TEAS Working Group
Internet Draft
Intended status: Informational
Expires: August 2017

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

February 16, 2017

Framework for Abstraction and Control of Traffic Engineered Networks

draft-ietf-teas-actn-framework-04

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

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 August 16, 2017.

Table of Contents

1. Introduction....3
1.1. Terminology....6
2. Business Model of ACTN....9
2.1. Customers....9
2.2. Service Providers....10
2.3. Network Providers....11
3. ACTN Architecture....12
3.1. Customer Network Controller....14
3.2. Multi Domain Service Coordinator....15
3.3. Physical Network Controller....16
3.4. ACTN Interfaces....17
4. VN Creation Process....20
4.1. VN Creation Example....20
5. Access Points and Virtual Network Access Points....22
5.1. Dual homing scenario....25
6. End Point Selection Based On Network Status....26
6.1. Pre-Planned End Point Migration....27
6.2. On the Fly End Point Migration....28

7. Manageability Considerations.....28
7.1. Policy.....29
7.2. Policy applied to the Customer Network Controller.....29
7.3. Policy applied to the Multi Domain Service Coordinator...30
7.4. Policy applied to the Physical Network Controller.....30
8. Security Considerations.....31
8.1. Interface between the Customer Network Controller and Multi Domain Service Coordinator (MDSC), CNC-MDSC Interface (CMI)...32
8.2. Interface between the Multi Domain Service Coordinator and Physical Network Controller (PNC), MDSC-PNC Interface (MPI)...32
9. References.....33
9.1. Informative References.....33
10. Contributors.....34
Authors' Addresses.....35

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 is used in this document to refer to a network that uses any connection-oriented technology under the control of a distributed or centralized control plane to support dynamic provisioning of end-to-end connectivity. Some examples of networks that are in scope of this definition are optical networks, MPLS Transport Profile (MPLS-TP) networks [RFC5654], and MPLS Traffic Engineering (MPLS-TE) networks [RFC2702].

One of the main drivers for Software Defined Networking (SDN) [RFC7149] 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 the Path Computation Element (PCE) [RFC4655] for TE-based networks. One of the advantages of SDN is its logically centralized control regime that allows a global view of the underlying networks. Centralized control in SDN helps improve network resource utilization compared with distributed network control. For TE-based networks, PCE is essentially equivalent to a logically centralized path computation function.

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

- Separation of service requests from service delivery so that the orchestration of a network is transparent from the point of view of the customer but remains responsive to the customer's services and business needs.

- Network abstraction: As described in [RFC7926], abstraction is the process of applying policy to a set of information about a TE network to produce selective information that represents the potential ability to connect across the domain. The process of abstraction presents the connectivity graph in a way that is independent of the underlying network technologies, capabilities, and topology so that it can be used to plan and deliver network services in a uniform way

- 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 separated service request/orchestration and resource abstraction has emerged as a key requirement for operators. In order to support multiple clients each with its own view of and control of the server network, a network operator needs to partition (or "slice") the network resources. The resulting slices can be assigned to each client for guaranteed usage which is a step further than shared use of common network resources.

Furthermore, each network represented to a client can be built from abstractions of the underlying networks so that, for example, a link in the client's network is constructed from a path or collection of paths in the underlying network.

We call the set of management and control functions used to provide these features Abstraction and Control of Traffic Engineered Networks (ACTN).

Particular attention needs to be paid to the multi-domain case, 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 virtual network topology. Such a view may be specific to a service, the set of consumed resources, or to a particular customer.

Network abstraction refers to presenting a customer with a view of the operator's network in such a way that the links and nodes in that view constitute an aggregation or abstraction of the real resources in the operator's network in a way that is independent of the underlying network technologies, capabilities, and topology. The customer operates an abstract network as if it was their own network, but the operational commands are mapped onto the underlying network through domains coordination.

The customer controller for a virtual or abstract network is envisioned to support many 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 ACTN framework described in this document facilitates:

. Abstraction of the underlying network resources to higher-layer applications and customers [RFC7926].

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

. Slicing of infrastructure to meet specific customers' service requirements.

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

. The possibility of providing a customer with a virtualized network.

. A virtualization/mapping network function that adapts the customer's requests for control of the virtual resources that have been allocated to the customer to control commands applied to the underlying network resources. Such a function performs

the necessary mapping, translation, isolation and security/policy enforcement, etc.

. The presentation to customers of networks as a virtualized topology 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 vertex on the graph representation of a TE topology. In a physical network a node corresponds to a network element (NE). In a sliced network, a node is some subset of the capabilities of a physical network element. In an abstract network, a node (sometimes called an abstract node) is a representation as a single vertex in the topology of the abstract network of one or more nodes and their connecting links from the physical network. The concept of a node represents the ability to connect from any access to the node (a link end) to any other access to that node, although "limited cross-connect capabilities" may also be defined to restrict this functionality. Just as network slicing and network abstraction may be applied recursively, so a node in a topology may be created by applying slicing or abstraction on the nodes in the underlying topology.

. Link: A link is an edge on the graph representation of a TE topology. Two nodes connected by a link are said to be "adjacent" in the TE topology. In a physical network, a link corresponds to a physical connection. In a sliced topology, a link is some subset of the capabilities of a physical connection. In an abstract network, a link (sometimes called an abstract link) is a representation as an edge in the topology of the abstract network of one or more links and the nodes they connect from the physical network. Abstract links may be realized by Label Switched Paths (LSPs) across the physical network that may be pre-established or could be only potentially achievable. Just as network slicing and network abstraction may be applied recursively, so a link in a topology may be created by applying slicing or abstraction on the links in the underlying topology. While most links are point-to-point, connecting just two nodes, the concept of a multi-access link exists where more than two nodes are collectively adjacent

and data sent on the link by one node will be equally delivered to all other nodes connected by the link.

. PNC: A Physical Network Controller is a domain controller that is responsible for controlling devices or NEs under its direct control. This can be an SDN controller, a Network Management System (NMS), an Element Management System (EMS), an active PCE or any other mean to dynamically control a set of nodes and that is implementing an NBI compliant with ACTN specification.

