Network Working Group
Internet Draft

Intended status: Informational
Expires: April 2015

Daniele Ceccarelli
Ericsson

Luyuan Fang
Microsoft

Young Lee
Huawei

Diego Lopez
Telefonica

Sergio Belotti
Alcatel-Lucent

Daniel King
Lancaster University

October 20, 2014

Framework for Abstraction and Control of Transport Networks

draft-ceccarelli-actn-framework-04.txt

Status of this Memo

This Internet-Draft will expire on April 20, 2015.

Abstract

This draft provides a framework for abstraction and control of transport networks.

Table of Contents

1. Terminology

This document uses the terminology defined in [RFC4655], and [RFC5440]. The following terminology is defined in this draft while PCE, PCC and PCEP are borrowed from [RFC4655] and [RFC5440].

ABNO	Application-Based Network Operations
CNC	Customer Network Controller
CVI	Customer-VNC Interface
PCC	Path Computation Client
PCE	Path Computation Entity
PCEP	Path Computation Protocol
PNC	Physical Network Controller
VL	Virtual Link
VN	Virtual Network
VNM	Virtual Network Mapping
VNC	Virtual Network Controller

VNE Virtual Network Element

VNS Virtual Network Service

VPI VNC-PNC Interface

2. Introduction

Transport 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.

Transport networks in this draft refer to a set of different type of connection-oriented networks, primarily Connection-Oriented Circuit Switched (CO-CS) networks and Connection-Oriented Packet Switched (CO-PS) networks. This implies that at least the following transport networks are in scope of the discussion of this draft: Layer 1(L1) and Layer 0 (L0) optical networks (e.g., Optical Transport Network (OTN), Optical Channel Data Unit (ODU), Optical Channel (OCh)/Wavelength Switched Optical Network (WSON)), Multi-Protocol Label Switching - Transport Profile (MPLS-TP), Multi-Protocol Label Switching - Traffic Engineering (MPLS-TE), as well as other emerging technologies with connection-oriented behavior. One of the characteristics of these network types is the ability of dynamic provisioning and traffic engineering such that resource guarantee can be provided to their clients.

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. In fact, in transport networks such separation of data and control plane was dictated at the onset due to the very different natures of the data plane (circuit switched Time Division Multiplexing (TDM) or Wavelength Division Multiplexing (WDM)) and a packet switched control plane. The decoupling of the control plane and the data plane is a major step towards allowing operators to gain the full control for optimized network design and operation. Moreover, another advantage 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 from a distributed network control. For TE-based transport network control, PCE is

essentially equivalent to a logically centralized control for path computation function.

As transport networks evolve, the need to provide network 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 uses.

Network slicing may be utilized for specific services and requested by higher-layer "applications", in this context types of application include management components such as Network Management Systems (NMS) and Operations Support Systems (OSS). Each customer is given a different partial view of the total topology and considering that it is operating with a single, stand-alone and consistent network.

Particular attention needs to be paid to the multi-domain case, where Abstraction and Control of Transport Networks (ACTN) can facilitate virtual network operation via the creation of a single virtualized network. 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, in general, refers to allowing the customers to utilize a certain amount of network resources as if they own them and thus control their allocated resources in a way most optimal with higher layer or application processes. This empowerment of customer control facilitates introduction of new services and applications as the customers are permitted to create, modify, and delete their virtual network services. The level of virtual control given to the customers can vary from a tunnel connecting two end-points to virtual network elements that consist of a set of virtual nodes and virtual links in a mesh network topology. 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 the set of consumed services as well as to a particular customer. As the Customer Network Controller is envisioned to support a plethora of distinct applications, there would be another level of virtualization from the customer to individual applications.

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

- Abstraction of the underlying network resources to higher-layer applications and users (customers); abstraction for a specific application or customer is referred to as virtualization in the ONF SDN architecture. [SDN-ARCH]

- Slicing infrastructure to connect multiple customers to meet specific application and users requirements;

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

- A computation scheme, via an information model, to serve various customers that request network connectivity and properties associated with it;

- A virtual network controller 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 coordination of the underlying transport topology, presenting it as an abstracted topology to the customers via open and programmable interfaces. This allows for the recursion of controllers in a customer-provider relationship.

The organization of this draft is as follows. Section 3 provides a discussion for a Business Model, Section 4 a Computation Model, Section 5 a Control and Interface model and Section 6 Design Principles.

3. Business Model of ACTN

The traditional Virtual Private Network (VPN) and Overlay Network (ON) models are built on the premise that one single network provider provides all virtual private or overlay networks to its customers. This model is simple to operate but has 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

3.1. 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 service 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 has 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 reasons why a bundled services offer is not enough but it is desirable to provide each of them with customized virtual network services. Advanced customers may own dedicated virtual resources, or share resources, but shared resources are likely to be governed by more complex SLA agreements; moreover they may have the ability to modify their service parameters directly (within the scope of their virtualized environments).As customers are geographically spread over multiple network provider domains, the necessary control and data interfaces to support such customer needs is no longer a single interface between the customer and one single network provider. With this premise, customers have to interface multiple providers to get their end-to-end network connectivity service and the associated topology information. Customers may have to support multiple virtual network services with differing service objectives and QoS requirements. For flexible and dynamic applications, customers may want to control their allocated virtual network resources in a dynamic fashion. To allow that, customers should be given an abstracted view of topology on which they can perform the necessary control decisions and take the corresponding actions. 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

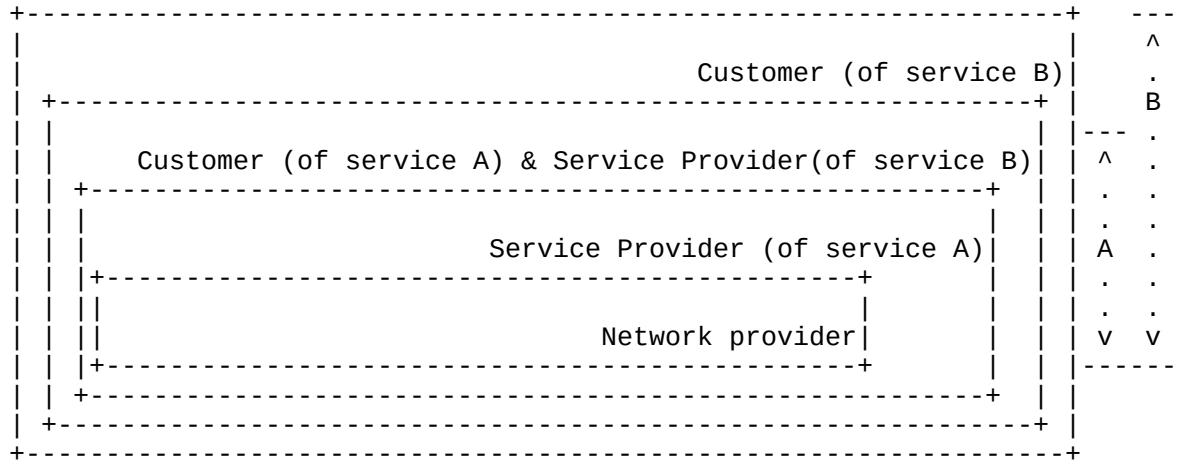


Figure 1: Network Recursiveness.

3.2. 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.

The ACTN network model is predicated upon this three tier model and is summarized in figure below:

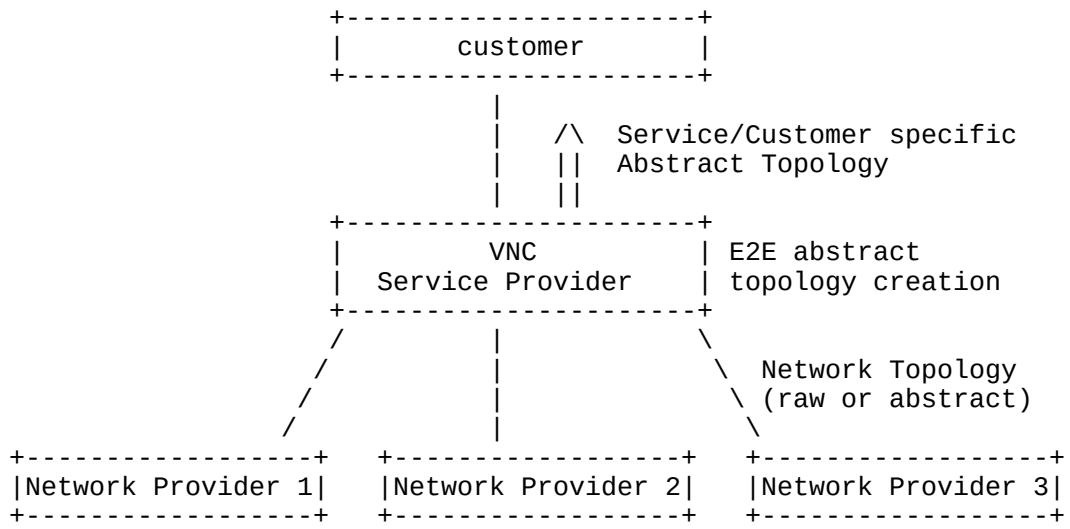


Figure 2: Three tier model.

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 clients, 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.

The network provider space is the one where recursiveness occurs. A customer-provider relationship between multiple service providers can be established leading to a hierarchical architecture of service provider controllers (NVCs).

3.3. 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.

4. Multi-Domain Model

Network operators build and operate multi-domain networks and these domains may be technology, administrative or vendor specific (vendor islands). Interoperability for dealing with different domains is a perpetual problem for operators. Due to these issues, new service introduction, often requiring connections that traverse multiple domains, need significant planning, and several manual operations to interface different vendor equipment and technology.

The creation of a virtualized environment allowing operators to view and control multi-subnet multi-technology networks into a single virtualized network highly facilitates network operators and will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

From Section 3 in which the generic ACTN business model was discussed, this section provides the application of the generic ACTN business model into multi-domain management context within a single

operator's Administrative Control. Thus, the following mapping is applied here:

Generic Business Model	Multi-domain Model
Customers	Multi-tenant Service Departments
Service Provider	Virtual Network Control Coordinator
Network Providers	Domain Networks

Figure 3 depicts the three-tier relationship of multi-domain model.

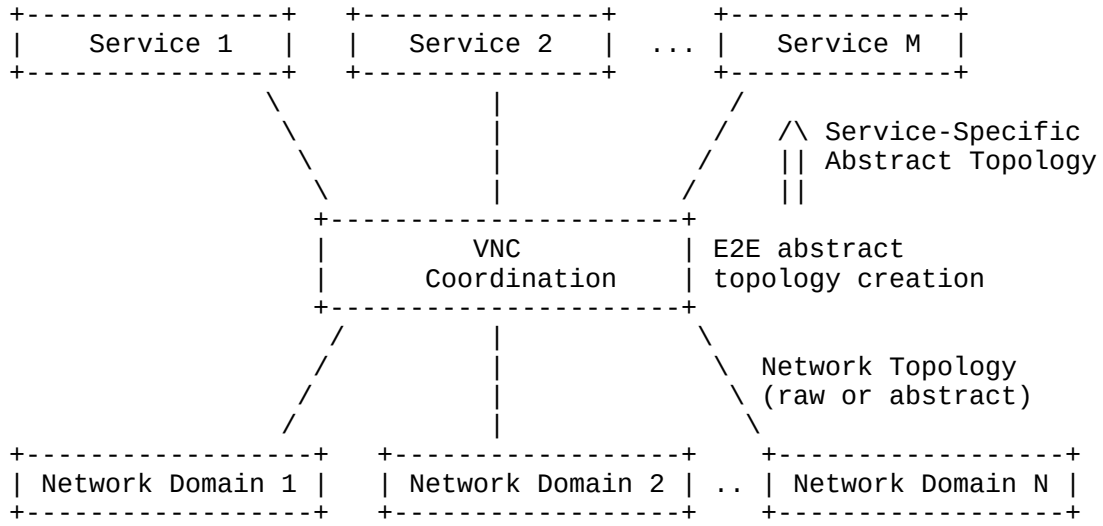


Figure 3: Multi-domain three-tier relationship

Figure 3 depicts the three entities that are internal to a single operator's control. Different services the operator support are sharing network resources via virtual network slicing. Each service has its own virtual network and manages based on this virtual network sliced for it. The VNC Coordination function facilitates the allocation of resources between the physical and the virtual.

Figure 4 depict a common scenario in which two different domains can be managed by a single VNC, which is in charge of acting as coordinator between them and presenting them as a single entity to its clients. For brevity's sake, the client is not depicted in the figure.

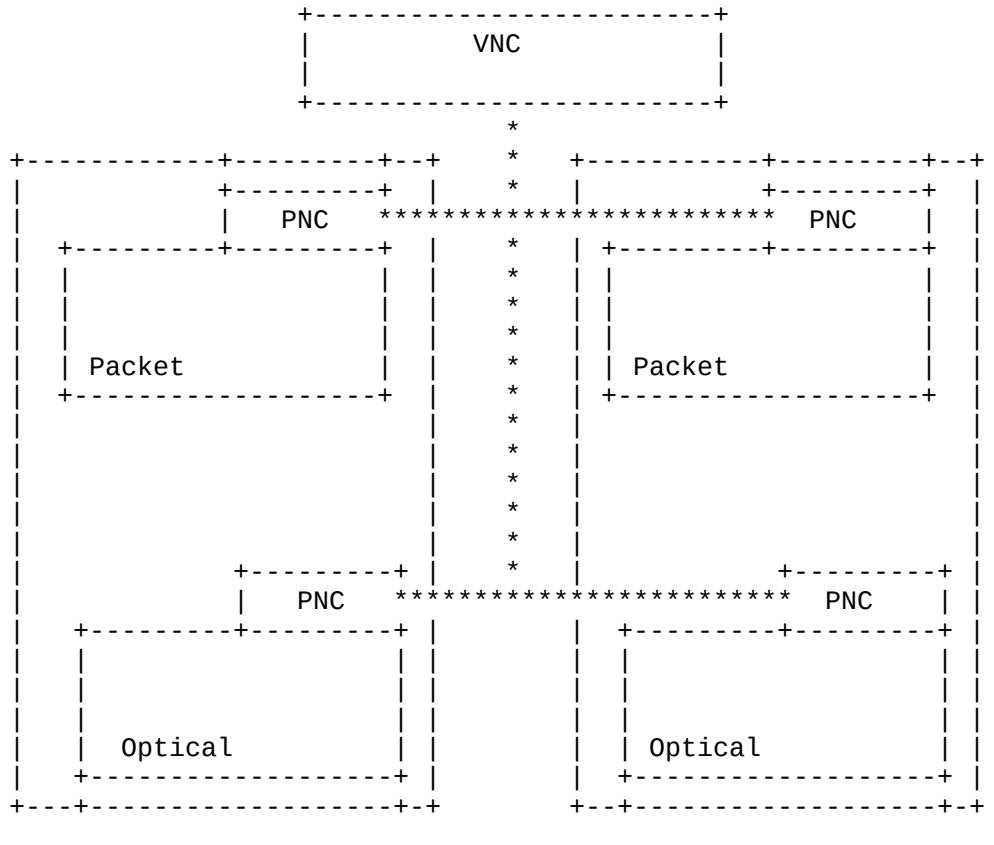


Figure 4: Multi-domain management for POI

In this figure the case of packet and optical domains controlled by different PNCs is shown but any combination can be considered, like e.g. a single PNC controlling the packet+optical domain 1 and different PNCs for domains 2.

5. Computation Model of ACTN

This section discusses ACTN framework from a computational point of view. As multiple customers run their virtualized network on a shared infrastructure (with either dedicated or shared resources), making efficient use of the underlying resources requires effective computational models and algorithms. This general problem space is known as Virtual Network Mapping or Embedding (VNM or VNE) [VNM-OP].

As VNM/VNE issues impose some additional compute models and algorithms for virtual network path computation, this section discusses key issues and constraints for virtual network path computation. Sections 5.1-5.3 discuss real-time processing aspect of computation model while the rest discuss policy-related or non real-time aspect of computation model.

5.1. Request Processing

This is concerned about whether a set of customer requests for VN creation can be dealt with in real-time or off line, and in the latter case, simultaneously or not. This depends on the nature of applications the customer support. There are applications and use cases, like e.g. management of catastrophic events or real time SLA negotiation, that require a real-time VN creation. If the customer does not require real-time instantiation of VN creation, the computation engine can process a set of VN creation requests simultaneously to improve network efficiency.

5.2. Computing Time

Depending on the nature of applications, how quickly a VN is instantiated from the time of request is an important factor. For dynamic applications that require instantaneous VN creation or VN changes from the existing one, the computation model/algorithm should support this constraint.

5.3. Path Constraints

There may be some factors of path constraints that can affect the overall efficiency. Path Split can lower VN request blocking if the underlying network can support such capability. A packet-based TE

network can support path split while circuit-based transport may have limitations.

Path migration is a technique that allows changes of nodes or link assignments of the established paths in an effort to accommodate new requests that would not be accepted without such path migration(s). This can improve overall efficiency, yet additional care needs to be applied to avoid any adverse impacts associated with changing the existing paths.

Re-optimization is a global process to re-shuffle all existing path assignments to minimize network resource fragmentation. Again, an extra care needs to be applied for re-optimization.

5.4. Types of Network Resources

When a customer makes a VN creation request to the substrate network, what kind of network resources is consumed is of concern of both the customer and service/network providers. The customer needs to put constraints (e.g. TE parameters, resiliency) for the provisioning of the VN, while the service and network providers need to choose which resources meet such constraints and possibly have fewest impact on the capability of serving other customers. For transport network virtualization, the network resource consumed is primarily network bandwidth that the required paths would occupy on the physical link(s). However, there may be other resource types such as CPU and memory that need to be considered for certain applications. These resource types shall be part of the VN request made by the customer.

5.5. Accuracy of Network Resource Representation

As the underlying transport network in itself may consist of a layered structure, it is a challenge how to represent these underlying physical network resources and topology into a form that can be reliably used by the computation engine that assigns customer requests into the physical network resource and topology.

5.6. Resource Sharing and Efficiency

Related to the accuracy of network resource representation is resource efficiency. As a set of independent customer VN is created and mapped onto physical network resources, the overall network resource utilization is the primary concern of the network provider.

In order to provide an efficient utilization of the resources of the provider network, it should be possible to share given physical

resources among a number of different VNs. Whether a virtual resource is sharable among a set of VNs (and hence of customers) is something the service provider needs to agree with each customer. Preemption and priority management are tools that could help provide an efficient sharing of physical resources among different VNs.

5.7. Guarantee of Client Isolation

While network resource sharing across a set of customers for efficient utilization is an important aspect of network virtualization, customer isolation has to be guaranteed. Admissions of new customer requests or any changes of other existing customer VNs must not affect any particular customer in terms of resource guarantee, security constraints, and other performance constraints. Admission Control

To coordinate the request process of multiple customers, an admission control will help maximize an overall efficiency.

6. Architecture Model for ACTN

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

6.1. ACTN Interfaces

To allow virtualization, the network has to provide open, programmable interfaces, in which customer applications can create, replace and modify virtual network resources in an interactive, flexible and dynamic fashion while having no impact on other customers. Direct customer control of transport network elements over existing interfaces (control or management plane) 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.

While the current network control plane is well suited for control of physical network resources via dynamic provisioning, path computation, etc., a virtual network controller needs to be built on top of physical network controller to support network virtualization. On a high-level, virtual network control refers to a mediation layer that performs several functions:

- Computation of customer resource requests into virtual network paths based on the global network-wide abstracted topology;

- Mapping and translation of customer virtual network slices into physical network resources;

- Creation of an abstracted view of network slices allocated to each customer, according to customer-specific objective functions, and to the customer traffic profile.

In order to facilitate the above-mentioned virtual control functions, the virtual network controller (aka., "virtualizer") needs to maintain two interfaces:

- One interface with the physical network controller functions which is termed as the Virtual Network Controller (VNC)-Physical Network Controller (PNC) Interface (VPI).

- Another interface with the Customer Network Controller for the virtual network, which is termed as Customer Network Controller (CNC) - Virtual Network Controller (VNC) Interface (CVI).

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:

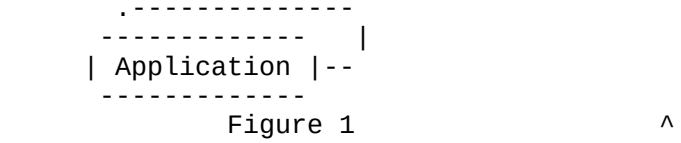


Figure 1

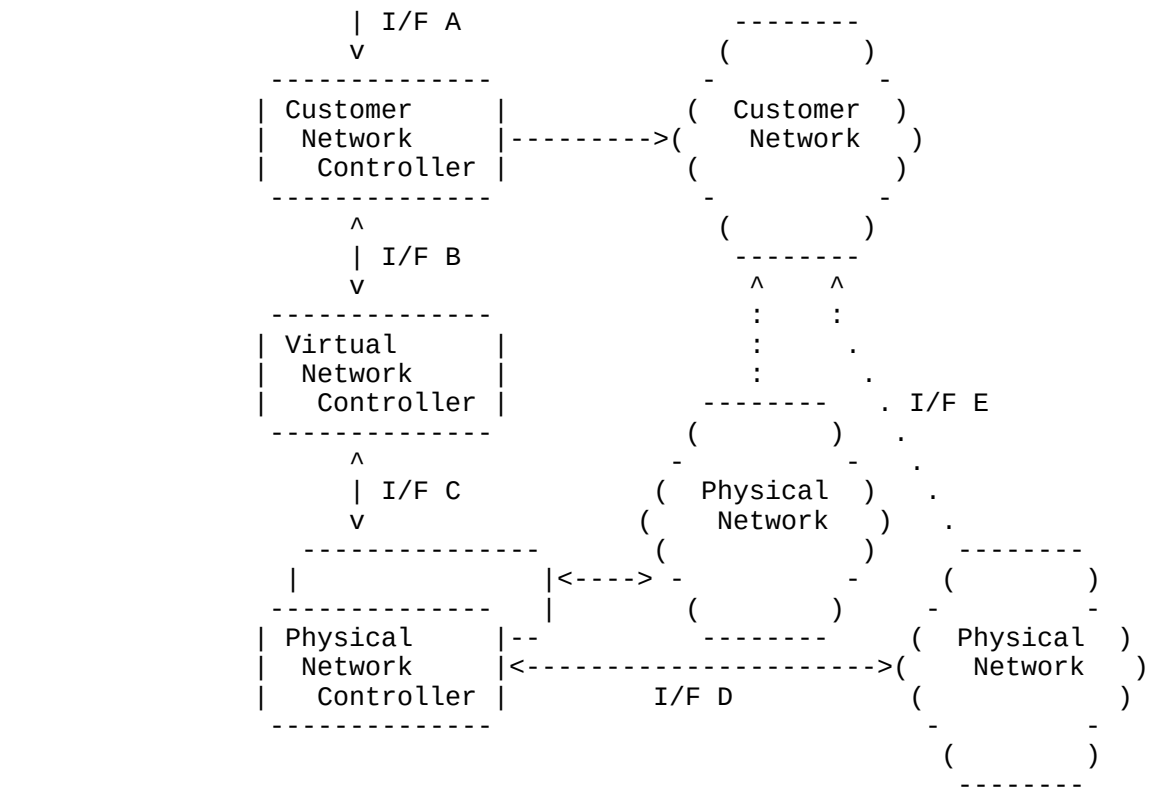


Figure 5. ACTN Interfaces

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: service topology, bandwidth and constraint information.

