TEAS Working Group
Internet Draft
Intended status: Informational
Expires: November 2016

Daniele Ceccarelli (Ed)
Ericsson
Young Lee (Ed)
Huawei

April 14, 2016

Framework for Abstraction and Control of Traffic Engineered Networks

draft-ceccarelli-teas-actn-framework-02

Status of this Memo

Copyright Notice

Abstract

Traffic Engineered networks have a variety of mechanisms to facilitate the
separation of the data plane and control plane. They also have a range of management and provisioning protocols to configure and activate network resources. These mechanisms represent key technologies for enabling flexible and dynamic networking.

Abstraction of network resources is a technique that can be applied to a single network domain or across multiple domains to create a single virtualized network that is under the control of a network operator or the customer of the operator that actually owns the network resources.

This draft provides a framework for Abstraction and Control of Traffic Engineered Networks (ACTN).

Table of Contents

1. Introduction

Traffic Engineered networks have a variety of mechanisms to facilitate separation of data plane and control plane including distributed signaling for path setup and protection, centralized path computation for planning and traffic engineering, and a range of management and provisioning protocols to configure and activate network resources. These mechanisms represent key technologies for enabling flexible and dynamic networking.

The term Traffic Engineered Network in this draft refers to any connection-oriented network that has the ability of dynamic provisioning, abstracting and orchestrating network resource to the network's clients. Some examples of networks that are in scope of this definition are optical networks, MPLS Transport Profile (MPLS-TP), MPLS Traffic Engineering (MPLS-TE), and other emerging technologies with connection-oriented behavior.

One of the main drivers for Software Defined Networking (SDN) is a decoupling of the network control plane from the data plane. This separation of the control plane from the data plane has been already achieved with the development of MPLS/GMPLS [GMPLS] and PCE [PCE] for TE-based transport networks. One of the advantages of SDN is its logically centralized control regime that allows a global view of the underlying network under its control. Centralized control in SDN helps improve network resources utilization compared with distributed network control. For TE-based transport network control, PCE is essentially equivalent to a logically centralized control for path computation function.

Two key aspects that need to be solved by SDN are:

- Network and service abstraction: Detach the network and service control from underlying technology and help customer express the network as desired by business needs.

- Coordination of resources across multiple domains and multiple layers to provide end-to-end services regardless of whether the domains use SDN or not.

As networks evolve, the need to provide resource and service abstraction has emerged as a key requirement for operators; this implies in effect the virtualization of network resources so that the network is "sliced" for different tenants shown as a dedicated portion of the network resources

Particular attention needs to be paid to the multi-domain case, where Abstraction and Control of Traffic Engineered Networks (ACTN) can facilitate virtual network operation via the creation of a single virtualized network or a seamless service. This supports operators in viewing and controlling different domains (at any dimension: applied technology, administrative zones, or vendor-specific technology islands) as a single virtualized network.

Network virtualization refers to allowing the customers of network operators (see Section 2.1) to utilize a certain amount of network resources as if they own them and thus control their allocated resources with higher layer or application processes that enables the resources to be used in the most optimal way. More flexible, dynamic customer control capabilities are added to the traditional VPN along with a customer specific virtual network view. Customers control a view of virtual network resources, specifically allocated to each one of them. This view is called an abstracted network topology. Such a view may be specific to a specific service, the set of consumed resources or to a particular customer. Customer controller of the virtual network is envisioned to support a plethora of distinct applications. This means that there may be a further level of virtualization that provides a view of resources in the customer's virtual network for use by an individual application.

The framework described in this draft is named Abstraction and Control of Traffic Engineered Network (ACTN) and facilitates:

- Abstraction of the underlying network resources to higher-layer applications and customers [TE-INFO].

- Virtualization of particular underlying resources, whose selection criterion is the allocation of those resources to a particular customer, application or service. [ONF-ARCH]

- Slicing infrastructure to connect multiple customers to meet specific customer's service requirements.

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

- Possibility of providing a customer with virtualized network or services (totally hiding the network).

- A virtualization/mapping network function that adapts customer requests to the virtual resources (allocated to them) to the supporting physical network control and performs the necessary mapping, translation, isolation and security/policy enforcement, etc.; This function is often referred to as orchestration.

- The presentation of the networks as a virtualized topology to the customers via open and programmable interfaces. This allows for the recursion of controllers in a customer-provider relationship.

1.1. Terminology

The following terms are used in this document. Some of them are newly defined, some others reference existing definition:

- Node: A node is a topological entity describing the "opaque" forwarding aspect of the topological component which represents the opportunity to enable forwarding between points at the edge of the node. It provides the context for instructing the formation, adjustment and removal of the forwarding. A node, in a VN network, can be represented by single physical entity or by a group of nodes moving from physical to virtual network.

- Link: A link is a topological entity describing the effective adjacency between two or more forwarding entities, such as two or more nodes. In its basic form (i.e., point-to-point Link) it associates an edge point of a node with an equivalent edge point on another node. Links in virtual network is in fact connectivity, realized by bandwidth engineering between any two nodes meeting certain criteria, for example, redundancy, protection, latency, not tied to any technology specific characteristics like timeslots or wavelengths. The link can be dynamic, realized by a service in underlay, or static.

- PNC domain: A PNC domain includes all the resources under the control of a single PNC. It can be composed by different routing domains, administrative domains and different layers. The interconnection between PNC domains can be a link or a node.

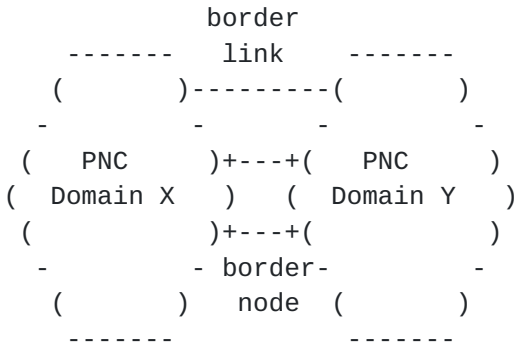

Figure 1 : PNC domain borders

- Virtual Network: A Virtual Network (VN) is a customer view of the transport network. It is composed by a set of physical resources sliced in the provider network and presented to the customer as a set of abstract resources i.e. virtual nodes and virtual links. Depending on the agreement between customer and provider a VN can be just represented by:

  - o How the end points can be connected with given SLA attributes(e.g., re satisfying the customer's objectives)
  - o A pre-configured set of physical resources
  - o Or as outcome of a dynamic request from customer.