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

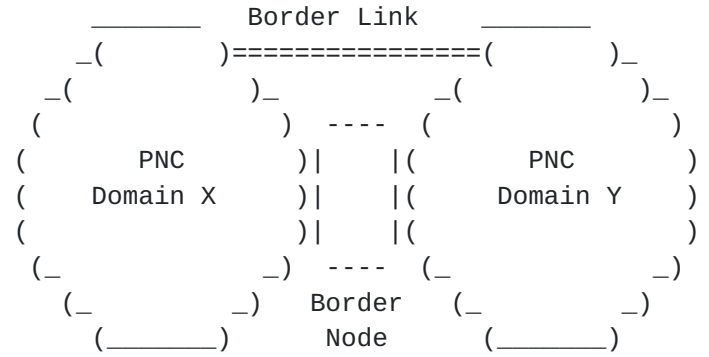


Figure 1: PNC Domain Borders

. A Virtual Network (VN) is a customer view of the TE network. It is presented by the provider as a set of physical and/or abstracted resources. Depending on the agreement between client and provider various VN operations and VN views are possible as follows:

  o VN Creation - VN could be pre-configured and created via offline negotiation between customer and provider. In other cases, the VN could also be created dynamically based on a request from the customer with given SLA attributes which satisfy the customer's objectives.

  o Dynamic Operations - The VN could be further modified or deleted based on a customer request to request. The customer can further act upon the virtual network

resources to perform end-to-end tunnel management (set-up/release/modify). These changes will result in subsequent LSP management at the operator's level.

o VN View:

a. The VN can be seen as set of end-to-end tunnels from a customer point of view, where each tunnel is referred as a VN member. Each VN member can then be formed by recursive slicing or abstraction of paths in underlying networks. Such end-to-end tunnels may comprise of customer end points, access links, intra-domain paths, and inter-domain links. In this view VN is thus a set of VN members.

b. The VN can also be seen as a topology comprising of physical, sliced, and abstract nodes and links. The nodes in this case include physical customer end points, border nodes, and internal nodes as well as abstracted nodes. Similarly the links include physical access links, inter-domain links, and intra-domain links as well as abstract links. The abstract nodes and links in this view can be pre-negotiated or created dynamically.

. Abstraction. This process is defined in [RFC7926].

. Abstract Link: The term "abstract link" is defined in [RFC7926].

. Abstract Topology: The topology of abstract nodes and abstract links presented through the process of abstraction by a lower layer network for use by a higher layer network.

. 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.

. Access Point (AP): An access point is used to keep confidentiality between the customer and the provider. It is a logical identifier shared between the customer and the provider, used to map the end points of the border node in both the customer and the provider NW. The AP can be used by the customer when requesting VN service to the provider.

. VN Access Point (VNAP): A VNAP is defined as the binding between an AP and a given VN and is used to identify the portion of the access and/or inter-domain 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 the 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.

There are three key entities in the ACTN model:

- Customers
- Service Providers
- Network Providers

These are described in the following sections.

2.1. Customers

Within the ACTN framework, different types of customers may be taken into account depending on the type of their resource needs, and on their number and type of access. For 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 for a service provider 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 a proxy and the services generally have very few dedicated resources (such as for subscriber drop), with everything else shared on the basis of some Service Level Agreement (LSA), 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 demands varying significantly 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 advanced customer 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. The primary focus of ACTN is Advanced Customers.

As customers are geographically spread over multiple network provider domains, they have to interface to 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 a view of the topology that spans all of the network providers. Customers of a given service provider can in turn offer a service to other customers in a recursive way.

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 (i.e, may or may not be network providers as described in Section 2.3). When a service provider is the same as the network provider, this is similar to existing VPN models applied to a single provider. This approach works well when the customer maintains a single interface with a single provider. When customer spans 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 distinct service providers interface to the customers. In this case, service providers are, themselves 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.

The ACTN network model is predicated upon this three tier model and is summarized in Figure 2:

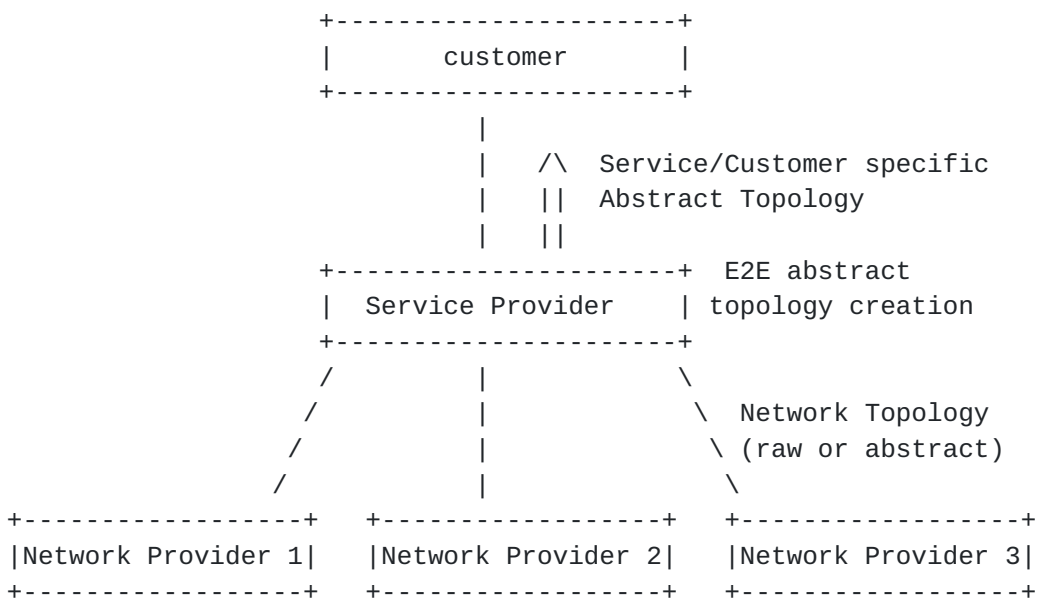


Figure 2: Three tier model.

There can be multiple service providers to which a customer may interface.

There are multiple types of service providers, for example:

- Data Center providers can be viewed as a service provider type as they own and operate data center resources for various WAN customers, and they can lease physical network resources from network providers.
- Internet Service Providers (ISP) are service providers 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 described in this architecture 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 model of ACTN showing the interfaces and the flow of control between components.

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

. Multi-domain coordination function: This function oversees the specific aspects of the different domains and builds a single abstracted end-to-end network topology in order to coordinate end-to-end path computation and path/service provisioning. Domain sequence path calculation/determination is also a part of this function.

. Virtualization/Abstraction function: This function provides an abstracted view of the underlying network resources for use by the customer - a customer may be the client or a higher level controller entity. This function includes network path computation based on customer service connectivity request constraints, path computation based on the global network-wide abstracted topology, and the creation of an abstracted view of network slices allocated to each customer. These operations depend on customer-specific network objective functions and customer traffic profiles.