- Interface B: The CNC-VNC Interface (CVI) is an interface between a Customer Network Controller and a Virtual Network Controller. It requests the creation of the network resources and topology for the service or application. The Virtual Network Controller may also report potential network topology availability if queried for current capability from the Customer Network Controller.

. Interface C: The VNC-PNC Interface (VPI) is an interface between a Virtual Network Controller and a Physical Network Controller. It communicates the creation request, if required, of new connectivity of bandwidth changes in the physical network, via the Physical Network Controller. In multi-domain environments, the VNC needs to establish multiple VPIs, 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.

. Interface E: A mapping of physical resources to overlay resources.

6.1.1. ACTN Interface Scope

The north-bound interface (NBI) interfaces, direct control interfaces to NEs (Interface D) and Interface E are outside of the scope of ACTN.

The interfaces within scope of ACTN are:

- Interface B: The CNC-VNC Interface (CVI)

The CVI interface should allow programmability, first of all, to the customer so they can create, modify and delete virtual network service instances. This interface should also support open standard information and data models that can transport abstracted topology.

- Interface C: The VNC-PNC Interface (VPI)

The VPI interface should allow programmability to service provider(s) (through VNCs) in such ways that control functions such as path computation, provisioning, and restoration can be facilitated. Seamless mapping and translation between physical resources and virtual resources should also be facilitated via this interface.

6.2. Key ACTN Entities

6.2.1. Customer Network Controller

A Virtual Network Service is instantiated by the Customer Network Controller via the CVI. As the Customer Network Controller directly interfaces the application stratum, it understands multiple

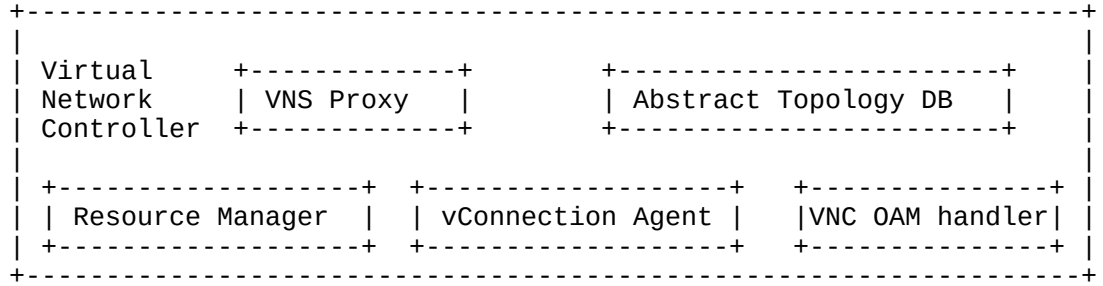
application requirements and their service needs. It is assumed that the Customer Network Controller and the VNC have a common knowledge on the end-point interfaces based on their business negotiation prior to service instantiation. End-point interfaces refer to customer-network physical interfaces that connect customer premise equipment to network provider equipment. Figure 6 shows an example physical network topology that supports multiple customers. In this example, customer A has three end-points A.1, A.2 and A.3. The interfaces between customers and transport networks are assumed to be 40G OTU links. For simplicity's sake, all network interfaces are assumed to be 40G OTU links and all network ports support ODU switching and grooming on the level of ODU1 and ODU2. Customer Network Controller for A provides its traffic demand matrix that describes bandwidth requirements and other optional QoS parameters (e.g., latency, diversity requirement, etc.) for each pair of end-point connections.

6.2.2. Virtual Network Controller

The virtual network controller sits between the customer network controller (the one issuing connectivity requests) and the physical network controller (the one managing the resources). The Virtual Network controller can be collocated with the physical network controller, especially in those cases where the service provider and the network provider are the same entity.

The architecture and building blocks of the VNC 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 [SDN-ARCH].

The following blocks do not identify the VNC architecture but only the functionalities required by the ACNT framework. Such functionalities could be implemented by functional blocks already defined in the existing SDN controller architectures:



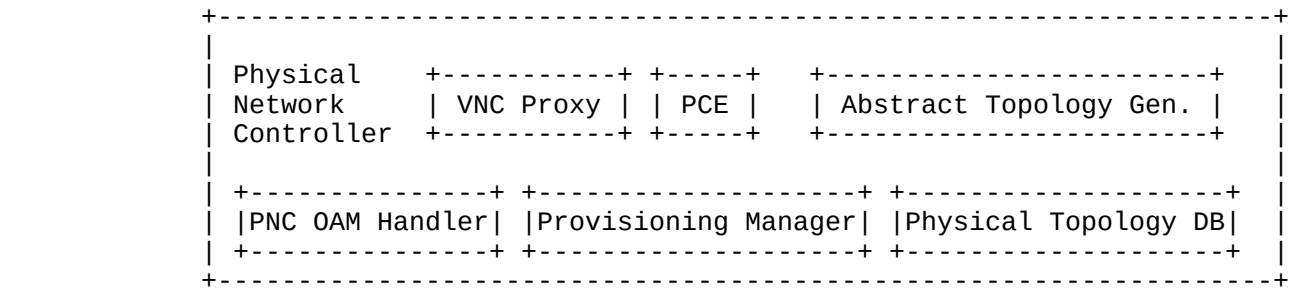
- VNS proxy: The VNS proxy is the functional module in charge of performing policy management and AAA (Authentication, authorization, and accounting) functions. It is the one that receives that VN instantiation and resource allocation requests from the Customer Network Controllers.
- Abstract Topology DB: This is the database where the abstract topology, generated by the VNC or received from the PNC, is stored. A different VN instance is kept for every different customer.
- Resource Manager: The resource manager is in charge of receiving VNS instantiation requests from the Customer Network Controller and, as a consequence, triggering a concurrent path computation request to the PCE in the PNC based on the traffic matrix. The Resource manager is also in charge of generating the abstract topology for the customer. It may request abstract network topology to PNC.
- vConnection Agent: This module is in charge of mapping VN setup commands into network provisioning requests to the PNC.
- VNC OAM handler: The VNC OAM handler is the module that is in charge of understanding how the network is operating, detecting faults and reacting to problems related to the abstract topology.

6.2.3. 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 VNC.

The architecture and building blocks of the PNC 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 [SDN-ARCH].

The following blocks do not identify the PNC architecture but only the functionalities required by the ACNT framework. Such functionalities could be implemented by functional blocks already defined in the existing SDN controller architectures:



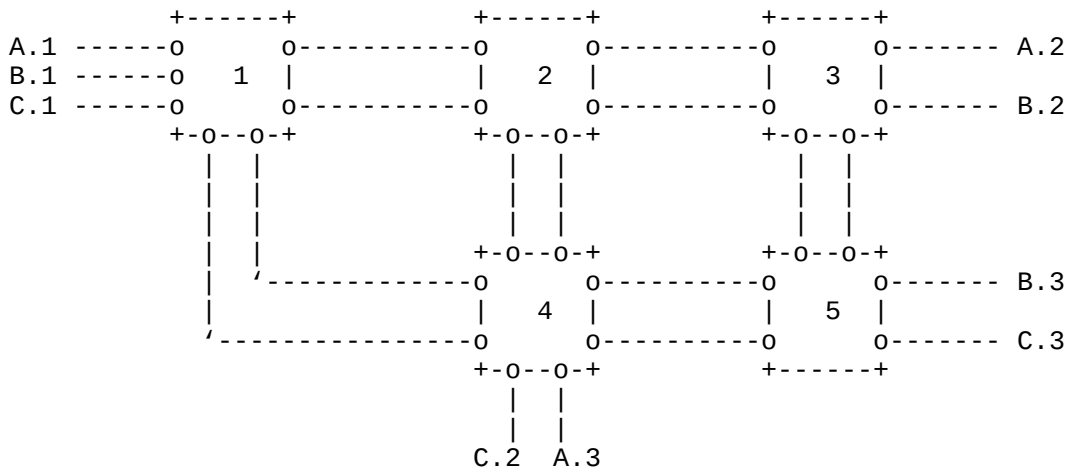
. VNC proxy: The VNC proxy is the functional module in charge of performing policy management and AAA (Authentication, authorization, and accounting) functions on requests coming from the VNC.
. PCE: This is the stateful PCE performing the path computation over the physical topology and that provides the vConnection agent with the network topology/network paths (LSPs).
. Abstract topology generator: the network topology can be passed to the VNC as raw or abstract. In case the topology is passed as abstract topology, this module is in charge of generating it from the physical topology DB. The module is optional.
. PNC OAM handler: it verifies that connections exists, implements monitoring functions to see if failures occurs. It is the proxy to an OSS/NMS system but does not duplicate any of OSS/NMS functionalities.
. Physical topology database: The physical topology database is mainly composed by two databases: the Traffic Engineering Database (TED) and the LSP Database (LSP-DB).
. Provisioning Manager: The Provisioning Manager is responsible for initiating direct requests, or relaying requests, for the establishment of connections. These direct requests might include instructions to the control plane running in the underlay networks, or may involve the programming of individual network devices to establish forwarding state in the network. This functional component and role is described in more detail in the Application-Based Network Operations (ABNO) architecture [ABNO], other controllers include the OpenFlow Controller [ONF].

6.3. Abstracted Topology Illustration

There are two levels of abstracted topology that needs to be maintained and supported for ACTN. Customer-specific Abstracted Topology refers to the abstracted view of network resources

allocated (shared or dedicated) to the customer. The granularity of this abstraction varies depending on the nature of customer applications. Figure 6 illustrates this.

Figure 6 shows how three independent customers A, B and C provide its respective traffic demand matrix to the VNC. The physical network topology shown in Figure 6 is the provider’s network topology generated by the PNC topology creation engine such as the link state database (LSDB) and Traffic Engineering DB (TEDB) based on control plane discovery function. This topology is internal to PNC and not available to customers. What is available to them is an abstracted network topology (a virtual network topology) based on the negotiated level of abstraction. This is a part of VNS instantiation between a client control and VNC.



Traffic Matrix for Customer A

	A.1	A.2	A.3
A.1	-	20G	20G
A.2	20G	-	10G
A.3	20G	10G	-

Traffic Matrix for Customer B

	B.1	B.2	B.3
B.1	-	40G	40G
B.2	40G	-	20G
B.3	40G	20G	-

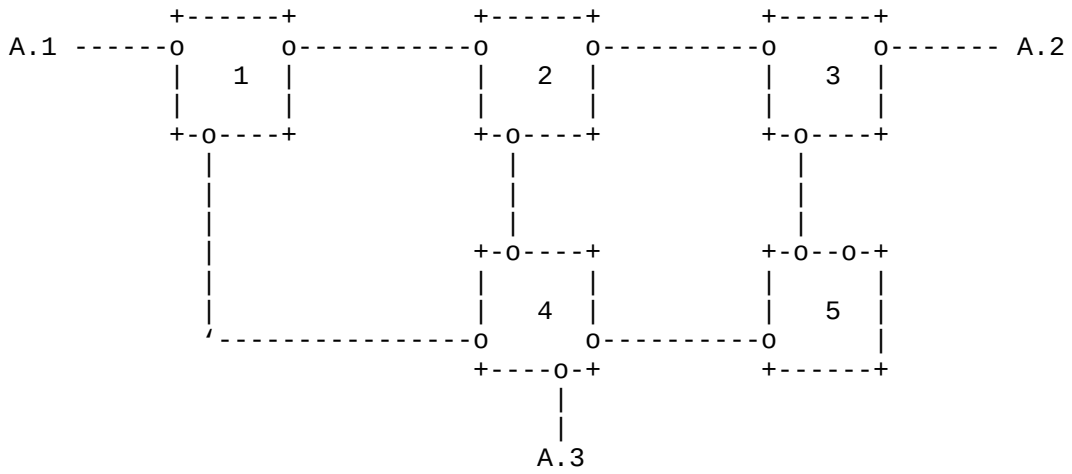
Traffic Matrix for Customer C

	C.1	C.2	C.3
C.1	-	20G	20G
C.2	20G	-	10G
C.3	20G	10G	-

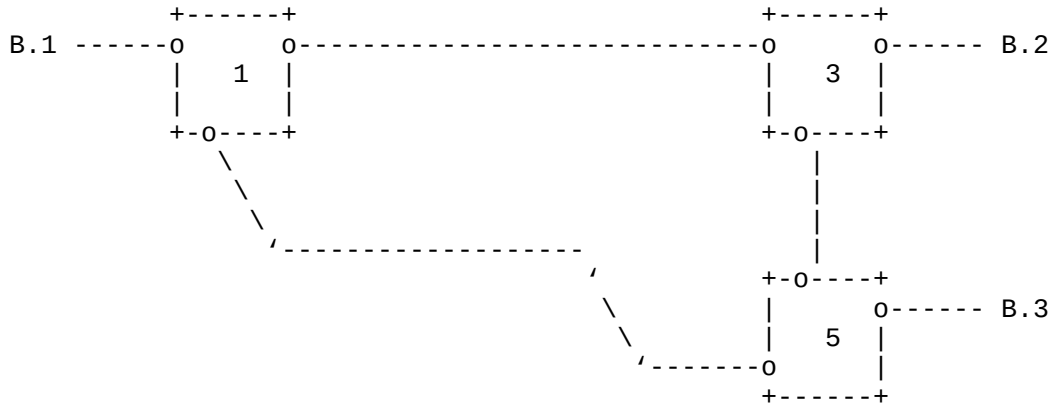
Figure 6: Physical network topology shared with multiple customers

Figure 7 depicts illustrative examples of different level of topology abstractions that can be provided by the VNC topology abstraction engine based on the physical topology base maintained by the PNC. The level of topology abstraction is expressed in terms of the number of virtual nodes (VNs) and virtual links (VLs). For example, the abstracted topology for customer A shows there are 5 VNEs and 10 VLs. This is by far the most detailed topology abstraction with a minimal link hiding compared to other abstracted topologies in Figure 7.

(a) Abstracted Topology for Customer A (5 VNEs and 10 VLs)



(b) Abstracted Topology for Customer B (3 VNEs and 6 VLs)



(c) Abstracted Topology for Customer C (1 VNE and 3 VLs)

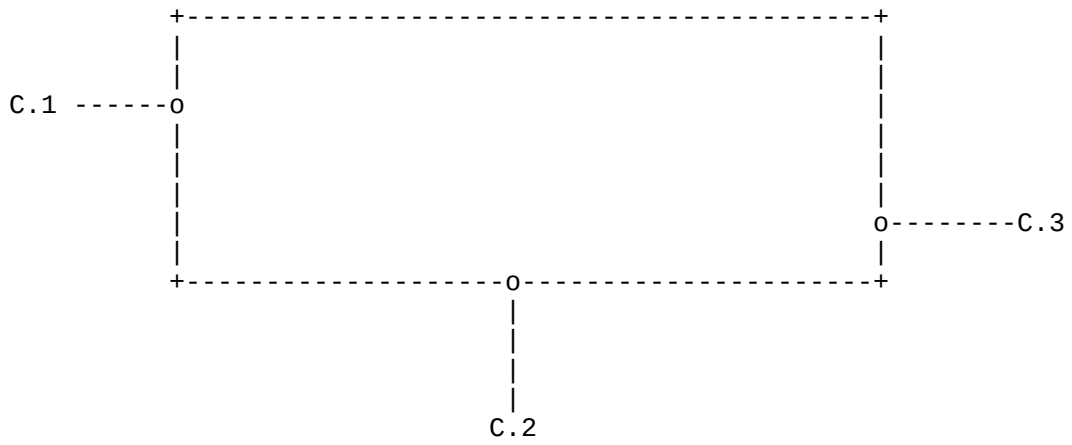


Figure 7: Topology Abstraction Examples for Customers

As different customers have different control/application needs, abstracted topologies for customers B and C, respectively show a much higher degree of abstraction. The level of abstraction is determined by the policy (e.g., the granularity level) placed for the customer and/or the path computation results by the PCE operated by the PNC. The more granular the abstraction topology is, the more control is given to the Customer Network Controller. If the Customer Network Controller has applications that require more granular control of virtual network resources, then the abstracted topology shown for customer A may be the right abstraction level for such controller. For instance, if the customer is a third-party virtual service broker/provider, then it would desire much more sophisticated control of virtual network resources to support different application needs. On the other hand, if the customer were only to support simple tunnel services to its applications, then the abstracted topology shown for customer C (one VNE and three VLs) would suffice.

6.4. ACTN Interface Interaction

The following list provides examples on the type of interaction and communication exchange between key ACTN interfaces:

- Interface B: Customer Network Controller to Virtual Network Controller.

1. Security/Policy Negotiation (Who are you?)
   a. External Entity vs. Internal Service Department
   b. Push/Pull support

2. VN Query (Can you give me VN?)
   a. VN end-points (CE end points)
   b. VN service requirement
   - Latency only
   - B/W guarantee
   - Latency and B/W guarantee together
   c. VN diversity
   - Node/Link disjoint from other VNs
   - VN level diversity (e.g., VN1 and VN2 must be disjoint)
   d. VN type
   - Path vector (tunnel)
   - Node/Links (graph)

3. VN Query Response (Available VNs)
   a. For VN,
   - This is what can be reserved for you
   - This is what is available beyond what is given to you (potential)

4. VN Instantiation Request (I need VN for my service, please instantiate my VN) - with or without VN Query
   a. VN end-points
   b. VN service requirement
   - Latency only
   - B/W guarantee
   - Latency and B/W guarantee together
   c. VN diversity
   - Node/Link disjoint from other VNs
   - VN level diversity (e.g., VN1 and VN2 must be disjoint)
   d. VN type
   - Path vector (tunnel)
   - Node/Links (graph)
   e. VN instance ID per service (unique ID to identify VNs)
   f. VN level policy
   - On-demand VN creation (time/day)

5. VN Instantiation Confirmation (VN instantiated to my physical networks)
   a. VN instance ID

b. Abstraction topology (with data model)
c. If failed to instantiate the requested VN, say why

6. VN lifecycle management/operation
a. Create (same as VN instantiate Request)
b. Delete
c. Modify
d. Update (VN level Performance Monitoring) under policy agreement

- Interface C: Virtual Network Controller to Physical Network Controller.

1. Security/Policy negotiation (who are you?)
a. Exchange of key, etc.
b. Domain preference + local policy exchange
- Push/Pull support
- Preferred peering points
- Preferred route

2. Topology Query /Response (Pull Model: Please give me your domain topology)
a. TED Abstraction level negotiation
- Physical topology (per policy)
- Abstract topology (per policy)
b. Node/Link metrics
- Node/Link Type (Border/Gateway, etc.)
- All TE metrics (SRLG, etc.)

3. Topology Update (Push Model from PNC to VNC)
a. Under policy agreement, topology changes to be pushed to VNC from PNC

4. VN Path Computation Request (Please give me a path)
a. VN Instance ID (Note: this is passed from CC to VNC)
b. End-point information
- CE ends
- Border points (if applicable)
c. All other PCE request info (PCEP)

5. VN Path Computation Reply (here’s the path info per your request)
a. Path level abstraction - LSP DB like

6. VN Path Setup Request / Reply (please setup my paths)
a. Per domain path request
- Single request

- Multiple requests - diversity path request, etc.
b. Domain sequence kept at VNC
c. Coordination of signaling (multi-domain)

7. VN Path Modification/Rerouting/re-grooming (please change these paths)
a. VN Instance ID

8. VN Performance Monitoring
a. VN Instance ID
b. VN Connection Failure and other degradation report
c. Pull/Push Models

7. Design Principles of ACTN

7.1. Network Security

Network security concerns are always one of the primary principles of any network design. ACTN is no exception. Due to the nature of heterogeneous VNs that are to be created, maintained and deleted flexibly and dynamically and the anticipated interaction with physical network control components, secure programming models and interfaces have to be available beyond secured tunnels, encryption and other network security tools.

7.2. Privacy and Isolation

As physical network resources are shared with and controlled by multiple independent customers, isolation and privacy for each customer has to be guaranteed.

Policy should be applied per client.

7.3. Scalability

As multiple VNs need to be supported seamlessly, there are potentially several scaling issues associated with ACTN. The VN Controller system should be scalable in supporting multiple parallel computation requests from multiple customers. New VN request should not affect the control and maintenance of the existing VNs. Any VN request should also be satisfied within a time-bound of the customer application request.

Interfaces should also be scalable as a large amount of data needs to be transported across customers to virtual network controllers and across virtual network controllers and physical network controllers.

7.4. Manageability and Orchestration

As there are multiple entities participating in network virtualization, seamless manageability has to be provided across every layer of network virtualization. Orchestration is an important aspect of manageability as the ACTN design should allow orchestration capability.

ACTN orchestration should encompass network provider multi-domains, relationships between service provider(s) and network provider(s), and relationships between customers and service/network providers.

Ease of deploying end-to-end virtual network services across heterogeneous network environments is a challenge.

7.5. Programmability

As discussed earlier in Section 5.5, the ACTN interfaces should support open standard interfaces to allow flexible and dynamic virtual service creation environments.

7.6. Network Stability

As multiple VNs are envisioned to share the same physical network resources, combining many resources into one should not cause any network instability. Provider network oscillation can affect readily both on virtual networks and the end-users.

Part of network instability can be caused when virtual network mapping is done on an inaccurate or unreliable resource data. Data base synchronization is one of the key issues that need to be ensured in ACTN design.

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.

[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.

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

[VNM-OP] Melo, M, et al. "Virtual Network Mapping - An Optimization Problem", Springer Berlin Heidelberg, January 2012.

[SDN-ARCH] Open Networking Foundation, "SDN Architecture", Issue 1, June 2014.

Appendix A

Contributors' Addresses

Dhruv Dhoddy
Huawei Technologies
dhruv.ietf@gmail.com

Dave Hood
Ericsson
dave.hood@ericsson.com

Authors' Addresses

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

Luyuan Fang
Email: luyuanf@gmail.com

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

Network Working Group
Internet Draft

Daniele Ceccarelli (Editor)
Ericsson

Intended status: Informational
Expires: September 2015

Young Lee (Editor)
Huawei

March 9, 2015

Framework for Abstraction and Control of Transport Networks

draft-ceccarelli-actn-framework-07.txt

Status of this Memo

Copyright Notice

Abstract

This draft provides a framework for abstraction and control of transport networks.