  In the first case the VN can be seen at customer level as an e2e connectivity that can be formed by recursive aggregation of lower layers tunnels within the provider domain.
  When the VN is pre-configured, it is provided after a static negotiation between customer and provider while in the third case VN can be dynamically created, deleted, or modified in response to requests from the customer. This implies dynamic changes of network resources reserved for the customer.
  In the second and third case , once that customer has obtained his VN, can act upon the virtual network resources to perform connection management (set-up/release/modify connections).

- Abstract Topology: Every lower controller in the provider network, when is representing its network topology to an higher layer, it may want to hide details of the actual network topology. In such case, an abstract topology may be used for this purpose. Abstract topology enhances scalability for the MDSC to operate multi-domain networks

- Access link: A link between a customer node and a provider node.

- Inter domain link: A link between domains managed by different PNCs. The MDSC is in charge of managing inter-domain links.

- Border node: A node whose interfaces belong to different domains. It may be managed by different PNCs or by the MDSC.

- Access Point (AP): An access point is defined on an access link. It is used to keep confidentiality between the customer and the provider. It is an identifier shared between the customer and the provider, used to map the end points of the border node in the provider NW. The AP can be used by the customer when requesting connectivity service to the provider. A number of parameters, e.g. available bandwidth, need to be associated to the AP to qualify it.

- VN Access Point (VNAP): A VNAP is defined within an AP as part of a given VN and is used to identify the portion of the AP, and hence of the access link) dedicated to a given VN.

2. Business Model of ACTN

The Virtual Private Network (VPN) [RFC4026] and Overlay Network (ON) models [RFC4208] are built on the premise that one single network provider provides all virtual private or overlay networks to its customers. These models are simple to operate but have some disadvantages in accommodating the increasing need for flexible and dynamic network virtualization capabilities.

The ACTN model is built upon entities that reflect the current landscape of network virtualization environments. There are three key entities in the ACTN model [ACTN-PS]:

- Customers
- Service Providers
- Network Providers

2.1. Customers

Within the ACTN framework, different types of customers may be taken into account depending on the type of their resource needs, on their

number and type of access. As example, it is possible to group them into two main categories:

Basic Customer: Basic customers include fixed residential users, mobile users and small enterprises. Usually the number of basic customers is high; they require small amounts of resources and are characterized by steady requests (relatively time invariant). A typical request for a basic customer is for a bundle of voice services and internet access. Moreover basic customers do not modify their services themselves; if a service change is needed, it is performed by the provider as proxy and they generally have very few dedicated resources (subscriber drop), with everything else shared on the basis of some SLA, which is usually best-efforts.

Advanced Customer: Advanced customers typically include enterprises, governments and utilities. Such customers can ask for both point to point and multipoint connectivity with high resource demand significantly varying in time and from customer to customer. This is one of the reasons why a bundled service offering is not enough and it is desirable to provide each of them with a customized virtual network service.

Advanced customers may own dedicated virtual resources, or share resources. They may also have the ability to modify their service parameters within the scope of their virtualized environments.

As customers are geographically spread over multiple network provider domains, they have to interface multiple providers and may have to support multiple virtual network services with different underlying objectives set by the network providers. To enable these customers to support flexible and dynamic applications they need to control their allocated virtual network resources in a dynamic fashion, and that means that they need an abstracted view of the topology that spans all of the network providers.

ACTN's primary focus is Advanced Customers.

Customers of a given service provider can in turn offer a service to other customers in a recursive way. An example of recursiveness with 2 service providers is shown below.

- Customer (of service B)
- Customer (of service A) & Service Provider (of service B)
- Service Provider (of service A)
- Network Provider

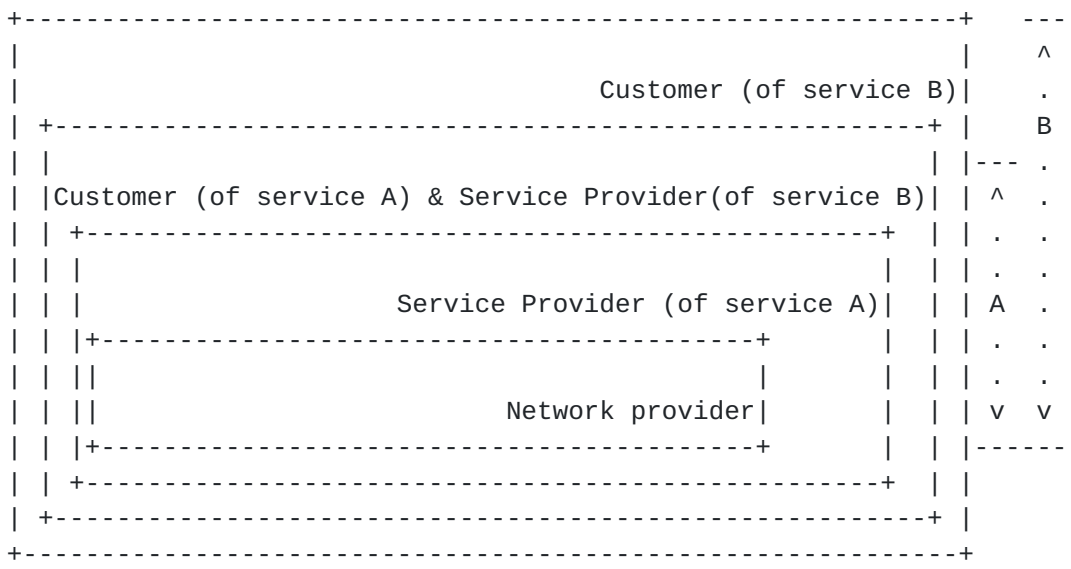

Figure 2 : Service Recursiveness.

