* [vn-id]
          +--rw vn-id                 uint32
          +--rw vn-name?              string
          +--rw vn-topology-id?       te-types:te-topology-id
          +--rw abstract-node?        -> /nw:networks/network/node/tet:te-node-
id
          +--rw vn-member-list* [vn-member-id]
          |  +--rw vn-member-id             uint32
          |  +--rw src
          |  |  +--rw src?            -> /actn/ap/access-point-list/access-
point-id
          |  |  +--rw src-vn-ap-id?   -> /actn/ap/access-point-list/vn-ap/vn-
ap-id
          |  |  +--rw multi-src?      boolean {multi-src-dest}?
          |  +--rw dest
          |  |  +--rw dest?            -> /actn/ap/access-point-list/access-
point-id
          |  |  +--rw dest-vn-ap-id?   -> /actn/ap/access-point-list/vn-ap/vn-
ap-id
          |  |  +--rw multi-dest?      boolean {multi-src-dest}?
          |  +--rw connetivity-matrix-id?   -> /nw:networks/network/node/
tet:te/te-
node-attributes/connectivity-matrices/connectivity-matrix/id
          |  +--ro oper-status?             identityref
          +--ro if-selected?          boolean {multi-src-dest}?
          +--rw admin-status?         identityref
          +--ro oper-status?          identityref
          +--rw vn-level-diversity?   vn-disjointness
```

3.5. Customized Control Plane

ACTN provides a YANG model that allows the customer network controller (CNC) to control VN via type 2 operation. Type 2 VN allows the customer to provision pertinent LSPs that connect their endpoints over the customized VN topology dynamically.

See the following tree structure from [actn-vn] as an example for the provisioning of LSPs over the VN topology via TE-topology's [TE-Topo] Connectivity Matrix's construct.

For some VN members of a VN, the customers are allowed to configure the actual path (i.e., detailed virtual nodes and virtual links) over the VN/abstract topology agreed mutually between CNC and MDSC prior to or a topology created by the MDSC as part of VN instantiation. Type 2 VN is always built on top of a Type 1 VN. If a Type 2 VN is desired for some or all of VN members of a type 1 VN (see the example in Section 2.1 of [ACTN-VN]), the TE-topology model can provide the following abstract topology (that consists of virtual nodes and virtual links) which is built on top of the Type 1 VN so that customers can configure path over this topology.

```
                 +----------------------------------------------+
                 |             S1               S2              |
                 |              O---------------O               |
                 |     ________/ \______         \              |
                 |    /                 \         \             |
                 |S3 /                   \ S4      \ S5         |
           L1----|-O----------------------O---------O-----------|------L4
                 |   \                     \         \          |
                 |    \                     \         \         |
                 |     \ S6                  \ S7      \ S8     |
                 |      O     ----------------O---------O-------|------L7
                 |     / \   /                 \   ____/        |
                 |S9  /   \ /S10                \ /             |
          L2-----|---O-----O---------------------O--------------|------L8
                 |  /                          S11              |
          L3-----|--                                            |
                 |                                              |
                 +----------------------------------------------+
```

Figure 3. Type 2 topology

3.6. The Gaps

ACTN allows the customers/users to subscribe and monitor VN/Tunnel level performance data such as latency. The low level latency and isolation characteristics that are sought by some VPN+ users such as

steering packets through specific queues resources are not in the scope of ACTN.

This implies that the device-level performance data such as queuing delay caused by various queuing mechanisms needs to be characterized and monitored by a device level YANG PM model. Then the Domain SDN controller (PNC) will need to estimate Domain LSP level PM data from device-level PM data. Finally, the MDSC will need to derive VN/Tunnel level PM data and present to the customers.

Another gap that needs to be filled up is how to coordinate non-TE element from the routing and signaling standpoints. Currently, ACTN is limited to TE elements. From an end-to-end network standpoint, the scope of VPN+ may encompass non-TE elements in some segments/domains as well as TE elements. How to seamlessly provide end-to-end tunnel management and the operations of abstraction of resources across non-TE and TE elements of the network will need to be worked out further.

4. Security Considerations

Virtual network instantiation involves the control of network resources in order to meet the service requirements of consumers. In some deployment models, the consumer is able to directly request modification in the behaviour of resources owned and operated by a service provider. Such changes could significantly affect the service provider's ability to provide services to other consumers. Furthermore, the resources allocated for or consumed by a consumer will normally be billable by the service provider.

Therefore, it is crucial that the mechanisms used in any virtual network system allow for authentication of requests, security of those requests, and tracking of resource allocations.

It should also be noted that while the partitioning of resources is virtual, the consumers expect and require that there is no risk of leakage of data from one slice to another, no transfer of knowledge of the structure or even existence of other virtual networks, and that changes to one virtual network (under the control of one consumer) should not have detrimental effects on the operation of other virtual networks (whether under control of different or the same consumers) beyond the limits allowed within the SLA. Thus, virtual networks are assumed to be private and to provide the appearance of genuine physical connectivity.

ACTN operates using the [netconf] or [restconf] protocols and

assumes the security characteristics of those protocols. Deployment models for ACTN should fully explore the authentication and other security aspects before networks start to carry live traffic.

5. IANA Considerations

This document has no actions for IANA.

6. Acknowledgements

Thanks to James Guichard, Stewart Bryant, Dong Jie for their insight and useful discussions about VPN+.

7. References

7.1. Informative References

[actn-framework] Ceccarelli, D. and Y. Lee, "Framework for Abstraction and Control of Traffic Engineered Networks", draft-ietf-teas-actn-framework, work in progress, February 2017.

[te-service-map] Y. Lee, D. Dhody, and D. Ceccarelli, "Traffic Engineering and Service Mapping Yang Model", draft-lee-teas-te-service-mapping-yang, work in progress.

[actn-vn] Y. Lee (Editor), "A Yang Data Model for ACTN VN Operation", draft-lee-teas-actn-vn-yang, work in progress.

[actn-info] Y. Lee, S. Belotti (Editors), "Information Model for Abstraction and Control of TE Networks (ACTN)", draft-ietf-teas-actn-info-model, work in progress.

[actn-pm-elemetry] Y. Lee, et al, "YANG models for ACTN TE Performance Monitoring Telemetry and Network Autonomics",draft-lee-teas-actn-pm-telemetry-autonomics, work in progress.

[vpn+] S. Bryant, and D. Jie, "Enhanced Virtual Private Networks (VPN+)", draft-bryant-rtgwg-enhanced-vpn, work in progress.

[TE-Tunnel] T. Saad (Editor), "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te, 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.

[L3SM] S. Litkowski, L.Tomotaki, and K. Ogaki, "YANG Data Model for L3VPN service delivery", draft-ietf-l3sm-l3vpn-service-model, work in progress.

[L2SM] B. Wen, et al, "A YANG Data Model for L2VPN Service Delivery", draft-ietf-l2sm-l2vpn-service-model, work in progress.

[L1CSM] G. Fioccola, et al, "A Yang Data Model for L1 Connectivity Service Model (L1CSM)", draft-fioccola-ccamp-l1csm-yang, work in progress.

8. Contributors

Authors' Addresses

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

Young Lee (Editor)
Huawei
Phone: (469)277-5838
Email: leeyoung@huawei.com

Jeff Tansura
Futurewei
Email: jefftant.ietf@gmail.com

Qin Wu
Huawei Technologies Co.,Ltd.
Email: bill.wu@huawei.com

Daniele Ceccarelli
Ericsson
Email: daniele.ceccarelli@ericsson.com