Table of Contents

1. Introduction

Transport 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.

Transport networks in this draft refer to a set of different type of connection-oriented networks, primarily Connection-Oriented Circuit Switched (CO-CS) networks and Connection-Oriented Packet Switched (CO-PS) networks. This implies that at least the following transport networks are in scope of the discussion of this draft: Layer 1(L1)

and Layer 0 (L0) optical networks (e.g., Optical Transport Network (OTN), Optical Channel Data Unit (ODU), Optical Channel (OCh)/Wavelength Switched Optical Network (WSON)), Multi-Protocol Label Switching - Transport Profile (MPLS-TP), Multi-Protocol Label Switching - Traffic Engineering (MPLS-TE), as well as other emerging technologies with connection-oriented behavior. One of the characteristics of these network types is the ability of dynamic provisioning and traffic engineering such that resource guarantees can be provided to their clients.

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 from a 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
. End to end coordination of multiple SDN and pre-SDN domains
  e.g. NMS, MPLS-TE or GMPLS.

As transport networks evolve, the need to provide network 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 Transport 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, in general, refers to allowing the customers to utilize a certain amount of network resources as if they own them and thus control their allocated resources in a way most optimal with higher layer or application processes. This empowerment of customer control facilitates introduction of new services and

applications as the customers are permitted to create, modify, and delete their virtual network services. 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 the set of consumed services as well as to a particular customer. As the Customer Network Controller is envisioned to support a plethora of distinct applications, there would be another level of virtualization from the customer to individual applications.

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

- Abstraction of the underlying network resources to higher-layer applications and users (customers); abstraction for a specific application or customer is referred to as virtualization in the ONF SDN architecture. [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-subnet multi-technology networks into a single virtualized network;

- Possibility of providing a customer with abstracted network or abstracted 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 multi-domain coordination of the underlying transport domains, presenting it as an abstracted topology to the customers via open and programmable interfaces. This allows for the recursion of controllers in a customer-provider relationship.

The organization of this draft is as follows. Section 2 provides a discussion for a Business Model, Section 3 ACTN Architecture, Section 4 ACTN Applicability, and Section 5 ACTN Interface requirements.

2. Business Model of ACTN

The traditional Virtual Private Network (VPN) and Overlay Network (ON) models are built on the premise that one single network provider provides all virtual private or overlay networks to its customers. This model is simple to operate but has 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 services offer is not enough but it is desirable to provide each of them with customized virtual network

services. Advanced customers may own dedicated virtual resources, or share resources, but shared resources are likely to be governed by more complex SLA agreements; moreover they may have the ability to modify their service parameters directly (within the scope of their virtualized environments. As customers are geographically spread over multiple network provider domains, the necessary control and data interfaces to support such customer needs is no longer a single interface between the customer and one single network provider. With this premise, customers have to interface multiple providers to get their end-to-end network connectivity service and the associated topology information. Customers may have to support multiple virtual network services with different service objectives and QoS requirements. For flexible and dynamic applications, customers may want to control their allocated virtual network resources in a dynamic fashion. To allow that, customers should be given an abstracted view of topology on which they can perform the necessary control decisions and take the corresponding actions. 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

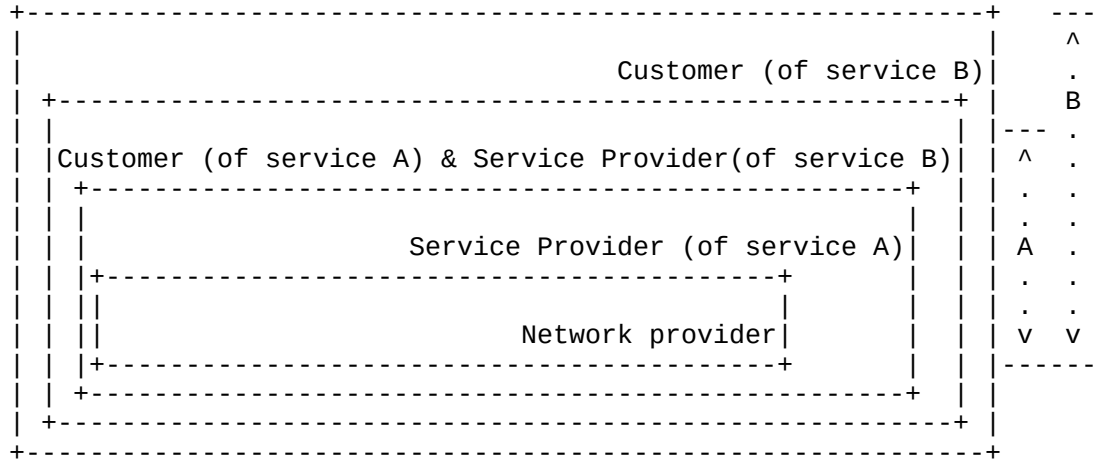
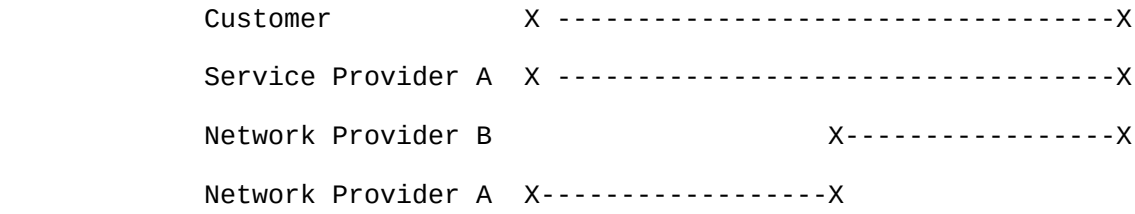


Figure 1: Network Recursiveness.

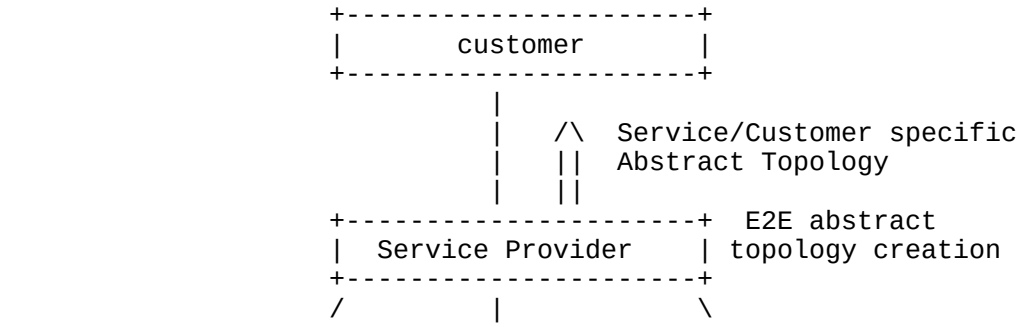
2.2. Service Providers

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.



The ACTN network model is predicated upon this three tier model and is summarized in figure below:



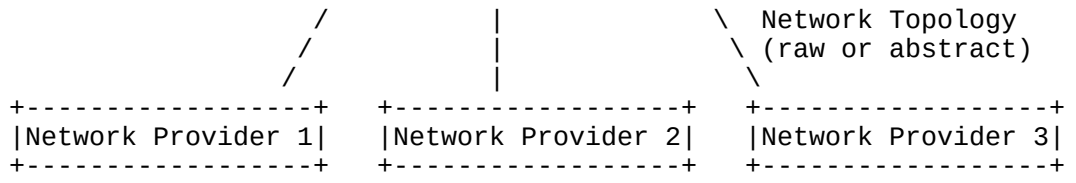


Figure 2: Three tier model.

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 clients, 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.

The network provider space is the one where recursiveness occurs. A customer-provider relationship between multiple service providers can be established leading to a hierarchical architecture of controllers within service provider network.

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 functionality is covering two types of services:

- 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 between customers' premises and service provider premises and are provided mostly by cloud providers or content delivery providers. The context may include, but not limited to a security function like firewall, a traffic optimizer, the provisioning of storage or computation capacity where the customer does not care whether the service is implemented in a given data center or another. These services may be hosted virtually by the provider or physically part of the network. This allows the service provider to hide his own resources (both network and data centers) and divert customer requests where most suitable. This is also known as "end points mobility" case and introduces new concepts of traffic and service provisioning and resiliency. (e.g. Virtual Machine mobility)." (See Section 4.2.3)

About the Customer service-related knowledge it includes:

- VN Service Requirements: The end customer would have specific service requirements for the VN including the customer endpoints access profile as well as the E2E customer service objectives. The ACTN framework architectural "entities" would monitor the E2E service during the lifetime of VN by focusing on both the connectivity provided by the network as well as the customer service objectives. These E2E service requirements go beyond the VN service requirements and include customer infrastructure as well.

- Application Service Policy: Apart for network connectivity, the customer may also require some policies for application specific features or services. The ACTN framework would take these application service policies and requirements into consideration while coordinating the virtual network operations, which require end customer connectivity for these advanced services.

While the "types" of controller defined are shown in Figure 3 below and are the following:

. CNC - Customer Network Controller

. MDSC - Multi Domain Service Coordinator
. PNC - Physical Network Controller

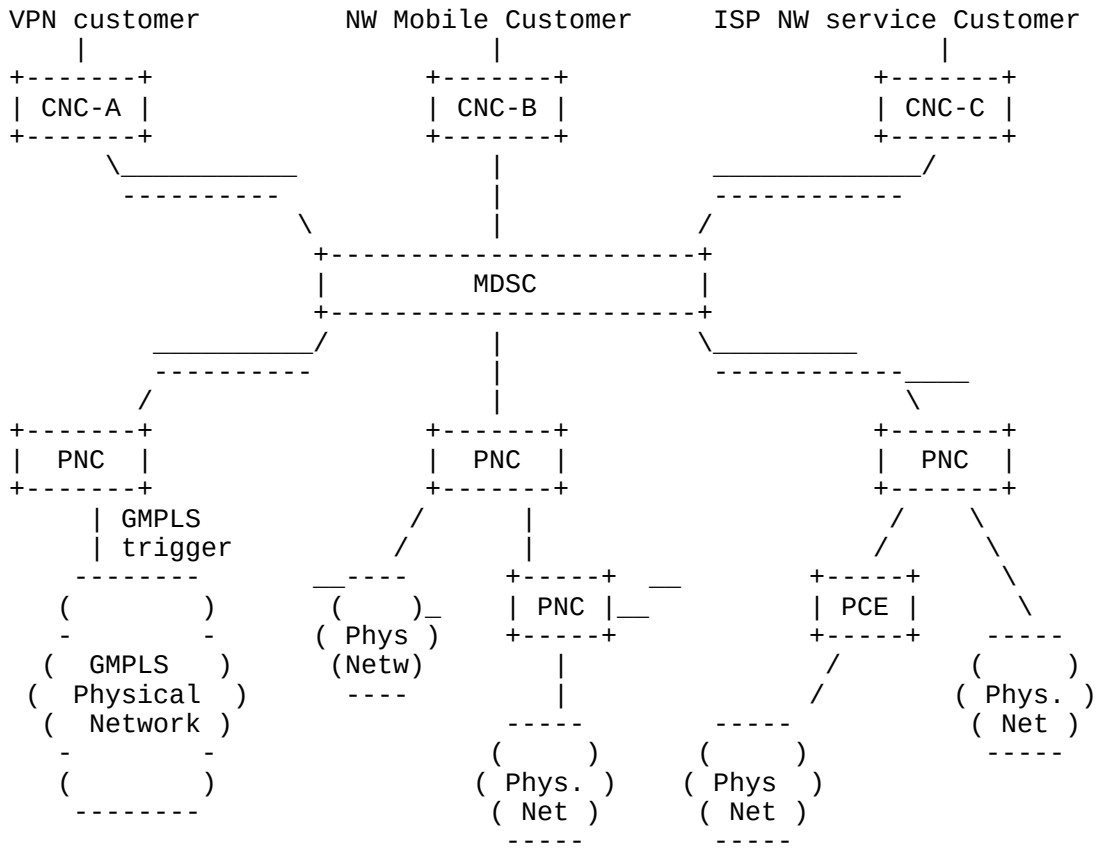


Figure 3: ACTN Control Hierarchy

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 application stratum, 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. Figure 10 in Appendix shows an example physical network topology that supports multiple customers. In this example, customer A has

three end-points A.1, A.2 and A.3. The interfaces between customers and transport networks are assumed to be 40G OTU links.

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.
A hierarchy of MDSCs can be foreseen for scalability and administrative choices.

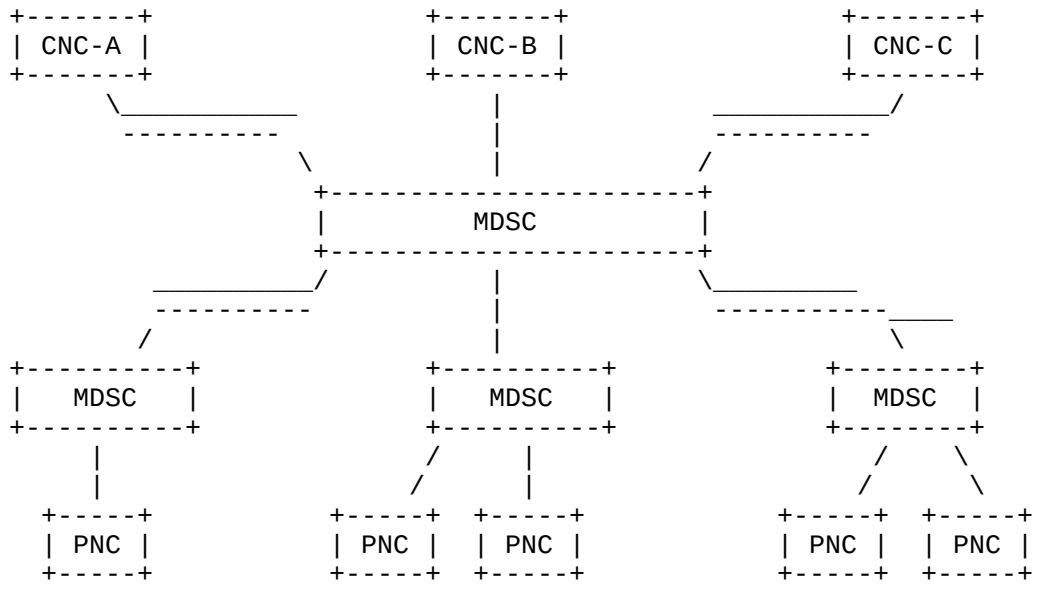


Figure 4: Controller recursiveness

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).
It should be noted that the interface between the parent MDSC and a child MDSC does not introduce any complexity as it is "internal" and "transparent" from the perspective of the CNCs and the PNCs and it makes use of the same interface model and its primitives as the CMI and MPI.

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.

While the current network control plane is well suited for control of physical network resources via dynamic provisioning, path computation, etc., a multi service domain controller needs to be built on top of physical network controller to support network virtualization. On a high-level, virtual network control refers to a mediation layer that performs several functions:

Figure 4 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 4 (ACTN Interfaces) below:

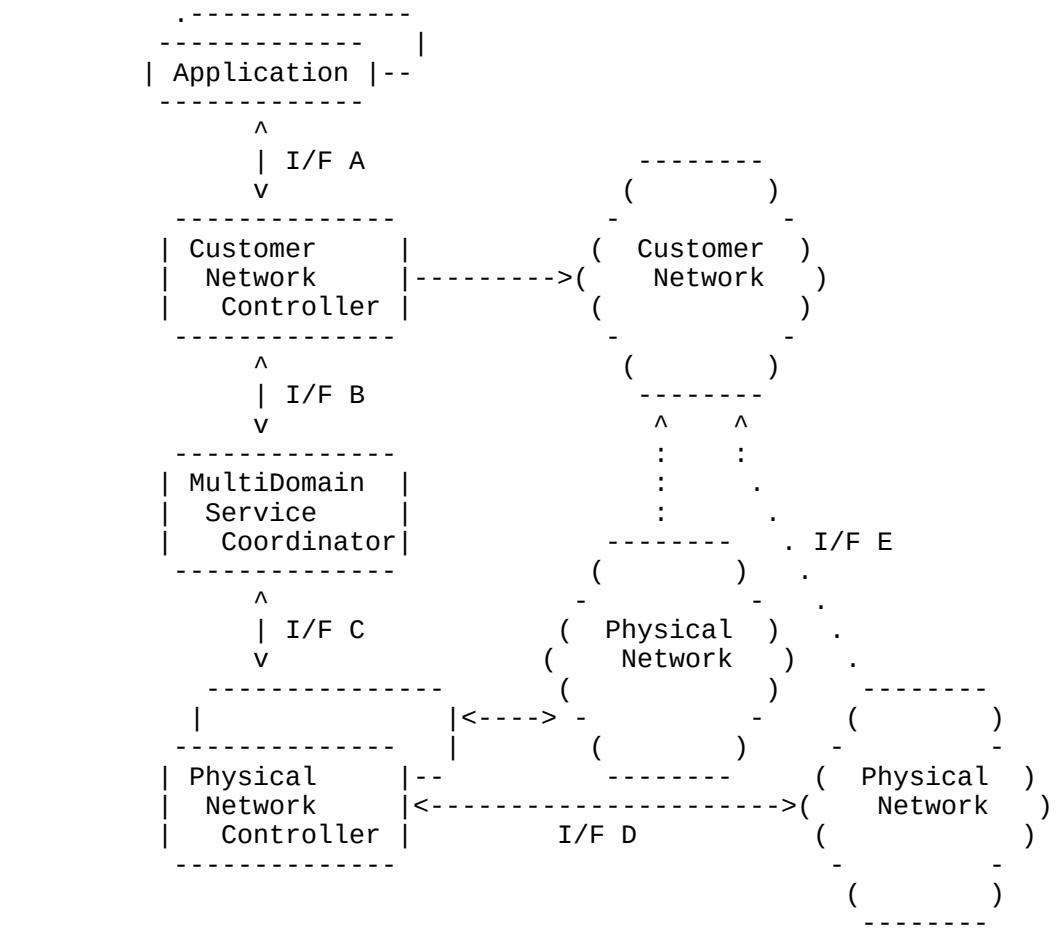


Figure 4: ACTN Interfaces

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.

. Interface E: A mapping of physical resources to overlay resources.

The interfaces within the ACTN scope are B and C.

3.5. Work in Scope of ACTN

This section provides a summary of use-cases in terms of two categories: (i) service-specific requirements; (ii) network-related requirements.

Service-specific requirements listed below are uniquely applied to the work scope of ACTN. Service-specific requirements are related to virtual service coordination function defined in Section 3. These requirements are related to customer’s VNs in terms of service policy associated with VNs such as service performance objectives, VN endpoint location information for certain required service-specific functions (e.g., security and others), VN survivability requirement, or dynamic service control policy, etc.

Network-related requirements are related to virtual network operation function defined in Section 3. These requirements are related to multi-domain and multi-layer signaling, routing, protection/restoration and synergy, re-optimization/re-grooming, etc. These requirements are not inherently unique for the scope of ACTN but some of these requirements are in scope of ACTN, especially for coherent/seamless operation aspect of multiple controller hierarchy.

The following table gives an overview of service-specific requirements and network-related requirements respectively for each ACTN use-case and identifies the work in scope of ACTN.

Details on these requirements will be developed into the information model in [ACTN-Info].

Use-case	Service-specific Requirements	Network-related Requirements	ACTN Work Scope
[Cheng]	- E2E service provisioning - Performance monitoring - Resource utilization abstraction	- Multi-layer (L2/L2.5) coordination - VNO for multi-domain transport networks	- Dynamic multi-layer coordination based on utilization is in scope of ACTN - YANG for utilization abstraction
[Dhody]	- Service awareness/ coordination between P/O.	- POI Performance monitoring - Protection/ Restoration synergy	- Performance related data model may be in scope of ACTN - Customer’s VN survivability policy enforcement for protection/restoration is unique to ACTN.
[Fang]	- Dynamic VM migration (service), Global load balancing (utilization efficiency), Disaster recovery - Service-aware network	- On-demand virtual circuit request - Network Path Connection request	- Multi-destination service selection policy enforcement and its related primitives/information are unique to

	query - Service Policy Enforcement		ACTN. - Service-aware network query and its data model can be extended by ACTN.
[Klee]		- Two stage path computation E2E signaling coordination - Abstraction of inter-domain info - Enforcement of network policy (peering, domain preference) - Network capability exchange (pull/push, abstraction level, etc.)	- Multi-domain service policy coordination to network primitives is in scope of ACTN
[Kumaki]	- On-demand VN creation - Multi-service level for VN - VN survivability /diversity/confidentiality		- All of the service-specific lists in the left column is unique to ACTN.
[Lopez]	- E2E accounting and resource usage data	- E2E connection management, path provisioning - E2E network	- Escalation of performance and fault management

	- E2E service policy enforcement	monitoring and fault management	data to CNC and the policy enforcement for this area is unique to ACTN.
-------	----------	----------	----------
[Shin]	- Current network resource abstraction Endpoint/DC dynamic selection (for VM migration)	- LB for recovery - Multi-layer routing and optimization coordination	- Multi-layer routing and optimization are related to VN's dynamic endpoint selection policy.
-------	----------	----------	----------
[Xu]	- Dynamic service control policy enforcement - Dynamic service control	- Traffic monitoring - SLA monitoring	- Dynamic service control policy enforcement and its control primitives are in scope of ACTN - Data model to support traffic monitoring data is an extension of YANG model ACTN can extend.

4. References

4.1. Informative References

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

[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.

[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.

5. 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

Network Working Group
Internet Draft
Intended status: Informational
Expires: January2015

Weiqiang Cheng
CMCC

Yunbin Xu
CATR

Guoying Zhang
CATR

July 21, 2014

ACTN Use-cases for Packet Transport Networks in Mobile Backhaul Networks
draft-cheng-actn-ptn-requirements-00.txt

Status of this Memo

This Internet-Draft is submitted 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 January 10, 2015.

Copyright Notice

Abstract

This document describes the key requirements for ACTN in carrier's transport networks, which mainly focus on the Packet Transport Networks.

Table of Contents

1. Introduction

MPLS-TP based packet transport network (PTN) has been widely used as mobile backhaul and enterprise customer private line/LAN solutions in many carrier's networks. The Packet Transport Networks work in different layers from L2 to L3 and in different areas such as access, metro and backbone networks. In the application scenarios, the most important requirements for operators are to solve the interoperability problems between multi-domain/multi-layer networks, realize the fast service provisioning, and improve the network operation efficiency.