2.2. Service Providers

Service providers are the providers of virtual network services to their customers. Service providers may or may not own physical network resources. When a service provider is the same as the network provider, this is similar to traditional VPN models. This model works well when the customer maintains a single interface with a single provider. When customer location spans across multiple independent network provider domains, then it becomes hard to facilitate the creation of end-to-end virtual network services with this model.

A more interesting case arises when network providers only provide infrastructure while service providers directly interface their customers. In this case, service providers themselves are customers of the network infrastructure providers. One service provider may need to keep multiple independent network providers as its end-users span geographically across multiple network provider domains as shown in Figure 2 where Service Provider A uses resources from Network Provider A and Network Provider B to offer a virtualized network to its customer.

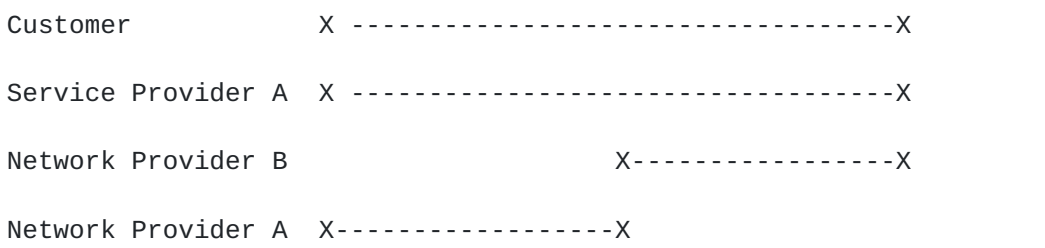

Figure 3 : A service Provider as Customer of Two Network Providers.

The ACTN network model is predicated upon this three tier model and is summarized in Figure 3:

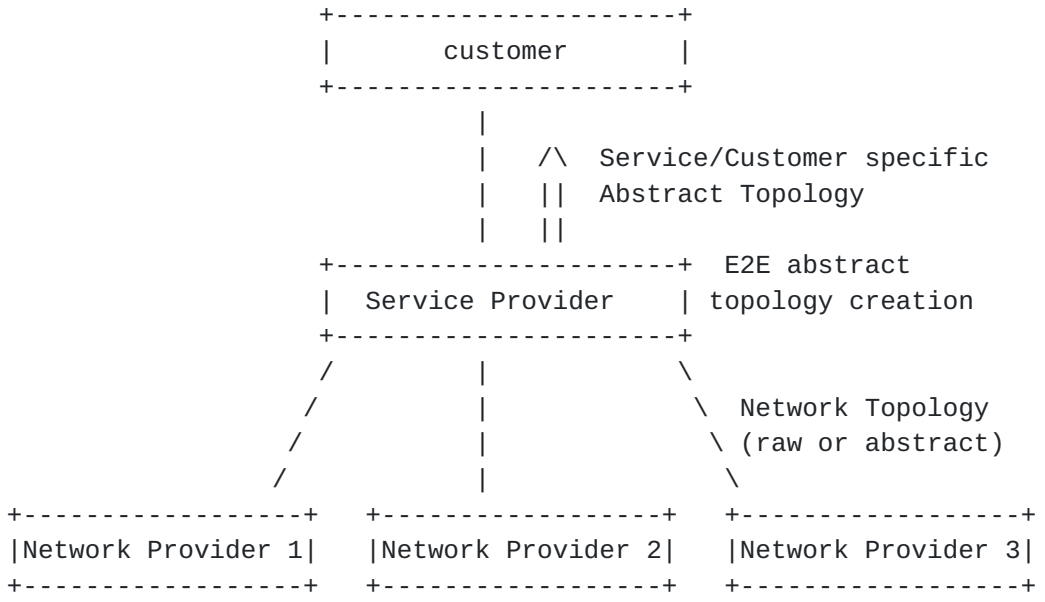

Figure 4 : Three tier model.

There can be multiple types of service providers.

- Data Center providers: can be viewed as a service provider type as they own and operate data center resources to various WAN customers, they can lease physical network resources from network providers.
- Internet Service Providers (ISP): can be a service provider of internet services to their customers while leasing physical network resources from network providers.
- Mobile Virtual Network Operators (MVNO): provide mobile services to their end-users without owning the physical network infrastructure.

2.3. Network Providers

Network Providers are the infrastructure providers that own the physical network resources and provide network resources to their customers. The layered model proposed by this draft separates the concerns of network providers and customers, with service providers acting as aggregators of customer requests.

3. ACTN architecture

This section provides a high-level control and interface model of ACTN.

The ACTN architecture, while being aligned with the ONF SDN architecture [ONF-ARCH], is presenting a 3-tiers reference model. It allows for hierarchy and recursiveness not only of SDN controllers but also of traditionally controlled domains. It defines three types of controllers depending on the functionalities they implement. The main functionalities that are identified are:

- Multi domain coordination function: With the definition of domain being "everything that is under the control of the same controller",it is needed to have a control entity that oversees the specific aspects of the different domains and to build a single abstracted end-to-end network topology in order to coordinate end-to-end path computation and path/service provisioning.

- Virtualization/Abstraction function: To provide an abstracted view of the underlying network resources towards customer, being it the client or a higher level controller entity. It includes computation of customer resource requests into virtual network paths based on the global network-wide abstracted topology and the creation of an abstracted view of network slices allocated to each customer, according to customer-

specific virtual network objective functions, and to the customer traffic profile.

. Customer mapping function: In charge of mapping customer VN setup commands into network provisioning requests to the Physical Network Controller (PNC) according to business OSS/NMS provisioned static or dynamic policy. Moreover it provides mapping and translation of customer virtual network slices into physical network resources

. Virtual service coordination: Virtual service coordination function in ACTN incorporates customer service-related knowledge into the virtual network operations in order to seamlessly operate virtual networks while meeting customer's service requirements.