. Customer mapping/translation function: This function is to map customer requests/commands into network provisioning requests that can be sent to the Physical Network Controller (PNC) according to business policies provisioned statically or dynamically at the OSS/NMS. Specifically, it provides mapping and translation of a customer's service request into a set of parameters that are specific to a network type and technology such that network configuration process is made possible.

. Virtual service coordination function: This function translates customer service-related information into virtual network service operations in order to seamlessly operate virtual networks while meeting a customer's service requirements. In

the context of ACTN, service/virtual service coordination includes a number of service orchestration functions such as multi-destination load balancing, guarantees of service quality, bandwidth and throughput. It also includes notifications for service fault and performance degradation and so forth.

The types of controller defined in the ACTN architecture are shown in Figure 3 below and are as follows:

- CNC - Customer Network Controller
- MDSC - Multi Domain Service Coordinator
- PNC - Physical Network Controller

Figure 3 also shows the following interfaces:

- CMI - CNC-MDSC Interface
- MPI - MDSC-PNC Interface

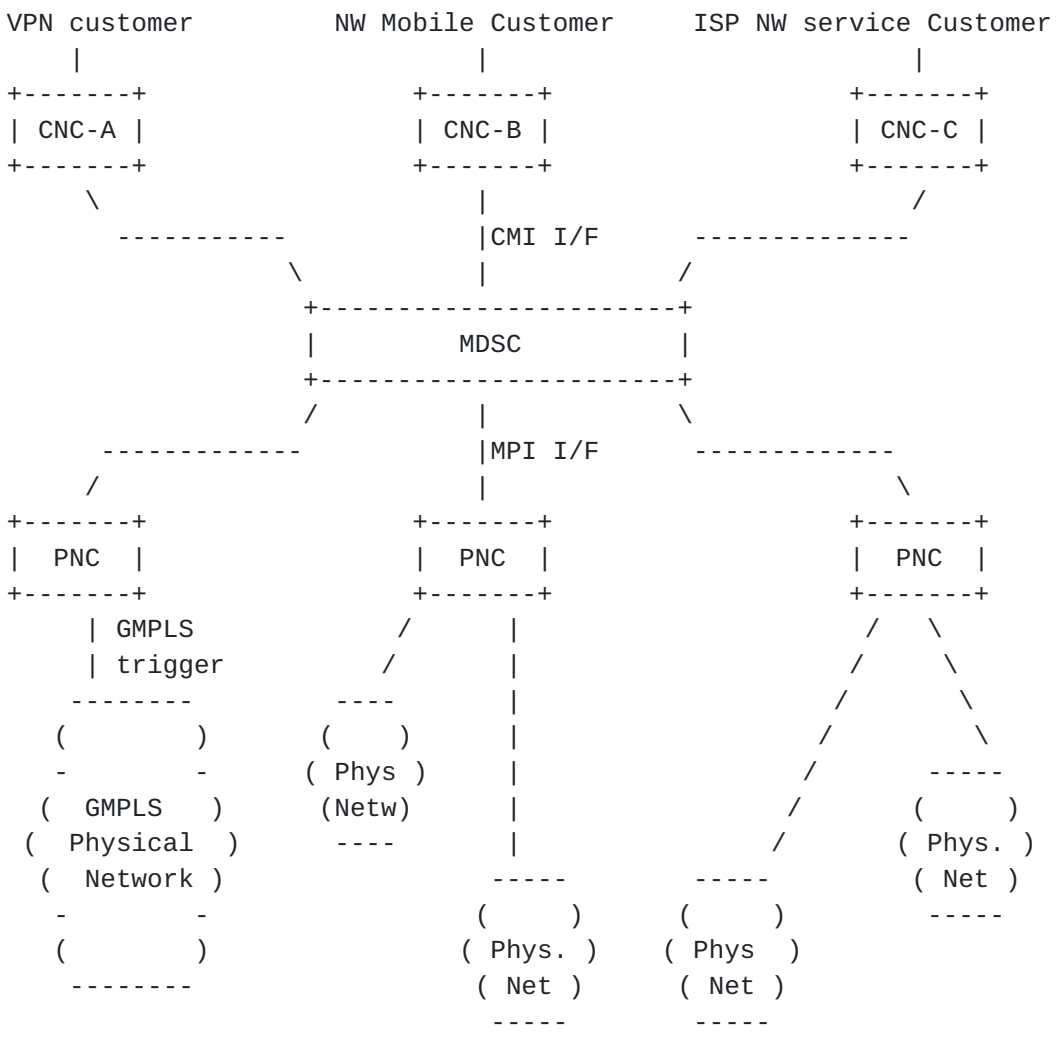


Figure 3: ACTN Control Hierarchy

3.1. Customer Network Controller

A Virtual Network Service is instantiated by the Customer Network Controller via the CNC-MDSC Interface (CMI). As the Customer Network Controller directly interfaces to 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 of the end-point interfaces based on their business negotiations prior to service instantiation. End-point interfaces refer to customer-network physical interfaces that connect customer premise equipment to network provider equipment.

3.2. Multi Domain Service Coordinator

The Multi Domain Service Coordinator (MDSC) sits between the CNC that issues connectivity requests and the Physical Network Controllers (PNCs) that manage 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 [RFC7491] and the ONF SDN architecture [ONF-ARCH].

The MDSC is the only building block of the architecture that can implement all four ACTN main functions, i.e., multi domain coordination, virtualization/abstraction, customer mapping/translation, and virtual service coordination. The first two functions of the MDSC, namely, multi domain coordination and virtualization/abstraction are referred to as network control/coordination functions while the last two functions, namely, customer mapping/translation and virtual service coordination are referred to as service control/coordination functions.
The key point of the MDSC (and of the whole ACTN framework) is detaching the network and service control from underlying technology to help the customer express the network as desired by business needs. The MDSC envelopes the instantiation of the right technology and network control to meet business criteria. In essence it controls and manages the primitives to achieve functionalities as desired by the CNC.
A hierarchy of MDSCs can be foreseen for scalability and administrative choices. In this case another interface needs to be defined, the MMI (MDSC-MDSC interface) as shown in Figure 4.