The PTN operators may use ACTN to improve efficiency of provision and operation, optimize the resources utilization, and promote the customer's experiences. This draft mainly discusses the key requirements for ACTN in carrier's Packet Transport Networks.

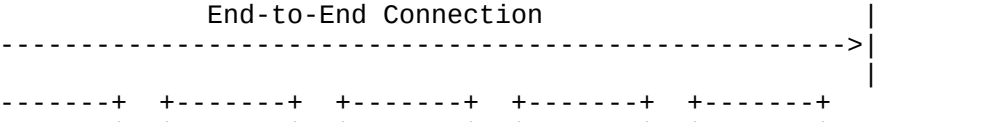
2. ACTN Requirement for Packet Transport Networks

2.1. End-to-End Enterprise Services Provisioning

The enterprise customer services are sensitive to the network quality, have strict time-limit requirement for service establishment. Faster end-to-end service provisioning may make the operators win the competition.

The operators had built a large scale of packet transport networks and divided them into different areas such as access, metro and backbone networks, each area has their own management systems. Currently in most application scenarios, PTN networks are using static provisioning with centralized Network management Systems (NMS). However, they are hard to meet the requirements of current enterprise services for fast provisioning and efficient operation.

The ACTN architecture [ACTN-FWK] should be considered to coordinate with traditional the networks management systems, so as to realize the end-to-end service provision.



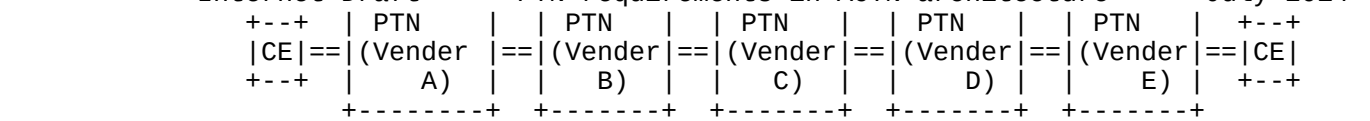


Figure 1 End-to-End Connection in Mobile Backhaul Networks

2.2. Multi-layer coordination Requirement in L2/L3 Packet Transport Networks

LTE backhauling requires the PTN to realize L3 network function. This function requires the management systems operate in different layers of networks, and leads to separate and fragmented network configuration. Further, the L2 PTN and L3 PTN networks may be provided by different venders, and make the end-to-end provisioning much more complex. In the ACTN architecture, new functions such as topology detection and virtualization, auto-routing calculation are introduced. With these functions, operator can improve the user experiences and lower the OPEX.

On the other hand, operators want to obtain the flow information and realize the load balancing within L3 PTN networks,

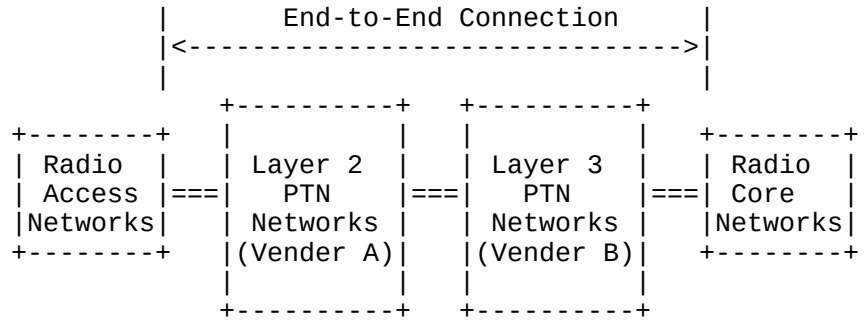


Figure 2 End-to-End Connection for L2&L3 PTN Networks

2.3. Optimizing the network resources utilization

The packet transport networks can support various performances monitoring matrix, such as traffic flow statistics, packet delay, delay variation, throughput and packet-loss rate, etc. All these performance parameters can support the enterprise customers SLA requirements. Through the performance monitoring, the PTN can

realize the service SLA optimization and network traffic optimization. See [ACTN-PERF] for related discussion.

3. Virtual Networks Operations for Packet Transport Networks

Figure 3 shows an example of virtual network operations for packet transport networks. In order to realize end-to-end service provision, the ACTN architecture [ACTN-FWK] should consider coordination with traditional network management systems. By the network virtualization and abstraction, the traditional networks can be considered as a virtual network for VNC service provider, which can be realized by network management systems providing an abstract agent for VNC, or the VNC providing traditional interface for NMS.

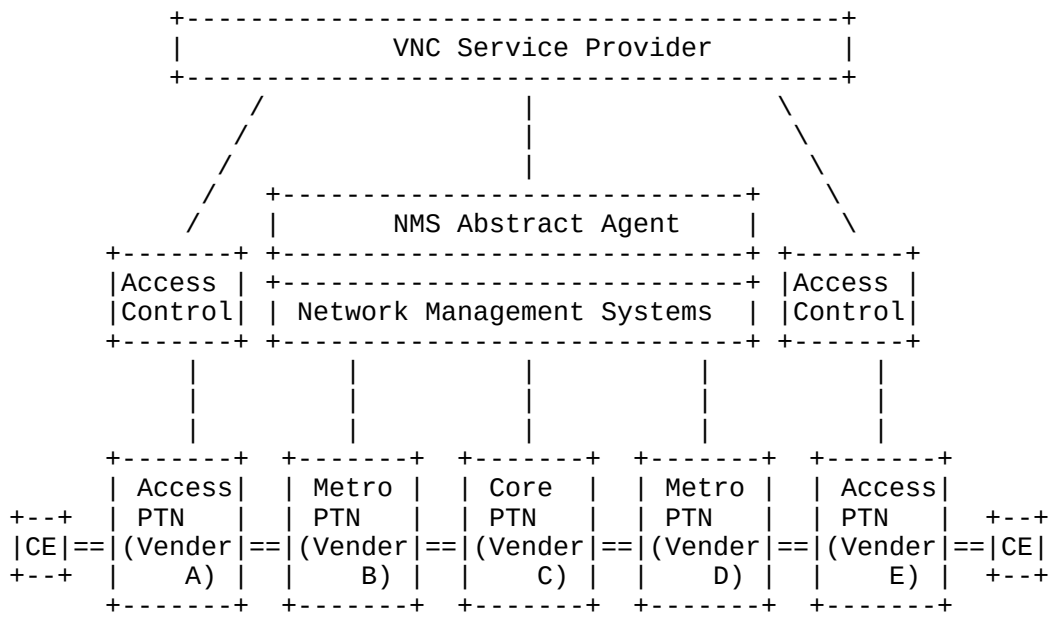


Figure 3 End-to-End Connection in Mobile Backhaul Networks

4. Security Considerations

This document raises no new security issues.

5. IANA Considerations

No new IANA considerations are raised by this document.

6. References

6.1. Informative References

[ACTN-FWK] Daniele C., Luyuan Fang, Yong Lee and Diego Lopez, "Framework for Abstraction and Control of Transport Networks", draft-ceccarelli-actn-framework-02.

[ACTN-PERF] Yunbin Xu, Weiqiang Cheng, Guoying Zhang and Haomian Zheng, "Use Cases and Requirements of Dynamic Service Control based on Performance Monitoring in ACTN Architecture", draft-xu-actn-perf-dynamic-service-control-01.

Authors's Address

Weiqiang Cheng
China Mobile Communication Company
No.32 Xuanwumen West Street, Xicheng District, Beijing, China
Email:chengweiqiang@chinamobile.com
Yunbin Xu
China Academy of Telecom Research
NO.52 Huayuan Beilu, Haidian District, Beijing, China
Email: xuyunbin@catr.cn
Guoying Zhang
China Academy of Telecom Research
NO.52 Huayuan Beilu, Haidian District, Beijing, China
Email: zhangguoying@catr.cn

ACTN BOF
Internet-Draft
Intended status: Informational
Expires: April 17, 2015

D. Dhody
X. Zhang
Huawei Technologies
O. Gonzalez de Dios
Telefonica
D. Ceccarelli
Ericsson
B. Yoon
ETRI

October 14, 2014

Packet Optical Integration (POI) Use Cases for Abstraction and Control of Transport Networks (ACTN)
draft-dhody-actn-poi-use-case-03

Abstract

This document describes the Abstraction and Control of Transport Networks (ACTN) use cases related to Packet and Optical Integration (POI), that may be potentially deployed in various transport networks and apply to different applications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 17, 2015.

Table of Contents

1. Introduction

Network operators build and operate multi-layered multi-domain networks and these domains may be technology, administrative or vendor specific (vendor islands). Interoperability for dealing with different domains is a perpetual problem for operators. Due to these issues, new service introduction, often requiring connections that traverse multiple domains, need significant planning, and several manual operations to interface different vendor equipment and technology accross IP and Optical layers.

The aim of Abstraction and Control of Transport Networks (ACTN) is to facilitate virtual network operation, creation of a virtualized environment allowing operators to view and control multi-subnet multi-technology networks into a single virtualized network. This will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

[ACTN-FWK] describes a business model of ACTN, comprising of customers, service providers and network providers. This separates the network operations on physical network from the business needs (based on virtual network). It further describes the architecture model for ACTN including the entities (Customer Network Controller(CNC), Virtual Network Controller(VNC), and Physical Network Controller(PNC)) thier interfaces.

Discussion with operators has highlighted a need for virtual network operation based on the abstraction of underlying technology and vendor domains. This would be used for a variety of key use cases, including:

- Physical network infrastructure providers who want to build virtual network operations infrastructure via standards-based interfaces that facilitates automation and operation of multiple virtual networks for both internal and external trust domains.

- Data Center operators that need to lease facility from a number of physical network infrastructure providers to offer their global data center applications and services. As they face multi-domain and diverse transport technology, interoperability based on standard-based abstraction will enable dynamic and flexible applications and services.

The transport networks are in an unique position to embrace the concepts of software defined networking (SDN) because of the existing separation in control and forwarding plane via GMPLS/ASON. The path computation element (PCE) [RFC4655] and its stateful extension [STATEFUL-PCE] can further provide a central control over the resources. Also [STATEFUL-PCE-INITIATED] provides capability to initiate and delete LSP dynamically. ACTN is focused on building over the existing blocks by adding programmability, access and control over abstract virtual topologies. [ACTN-PROBLEM] and [ACTN-FWK] provide detailed information regarding this work. This document focuses on the Packet and Optical Integration (POI) use cases of ACTN. We refer to POI as packet over any connection-oriented transport technologies such as MPLS-TE, MPLS-TP, OTN or WSON.

It is preferable to coordinate network resource control and utilization rather than controlling and optimizing resources at each network layer (packet and optical transport network) independently. This facilitates network efficiency and network automation.

In a multi-layer network via client and server networking roles, Label Switched Paths (LSPs) in a server (lower) layer are used to carry client (higher) layer LSPs across the server (lower) layer

network. POI in a distributed control plane environment may be achieved by some of the existing mechanism as specified in [RFC4208] and [RFC5623]. This document explores the POI use cases of ACTN to help provide programmable network services like orchestration, access to abstract topology and control over the resources.

Increasingly there is a need for packet and optical transport networks to work together to provide accelerated services. Transport networks can provide useful information to the packet network allowing it to make intelligent decisions and control its allocated resources.

1.1. POI Scenario

This section explores some typical scenario for packet and optical integration (POI). These include, but not limited to, a single administrative domain as well as Carriers-of-Carrier case.

Figure 1 shows a single administrative domain comprising of both Packet and Optical transport networks. A POI coordinator would help build and operate a multi-layered multi-domain allowing operators to view and control a single virtualized network.

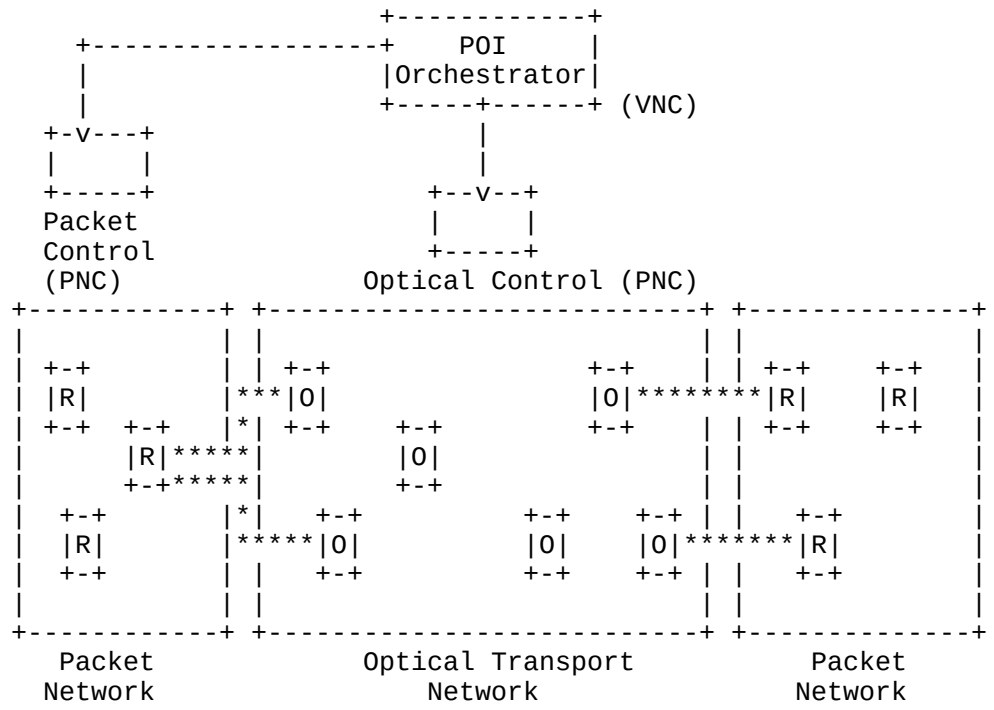


Figure 1: POI for single adminstration

Figure 2 shows a Carriers-of-Carrier case, where an optical transport infrastructure provider provides ACTN service to the ISP.

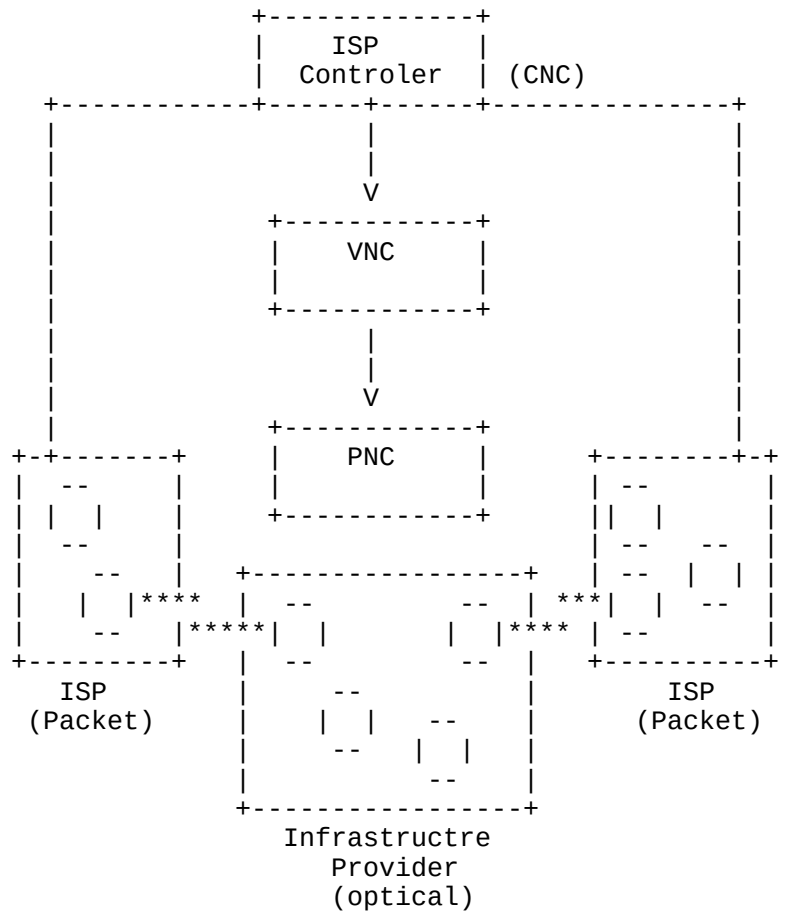


Figure 2: POI for Carriers-of-Carrier

2. Terminology

The following terms are as defined in [ACTN-FWK]:

- CNC:Customer Network Controller
- PNC:Physical Network Controller
- VNC:Virtual Network Controller

The following terminology is used in this document.

ACTN: Abstraction and Control of Transport Networks.

PCE: Path Computation Element. An entity (component, application, or network node) that is capable of computing a network path or route based on a network graph and applying computational constraints.

POI: Packet and Optical Integration

VNTM: Virtual Network Topology Manager

3. Packet Optical Integration

Connections (or tunnels) formed across the optical transport network, can be used as virtual TE links in the packet network. The relationship is reduced to determining which tunnels to set up, how to trigger them, how to route them, and what capacity to assign them. As the demands in the packet network vary, these tunnels may need to be modified.

One possible way to envision POI is via considering packet network as customer i.e. an entity in packet network - (maybe a Path Computation Element (PCE), Virtual Network Topology Manager (VNTM) [RFC5623], Controller etc..) should be aware of the abstract topology of the optical transport network. This entity is the customer network controller (CNC) as per [ACTN-FWK] which interacts with Virtual Network Controller (VNC). This is shown in Figure 2. Another way would be to consider Packet and Optical transport networks as domains and a POI coordinator (VNC) to help build and operate a multi-layered multi-domain network allowing operators to view and control a single virtualized network as shown in Figure 1.

In either case, the abstract topology may consist of established tunnels in optical transport network or ones that can be created on demand. The level of abstraction is dependent on various management, security and policy considerations. This abstract topology information in the packet network can be utilized in various cases, as detailed in the following sections.

3.1. Traffic Planning, Monitoring and Automatic Network Adjustments

Currently there is a schism between network planning for packet and optical transport networks. Sometimes these networks are administered, operated and planned independently even when they are a part of a single trusted domain. Any change in traffic requirements requires long business process to make changes in the network. In dynamic networks this is no longer acceptable.

A unified Packet+Optical traffic planning tool can be developed which uses the traffic demand matrix to plan the optical transport network.

Further based on traffic demand changes, historical data, traffic prediction and monitoring, changes should be made to the optical transport network. An access to abstract topology of the optical transport network based on established and potential (on-demand) tunnels in optical transport network can provide mechanism to handle this.

Further optical bypass may be established automatically to offload the continuous changing traffic to optical transport network allowing streamlined business process between packet and optical transport networks.

3.1.1. Automated Congestion Management

Congestion management and synergized network optimization for packet and optical transport networks can eliminate the need for overbooking of optical transport networks as dumb pipes. Application could be written that provide automated congestion management and network optimization. Automated congestion management recognizes prolonged congestion in the network and works with the controllers to add bandwidth at an optical transport layer, to alleviate the congestion, or make changes in the packet layer to reroute traffic around the congestion.

For such applications there is a clear need for an abstract network topology of optical transport layer, further there is also a need for a synergy of cost and SLA across optical and packet networks.

3.2. Protection and Restoration Synergy

The protection and restoration are usually handled individually in Packet and optical layer. There is a need for synergy and optimized handling of protection of resources across layers. A lot more resources in the optical transport network are booked for backup then actually required since there is a lack of coordination between packet and optical layers. The access to abstract graph of optical transport network with information pertaining to backup path information can help the packet network to handle protection, shared risk, fault restoration in an optimized way. Informing the packet network about both working and protection path which are either already established, or potential path can be useful.

A significant improvements in overall network availability that can be achieved by using optical transport shared-risk link group (SRLG) information to guide packet network decisions; for example, to avoid or minimize common SRLGs for the main (working) path and the loop free alternative or traffic engineered fast reroute (LFA/TE FRR) back-up path. Shared risk information need to be synergized between

the packet and optical. A mechanism to provide abstracted SRLG information can help the packet network consider this information while handling protection and restoration.

3.3. Service Awareness

In certain networks like financial information network (stock/ commodity trading) and enterprises using cloud based applications, Latency (delay), Latency-Variation (jitter), Packet Loss and Bandwidth Utilization are associated with the SLA. These SLAs must be synergized across packet and optical transport networks. Network optimization evaluates network resource usage at all layers and recommends or executes service path changes while ensuring SLA compliance. It thus makes more effective use of the network, and relieves current or potential congestion.

The main economic benefits of ACTN arise from its ability to maintain the SLA of the services at reduced overall network cost considering both packet and optical transport network. Operational benefits of the ACTN also stem from greater flexibility in handling dynamic traffic such as demand uncertainty or variations over time, or optimization based on cost or latency, or improved handling of catastrophic failures.

3.4. Coordination between Multiple Network Domains

In some deployments, optical transport network may further be divided into multiple domains, an abstracted topology comprising of multiple optical domains MAY be provided to the packet network. A Seamless aggregation and orchestration across multiple optical transport domains is achieved via the VNC, a great help in such deployments.

Another interesting deployment involves multiple packet network domains. There exist scenarios where the topology provided to the packet network domains may be different based on the initial demand matrix as well as, management, security and policy considerations.

The ACTN framework as described in [ACTN-FWK] should support the aggregation and orchestration across network domains and layers.

Further Figure 3 shows a multi-domain scenario where multiple PNC (each controlling a packet or optical domain) and a VNC coordinating among them and providing a consolidated view.