The virtual services that are coordinated under ACTN can be split into two categories:

. Service-aware Connectivity Services: This category includes all the network service operations used to provide connectivity between customer end-points while meeting policies and service related constraints. The data model for this category would include topology entities such as virtual nodes, virtual links, adaptation and termination points and service-related entities such as policies and service related constraints. (See Section 4.2.2)

. Network Function Virtualization Services: These kinds of services are usually setup in NFV (e.g. cloud) providers and require connectivity between a customer site and the NFV provider site (e.g. a data center). These VNF services may include a security function like firewall, a traffic optimizer, the provisioning of storage or computation capacity. In these cases the customer does not care whether the service is implemented in a given data center or another. This allows the network provider divert customer requests where most suitable. This is also known as "end points mobility" case. (See Section 4.2.3)

The types of controller defined are shown in Figure 4 below and are the following:

. CNC - Customer Network Controller
. MDSC - Multi Domain Service Coordinator

. PNC - Physical Network Controller

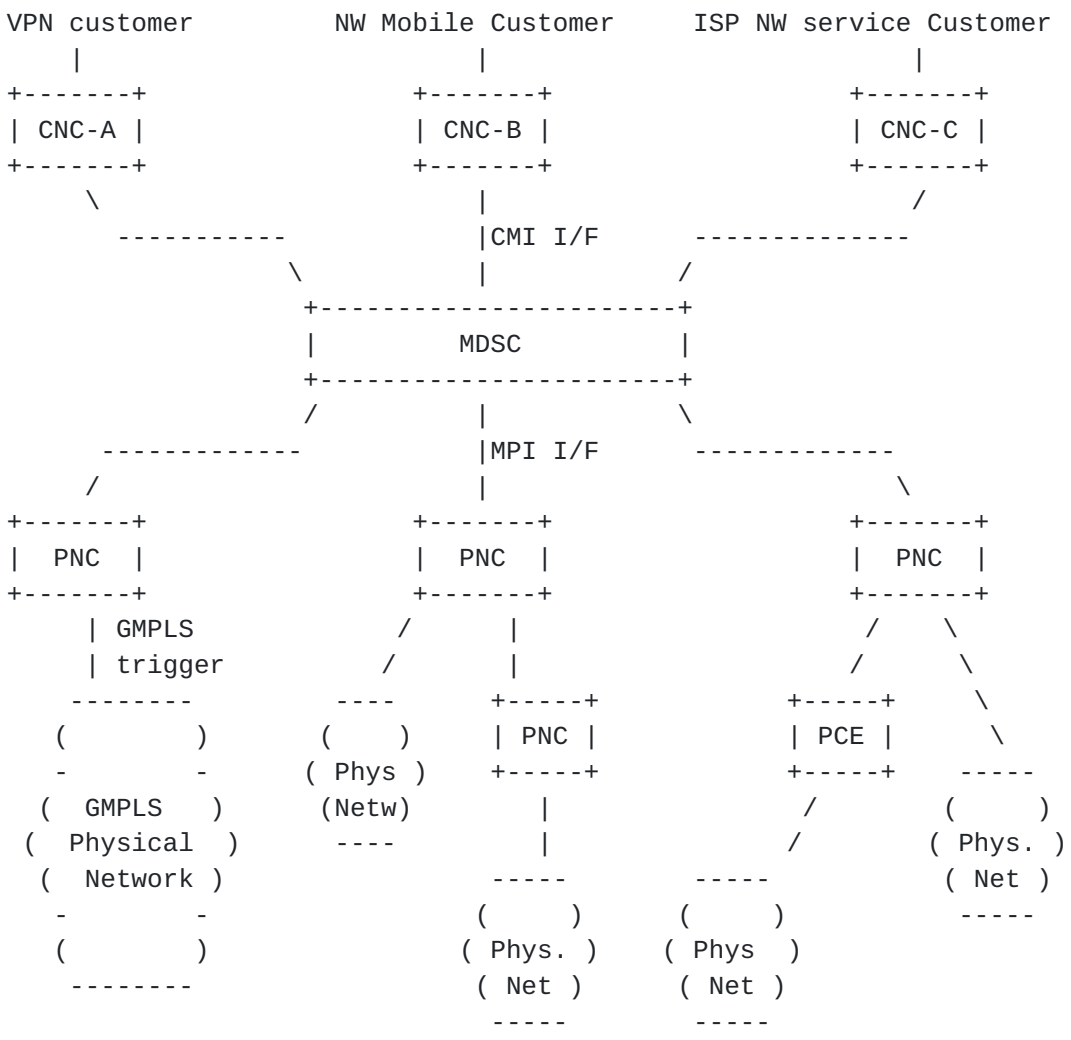

Figure 5 : ACTN Control Hierarchy

3.1. Customer Network Controller

A Virtual Network Service is instantiated by the Customer Network Controller via the CMI (CNC-MDSC Interface). As the Customer Network Controller directly interfaces the applications, it understands multiple application requirements and their service needs. It is assumed that the Customer Network Controller and the MDSC have a common knowledge on the end-point interfaces based on their business negotiation prior to service instantiation. End-point interfaces refer to customer-network physical interfaces that connect customer premise equipment to network provider equipment.

In addition to abstract networks, ACTN allows to provide the CNC with services. Example of services include connectivity between one of the customer's end points with a given set of resources in a data center from the service provider.

3.2. Multi Domain Service Coordinator

The MDSC (Multi Domain Service Coordinator) sits between the CNC (the one issuing connectivity requests) and the PNCs (Physical Network Controllersr - the ones managing the physical network resources). The MDSC can be collocated with the PNC, especially in those cases where the service provider and the network provider are the same entity.

The internal system architecture and building blocks of the MDSC are out of the scope of ACTN. Some examples can be found in the Application Based Network Operations (ABNO) architecture [ABNO] and the ONF SDN architecture [ONF-ARCH].

The MDSC is the only building block of the architecture that is able to implement all the four ACTN main functionalities, i.e. multi domain coordination function, virtualization/abstraction function, customer mapping function and virtual service coordination. The key point of the MDSC and the whole ACTN framework is detaching the network and service control from underlying technology and help customer express the network as desired by business needs. The MDSC envelopes the instantiation of right technology and network control to meet business criteria. In essence it controls and manages the primitives to achieve functionalities as desired by CNC
A hierarchy of MDSCs can be foreseen for scalability and administrative choices.