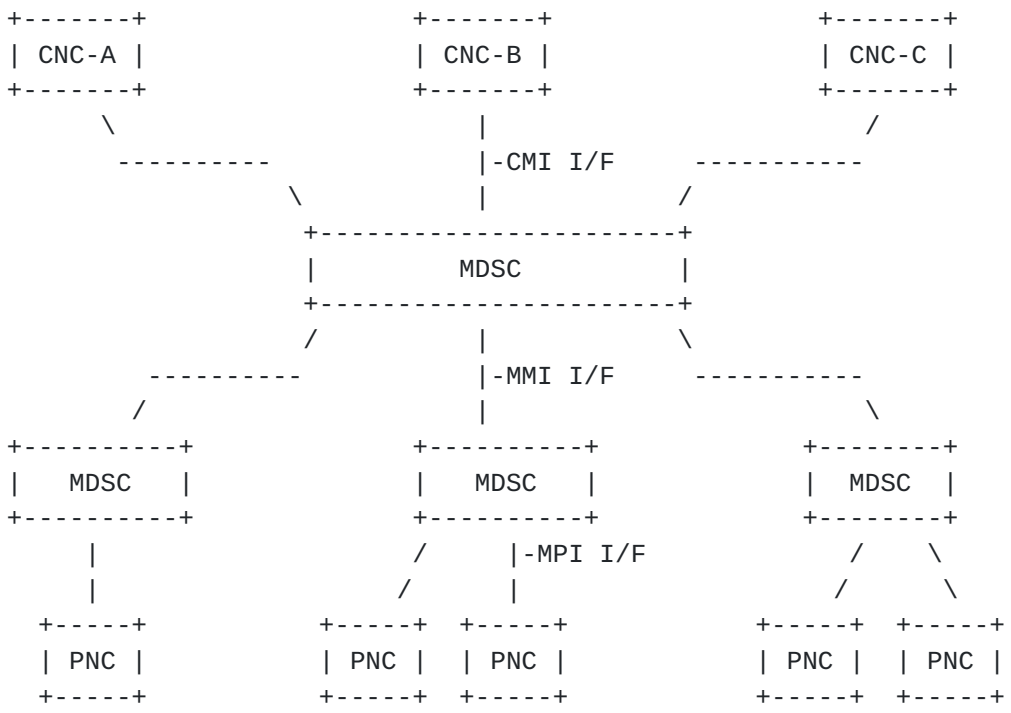


Figure 4: Controller recursiveness

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 the case where there is a hierarchy of MDSCs, the interface above the top MDSC (i.e., CMI) and the interface below the bottom MDSCs (i.e., SBI) remain the same. The recursion of MDSCs in the middle layers within this hierarchy of MDSCs may take place via the MMI. Please see Section 4 for details of the ACTN interfaces.

In addition to that, it could also be possible to have an M:1 relationship between MDSCs 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 (PNC) oversees configuring the network elements, monitoring the topology (physical or virtual) of

the network, and passing information about the topology (either raw or abstracted) to the MDSC.

The internal architecture of the PNC, its 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 [RFC7491] 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 main ACTN main functions: multi domain coordination and virtualization/abstraction function.

3.4. ACTN Interfaces

To allow virtualization and multi domain coordination, the network has to provide open, programmable interfaces, through 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 Section 3.3, the network control plane for transport networks has been separated from the 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).

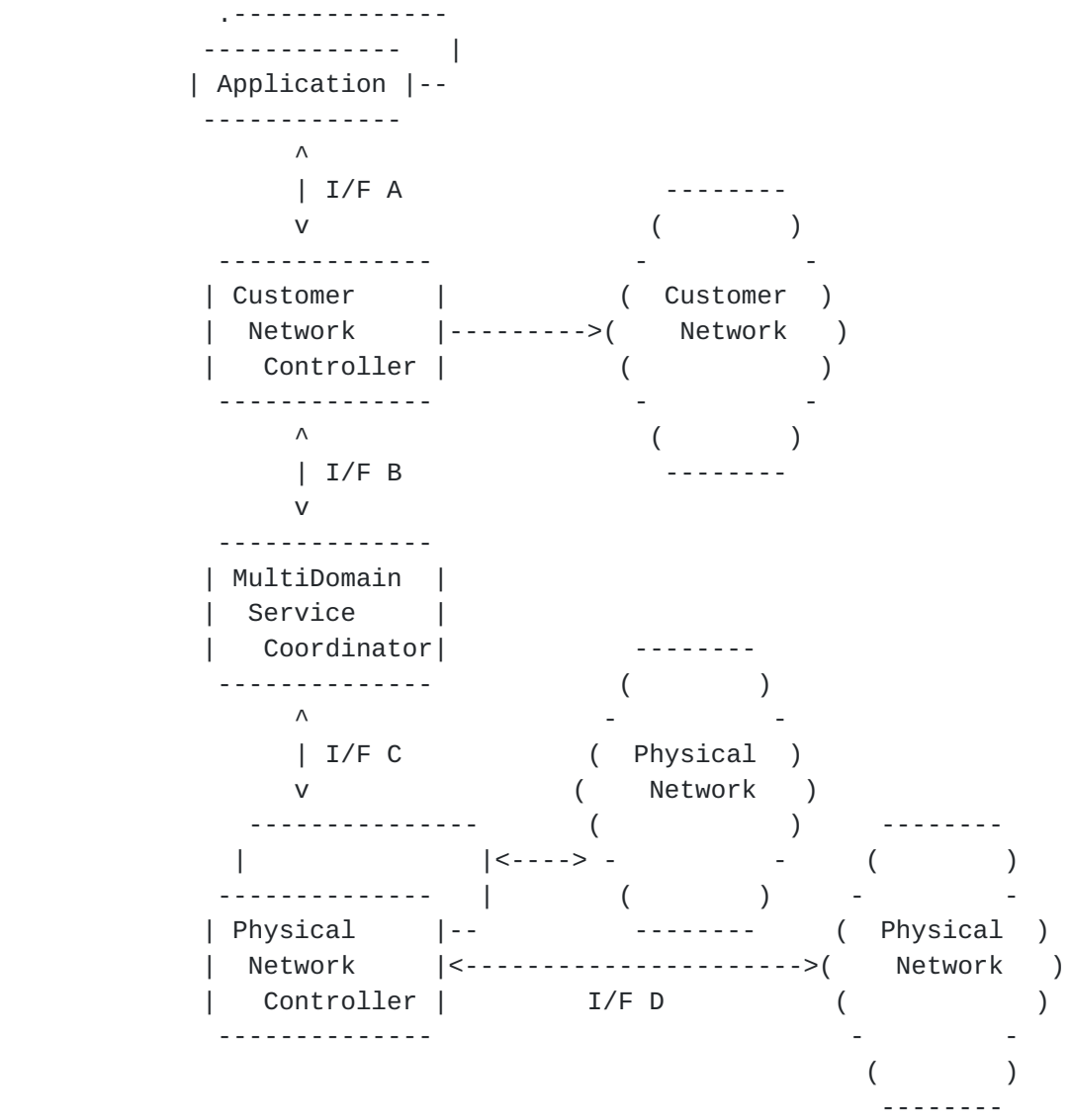


Figure 5: ACTN Interfaces

The interfaces and functions are described below:

. Interface A: A north-bound interface (NBI) that communicates the service request or application demand. A request includes specific service properties, including service type, topology, bandwidth, and constraint information.