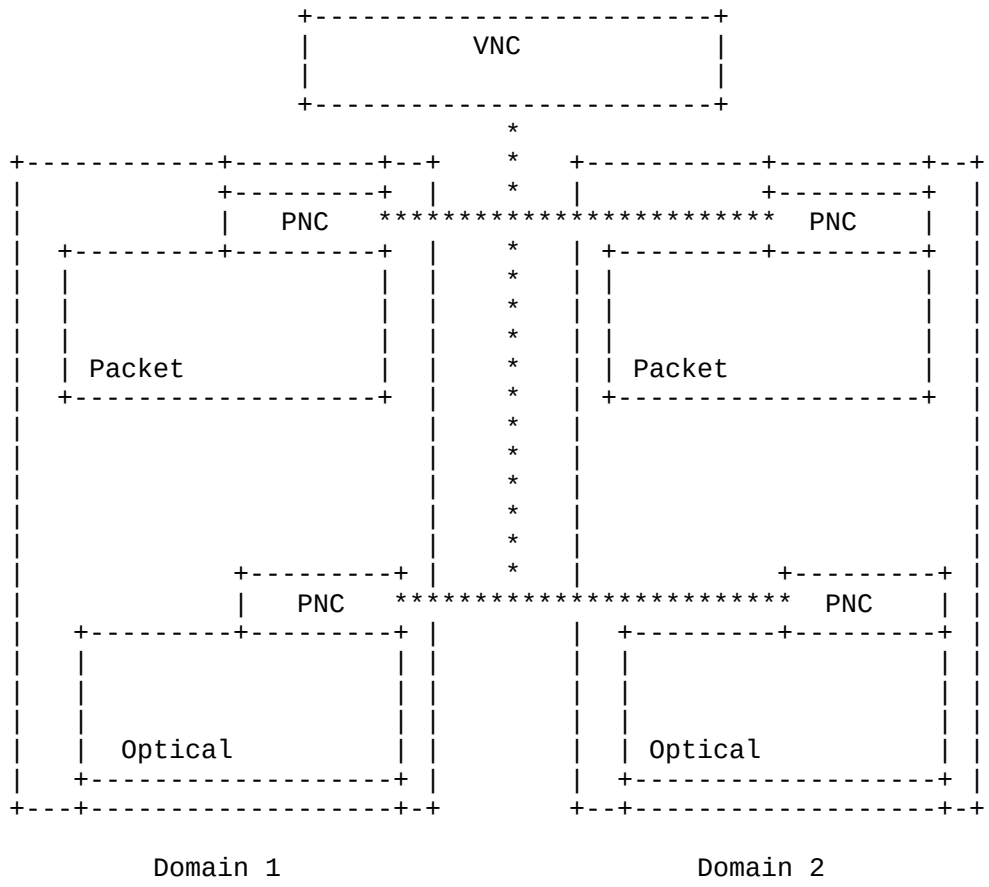


Figure 3: Coordination between Multiple Network Domains

4. Typical Workflow

Consider a two-layer network where the higher-layer network is a packet-based IP/MPLS or GMPLS network and the lower-layer network is a GMPLS-controlled optical network both under a common administrative control.

The PNC in both layers are under a common VNC that coordinates between the two layers. And this multi-layer network is used to interconnect DCs, where the DC controller (customer network controller - CNC) takes charge as shown in Figure 4.

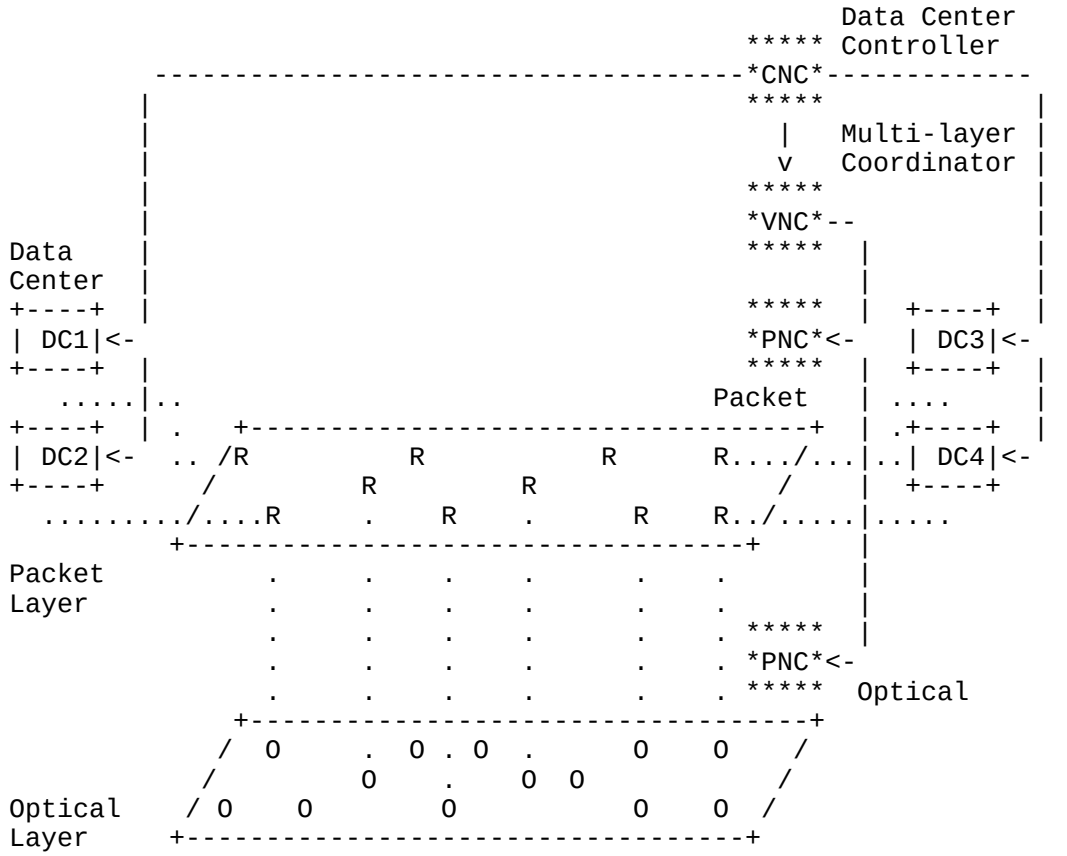


Figure 4: Typical Workflow

Data centre controller (as Customer Network Controller) interfaces the data centre application stratum, it understands multiple DC application requirements and their service needs. DC Controller provides its traffic demand matrix that describes bandwidth requirements and other optional QoS parameters (e.g., latency, diversity requirement, etc.) for each pair of inter-DC connections. The VNC (multi-layer coordinator) sits between the DC controller (CNC - the one issuing connectivity requests) and the physical network controllers (the one managing the resources). In this case each layer has its own PNC managing the resources in each layer with VNC acting as a multi-layer coordinator. The PNC is in charge of configuring the network elements, monitoring the physical topology of the network and passing it, either raw or abstracted, to the VNC.

VNC with the help of PNC(s) coordinates network resource control and utilization facilitating network efficiency and network automation. The VNC are also responsible for the abstract topology and the level of abstraction, which facilitate various DC usecases like VM Migrations, global load balancing among geographically distributed DCs, Business continuity and disaster recovery etc using the ACTN framework in an elastic and dynamic and way, improving overall network operations and scaling.

Based on the Data centre controller's (acting as CNC) requests for virtual network paths, the VNC mediates with the PNCs and maps these 'virtual' request to inter-layer coordinated path computation and provisioning requests in the 'physical' domain to the PNC. Thus VNC acts as a multi-layer coordinator both in respect to multi-layer end to end optimized path computation as well as multi-layer signaling and provisioning. The path computation and abstract topology creation would be based on the guidelines set by the CNC including the optimization criteria, traffic profile, policy etc.

In case the PNC could not fulfill the desired request from VNC and indirectly from DC controller, there should be a feedback loop to the VNC so that suitable actions including path recalculation and signaling, negotiation of parameters and attributes with DC controller etc can be undertaken. Thus VNC effectively arbitrate between the customers (DC) and the existing network (PNC) in this example.

5. Security Considerations

TBD.

6. IANA Considerations

None, this is an informational document.

7. Acknowledgments

8. References

8.1. Normative References

[ACTN-FWK] Ceccarelli, D., Fang, L., Lee, Y., and D. Lopez, "Framework for Abstraction and Control of Transport Networks (draft-ceccarelli-actn-framework)", September 2014.

8.2. Informative References

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and 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., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, August 2006.

[RFC5623] Oki, E., Takeda, T., Le Roux, JL., and A. Farrel, "Framework for PCE-Based Inter-Layer MPLS and GMPLS Traffic Engineering", RFC 5623, September 2009.

[STATEFUL-PCE] Crabbe, E., Medved, J., Minei, I., and R. Varga, "PCEP Extensions for Stateful PCE [draft-ietf-pce-stateful-pce]", June 2014.

[STATEFUL-PCE-INITIATED] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model [draft-ietf-pce-pce-initiated-lsp]", June 2014.

[ACTN-PROBLEM] Lee, Y., King, D., Boucadair, M., Jing, R., and L. Contreras Murillo, "Problem Statement for Abstraction and Control of Transport Networks (draft-leeking-actn-problem-statement)", September 2014.

Appendix A. Contributor Addresses

Udayasree Palle
Huawei Technologies
Leela Palace
Bangalore, Karnataka 560008
INDIA

EMail: udayasree.palle@huawei.com

Authors' Addresses

Dhruv Dhody
Huawei Technologies
Leela Palace
Bangalore, Karnataka 560008
INDIA

EMail: dhruv.ietf@gmail.com

Xian Zhang
Huawei Technologies
Bantian, Longgang District
Shenzhen, Guangdong 518129
P.R.China

EMail: zhang.xian@huawei.com

Oscar Gonzalez de Dios
Telefonica
SPAIN

EMail: ogondio@tid.es

Daniele Ceccarelli
Ericsson
Via E. Melen 77, Genova - Erzelli
Italy

EMail: daniele.ceccarelli@ericsson.com

Bin-Yeong Yoon
ETRI
South Korea

EMail: byyun@etri.re.kr

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 1, 2017

D. Dhody
X. Zhang
Huawei Technologies
O. Gonzalez de Dios
Telefonica
D. Ceccarelli
Ericsson
B. Yoon
ETRI

October 28, 2016

Packet Optical Integration (POI) Use Cases for Abstraction and Control of TE Networks (ACTN)
draft-dhody-actn-poi-use-case-07

Abstract

This document describes the Abstraction and Control of TE Networks (ACTN) use cases related to Packet and Optical Integration (POI), that may be potentially deployed in various TE networks and apply to different applications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on May 1, 2017.

Table of Contents

1. Introduction

Network operators build and operate multi-layered multi-domain networks and these domains may be technology, administrative or vendor specific (vendor islands). Interoperability for dealing with different domains is a perpetual problem for operators. Due to these issues, new service introduction, often requiring connections that traverse multiple domains, need significant planning, and several manual operations to interface different vendor equipment and technology accross IP and Optical layers.

The aim of Abstraction and Control of Transport Networks (ACTN) is to facilitate virtual network operation, creation of a virtualized environment allowing operators to view and control multi-subnet multi-technology networks into a single virtualized network. This will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

[ACTN-REQ] describes high-level ACTN requirements some of which are derived from the usecases described in this document.

[ACTN-FWK] describes a business model of ACTN, comprising of customers, service providers and network providers. This separates the network operations on physical network from the business needs (based on virtual network). It further describes the architecture model for ACTN including the entities (Customer Network Controller(CNC), Mult-domain Service Coordinator(MDSC), and Physical Network Controller(PNC)) thier interfaces.

Discussion with operators has highlighted a need for virtual network operation based on the abstraction of underlying technology and vendor domains. This would be used for a variety of key use cases, including:

- Physical network infrastructure providers who want to build virtual network operations infrastructure via standards-based interfaces that facilitates automation and operation of multiple virtual networks for both internal and external trust domains.

- Data Center operators that need to lease facility from a number of physical network infrastructure providers to offer their global data center applications and services. As they face multi-domain and diverse transport technology, interoperability based on standard-based abstraction will enable dynamic and flexible applications and services.

The transport networks are in an unique position to embrace the concepts of software defined networking (SDN) because of the existing separation in control and forwarding plane via GMPLS/ASON. The path computation element (PCE) [RFC4655] and its stateful extension [STATEFUL-PCE] can further provide a central control over the resources. Also [STATEFUL-PCE-INITIATED] provides capability to initiate and delete LSP dynamically. ACTN is focused on building over the existing blocks by adding programmability, access and control over abstract virtual topologies. [ACTN-FWK] provide detailed information regarding this work. This document focuses on the Packet and Optical Integration (POI) use cases of ACTN. We refer to POI as packet over any connection-oriented transport technologies such as MPLS-TE, MPLS-TP, OTN or WSON.

It is preferable to coordinate network resource control and utilization rather than controlling and optimizing resources at each network layer (packet and optical transport network) independently. This facilitates network efficiency and network automation.

In a multi-layer network via client and server networking roles, Label Switched Paths (LSPs) in a server (lower) layer are used to carry client (higher) layer LSPs across the server (lower) layer network. POI in a distributed control plane environment may be achieved by some of the existing mechanism as specified in [RFC4208] and [RFC5623]. This document explores the POI use cases of ACTN to help provide programmable network services like orchestration, access to abstract topology and control over the resources.

Increasingly there is a need for packet and optical transport networks to work together to provide accelerated services. Transport networks can provide useful information to the packet network allowing it to make intelligent decisions and control its allocated resources.

1.1. POI Scenario

This section explores some typical scenario for packet and optical integration (POI). These include, but not limited to, a single administrative domain as well as Carriers-of-Carrier case.

Figure 1 shows a single administrative domain comprising of both Packet and Optical transport networks. A POI coordinator would help build and operate a multi-layered multi-domain allowing operators to view and control a single virtualized network.

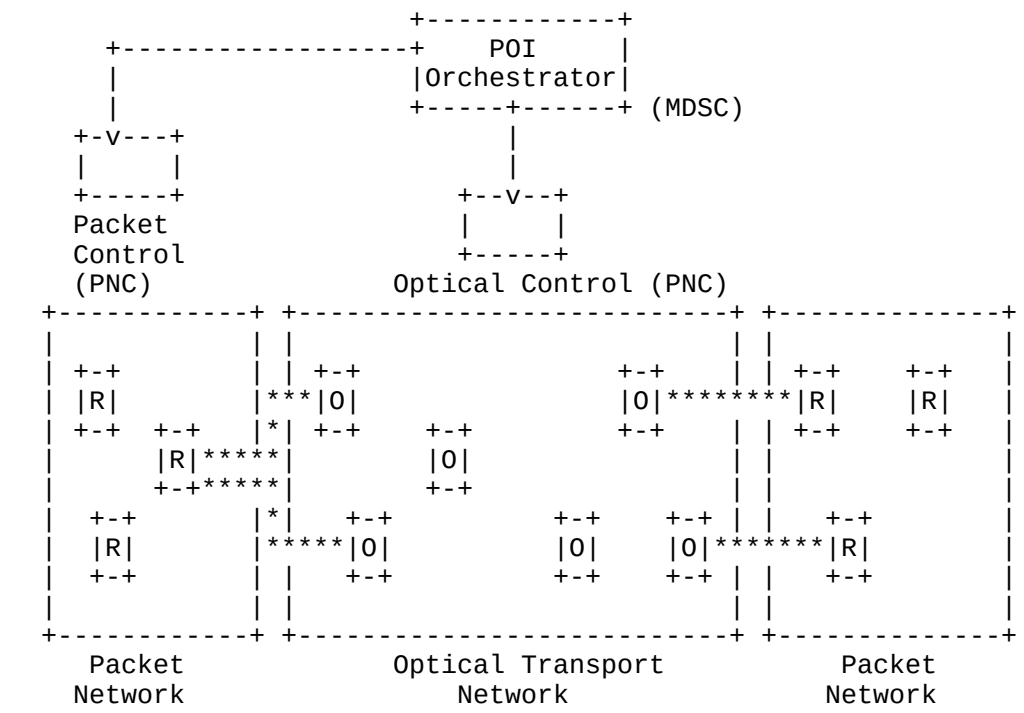


Figure 1: POI for single adminstration

Figure 2 shows a Carriers-of-Carrier case, where an optical transport infrastructure provider provides ACTN service to the ISP.

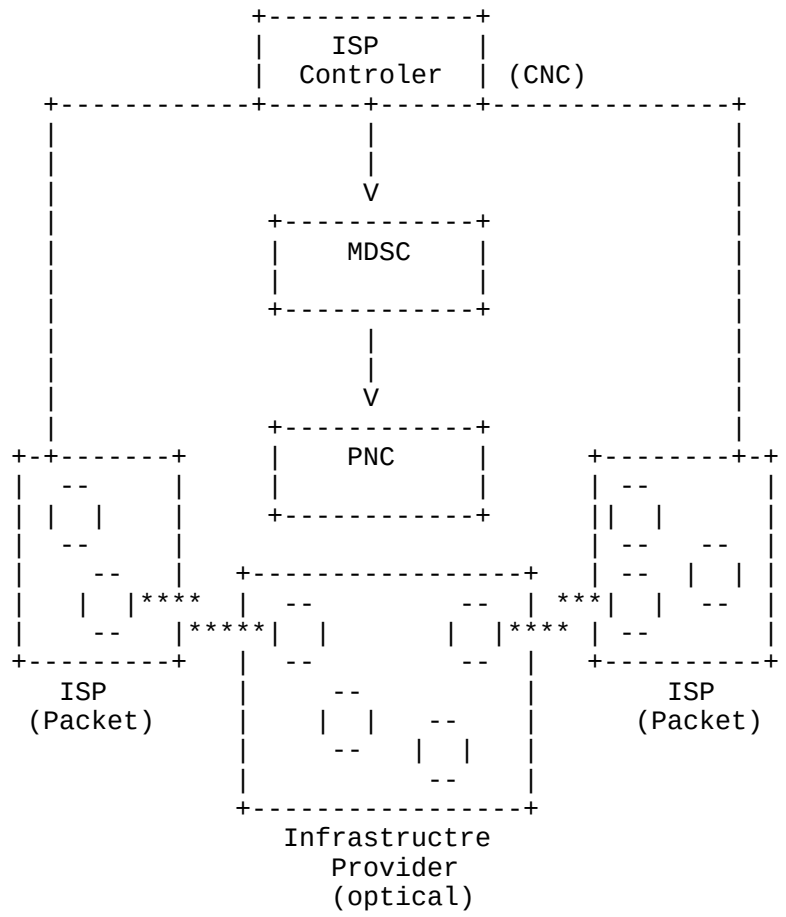


Figure 2: POI for Carriers-of-Carrier

2. Terminology

The following terms are as defined in [ACTN-FWK]:

- CNC:Customer Network Controller
- PNC:Physical Network Controller
- MDSC:Multi-domain Service Coordinator

The following terminology is used in this document.

ACTN: Abstraction and Control of Transport Networks.

PCE: Path Computation Element. An entity (component, application, or network node) that is capable of computing a network path or route based on a network graph and applying computational constraints.

POI: Packet and Optical Integration

VNTM: Virtual Network Topology Manager

3. Packet Optical Integration

Connections (or tunnels) formed across the optical transport network, can be used as virtual TE links in the packet network. The relationship is reduced to determining which tunnels to set up, how to trigger them, how to route them, and what capacity to assign them. As the demands in the packet network vary, these tunnels may need to be modified.

One possible way to envision POI is via considering packet network as customer i.e. an entity in packet network - (maybe a Path Computation Element (PCE), Virtual Network Topology Manager (VNTM) [RFC5623], Controller etc..) should be aware of the abstract topology of the optical transport network. This entity is the customer network controller (CNC) as per [ACTN-FWK] which interacts with MDSC. This is shown in Figure 2. Another way would be to consider Packet and Optical transport networks as domains and a POI coordinator (MDSC) to help build and operate a multi-layered multi-domain network allowing operators to view and control a single virtualized network as shown in Figure 1.

In either case, the abstract topology may consist of established tunnels in optical transport network or ones that can be created on demand. The level of abstraction is dependent on various management, security and policy considerations. This abstract topology information in the packet network can be utilized in various cases, as detailed in the following sections.

3.1. Traffic Planning, Monitoring and Automatic Network Adjustments

Currently there is a schism between network planning for packet and optical transport networks. Sometimes these networks are administered, operated and planned independently even when they are a part of a single trusted domain. Any change in traffic requirements requires long business process to make changes in the network. In dynamic networks this is no longer acceptable.

A unified Packet+Optical traffic planning tool can be developed which uses the traffic demand matrix to plan the optical transport network.

Further based on traffic demand changes, historical data, traffic prediction and monitoring, changes should be made to the optical transport network. An access to abstract topology of the optical transport network based on established and potential (on-demand) tunnels in optical transport network can provide mechanism to handle this.

Further optical bypass may be established automatically to offload the continuous changing traffic to optical transport network allowing streamlined business process between packet and optical transport networks.

3.1.1. Automated Congestion Management

Congestion management and synergized network optimization for packet and optical transport networks can eliminate the need for overbooking of optical transport networks as dumb pipes. Application could be written that provide automated congestion management and network optimization. Automated congestion management recognizes prolonged congestion in the network and works with the controllers to add bandwidth at an optical transport layer, to alleviate the congestion, or make changes in the packet layer to reroute traffic around the congestion.

For such applications there is a clear need for an abstract network topology of optical transport layer, further there is also a need for a synergy of cost and SLA across optical and packet networks.

3.2. Protection and Restoration Synergy

The protection and restoration are usually handled individually in Packet and optical layer. There is a need for synergy and optimized handling of protection of resources across layers. A lot more resources in the optical transport network are booked for backup then actually required since there is a lack of coordination between packet and optical layers. The access to abstract graph of optical transport network with information pertaining to backup path information can help the packet network to handle protection, shared risk, fault restoration in an optimized way. Informing the packet network about both working and protection path which are either already established, or potential path can be useful.

A significant improvements in overall network availability that can be achieved by using optical transport shared-risk link group (SRLG) information to guide packet network decisions; for example, to avoid or minimize common SRLGs for the main (working) path and the loop free alternative or traffic engineered fast reroute (LFA/TE FRR) back-up path. Shared risk information need to be synergized between

the packet and optical. A mechanism to provide abstracted SRLG information can help the packet network consider this information while handling protection and restoration.

3.3. Service Awareness

In certain networks like financial information network (stock/ commodity trading) and enterprises using cloud based applications, Latency (delay), Latency-Variation (jitter), Packet Loss and Bandwidth Utilization are associated with the SLA. These SLAs must be synergized across packet and optical transport networks. Network optimization evaluates network resource usage at all layers and recommends or executes service path changes while ensuring SLA compliance. It thus makes more effective use of the network, and relieves current or potential congestion.

The main economic benefits of ACTN arise from its ability to maintain the SLA of the services at reduced overall network cost considering both packet and optical transport network. Operational benefits of the ACTN also stem from greater flexibility in handling dynamic traffic such as demand uncertainty or variations over time, or optimization based on cost or latency, or improved handling of catastrophic failures.

3.4. Coordination between Multiple Network Domains

In some deployments, optical transport network may further be divided into multiple domains, an abstracted topology comprising of multiple optical domains may be provided to the packet network. A Seamless aggregation and orchestration across multiple optical transport domains is achieved via the MDSC, a great help in such deployments.

Another interesting deployment involves multiple packet network domains. There exist scenarios where the topology provided to the packet network domains may be different based on the initial demand matrix as well as, management, security and policy considerations.

The ACTN framework as described in [ACTN-FWK] should support the aggregation and orchestration across network domains and layers.

Further Figure 3 shows a multi-domain scenario where multiple PNC (each controlling a packet or optical domain) and a MDSC coordinating among them and providing a consolidated view.