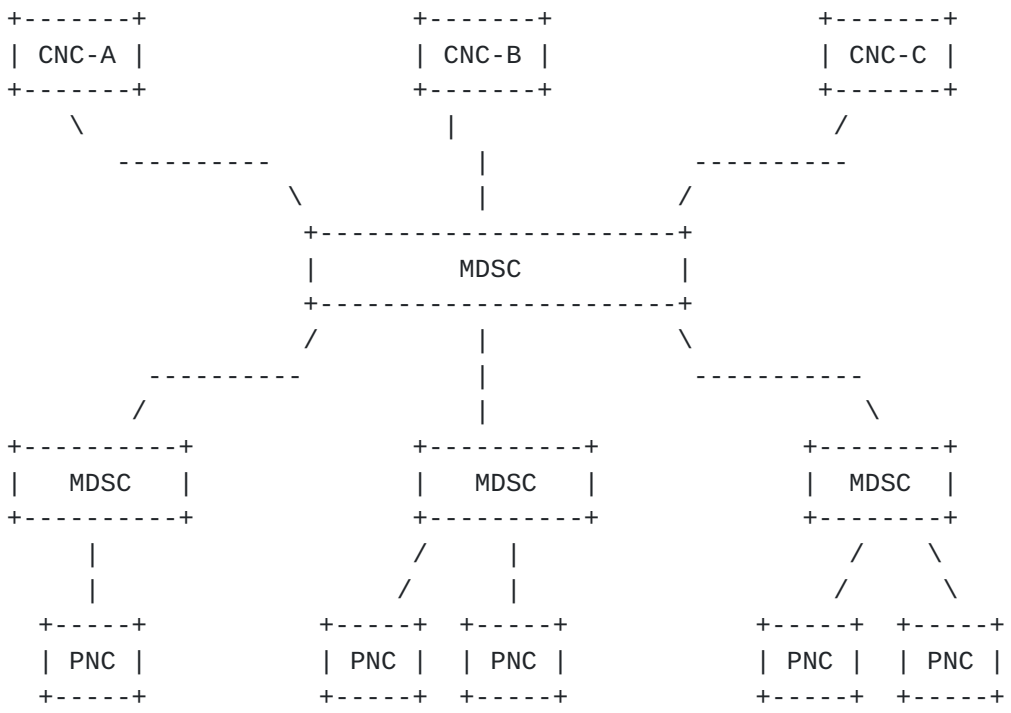

Figure 6 : Controller recursiveness

A key requirement for allowing recursion of MDSCs is that a single interface needs to be defined both for the north and the south bounds.
In order to allow for multi-domain coordination a 1:N relationship must be allowed between MDSCs and between MDSCs and PNCs (i.e. 1 parent MDSC and N child MDSC or 1 MDSC and N PNCs). In addition to that it could be possible to have also a M:1 relationship between MDSC and PNC to allow for network resource partitioning/sharing among different customers not necessarily connected to the same MDSC (e.g. different service providers).

3.3. Physical Network Controller

The Physical Network Controller is the one in charge of configuring the network elements, monitoring the physical topology of the network and passing it, either raw or abstracted, to the MDSC.

The internal architecture of the PNC, his building blocks and the way it controls its domain, are out of the scope of ACTN. Some examples can be found in the Application Based Network Operations (ABNO) architecture [ABNO] and the ONF SDN architecture [ONF-ARCH]

The PNC, in addition to being in charge of controlling the physical network, is able to implement two of the four ACTN main functionalities: multi domain coordination function and virtualization/abstraction function
A hierarchy of PNCs can be foreseen for scalability and administrative choices.

3.4. ACTN interfaces

To allow virtualization and multi domain coordination, the network has to provide open, programmable interfaces, in which customer applications can create, replace and modify virtual network resources and services in an interactive, flexible and dynamic fashion while having no impact on other customers. Direct customer control of transport network elements and virtualized services is not perceived as a viable proposition for transport network providers due to security and policy concerns among other reasons. In addition, as discussed in the previous section, the network control plane for transport networks has been separated from data plane and as such it is not viable for the customer to directly interface with transport network elements.

Figure 5 depicts a high-level control and interface architecture for ACTN. A number of key ACTN interfaces exist for deployment and operation of ACTN-based networks. These are highlighted in Figure 5 (ACTN Interfaces) below:

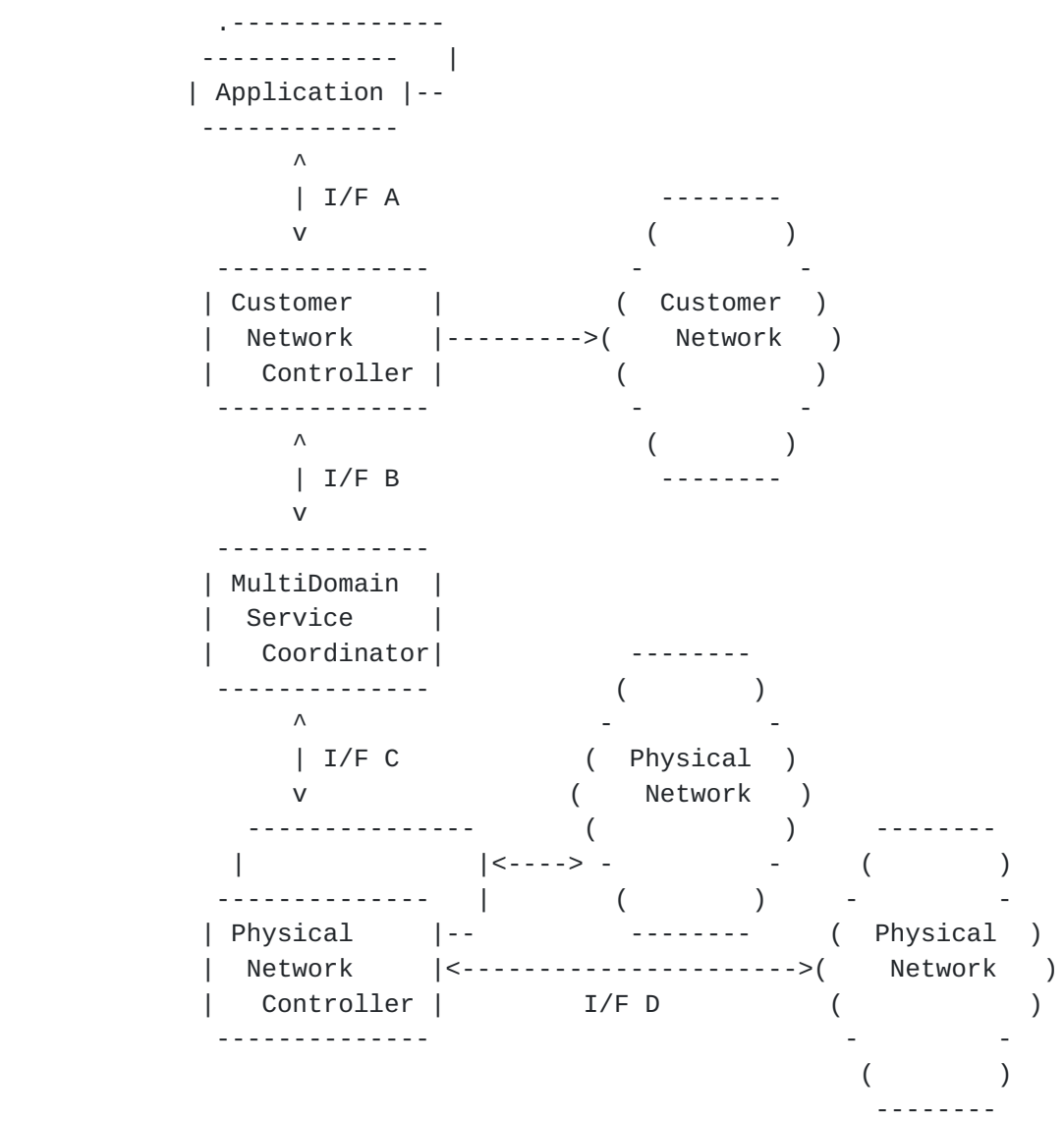

Figure 7 : ACTN Interfaces

The interfaces and functions are described below:

- Interface A: A north-bound interface (NBI) that will communicate the service request or application demand. A request will include specific service properties, including: services, topology, bandwidth and constraint information.

- Interface B: The CNC-MDSC Interface (CMI) is an interface between a Customer Network Controller and a Multi Service Domain Controller. It requests the creation of the network resources, topology or services for the applications. The Virtual Network Controller may also report potential network

topology availability if queried for current capability from the Customer Network Controller.

. Interface C: The MDSC-PNC Interface (MPI) is an interface between a Multi Domain Service Coordinator and a Physical Network Controller. It communicates the creation request, if required, of new connectivity of bandwidth changes in the physical network, via the PNC. In multi-domain environments, the MDSC needs to establish multiple MPIs, one for each PNC, as there are multiple PNCs responsible for its domain control.

. Interface D: The provisioning interface for creating forwarding state in the physical network, requested via the Physical Network Controller.

The interfaces within the ACTN scope are B and C.

4. VN creation process

The provider can present to the customer different level of network abstraction, spanning from one extreme (say "black") where nothing is shown, just the APs, to the other extreme (say "white") where a slice of the network is shown to the customer. There are shades of gray in between where a number of abstract links and nodes can be shown.

The VN creation is composed by two phases: Negotiation and Implementation.

Negotiation: In the case of grey/white topology abstraction, there is an a priori phase in which the customer agrees with the provider on the type of topology to be shown, e.q. 10 virtual links and 5 virtual nodes with a given interconnectivity. This is something that is assumed to be preconfigured by the operator off-line, what is online is the capability of modifying/deleting something (e.g. a virtual link). In the case of "black" abstraction this negotiation phase does not happen, in the sense that the customer can only see the APs of the network.

Implementation: In the case of black topology abstraction, the customers can ask for connectivity with given constraints/SLA

between the APs and LSPs/tunnels are created by the provider to satisfy the request. What the customer sees is only that his CEs are connected with a given SLA. In the case of grey/white topology the customer creates his own LSPs accordingly to the topology that was presented to him.

5. Access Points and Virtual Network Access Points

In order not to share unwanted topological information between the customer domain and provider domain, a new entity is defined and associated to an access link, the Access Point (AP). See the definition of AP in Section 1.1.

A customer node will use APs as the end points for the request of VNs.

A number of parameters need to be associated to the APs. Such parameters need to include at least: the maximum reservable bandwidth on the link, the available bandwidth and the link characteristics (e.g. switching capability, type of mapping).

Editor note: it is not appropriate to define link characteristics like bandwidth against a point (AP). A solution needs to be found.

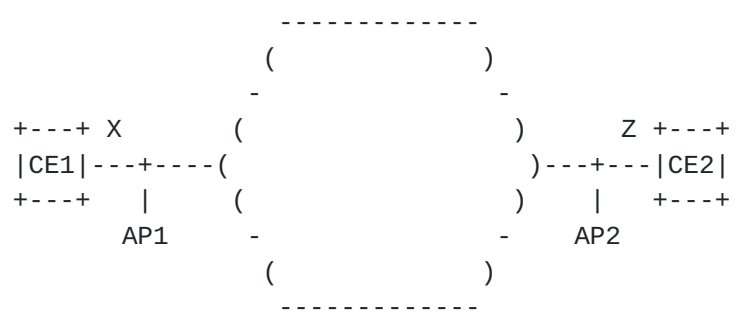

Figure 8 : APs definition customer view

Let's take as example a scenario in which CE1 is connected to the network via a 10Gb link and CE2 via a 40Gb link. Before the creation of any VN between AP1 and AP2 the customer view can be summarized as follows:

AP id	MaxResBw	AvailableBw	CE,port
AP1	10Gb	10Gb	CE1,portX
AP2	40Gb	40Gb	CE2,portZ

Table 1: AP - customer view

On the other side what the provider sees is:

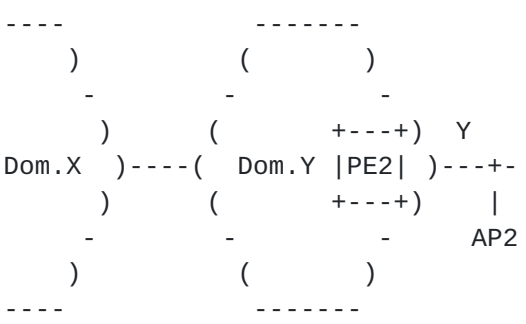

Figure 9 : Provider view of the AP

Which in the example above ends up in a summarization as follows:

AP id	MaxResBw	AvailableBw	PE,port
AP1	10Gb	10Gb	PE1,portW
AP2	40Gb	40Gb	PE2,portY

Table 2: AP - provider view

The second entity that needs to be defined is a structure within the AP that is linked to a VN and that is used to allow for different VN to be provided starting from the same AP. It also allows reserving the bandwidth for the VN on the access link. Such entity is called Virtual Network Access Point. For each virtual network is defined on an AP, a different VNAP is created.