. Interface B: The CNC-MDSC Interface (CMI) is an interface between a CNC and an MDSC. It is used to request the creation of network resources, topology or services for the

applications. Note that all service related information conveyed via Interface A (i.e., specific service properties, including service type, topology, bandwidth, and constraint information) needs to be transparently carried over this interface. The MDSC may also report potential network topology availability if queried for current capability from the CNC. The CMI is the interface with the highest level of abstraction, where the Virtual Networks are modelled and presented to the customer/CNC. Most of the information over this interface is technology agnostic, even if in some cases it should be possible to explicitly request for a VN to be created at a given layer in the network (e.g. ODU VN or MPLS VN).

. Interface C: The MDSC-PNC Interface (MPI) is an interface between an MDSC and a PNC. It communicates the creation requests for new connectivity or for bandwidth changes in the physical network. In multi-domain environments, the MDSC needs to establish multiple MPIs, one for each PNC, as there is one PNC responsible for control of each domain. The MPI could have different degrees of abstraction and present an abstracted topology hiding technology specific aspects of the network or convey technology specific parameters to allow for path computation at the MDSC level. Please refer to CCAMP Transport NBI work for the latter case [Transport NBI].

. 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 while interfaces A and D are out of the scope of ACTN and are only shown in Figure 5 to give a complete context of ACTN.
As previously stated in Section 3.2 there might be a third interface in ACTN scope, the MMI. The MMI is a special case of the MPI and behaves similarly to an MPI to support general functions performed by the MDSCs such as abstraction function and provisioning function. From an abstraction point of view, the top level MDSC which interfaces the CNC operates on a higher level of abstraction (i.e., less granular level) than the lower level MSDCs. As such, the MMI carries more abstract TE information than the MPI.

Please note that for all the three interfaces, when technology specific information needs to be included, this info will be add-ons on top of the general abstract topology. As far as general topology

abstraction standpoint, all interfaces are still recursive in nature.

4. VN Creation Process

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

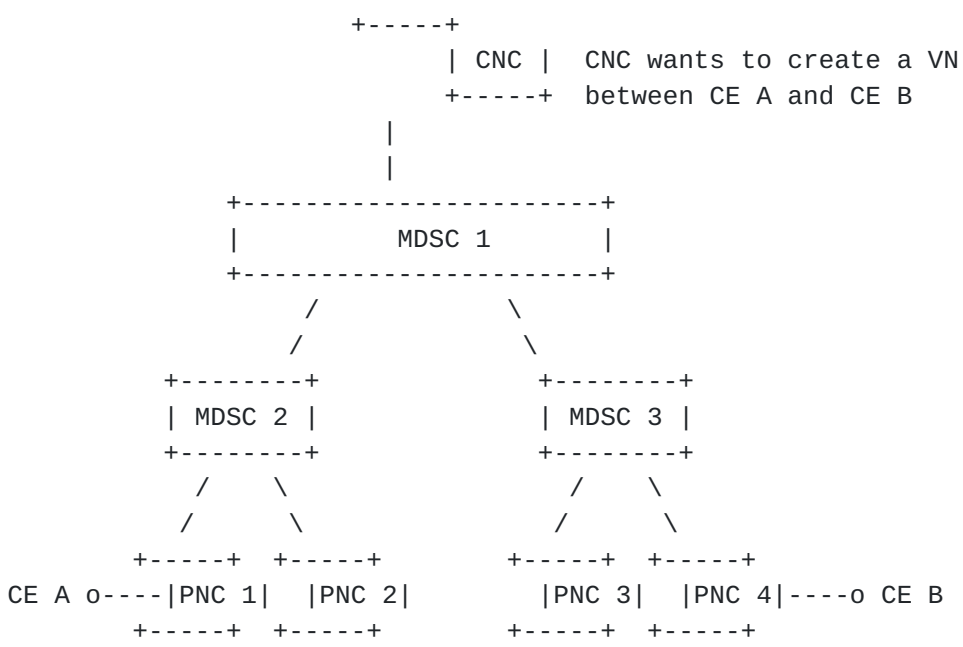
VN creation is composed of two phases: Negotiation and Implementation.

Negotiation: In the case of gray/white topology abstraction, there is an initial phase in which the customer agrees with the provider on the type of topology to be shown (e.g., 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 on-line is the capability to modify/delete something (e.g., a virtual link). In the case of "black" abstraction this negotiation phase does not happen because there is nothing to negotiate: the customer can only see the APs of the network.

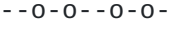
Implementation: In the case of black topology abstraction, the customers can ask for connectivity with given constraints/SLA between the APs and LSPs/tunnels created by the provider to satisfy the request. What the customer sees is only that his CEs are connected with a given SLA. In the case of grey/white topology the customer creates his own LSPs accordingly to the topology that was presented to him.

4.1. VN Creation Example

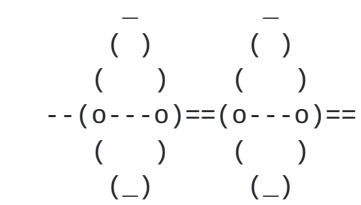
This section illustrates how a VN creation process is conducted over a hierarchy of MDSCs via MMIs and MPIs, which is shown in Figure 6.



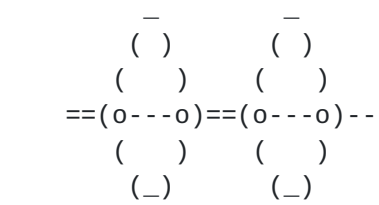
Topology Seen at MDSC 1



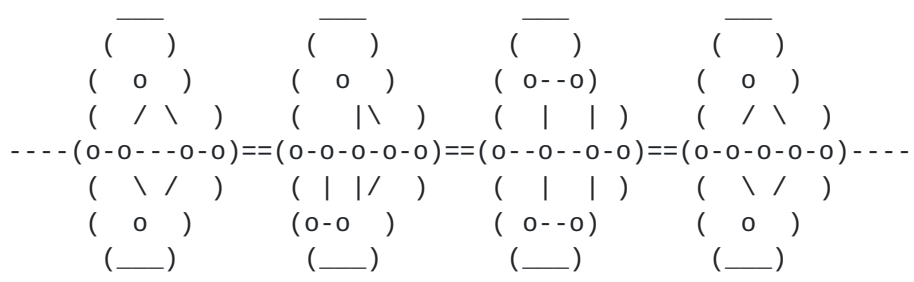
Topology Seen at MDSC 2



Topology Seen at MDSC 3



Actual Topology



Where o is a node and -- is a link and === a border link

Figure 6: Illustration of topology abstraction granularity levels in the MDSC Hierarchy