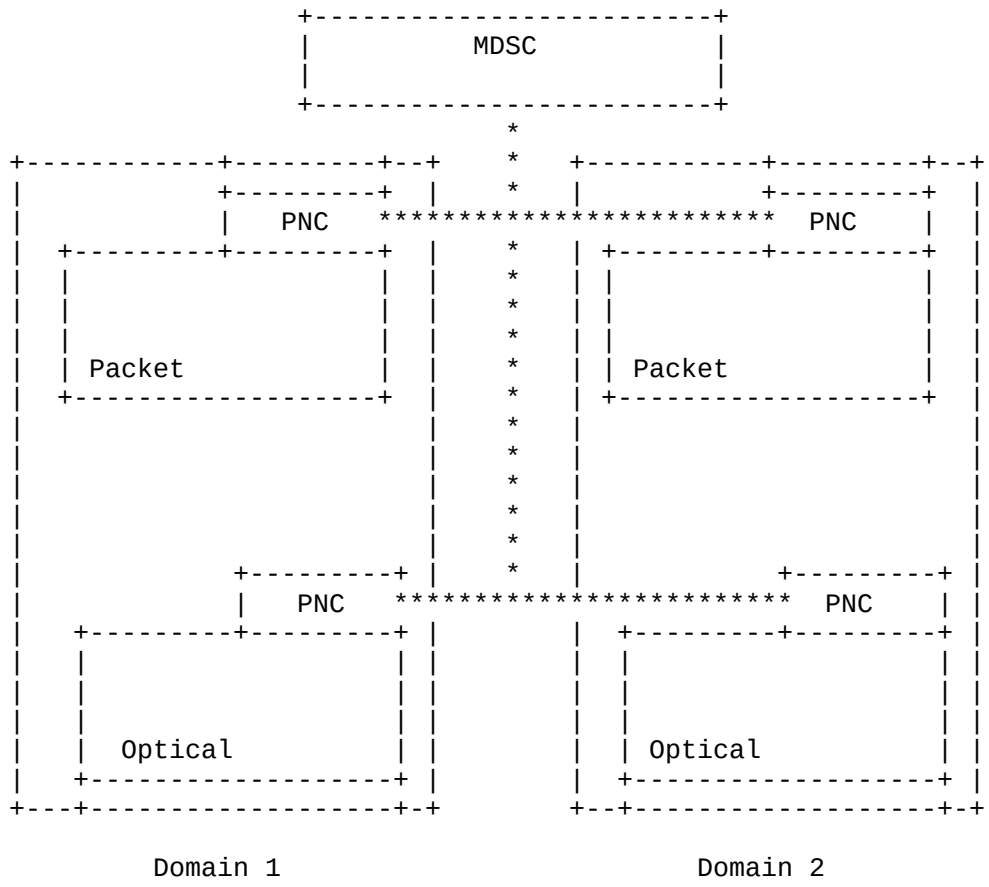


Figure 3: Coordination between Multiple Network Domains

4. Typical Workflow

Consider a two-layer network where the higher-layer network is a packet-based IP/MPLS or GMPLS network and the lower-layer network is a GMPLS-controlled optical network both under a common administrative control.

The PNC in both layers are under a common MDSC that coordinates between the two layers. And this multi-layer network is used to interconnect DCs, where the DC controller (customer network controller - CNC) takes charge as shown in Figure 4.

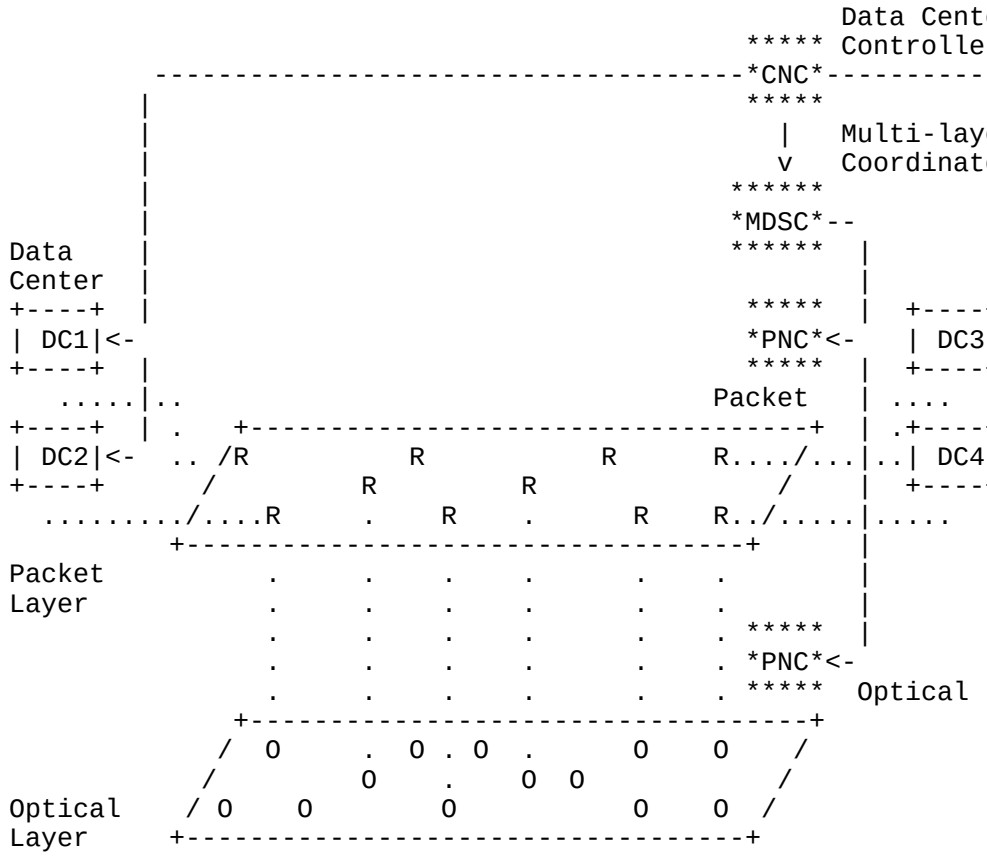


Figure 4: Typical Workflow

Data centre controller (as Customer Network Controller) interfaces the data centre application stratum, it understands multiple DC application requirements and their service needs. DC Controller provides its traffic demand matrix that describes bandwidth requirements and other optional QoS parameters (e.g., latency, diversity requirement, etc.) for each pair of inter-DC connections. The MDSC (multi-layer coordinator) sits between the DC controller (CNC - the one issuing connectivity requests) and the physical network controllers (the one managing the resources). In this case each layer has its own PNC managing the resources in each layer with MDSC acting as a multi-layer coordinator. The PNC is in charge of configuring the network elements, monitoring the physical topology of the network and passing it, either raw or abstracted, to the MDSC.

MDSC with the help of PNC(s) coordinates network resource control and utilization facilitating network efficiency and network automation. The MDSC are also responsible for the abstract topology and the level of abstraction, which facilitate various DC usecases like VM Migrations, global load balancing among geographically distributed DCs, Business continuity and disaster recovery etc using the ACTN framework in an elastic and dynamic and way, improving overall network operations and scaling.

Based on the Data centre controller's (acting as CNC) requests for virtual network paths, the MDSC mediates with the PNCs and maps these 'virtual' request to inter-layer coordinated path computation and provisioning requests in the 'physical' domain to the PNC. Thus MDSC acts as a multi-layer coordinator both in respect to multi-layer end to end optimized path computation as well as multi-layer signaling and provisioning. The path computation and abstract topology creation would be based on the guidelines set by the CNC including the optimization criteria, traffic profile, policy etc.

In case the PNC could not fulfill the desired request from MDSC and indirectly from DC controller, there should be a feedback loop to the MDSC so that suitable actions including path recalculation and signaling, negotiation of parameters and attributes with DC controller etc can be undertaken. Thus MDSC effectively arbitrate between the customers (DC) and the existing network (PNC) in this example.

5. Security Considerations

TBD.

6. IANA Considerations

None, this is an informational document.

7. Acknowledgments

8. References

8.1. Normative References

[ACTN-FWK] Ceccarelli, D. and Y. Lee, "Framework for Abstraction and Control of Traffic Engineered Networks", draft-ietf-teas-actn-framework-01 (work in progress), October 2016.

[ACTN-REQ]
Lee, Y., Dhody, D., Belotti, S., Pithewan, K., and D. Ceccarelli, "Requirements for Abstraction and Control of TE Networks", draft-ietf-teas-actn-requirements-03 (work in progress), July 2016.

8.2. Informative References

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and 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, DOI 10.17487/RFC4208, October 2005, <http://www.rfc-editor.org/info/rfc4208>.

[RFC4655] Farrel, A., Vasseur, J., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <http://www.rfc-editor.org/info/rfc4655>.

[RFC5623] Oki, E., Takeda, T., Le Roux, JL., and A. Farrel, "Framework for PCE-Based Inter-Layer MPLS and GMPLS Traffic Engineering", RFC 5623, DOI 10.17487/RFC5623, September 2009, <http://www.rfc-editor.org/info/rfc5623>.

[STATEFUL-PCE]
Crabbe, E., Minei, I., Medved, J., and R. Varga, "PCEP Extensions for Stateful PCE", draft-ietf-pce-stateful-pce-16 (work in progress), September 2016.

[STATEFUL-PCE-INITIATED]
Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model", draft-ietf-pce-pce-initiated-lsp-07 (work in progress), July 2016.

Appendix A. Contributor Addresses

Udayasree Palle
Huawei Technologies
Divyashree Techno Park, Whitefield
Bangalore, Karnataka 560066
India

EMail: udayasree.palle@huawei.com

Authors' Addresses

Dhruv Dhody
Huawei Technologies
Divyashree Techno Park, Whitefield
Bangalore, Karnataka 560066
India

EMail: dhruv.ietf@gmail.com

Xian Zhang
Huawei Technologies
Bantian, Longgang District
Shenzhen, Guangdong 518129
P.R.China

EMail: zhang.xian@huawei.com

Oscar Gonzalez de Dios
Telefonica
Spain

EMail: ogondio@tid.es

Daniele Ceccarelli
Ericsson
Via E. Melen 77, Genova - Erzelli
Italy

EMail: daniele.ceccarelli@ericsson.com

Bin-Yeong Yoon
ETRI
South Korea

EMail: byyun@etri.re.kr

Network Working Group
Internet Draft
Intended status: Informational
Expires: March 29, 2015

Luyuan Fang
Microsoft

September 29, 2014

ACTN Use Case for Multi-domain Data Center Interconnect

draft-fang-actn-multidomain-dci-01.txt

Status of this Memo

Copyright Notice

Abstract

This document discusses a use case for data center operators that need to interface multi-domain transport networks to offer their global data center applications and services. As data center operators face multi-domain and diverse transport technology, interoperability based on standard-based abstraction is required to support dynamic and flexible applications and services.

Table of Contents

1. Introduction

This document discusses a use case for data center operators that need to interface multi-domain transport networks to offer their global data center applications and services. As data center providers face multi-domain and diverse transport technology, interoperability based on standard-based abstraction is required to support dynamic and flexible applications and services.

This use case is a part of the overarching work, called Abstraction and Control of Transport Networks (ACTN). The goal of ACTN is to facilitate virtual network operation by:

. The creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-admin, multi-vendor, multi-technology networks and

. The operation and control/management of these multiple networks as a single virtualized network.

This will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

Related documents are the ACTN-framework [ACTN-Frame] and the problem statement [ACTN-PS].

Multi-domain transport networks herein are referred to physical WAN infrastructure whose operation may or may not belong to the same administrative domain as the data center operation. Some data center operators may wholly own the entire physical WAN infrastructure while others may own partially or even not at all. In all cases, data center operation needs to establish multi-domain relationships with one or more physical network infrastructure operations.

Data center based applications are used to provide a wide variety of services such as video gaming, cloud storage and computing, grid application, data base tools, and mobile applications, and others. High-bandwidth video applications such as remote medical surgery, video streaming for live concerts and sporting events are also emerging. This document is mainly concerned with data center applications that in aggregate or individually make substantial bandwidth demands that traverse multi-domain transport networks, some of which may belong to different administrative domains. In addition, these applications may require specific bounds on QoS related parameters such as guaranteed bandwidth, latency and jitter and others.

The organization of this document is as follows: Section 2 will discuss multi-domain Data Center interconnection and its various application scenarios. Section 3 will discuss the issues and challenges for Multi-domain Data Center Interconnection Operations Architecture. Section 4 will provide high-level requirements.

2. Multi-domain Data Center Interconnection Applications

2.1. VM Migration

A key enabler for data center cost savings, consolidation, flexibility and application scalability has been the technology of compute virtualization or Virtual Machines (VMs). A VM to the software application looks like a dedicated processor with dedicated memory and dedicated operating system. In modern data centers or "computing clouds", the smallest unit of computing resource is the VM. In public data centers one can buy computing capacity in terms of VMs for a particular amount of time. Though different VM

configurations may be offered that are optimized for different types of processing (e.g., memory intensive, throughput intensive).

VMs offer not only a unit of compute power but also as an "application environment" that can be replicated, backed up and moved. Although VM migration started in the LAN, the need for inter-DC VM migration for workload burst/overflow management on the WAN has been a real need for Data Center Operators.

Virtual machine migration has a variety of modes: (i) scheduled vs. dynamic; (ii) bulk vs. sequential; (iii) point-to-point vs. point-to-multi-point. Transport network capability can impact virtual machine migration strategy. For certain mission critical applications, dynamic bandwidth guarantee as well as performance guarantee must be provided by the network. Make-before-break capability is also critical to support seamless migration.

2.2. Global Load Balancing

As the many data center applications are distributed geographically across many data centers and over multi-domain networks, load balancing is no longer a local decision. As such, the decision as to selecting a server for an application request from the users or selecting data centers for migrating or instantiating VMs needs to be done globally. This refers to global load balancing.

There are many factors that can negatively affect the quality of experience (QoE) for the application. Among them are: the utilization of the servers, the underlying network loading conditions within a data center (LAN), the underlying network loading conditions between data centers (MAN/WAN), the underlying network conditions between the end-user and data center (Access Network). To allow data center operators to facilitate global load balancing over heterogeneous multi-domain transports from access networks to metro/core transport networks, on-line network resource information needs to be abstracted and represented from each involving network domain.

2.3. Disaster Recovery

For certain applications, disaster recovery in real-time is required. This requires transport of extremely large amount of data from various data center locations to other locations and a quick feedback mechanism between data center operator and infrastructure network providers to facilitate the complexity associated with real-time disaster recovery.

As this operation requires real-time concurrent connections with a large amount of bandwidth, a strict guarantee of bandwidth and a

very low latency between a set of data centers, the underlying physical network infrastructure is required to support these network capability. Moreover, as the data center operator interfaces multiple network infrastructure providers, standard-based interfaces and a common ways to abstract network resources and connections are necessary to facilitate its operations.

2.4. On-demand Virtual Connection/Circuit Services

Related to the real-time operations discussed in other applications in the previous sections, many applications require on-demand virtual connection/circuit services with an assured quality of service across multiple domain transport networks.

The on-demand aspect of this service applies not only in setting up the initial virtual connections/circuits but also in increasing bandwidth, changing the QoS/SLA, adding a new protection scheme to an existing service.

The on-demand network query to estimate available SLA/QoS (e.g., BW availability, latency range, etc.) between a few data center locations is also part of this application.

3. Issues and Challenges for Multi-domain Data Center Interconnection Operations

This section discusses operational issues and challenges for multi-domain data center interconnection. Figure 1 shows a typical multi-domain data center interconnection operations architecture.

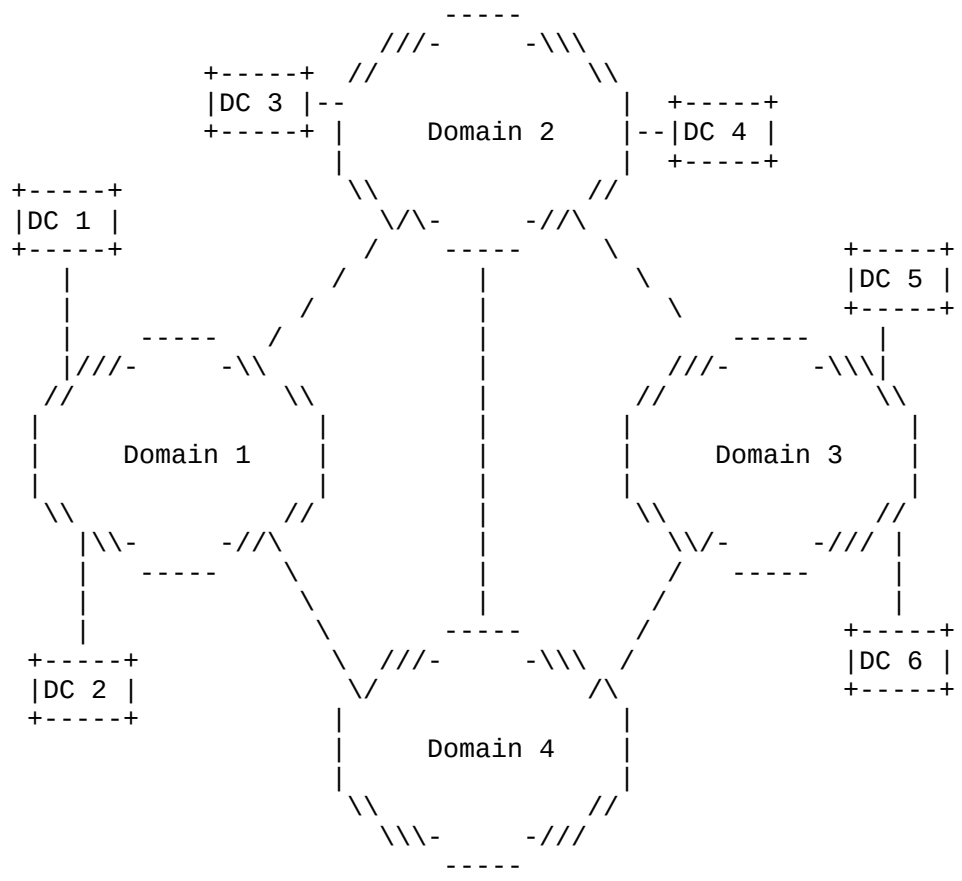


Figure 1. Multi-domain Data Center Interconnect Operations Architecture

Figure 1 shows several characteristics pertaining to current multi-domain data center operations.

1. Data centers are geographically spread and homed on possibly a number of mutually independent physical network infrastructure provider domains.

2. Between the data center operator domain and each of mutually independent physical network provider domains must establish trusted relationships amongst the involved entities. In some cases where data center operator owns the whole or partial physical

network infrastructure domains, a trusted relationship is still required between the data center operation and the network operations due to organizational boundaries although it is less strict than a pure multi-domain case.

3. Data center operator may lease facility from physical network infrastructure providers for intra-domain connectivity or own the facility. For instance, there may be an intra-domain leased facility for connectivity between DC 1 to DC 2. It is also possible that the data center provider may own this intra-domain facility such as dark fibers for connectivity between DC 1 and DC 2.

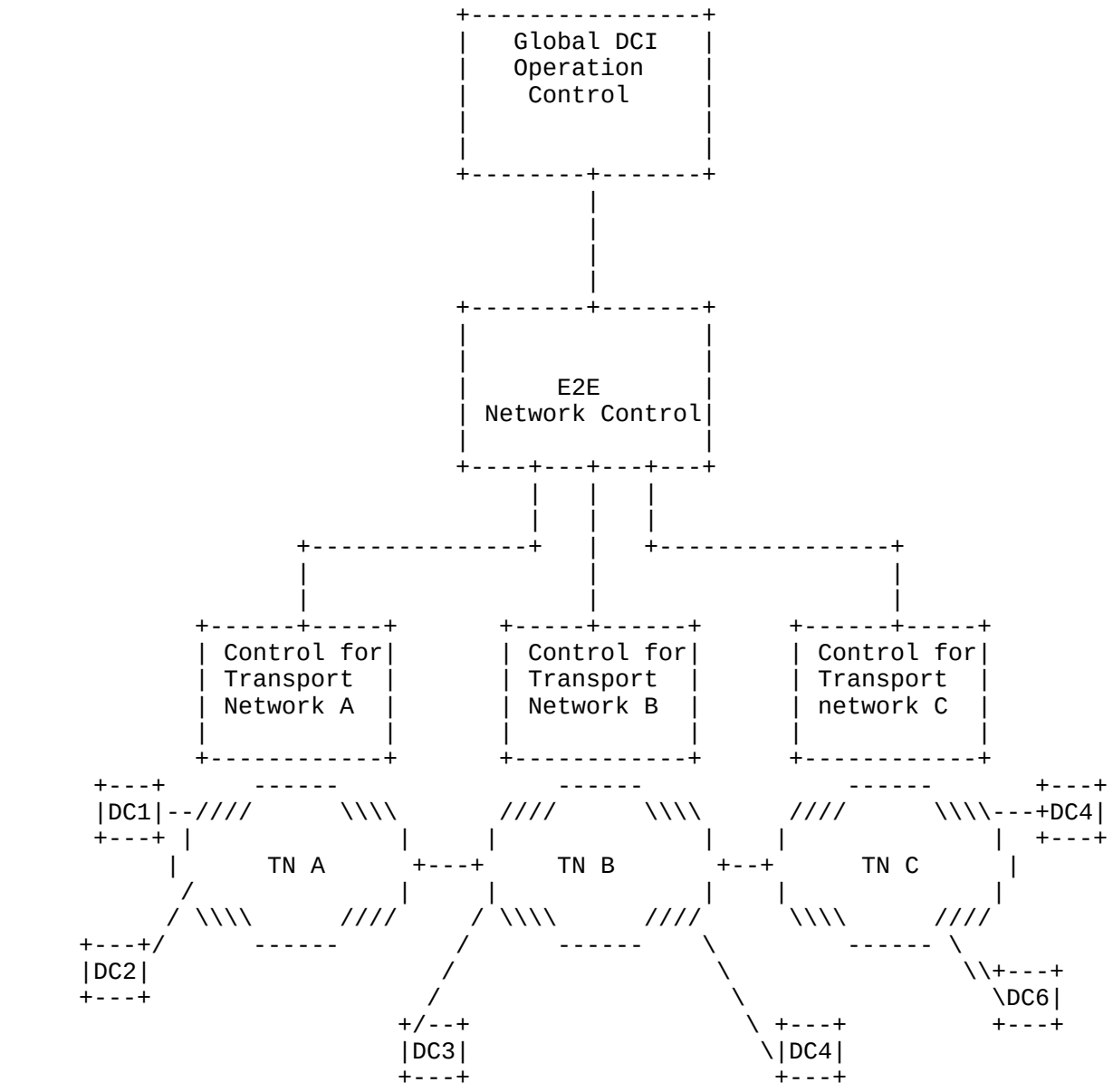
4. There may be need for connectivity that may traverse multi-domain networks. For instance, Data Center 1 may have VMs that need to be transported to Data Center 6. Typically, multi-domain connectivity is arranged statically such that the routes are pre-negotiated with the involved operators. For instance, if Data Center 1 were to send its VMs to Data Center 6, the route may take on Domain 1 - Domain 4 - Domain 3 based on a pre-negotiated agreement prior to connectivity request. In such case, the inter-domain facilities between Domains 1 & 4 Domains 4 & 3 are a part of this pre-negotiated agreement. There could be alternative route choices. Whether there may be alternate routing or not is subject to policy. Alternate routing may be static or dynamic depending on policy.