In the simple scenario depicted above we suppose to create two virtual networks. The first one has with VN identifier 9 between AP1

and AP2 with and bandwidth of 1Gbps, while the second one with VN id 5, again between AP1 and AP2 and bandwidth 2Gbps.

The customer view would evolve as follows:

AP/VNAPid	MaxResBw	AvailableBw	PE,port
AP1	10Gbps	7Gbps	PE1,portW
-VNAP1.9	1Gbps	N.A.	
-VNAP1.5	2Gbps	N.A	
AP2	40Gb	37Gb	PE2,portY
-VNAP2.9	1Gbps	N.A.	
-VNAP2.5	2Gbps	N.A	

Table 3: AP and VNAP - provider view after VN creation

5.1. Dual homing scenario

Often there is a dual homing relationship between a CE and a pair of PE. This case needs to be supported also by the definition of VN, AP and VNAP. Suppose to have CE1 connected to two different PE in the operator domain via AP1 and AP2 and the customer needing 5Gbps of bandwidth between CE1 and CE2.

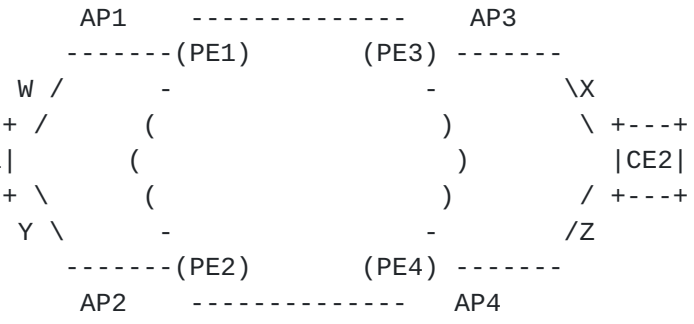

Figure 10 : Dual homing scenario

In this case the customer will request for a VN between AP1, AP2 and AP3 specifying a dual homing relationship between AP1 and AP2. As a consequence no traffic will be flowing between AP1 and AP2. The dual homing relationship would then be mapped against the VNAPs (since other independent VNs might have AP1 and AP2 as end points).

The customer view would be as follows:

AP/VNAPid	MaxResBw	AvailableBw	CE,port	Dual Homing
AP1 -VNAP1.9	10Gbps 5Gbps	5Gbps N.A.	CE1,portW	VNAP2.9
AP2 -VNAP2.9	40Gbps 5Gbps	35Gbps N.A.	CE1,portY	VNAP1.9
AP3 -VNAP3.9	40Gbps 5Gbps	35Gbps N.A.	CE2,portZ	NONE

Table 4: Dual homing - customer view after VN creation

6. End point selection & mobility

Virtual networks could be used as the infrastructure to connect a number of sites of a customer among them or to provide connectivity between customer sites and virtualized network functions (VNF) like for example virtualized firewall, vBNG, storage, computational functions.

6.1. End point selection & mobility

A VNF could be deployed in different places (e.g. data centers A, B or C in figure below) but the VNF provider (=ACTN customer) doesn't know which is the best site where to install the VNF from a network point of view (e.g. latency). For example it is possible to compute the path minimizing the delay between AP1 and AP2, but the customer doesn't know a priori if the path with minimum delay is towards A, B or C.

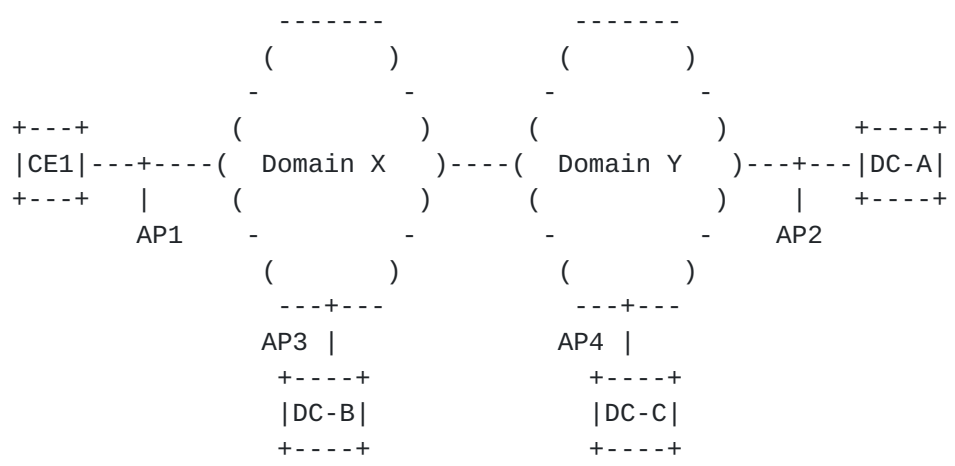

Figure 11 : End point selection

In this case the VNF provider (=ACTN customer) should be allowed to ask for a VN between AP1 and a set of end points. The list of end points is provided by the VNF provider. When the end point is identified the connectivity can be instantiated and a notification can be sent to the VNF provider for the instantiation of the VNF.