In the example depicted in Figure 6, there are four domains under control of the respective PNCs, namely, PNC 1, PNC 2, PNC3 and PNC4. Assume that MDSC 2 is controlling PNC 1 and PNC 2 while MDSC 3 is controlling PNC 3 and PNC 4. Let us assume that each of the PNCs provides a grey topology abstraction in which to present only border nodes and border links. The abstract topology MDSC 2 would operate is shown on the left side of MDSC 2 in Figure 6. It is basically a combination of the two topologies the PNCs (PNC 1 and PNC 2) provide. Likewise, the abstract topology MDSC 3 would operate is shown on the right side of MDSC 3 in Figure 6. Both MDSC 2 and MDSC 3 provide a grey topology abstraction in which each PNC domain is presented as one virtual node to its top level MDSC 1. Then the MDSC 1 combines these two topologies updated by MDSC 2 and MDSC 3 to create the abstraction topology to which it operates. MDSC 1 sees the whole four domain networks as four virtual nodes connected via virtual links. This illustrates the point discussed in Section 3.4: The top level MDSC operates on a higher level of abstraction (i.e., less granular level) than the lower level MSDCs. As such, the MMI carries more abstract TE information than the MPI.
In the process of creating a VN, the same principle applies. Let us assume that a customer wants to create a virtual network that connects its CE A and CE B which is depicted in Figure 6. Upon receipt of this request generated by the CNC, MDSC 1, based on its abstract topology at hand, determines that CE A is connected a virtual node in domain 1 and CE B is connected to a virtual node in domain 4 and. MDSC 1 further determines that domain 2 and domain 3 are interconnected to domain 1 and 4 respectively. MDSC 1 then partitions the original VN request from the CNC into two separate VN requests and make a VN creation request, respectively to MDSC 2 and MDSC 3. MDSC 1 for instance make a VN request to MDSC 2 to connect two virtual nodes. When MDSC 2 receives this VN request from MDSC 1, it further partitions into two separate requests respectively to PNC 1 and PNC 2. This illustration shows that VN creation request process recursively takes place over MMI and MPI.

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 which is referred to as 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 as shown in Figure 7.

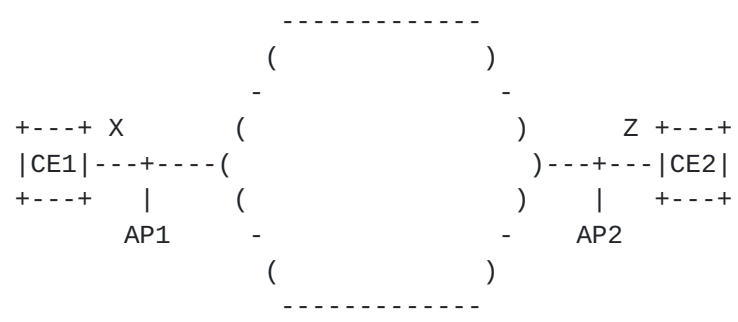


Figure 7: APs definition customer view

Let's take as an example a scenario shown in Figure 7. 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 shown in Table 1:

	End Point	Access Link Bandwidth	
AP id	CE,port	MaxResBw	AvailableBw
AP1	CE1,portX	10Gb	10Gb
AP2	CE2,portZ	40Gb	40Gb

Table 1: AP - customer view

On the other hand, what the provider sees is shown in Figure 8.

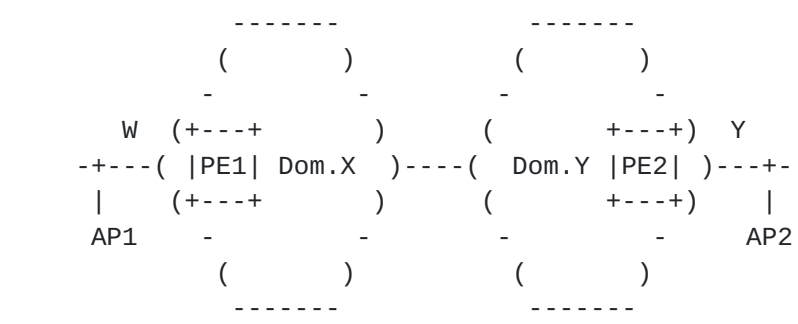


Figure 8: Provider view of the AP

Which results in a summarization as shown in Table 2.

End Point		Access Link Bandwidth	
AP id	PE,port	MaxResBw	AvailableBw
AP1	PE1,portW	10Gb	10Gb
AP2	PE2,portY	40Gb	40Gb

Table 2: AP - provider view

A Virtual Network Access Point (VNAP) needs to be defined as binding between the AP that is linked to a VN and that is used to allow for different VNs to start from the same AP. It also allows for traffic engineering on the access and/or inter-domain links (e.g., keeping track of bandwidth allocation). A different VNAP is created on an AP for each VN.

In the simple scenario depicted above we suppose we want to create two virtual networks. The first with VN identifier 9 between AP1 and AP2 with bandwidth of 1Gbps, while the second with VN id 5, again between AP1 and AP2 and with bandwidth 2Gbps.

The provider view would evolve as shown in Table 3.

	End Point	Access Link/VNAP Bw	
AP/VNAPid	PE,port	MaxResBw	AvailableBw
AP1	PE1,portW	10Gbps	7Gbps
-VNAP1.9		1Gbps	N.A.
-VNAP1.5		2Gbps	N.A
AP2	PE2,portY	40Gbps	37Gbps
-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 PEs. This case needs to be supported by the definition of VN, APs and VNAPs. Suppose CE1 connected to two different PEs in the operator domain via AP1 and AP2 and that the customer needs 5Gbps of bandwidth between CE1 and CE2. This is shown in Figure 9.