5. These transport network domains may be diverse in terms of local policy, transport technology and its capability and vendor equipment. Due to this diversity, new service introduction, requiring connections that traverse multiple domains, need significant planning, and several manual operations to interface different vendor equipment and technology. New applications requiring dynamic and elastic services and real-time mobility may be hampered by these manual operational factors.

4. Control Hierarchy

This section provides a control hierarchy for multi-domain DC operations.

Figure 2 shows a control hierarchy for multi-domain Data Center Interconnection operation.



There are a number of important considerations to support a global multi-domain data center interconnection operation.

1. Need a hierarchical operation/control.

2. Build on top of existing network control technologies/domains to be able to E2E network control to help global DCI operation/control.

3. Need standard-based abstraction/APIs and protocols between E2E network control and global DCI operation control and between E2E network control and domain transport network controls.

5. Requirements

This section provides high-level requirements to fulfill multi-domain data center interconnection to support various applications discussed in the previous sections.

1. The interfaces between the Data Center Operation and each transport network domain SHOULD support standards-based abstraction with a common information/data model.

2. The Data Center Operation should be able to create a single virtual network view.

3. The following capability should be supported:

    a. Network Query (Pull Model) from the Data Center Operation to each transport network domain to collect potential resource availability (e.g., BW availability, latency range, etc.) between a few data center locations.

        i. The level of abstracted topology (e.g., tunnel-level, graph-form, etc.)

    b. Network Path Computation Request from the Data Center Operation to each transport network domain to estimate the path availability.

    c. Network Virtual Connections/Circuits Request from the Data Center Operation to each transport domain to establish an end-to-end virtual connections/circuits.

        i. The type of the connection: P2P, P2MP, etc.

        ii. Concurrency of the request (this indicates if the connections must be simultaneously available or not in case of multiple connection requests).

        iii. The duration of the connections

iv. SLA/QoS parameters: minimum guaranteed bandwidth, latency range, etc.

v. Protection/Reroute Options (e.g., SRLG requirement, etc.)

vi. Policy Constraints (e.g., peering preferences, etc.)

d. Network Virtual Connections/Circuits Modification Request from the Data Center Operation to each transport domain to change QoS/SLA, protection schemes of the existing connections/circuits.

e. Network Abnormality Report (Push Model) from each transport domain to the Data Center Operation indicating the service impacting network conditions or the potential degradation indications of the existing virtual connections/circuits.

6. References

[ACTN-Frame] D. Ceccarelli, L. Fang, Y. Lee and D. Lopez, "Framework for Abstraction and Control of Transport Networks," draft-ceccarelli-actn-framework, work in progress.

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

7. Authors' Addresses

Luyuan Fang
Microsoft
Email : lufang@microsoft.com

Intellectual Property Statement

Disclaimer of Validity

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Network Working Group
Internet Draft
Intended status: Informational
Expires December 2014

Kwang-koog Lee
Hosong Lee
KT

June 24, 2014

ACTN Use-case for On-demand E2E Connectivity Services in Multiple Vendor Domain Transport Networks

draft-klee-actn-connectivity-multi-vendor-domains-01.txt

Status of this Memo

Copyright Notice

Abstract

This document provides a use-case that addresses the need for facilitating the application of virtual network abstractions and the control and management of on-demand end-to-end provisioning of connections that traverse multiple vendor domain transport networks.

These abstractions shall help create a virtualized environment supporting operators in viewing and controlling different vendor domains, especially for on-demand network connectivity service for a single operator.

Table of Contents

1. Introduction

Network operators build and operate their network using multiple domains in different dimensions. Domains may be defined by a collection of links and nodes (each of a different technology), administrative zones under the concern of a particular business entity, or vendor-specific "islands" where specific control mechanisms have to be applied. Establishing end-to-end connections spanning several of these domains is a perpetual problem for operators, which need to address both interoperability and operational concerns at the control and data planes.

The introduction of new services, often requiring connections that traverse multiple domains, needs significant planning, and several manual operations to interface multiple vendor-specific domains in which specific control/management mechanisms of the vendor equipment have to be applied (e.g., EMS/NMS, OSS/BSS, control plane, SDN controller, etc.). Undoubtedly, establishing an on-demand end-to-end connection which requires provisioning based on dynamic resource information is more difficult in the current network context.

This document provides a use-case that addresses the need for creating a virtualized environment supporting operators in viewing and controlling different vendor domains, especially for on-demand

network connectivity service for a single operator. This will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

This use-case is a part of the overarching work, called Abstraction and Control of Transport Networks (ACTN). Related documents are the ACTN-framework [ACTN-Frame] and the problem statement [ACTN-PS].

2. On-demand End-to-end Connectivity in Multi-vendor Domain Transport Networks

This section provides an architecture example to illustrate the context of the current challenges and issues operators face in delivering on-demand end-to-end connectivity services in operators' multi-vendor domain transport networks.

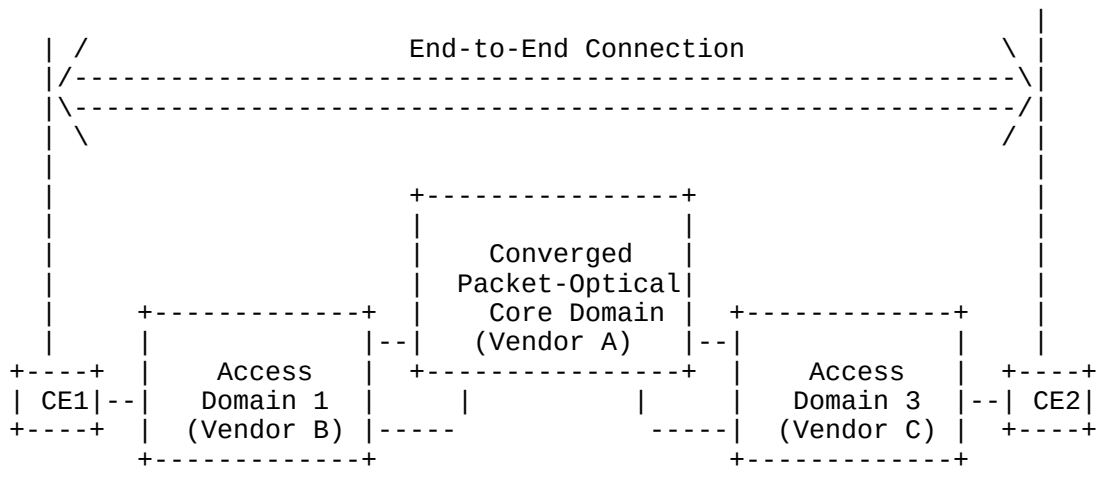


Figure 1. Multi-vendor Domains

As an illustrative example, consider a multi-domain transport network consisting of three domains: one core converged packet-optical domain (Vendor A) and two access domains (Vendors B and C). Each access domain is managed by its domain control/management mechanism which is often a proprietary vendor-specific scheme. The core domain is also managed by Vendor A's proprietary control/management mechanism (e.g., EMS/NMS, OSS/BSS, Control Plane, SDN Controller, or any combination of these entities, etc.) that may not interoperate with access domain control/management mechanisms or at best partially interoperate if Vendor A is same as Vendor B or Vendor C.

Due to these domain boundaries, facilitating on-demand end-to-end connections (e.g., Ethernet Virtual Connections, etc.) that traverse multi-domains is not readily achieved. These domain controls are optimized for its local operation and in most cases not suited for controlling the end-to-end connectivity services. For instance, the discovery of the edge nodes that belong to other domains is hard to achieve partly because of the lack of the common API and its information model and control mechanisms thereof to disseminate the relevant information.

Moreover, the path computation for any on-demand end-to-end connection would need abstraction of dynamic network resources and ways to find an optimal path that meets the connection’s service requirements. This would require knowledge of both the domain level dynamic network resource information and the inter-domain connectivity information including domain gateway/peering points and the local domain policy.

From an on-demand connection provisioning perspective, in order to facilitate a fast and reliable end-to-end signaling, each domain operation and management elements should ideally speak the same control protocols to its neighboring domains. However, this is not possible for the current network context unless a folk-lift green field technology deployment with a single vendor solution would be done. Although each domain applies the same protocol for the data plane, an end-to-end connectivity traversing multiple domains might not be provided due to a management and control mechanism focusing only on its own domain.

From a network connectivity management perspective, it would require a mechanism to disseminate any connectivity issues from the local domain to the other domains whenever the local domain cannot resolve a connectivity issues. This is hard to achieve due to the lack of the common API and its agreed-upon information model and control mechanisms thereof to disseminate the relevant information.

From an operation’s perspective, the current network environments are not conducive to offering on-demand end-to-end connectivity services in multi-vendor domain transport networks. For instance, when the performance monitoring inquiry is requested, operators manually monitor each domain and aggregate the performance results. However, it may not be precise because of the different measurement timing employed by each domain.

3. Requirements

In the previous section, we discussed the current challenges and issues that prevent operators from offering on-demand end-to-end connectivity services in multi-vendor domain transport networks.

This section provides a high-level requirement for enabling on-demand end-to-end connectivity services in multi-vendor domain transport networks in a single operator environment.

Figure 2 shows information flow requirements of the aforementioned context.

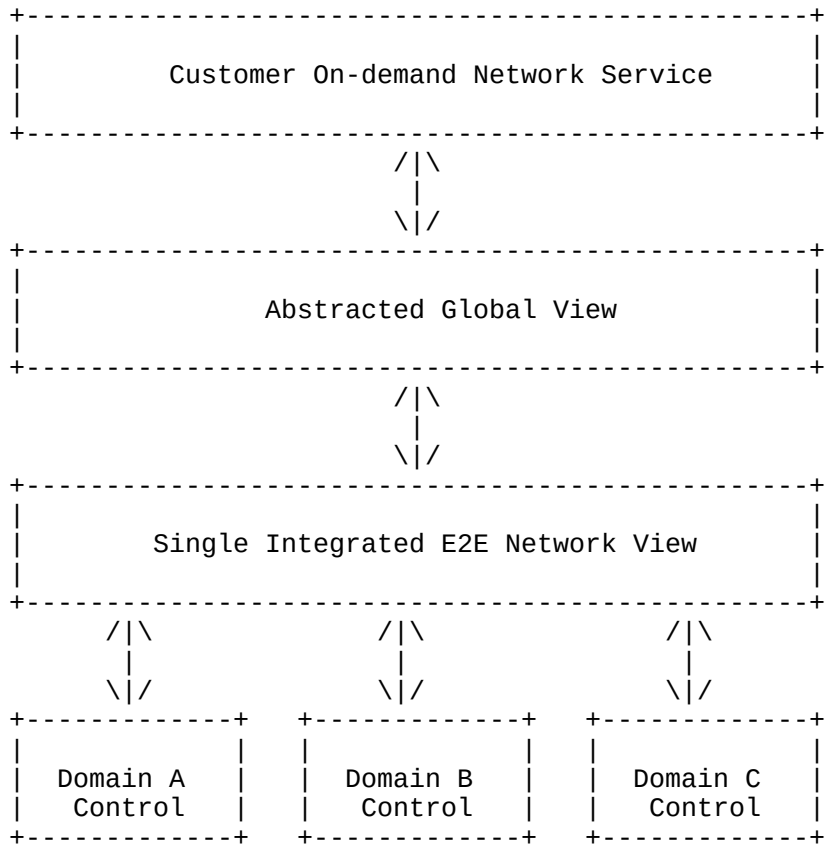


Figure 2. Information Flow Requirements for Enabling On-demand Network Connectivity Service in Multi-vendor Domain Networks

There are a number of key requirements from Figure 2.

- A single integrated end-to-end network view is necessary to be able to compute paths and provision the end-to-end paths that traverse multiple vendor domains.

- In order to create a single integrated end-to-end network view, discovery of inter-connection data between domains including the

domain border nodes/links is necessary. (The entity to collect domain-level data is responsible for collecting inter-connection links/nodes)

- The entity to collect domain-level data should recognize interoperability method between each domain. (There might be several interoperability mechanisms according to technology being applied.)

- The entity responsible to collect domain-level data and create an integrated end-to-end view should support push/pull model with respect to all its interfaces.

- The same entity should coordinate a signaling flow for end-to-end connections to each domain involved. (This entity to domain control is analogous to an NMS to EMS relationship)

- The entity responsible to create abstract global view should support push/pull model with respect to all its interfaces. (Note that the two entities (an entity to create an integrated end-to-end view and an entity to create an abstracted global view) can be assumed by the same entity, which is an implementation issue.

- There is a need for a common API between each domain control to the entity that is responsible for creating a single integrated end-to-end network view. At the minimum, the following items are required on the API:

    o Programmability of the API.

    o The multiple levels/granularities of the abstraction of network resource (which is subject to policy and service need).

    o The abstraction of network resource should include customer end points and inter-domain gateway nodes/links.

    o Any physical network constraints (such as SRLG, link distance, etc.) should be reflected in abstraction.

    o Domain preference and local policy (such as preferred peering point(s), preferred route, etc.)

    o Domain network capability (e.g., support of push/pull model).

- The entity responsible for abstraction of a global view into a customer view should provide a programmable API to allow the flexibility.

- Abstraction of a global view into a customer view should be provided to allow customer to dynamically request network on-demand services including connectivity services.

- What level of details customer should be allowed to view network is subject to negotiation between the customer and the operator.

4. References

[ACTN-Frame] D. Ceccarelli, L. Fang, Y. Lee and D. Lopez, "Framework for Abstraction and Control of Transport Networks," draft-ceccarelli-actn-framework, work in progress.

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

5. Acknowledgement

The authors wish to thank Young Lee for the discussions in the document.

6. Contributors

Authors' Addresses

Kwang-koog Lee

KT
Email: kwangkoog.lee@kt.com

Hosong Lee

KT
Email: hosong.lee@kt.com

Intellectual Property Statement

Disclaimer of Validity

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Network Working Group
Internet Draft
Intended status: Informational
Expires April 2014

Kwang-koog Lee
Hosong Lee
KT
Ricard Vilata
CTTC
Victor Lopez
Telefonica

November 10, 2014

ACTN Use-case for On-demand E2E Connectivity Services in Multiple Vendor Domain Transport Networks

draft-klee-actn-connectivity-multi-vendor-domains-02.txt

Status of this Memo

Copyright Notice

carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document provides a use-case that addresses the need for facilitating the application of virtual network abstractions and the control and management of on-demand end-to-end provisioning of connections that traverse multiple vendor domain transport networks.

These abstractions shall help create a virtualized environment supporting operators in viewing and controlling different vendor domains, especially for on-demand network connectivity service for a single operator.

Table of Contents

1. Introduction

Network operators build and operate their network using multiple domains in different dimensions. Domains may be defined by a collection of links and nodes (each of a different technology), administrative zones under the concern of a particular business entity, or vendor-specific "islands" where specific control mechanisms have to be applied. Due to the technology of each vendor, the optical components cannot be interconnected. Therefore each optical domain becomes an isolated island in terms of provisioning. The network operators use vendor-specific NMS implementations along with an operator-tailored umbrella provisioning system, which may include a technology specific Operations Support System (OSS). Thanks to the evolution of vendor specific SDN controllers, the network operators require a network entity, which abstract the details of the optical layer while enabling end-to-end provisioning of services. The establishment of end-to-end connections spanning several of these domains is a perpetual problem for operators, which need to address both interoperability and operational concerns at the control and data planes.

The introduction of new services, often requiring connections that traverse multiple domains, needs significant planning, and several manual operations to interface multiple vendor-specific domains in which specific control/management mechanisms of the vendor equipment have to be applied (e.g., EMS/NMS, OSS/BSS, control plane, SDN controller, etc.). Undoubtedly, establishing an on-demand end-to-end connection which requires provisioning based on dynamic resource information is more difficult in the current network context.

This document provides a use-case that addresses the need for creating a virtualized environment supporting operators in viewing and controlling different vendor domains, especially for on-demand network connectivity service for a single operator. This will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

This use-case is a part of the overarching work, called Abstraction and Control of Transport Networks (ACTN). Related documents are the ACTN-framework [ACTN-Frame] and the problem statement [ACTN-PS].

2. On-demand End-to-end Connectivity in Multi-vendor Domain Transport Networks

This section provides an architecture example to illustrate the context of the current challenges and issues operators face in delivering on-demand end-to-end connectivity services in operators' multi-vendor domain transport networks.

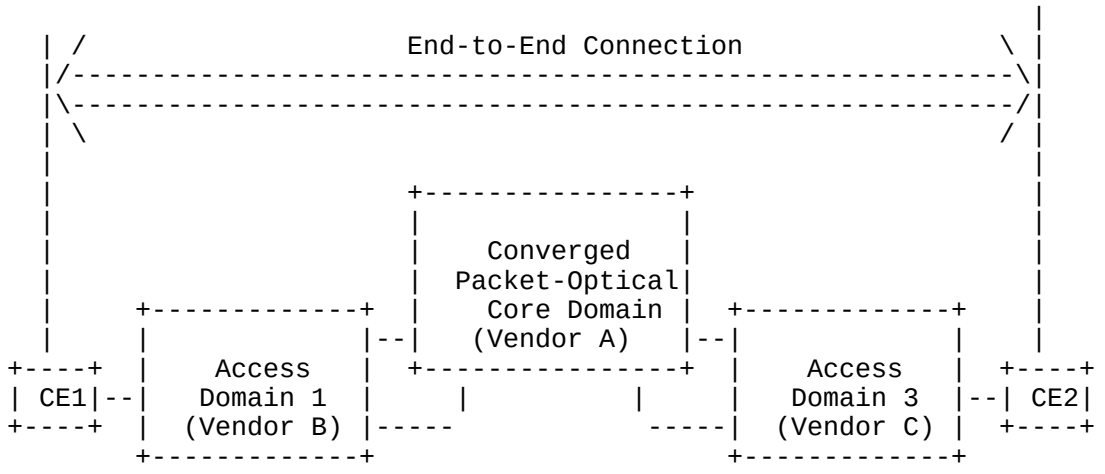


Figure 1. Multi-vendor Domains

As an illustrative example, consider a multi-domain transport network consisting of three domains: one core converged packet-optical domain (Vendor A) and two access domains (Vendors B and C). Each access domain is managed by its domain control/management mechanism which is often a proprietary vendor-specific scheme. The core domain is also managed by Vendor A's proprietary control/management mechanism (e.g., EMS/NMS, OSS/BSS, Control Plane, SDN Controller, or any combination of these entities, etc.) that may not interoperate with access domain control/management mechanisms or at best partially interoperate if Vendor A is same as Vendor B or Vendor C.

Due to these domain boundaries, facilitating on-demand end-to-end connections (e.g., Ethernet Virtual Connections, etc.) that traverse multi-domains is not readily achieved. These domain controls are optimized for its local operation and in most cases not suited for controlling the end-to-end connectivity services. For instance, the discovery of the edge nodes that belong to other domains is hard to achieve partly because of the lack of the common API and its information model and control mechanisms thereof to disseminate the relevant information.

Moreover, the path computation for any on-demand end-to-end connection would need abstraction of dynamic network resources and ways to find an optimal path that meets the connection's service requirements. This would require knowledge of both the domain level dynamic network resource information and the inter-domain connectivity information including domain gateway/peering points and the local domain policy.

From an on-demand connection provisioning perspective, in order to facilitate a fast and reliable end-to-end signaling, each domain operation and management elements should ideally speak the same control protocols to its neighboring domains. However, this is not possible for the current network context unless a folk-lift green field technology deployment with a single vendor solution would be done. Although each domain applies the same protocol for the data plane, an end-to-end connectivity traversing multiple domains might not be provided due to a management and control mechanism focusing only on its own domain.

From a network connectivity management perspective, it would require a mechanism to disseminate any connectivity issues from the local domain to the other domains whenever the local domain cannot resolve a connectivity issues. This is hard to achieve due to the lack of the common API and its agreed-upon information model and control mechanisms thereof to disseminate the relevant information.

From an operation’s perspective, the current network environments are not conducive to offering on-demand end-to-end connectivity services in multi-vendor domain transport networks. For instance, when the performance monitoring inquiry is requested, operators manually monitor each domain and aggregate the performance results. However, it may not be precise because of the different measurement timing employed by each domain.

3. Requirements

In the previous section, we discussed the current challenges and issues that prevent operators from offering on-demand end-to-end connectivity services in multi-vendor domain transport networks.

This section provides a high-level requirement for enabling on-demand end-to-end connectivity services in multi-vendor domain transport networks in a single operator environment.

Figure 2 shows information flow requirements of the aforementioned context.

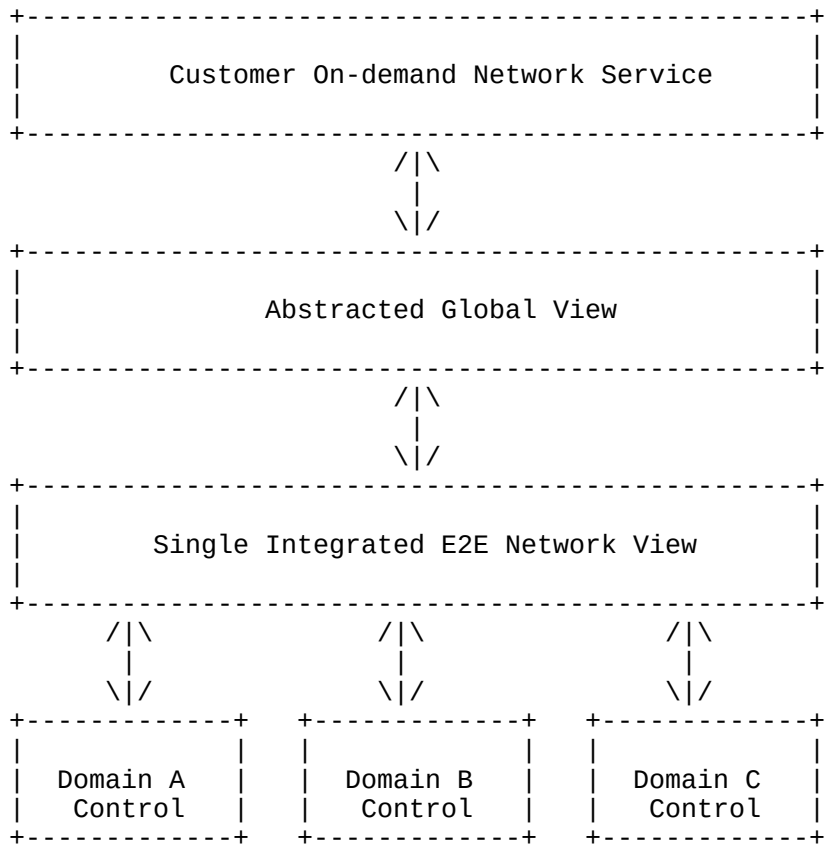


Figure 2. Information Flow Requirements for Enabling On-demand Network Connectivity Service in Multi-vendor Domain Networks

There are a number of key requirements from Figure 2.