6.2. Preplanned end point migration

A premium SLA for VNF service provisioning consists on the offering of a protected VNF instantiated on two or more sites and with a hot stand-by protection mechanism. In this case the VN should be provided so to switch from one end point to another upon a trigger from the VNF provider or an automatic failure detection mechanism. An example is provided in figure below where the request from the VNF provider is for connectivity with given constraint and resiliency between CE1 and a VNF with primary installation in DC-A and a protection in DC-C.

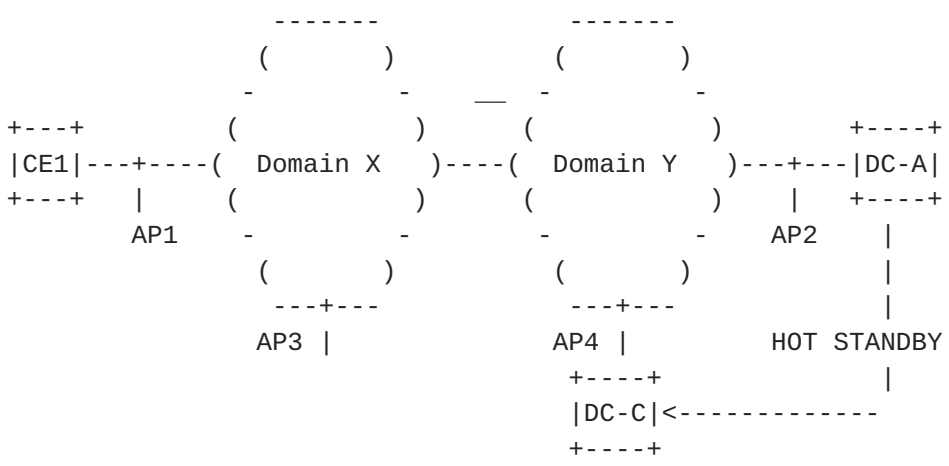

Figure 12 : Preplanned endpoint migration

6.3. On the fly end point migration

The one the fly end point migration concept is very similar to the end point selection one. The idea is to give the provider not only the list of sites where the VNF can be installed, but also a mechanism to notify changes in the network that have impacts on the SLA. After an handshake with the customer controller/applications, the bandwidth in network would be moved accordingly with the moving of the VNFs.

7. Security

TBD

8. References

8.1. Informative References

[PCE] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", IETF RFC 4655, August 2006.

[RFC4026] L. Andersson, T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, March 2005.

[RFC4208] G. Swallow, J. Drake, H.Ishimatsu, Y. Rekhter, "Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, October 2005.

[PCE-S] Crabbe, E, et. al., "PCEP extension for stateful PCE",draft-ietf-pce-stateful-pce, work in progress.

[GMPLS] Manning, E., et al., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, October 2004.

[NFV-AF] "Network Functions Virtualization (NFV); Architectural Framework", ETSI GS NFV 002 v1.1.1, October 2013.

[ACTN-PS] Y. Lee, D. King, M. Boucadair, R. Jing, L. Contreras Murillo, "Problem Statement for Abstraction and Control of Transport Networks", draft-leeking-actn-problem-statement, work in progress.

[ONF] Open Networking Foundation, "OpenFlow Switch Specification Version 1.4.0 (Wire Protocol 0x05)", October 2013.

[TE-INFO] A. Farrel, Editor, "Problem Statement and Architecture for Information Exchange Between Interconnected Traffic Engineered Networks", draft-ietf-teas-interconnected-te-info-exchange, work in progress.

[ABNO] King, D., and Farrel, A., "A PCE-based Architecture for Application-based Network Operations", draft-farrkingel-pce-abno-architecture, work in progress.

[ACTN-Info] Y. Lee, S. Belotti, D. Dhody, "Information Model for Abstraction and Control of Transport Networks", draft-leebelotti-teas-actn-info, work in progress.

[Cheng] W. Cheng, et. al., "ACTN Use-cases for Packet Transport Networks in Mobile Backhaul Networks", draft-cheng-actn-ptn-requirements, work in progress.

[Dhody] D. Dhody, et. al., "Packet Optical Integration (POI) Use Cases for Abstraction and Control of Transport Networks (ACTN)", draft-dhody-actn-poi-use-case, work in progress.

[Fang] L. Fang, "ACTN Use Case for Multi-domain Data Center Interconnect", draft-fang-actn-multidomain-dci, work in progress.

[Klee] K. Lee, H. Lee, R. Vilata, V. Lopez, "ACTN Use-case for On-demand E2E Connectivity Services in Multiple Vendor Domain Transport Networks", draft-klee-actn-connectivity-multi-vendor-domains, work in progress.

[Kumaki] K. Kumaki, T. Miyasaka, "ACTN : Use case for Multi Tenant VNO ", draft-kumaki-actn-multitenant-vno, work in progress.

[Lopez] D. Lopez (Ed), "ACTN Use-case for Virtual Network Operation for Multiple Domains in a Single Operator Network", draft-lopez-actn-vno-multidomains, work in progress.

[Shin] J. Shin, R. Hwang, J. Lee, "ACTN Use-case for Mobile Virtual Network Operation for Multiple Domains in a Single Operator Network", draft-shin-actn-mvno-multi-domain, work in progress.

[Xu] Y. Xu, et. al., "Use Cases and Requirements of Dynamic Service Control based on Performance Monitoring in ACTN Architecture", draft-xu-actn-perf-dynamic-service-control, work in progress.

9. Contributors

Authors' Addresses

Daniele Ceccarelli (Editor)
Ericsson
Torshamnsgatan,48
Stockholm, Sweden
Email: daniele.ceccarelli@ericsson.com

Young Lee (Editor)
Huawei Technologies
5340 Legacy Drive
Plano, TX 75023, USA
Phone: (469)277-5838
Email: leeyoung@huawei.com

Luyuan Fang
Email: luyuanf@gmail.com

Diego Lopez
Telefonica I+D
Don Ramon de la Cruz, 82
28006 Madrid, Spain
Email: diego@tid.es

Sergio Belotti
Alcatel Lucent
Via Trento, 30
Vimercate, Italy
Email: sergio.belotti@alcatel-lucent.com

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

Dhruv Dhoddy
Huawei Technologies
dhruv.ietf@gmail.com

Gert Grammel
Juniper Networks
ggrammel@juniper.net