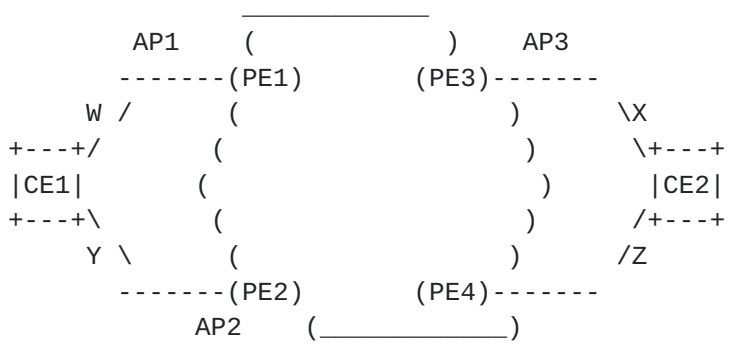


Figure 9: Dual homing scenario

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 flow 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 shown in Table 4.

	End Point	Access Link/VNAP Bw			
AP/VNAPid	CE,port	MaxResBw	AvailableBw	Dual Homing	
AP1 -VNAP1.9	CE1,portW	10Gbps 5Gbps	5Gbps N.A.	VNAP2.9	
AP2 -VNAP2.9	CE1,portY	40Gbps 5Gbps	35Gbps N.A.	VNAP1.9	
AP3 -VNAP3.9	CE2,portX	40Gbps 5Gbps	35Gbps N.A.	NONE	

Table 4: Dual homing - customer view after VN creation

6. End Point Selection Based On Network Status

A further advanced application of ACTN is in the case of Data Center selection, where the customer requires the Data Center selection to be based on the network status; this is referred to as Multi-Destination in [ACTN-REQ]. In terms of ACTN, a CNC could request a connectivity service (virtual network) between a set of source Aps and destination APs and leave it up to the network (MDSC) to decide which source and destination access points to be used to set up the connectivity service (virtual network). The candidate list of source and destination APs is decided by a CNC (or an entity outside of ACTN) based on certain factors which are outside the scope of ACTN.

Based on the AP selection as determined and returned by the network (MDSC), the CNC (or an entity outside of ACTN) should further take care of any subsequent actions such as orchestration or service setup requirements. These further actions are outside the scope of ACTN.

Consider a case as shown in Figure 10, where three data centers are available, but the customer requires the data center selection to be based on the network status and the connectivity service setup between the AP1 (CE1) and one of the destination APs (AP2 (DC-A), AP3 (DC-B), and AP4 (DC-C)). The MDSC (in coordination with PNCs) would select the best destination AP based on the constraints,

optimization criteria, policies, etc., and setup the connectivity service (virtual network).

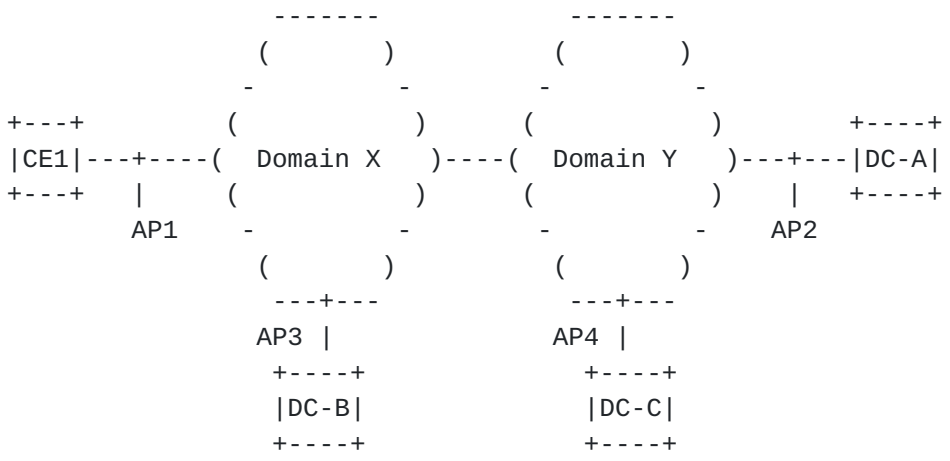


Figure 10: End point selection based on network status

6.1. Pre-Planned End Point Migration

Further in case of Data Center selection, customer could request for a backup DC to be selected, such that in case of failure, another DC site could provide hot stand-by protection. As shown in Figure 10 DC-C is selected as a backup for DC-A. Thus, the VN should be setup by the MDSC to include primary connectivity between AP1 (CE1) and AP2 (DC-A) as well as protection connectivity between AP1 (CE1) and AP4 (DC-C).

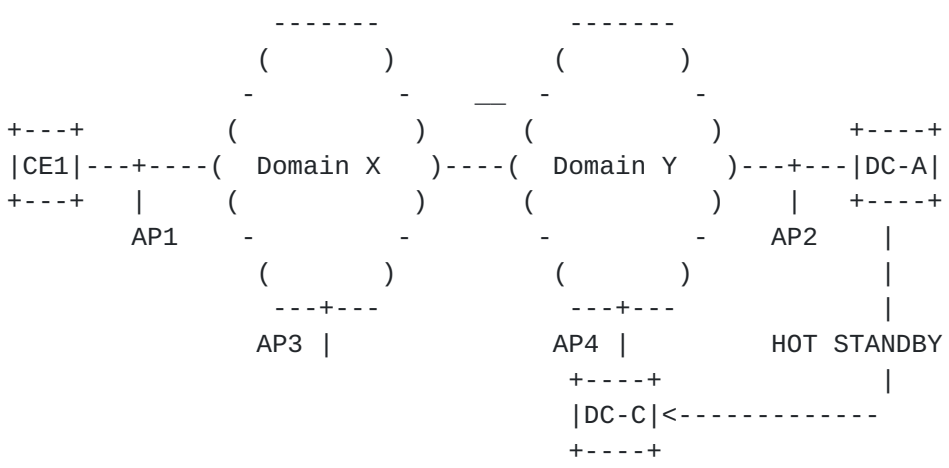


Figure 10: Pre-planned end point migration

6.2. On the Fly End Point Migration

Compared to pre-planned end point migration, on the fly end point selection is dynamic in that the migration is not pre-planned but decided based on network condition. Under this scenario, the MDSC would monitor the network (based on the VN SLA) and notify the CNC in case where some other destination AP would be a better choice based on the network parameters. The CNC should instruct the MDSC when it is suitable to update the VN with the new AP if it is required.

7. Manageability Considerations

The objective of ACTN is to manage traffic engineered resources, and provide a set of mechanism to allow clients to request virtual connectivity across server network resources. ACTN will support multiple clients each with its own view of and control of the server network, the network operator will need to partition (or "slice") their network resources, and manage them resources accordingly.

The ACTN platform will, itself, need to support the request, response, and reservations of client and network layer connectivity. It will also need to provide performance monitoring and control of traffic engineered resources. The management requirements may be categorized as follows:

- Management of external ACTN protocols
- Management of internal ACTN protocols

. Management and monitoring of ACTN components
. Configuration of policy to be applied across the ACTN system

7.1. Policy

It is expected that a policy will be an important aspect of ACTN control and management. Typically, policies are used via the components and interfaces, during deployment of the service, to ensure that the service is compliant with agreed policy factors (often described in Service Level Agreements - SLAs), these include, but are not limited to: connectivity, bandwidth, geographical transit, technology selection, security, resilience, and economic cost.

Depending on the deployment the ACTN deployment architecture, some policies may have local or global significance. That is, certain policies may be ACTN component specific in scope, while others may have broader scope and interact with multiple ACTN components. Two examples are provided below:

. A local policy might limit the number, type, size, and scheduling of virtual network services a customer may request via its CNC. This type of policy would be implemented locally on the MDSC.

. A global policy might constrain certain customer types (or specific customer applications) to only use certain MDSCs, and be restricted to physical network types managed by the PNCs. A global policy agent would govern these types of policies.

This objective of this section is to discuss the applicability of ACTN policy: requirements, components, interfaces, and examples. This section provides an analysis and does not mandate a specific method for enforcing policy, or the type of policy agent that would be responsible for propagating policies across the ACTN components. It does highlight examples of how policy may be applied in the context of ACTN, but it is expected further discussion in an applicability or solution specific document, will be required.

7.2. Policy applied to the Customer Network Controller

A virtual network service for a customer application will be requested from the CNC. It will reflect the application requirements and specific service policy needs, including bandwidth, traffic type and survivability. Furthermore, application access and type of

virtual network service requested by the CNC, will be need adhere to specific access control policies.

7.3. Policy applied to the Multi Domain Service Coordinator

A key objective of the MDSC is to help the customer express the application connectivity request via its CNC as set of desired business needs, therefore policy will play an important role.

Once authorised, the virtual network service will be instantiated via the CNC-MDSC Interface (CMI), it will reflect the customer application and connectivity requirements, and specific service transport needs. The CNC and the MDSC components will have agreed connectivity end-points, use of these end-points should be defined as a policy expression when setting up or augmenting virtual network services. Ensuring that permissible end-points are defined for CNCs and applications will require the MDSC to maintain a registry of permissible connection points for CNCs and application types.

It may also be necessary for the MDSC to resolve policy conflicts, or at least flag any issues to administrator of the MDSC itself. Conflicts may occur when virtual network service optimisation criterion are in competition. For example, to meet objectives for service reachability a request may require an interconnection point between multiple physical networks; however, this might break a confidentially policy requirement of specific type of end-to-end service. This type of situation may be resolved using hard and soft policy constraints.

7.4. Policy applied to the Physical Network Controller

The PNC is responsible for configuring the network elements, monitoring physical network resources, and exposing connectivity (direct or abstracted) to the MDSC. It is therefore expected that policy will dictate what connectivity information will be exported between the PNC, via the MDSC-PNC Interface (MPI), and MDSC.

Policy interactions may arise when a PNC determines that it cannot compute a requested path from the MDSC, or notices that (per a locally configured policy) the network is low on resources (for example, the capacity on key links become exhausted). In either case, the PNC will be required to notify the MDSC, which may (again

per policy) act to construct a virtual network service across another physical network topology.

Furthermore, additional forms of policy-based resource management will be required to provide virtual network service performance, security and resilience guarantees. This will likely be implemented via a local policy agent and subsequent protocol methods.

8. Security Considerations

The ACTN framework described in this document defines key components and interfaces for managed traffic engineered networks. Securing the request and control of resources, confidentially of the information, and availability of function, should all be critical security considerations when deploying and operating ACTN platforms.

Several distributed ACTN functional components are required, and as a rule implementations should consider encrypting data that flow between components, especially when they are implemented at remote nodes, regardless if these are external or internal network interfaces.

The ACTN security discussion is further split into two specific categories described in the following sub-sections:

- Interface between the Customer Network Controller and Multi Domain Service Coordinator (MDSC), CNC-MDSC Interface (CMI)

- Interface between the Multi Domain Service Coordinator and Physical Network Controller (PNC), MDSC-PNC Interface (MPI)

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.

The conclusion is that 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.

8.1. Interface between the Customer Network Controller and Multi Domain Service Coordinator (MDSC), CNC-MDSC Interface (CMI)

The role of the MDSC is to detach the network and service control from underlying technology to help the customer express the network as desired by business needs. It should be noted that data stored by the MDSC will reveal details of the virtual network services, and which CNC and application is consuming the resource. The data stored must therefore be considered as a candidate for encryption.

CNC Access rights to an MDSC must be managed. MDSC resources must be properly allocated, and methods to prevent policy conflicts, resource wastage and denial of service attacks on the MDSC by rogue CNCs, should also be considered.

A CNC-MDSC protocol interface will likely be an external protocol interface. Again, suitable authentication and authorization of each CNC connecting to the MDSC will be required, especially, as these are likely to be implemented by different organisations 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.

8.2. Interface between the Multi Domain Service Coordinator and Physical Network Controller (PNC), MDSC-PNC Interface (MPI)

The function of the Physical Network Controller (PNC) is to configure network elements, provide performance and monitoring functions of the physical elements, and export physical topology (full, partial, or abstracted) to 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.

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.

9. References

9.1. Informative References

[RFC2702] Awduche, D., et. al., "Requirements for Traffic Engineering Over MPLS", RFC 2702, September 1999.

[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.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", IETF RFC 4655, August 2006.

[RFC5654] Niven-Jenkins, B. (Ed.), D. Brungard (Ed.), and M. Betts (Ed.), "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[RFC7149] Boucadair, M. and Jacquenet, C., "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, March 2014.

[RFC7926] A. Farrel (Ed.), "Problem Statement and Architecture for Information Exchange between Interconnected Traffic-Engineered Networks", RFC 7926, July 2016.

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

[ONF-ARCH] Open Networking Foundation, "SDN architecture", Issue 1.1, ONF TR-521, June 2016.

[RFC7491] King, D., and Farrel, A., "A PCE-based Architecture for Application-based Network Operations", RFC 7491, March 2015.

[Transport NBI] Busi, I., et al., "Transport North Bound Interface Use Cases", draft-tnbidt-ccamp-transport-nbi-use-cases, work in progress.

10. Contributors

Adrian Farrel
Old Dog Consulting
Email: adrian@olddog.co.uk

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

Khuzema Pithewan
Infinera
Email: kpithewan@infinera.com

Michael Scharf
Nokia
Email: michael.scharf@nokia.com

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
Microsoft
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@nokia.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