- A single integrated end-to-end network view is necessary to be able to provision the end-to-end paths that traverse multiple vendor domains. In this approach the scalability and confidentiality problems are solved, but new considerations must be taken into account:

  - o Limited awareness, by the VNC, of the intra-domain resources availability.

  - o Sub-optimal path selection.

- The path computations shall be performed in two stages: first on the abstracted end-to-end network view (happening at VNC), and on the second stage it shall be expanded by each PNC.

- In order to create a single integrated end-to-end network view, discovery of inter-connection data between domains including the domain border nodes/links is necessary. (The entity to collect domain-level data is responsible for collecting inter-connection links/nodes)

- The entity to collect domain-level data should recognize interoperability method between each domain. (There might be several interoperability mechanisms according to technology being applied.)

- The entity responsible to collect domain-level data and create an integrated end-to-end view should support push/pull model with respect to all its interfaces.

- The same entity should coordinate a signaling flow for end-to-end connections to each domain involved. (This entity to domain control is analogous to an NMS to EMS relationship)

- The entity responsible to create abstract global view should support push/pull model with respect to all its interfaces. (Note that the two entities (an entity to create an integrated end-to-end view and an entity to create an abstracted global view) can be assumed by the same entity, which is an implementation issue.

- Hierarchical composition of integrated network views should be enabled by a common API between NorthBound Interface of the Single Integrated End-to-End view (handled by VNC) and Domain Control (handled by PNC).

- There is a need for a common API between each domain control to the entity that is responsible for creating a single integrated end-to-end network view. At the minimum, the following items are required on the API:

    o Programmability of the API.

    o The multiple levels/granularities of the abstraction of network resource (which is subject to policy and service need).

    o The abstraction of network resource should include customer end points and inter-domain gateway nodes/links.

  - Any physical network constraints (such as SRLG, link distance, etc.) should be reflected in abstraction.

  - Domain preference and local policy (such as preferred peering point(s), preferred route, etc.)

  - Domain network capability (e.g., support of push/pull model).

- The entity responsible for abstraction of a global view into a customer view should provide a programmable API to allow the flexibility. Abstraction might be provided by representing each domain as a virtual node (node abstraction) or a set of virtual nodes and links (link abstraction). Node abstraction creates a network topology composed by nodes representing each network domain and the inter-domain links between the border nodes of each domain.

  - Abstraction of a global view into a customer view should be provided to allow customer to dynamically request network on-demand services including connectivity services.

  - What level of details customer should be allowed to view network is subject to negotiation between the customer and the operator.

4. References

[ACTN-Frame] D. Ceccarelli, L. Fang, Y. Lee and D. Lopez, "Framework for Abstraction and Control of Transport Networks," draft-ceccarelli-actn-framework, work in progress.

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

5. Acknowledgement

The authors wish to thank Young Lee for the discussions in the document.

6. Contributors

Authors' Addresses

Kwang-koog Lee

KT
Email: kwangkoog.lee@kt.com

Hosong Lee

KT
Email: hosong.lee@kt.com

Ricard Vilata
CTTC
Email: ricard.vilalta@cttc.es

Victor Lopez
Telefonica
Email: victor.lopezalvarez@telefonica.com

Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 30, 2014

K. Kumaki
T. Miyasaka
KDDI Corporation

May 29, 2014

ACTN : Use case for Multi Tenant VNO
draft-kumaki-actn-multitenant-vno-00

Abstract

This document provides a use case that addresses the need for facilitating virtual network operation: creation and operation of multi-tenant virtual networks that use the common core network resources. This will accelerate a rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services. This use case addresses the aforementioned needs within a single operator network.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on November 30, 2014.

Copyright Notice

Table of Contents

1. Introduction

This document provides a use case that addresses the need for facilitating virtual network operation: creation and operation of multi-tenant virtual networks that use the common core network resources. This will accelerate a rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services. This use case supports Abstraction and Control of Transport Networks (ACTN). The aim of ACTN is to facilitate virtual network operation, creation of a virtualized environment allowing operators to view and control multi-subnet multi-technology networks into a single virtualized network. Related documents are: [I-D.leeking-actn-problem-statement] and [I-D.ceccarelli-actn-framework] which provide detailed information regarding this work.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Motivation

One of the main motivations for multi-tenant virtual networks that share the common core transport network resource is to increase the network utilization of the core transport network. As each service network has evolved in a different time with different service needs, many dedicated overlay networks have formed to support different service needs. This results in an inefficient use of network resources and the complexity in operating such diverse service networks. Due to the lack of the coordination across different service networks and the common service platform, the introduction of new services is not as speedy as the operators' desire. Part of the reasons for this difficulty is due to the lack of the virtual network infrastructure. Figure 1 shows an illustration of the current multiple service network architecture.

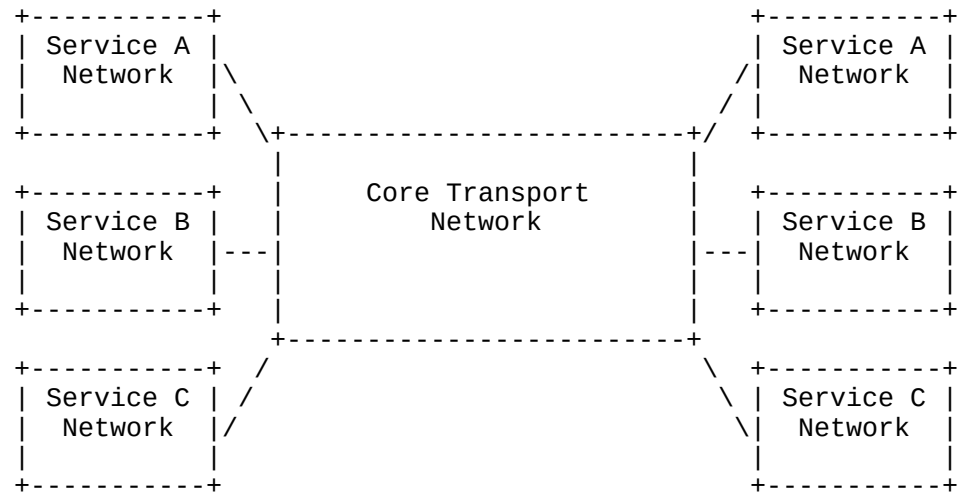


Figure 1: Multiple Services Network Architecture

The characteristics of the multiple services network are as follows:

- Each service has its own dedicated access points (e.g., PE routers) in the core network.

- Each service or a group of services may be operated in a different service operations department within an operator. For instance, the VPN service and the mobile service may be operated by two different departments while whole sale Internet service by another department.

- There may be dedicated core transport network resources for some services to ensure a strict service guarantee.

- There may be little or no coordination for operating multiple services in terms of network resource allocation or sharing of the resources.

4. Multi-tenant Virtual Network Consolidation

This section discusses key aspects to support multi-tenant virtual network consolidation.

4.1. Service Consolidation

Multi-tenant virtual network operation should support different services as the tenants that share the common core transport network resources. Therefore, it is important to understand the type of various services and its service requirement.

4.2. VPN Service Consolidation

Network providers have many different service networks such as VPNs of various types and different QoS requirements. Within VPNs, there are several QoS levels. Some VPN is best-effort VPN while other VPNs require a strict QoS such as bandwidth guarantee and latency. Therefore, multi-level VPNs should be supported in multi-tenant virtual network consolidation.

4.3. Network Wholesale Service

Network providers want to provide a network resource (i.e. a network slice) to ISPs. In this case, the network provider must guarantee the SLA to each ISP. There may be different level of SLA as well as different level of virtual network granularity for each ISP. The ISP should be given its virtual network(s) as well as an independent domain control of allocated virtual network(s). It is also to be noted that there may be different grade of services required depending on the nature of the whole sale. For instance, CATV operator may require a different grade of service than best-effort internet services. Therefore, multi-level wholesale services should be supported in multi-tenant virtual network consolidation. Also, network providers should not provide unnecessary network information (e.g. TE database and IGP information in core transport network) to ISPs. To provide unnecessary information in core transport network poses security issues. Therefore, network providers should provide only necessary network information to create ISP’s virtual network.

4.4. On-demand Network Service

Some ISPs may need a network resource (i.e. a network slice) during the specific time and period. This is referred to as on-demand network service. This implies that virtual networks should be created/deleted dynamically and the resources (e.g. bandwidth) of virtual networks should be added/decreased dynamically.

4.5. Redundant Network Service

Some service requires a number of redundant network paths that are physically diverse from one another. This implies that the virtual networks should indicate link and node diversity constraints.

4.6. Mobile/LTE Access Service

Consumer mobile/LTE access can be a tenant that shares the resources of the core transport network. In such case, a strict latency with a guaranteed bandwidth should be supported by multi-tenant virtual network operation.

5. Multi-tenant Virtual Network Operation Coordination

The following Figure 2 depicts a functional control architecture that shows the need to support virtual networks to a number of different service networks that share the common core network resources.

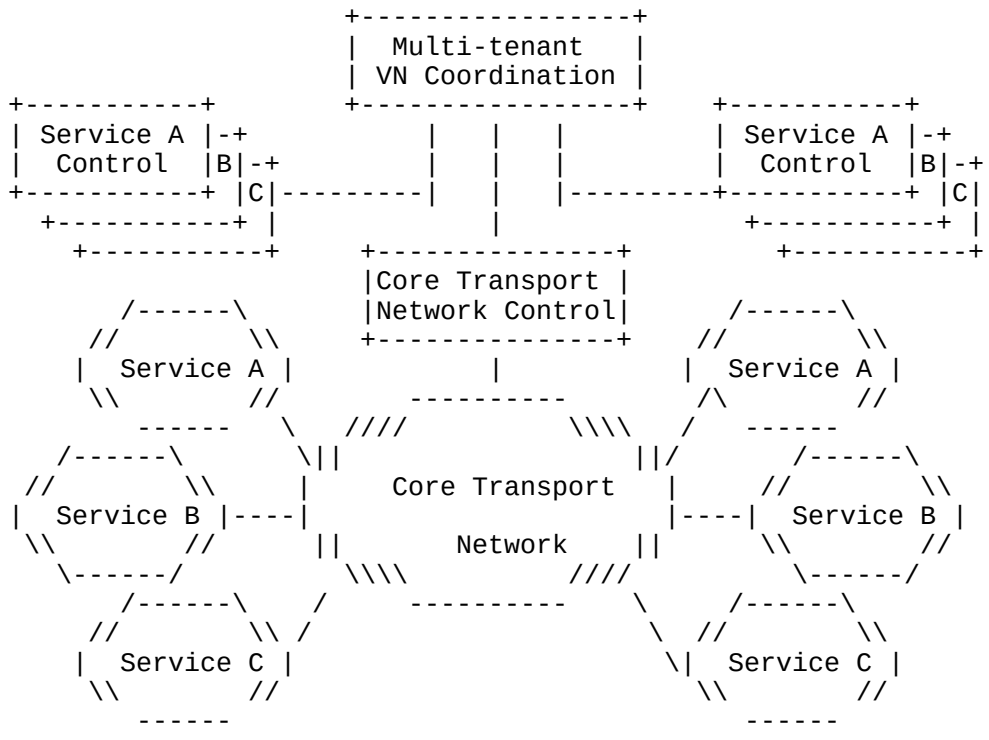


Figure 2: Multi-tenant control architecture

There are a few characteristics of the above architecture.

1. The core transport network is the common transport network resource pool for a number of multiple tenants, which is referred to as network tenancy.

2. Each service is a client to the common transport network.

3. Each service should be guaranteed its operational independence from other services. The separation of service control (depicted as separate boxes) in the above figure represents an operational independence.

4. The virtual network for each service is created and assigned by the multi-tenant virtual network coordination function. This is a functional entity that communicates with each service control and the core transport network control/management entities in order to coordinate with the necessary communication.

5. Each service instantiates its service instance based on its virtual network.

6. Each service is in control of its virtual network and operates on the virtual network.

7. As a number of services carried on the common transport network sharing a common network resource, operational independence for each service has to be guaranteed as if each service owns its dedicated resources.

8. The level of abstraction of a virtual network is determined by each service and may differ from one another. In some cases, a virtual network should represent a graph form of topology abstraction of the virtual network.

6. High-level Requirements for Multi-tenant Virtual Network Operations

Based on the discussion in the previous sections, this section provides the overall requirements that must be supported.

6.1. Dynamic binding - On-demand Virtual Network Service Creation

The solution needs to provide the ability to create a new virtual network on demand. The virtual network should be built dynamically.

6.2. Domain Control Plane/Routing Layer Separation

The solution needs to support an independent control plane for a domain service control. This implies that each service domain has

its own VN control scheme that is independent of other domain or the core transport network control.

6.3. Separate Operation of Virtual Services

The solution needs to support an independent operation of a virtual network and a service. Each Service Administrators should be able to control and manage its virtual network in terms of policy and resource allocation (e.g., CPU, Memory, other resources.) In addition, the virtualized networks should not affect each other in any way.

6.4. QoS/SLA

The solution needs to provide an independent QoS/SLA per a virtual network depending on a service level. Each QoS on the virtual network should support multiple service levels. Each SLA on the virtual network should fulfill a bandwidth and a latency required by each service.

6.5. VN diversity

Each service should be able to create multiple diverse VNs for the diversity purpose. The diversity for VNs must be physically diverse in the core transport network. This implies that the core transport network control/management plane must be able to factor the SRLG information when creating multiple VNs to ensure VN diversity.

6.6. Security Concerns

The solution needs to keep the confidentiality between the services. A service should not have the connectivity to an another service through the common core transport network.

7. Acknowledgments

The authors wish to thank Young Lee for the discussions in the document.

8. IANA Considerations

9. Security Considerations

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

10.2. Informational References

[I-D.ceccarelli-actn-framework]
Ceccarelli, D., Fang, L., Lee, Y., and D. Lopez, "Framework for Abstraction and Control of Transport Networks", draft-ceccarelli-actn-framework-01 (work in progress), February 2014.

[I-D.leeking-actn-problem-statement]
Lee, Y., King, D., Boucadair, M., and R. Jing, "Problem Statement for Abstraction and Control of Transport Networks", draft-leeking-actn-problem-statement-01 (work in progress), February 2014.

Authors' Addresses

Kenji Kumaki
KDDI Corporation
Garden Air Tower
Iidabashi, Chiyoda-ku, Tokyo, 102-8460
Japan

Email: ke-kumaki@kddi.com

Takuya Miyasaka
KDDI Corporation
Garden Air Tower
Iidabashi, Chiyoda-ku, Tokyo, 102-8460
Japan

Email: ta-miyasaka@kddi.com

Network Working Group
Internet Draft

Intended status: Informational
Expires: December 2015

Young Lee
Huawei
Daniel King
Lancaster University
M. Boucadair
France Telecom
R. Jing
China Telecom
L. Contreras Murillo
Telefonica

September 29, 2014

Problem Statement for Abstraction and Control of Transport Networks

draft-leeking-actn-problem-statement-03.txt

Status of this Memo

Copyright Notice

Abstract

Previously transport networks were typically static, lacked flexibility, and required long planning times when deploying new services. Network Providers and Service Providers have embraced technologies that allow separation of data plane and control plane, distributed signaling for path setup and protection, and centralized path computation for service planning and traffic engineering. Although these technologies provide significant benefits, they do not meet the growing need for network programmability, automation, resource sharing, and service elasticity necessary for meeting operator's requirement for their virtual network operation.

Virtual network operation refers to the creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-admin, multi-vendor, multi-technology networks and to operate, control and manage these multiple networks as if a single virtualized network. Another dimension of virtual network operation is associated with use of the common core transport network resource by multi-tenant service networks as a way of providing a virtualized infrastructure to flexibly offer new services and applications.

The work effort investigating this problem space is known as Abstraction and Control of Transport Networks (ACTN). This document provides an ACTN problem description, scope of work, and outlines the core requirements to facilitate virtual network operation.

Table of Contents

1. Introduction

Customers continue to demand new services that are time scheduled, dynamic, and underpinned by a Pay As You Go billing model. These services are provided to customers by network operators and service providers and give rise to a variety of applications for office automation, data backup and retrieval, distributed computing, and high-quality media broadcasting. They offer Network and Service Providers new revenue generation opportunities, and these services typically have different traffic characteristics from established network services such as file hosting, web, and email. Deploying and operating these new applications and services using traditional network technologies and architectures limits network efficiency, scalability, and elasticity (i.e., capable of adapting to customer and application demands).

Network virtualization has been a significant innovation towards meeting customer demands, and enabling new applications and services. Separating network resources, and representing resources and topologies via abstracted concepts, facilitate effective sharing, or slicing, of physical infrastructure into virtual network service instances corresponding to multiple virtual network topologies that may be used by specific applications, services and users. Further development is required to allow customers to create, modify, and delete virtual network services dynamically.

Previously transport networks were typically static, lacked flexibility, and required long planning times when deploying new services. Network Providers and Service Providers have embraced technologies that allow separation of data plane and control plane, distributed signaling for path setup and protection, and centralized path computation for service planning and traffic engineering. Although these technologies provide significant benefits, they do not meet the growing need for network programmability, automation, resource sharing, and service elasticity necessary for meeting operator’s requirement for their virtual network operation.

Virtual network operation refers to the creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-admin, multi-vendor, multi-technology networks and to operate, control and manage these multiple networks as single virtualized network. Another dimension of virtual network operation is associated with use of the common core transport network resource

by multi-tenant service networks as a way of providing a virtualized infrastructure to flexibly offer new services and applications.

Abstraction and Control of Transport Networks (ACTN) defines new methods and capabilities for the deployment and operation of transport network resource. These are summarized as:

- Coordination and abstraction of underlying transport network resources to higher-layer applications and customers (note that higher-layer applications and customers could be internal users of the core transport network resource such as various service networks);
- Multi-domain virtual network operation that facilitates multi-admin, multi-vendor, multi-technology networks as a single virtualized network.
- Multi-tenant virtual network operation that consolidates different network services and applications to allow slicing of network resources to meet specific service, application and customer requirements;
- Provision of a computation scheme and virtual control capability, via a data model, to customers who request virtual network services (note that these customers could be service providers themselves);

This document provides an ACTN problem description and scope of work, and outlines the core requirements to facilitate virtual network operation.

1.1. Terminology

This document uses the terminology defined in [RFC4655], and [RFC5440]. Additional terms are defined below.

- Customers:

Customers are users of virtual network services. They are provided with an abstract resource view of the network resource (known as "a slice") to support their users and applications. In some cases, customers may have to support multiple virtual network services with different service objectives and QoS requirements to support multiple types of users and applications. Customers can be internal trusted parties with respect to the provider such as wholesale service department, etc. Customers can also be trusted external parties with respect to the provider.

- Service Providers (also Virtual Network Service Provider):

Service Providers are the providers of virtual network services to their customers. Service Providers typically lease resources from single or multiple Network Providers' facilities to create virtual network services and offer end-to-end services to their customers. A Virtual Network Service Provider is a type of Service Provider, except that they may own no physical equipment or infrastructure, or have limited physical infrastructure and will require virtual resources for offering the final service, and only provide services built upon virtual network infrastructure. In general, this document does not distinguish between a Virtual Network Service Provider and Service Provider.

- Network Providers:

Network Providers are the infrastructure providers that own the physical network resources and provide transport network resources to their customers. Service Providers can be the customers of Network Providers or can be the Network Providers themselves.

- Network Virtualization:

Network virtualization, refers to allowing the customers to Utilize a certain network resources as if they own them and thus allows them to control their allocated resources in a way most optimal with higher layer or application processes. This customer control facilitates the introduction of new applications (on top of available services) as the customers are given programmable interfaces to create, modify, and delete their virtual network

services.

- Transport Networks

Transport networks are defined as network infrastructure that provides connectivity and bandwidth for customer services. They are characterized by their ability to support server layer provisioning and traffic engineering for client layer services, such that resource guarantees may be provided to their customers. Transport networks in this document refer to a set of different type of connection-oriented networks, which include Connection-Oriented Circuit Switched (CO-CS) networks and Connection-Oriented Packet Switched (CO-PS) networks. This implies that at least the following transport networks are in scope: Layer 1 (L1) and Layer 0 (L0) optical networks (e.g., OTN, ODU, OCh/WSON), MPLS-TP, MPLS-TE, as well as other emerging network technologies with connection-oriented behavior.

2. Relationship with Existing Technologies & Other Industry initiatives

2.1. Virtual Private Networks

A Virtual Private Network (VPN) is a well-known concept [RFC4110], [RFC4664] and [RFC4847], and may be used to connect Multiple distributed sites via a variety of transport technologies, sometimes over shared network infrastructure.

Typically VPNs are managed and provisioned directly by the Network Provider or a VPN Service Provider. VPN systems may be Classified by:

- Protocol mechanisms used to tunnel the traffic;
- Tunnel termination point and/or location;
- Type of connectivity, site-to-site or remote-access;
- Quality of Service (QoS) capabilities;

- o Level of security provided;
- o Emulated service connectivity layer (layer 1, layer 2, layer 3);

Existing VPN solutions are largely technology specific and offer limited elasticity, although some technologies offer greater flexibility (i.e., layer 2 VPNs [RFC4664] and layer 3 VPNs [RFC4110]) when compared with layer 1 VPNs [RFC4847], all technologies are often deployed using pre-defined configurations. [RFC4847] describes virtual networks in terms of ITU-T Y.1312 and Y.1313. Those Recommendations address both the data plane and control plane aspects of VPNs. Concepts of private and shared VPNs are described.

The transport layer is achieved by utilizing a variety of technology-specific interfaces - e.g. Gigabit Ethernet (GE), Synchronous Digital Hierarchy (SDH), or Asynchronous Transfer Mode (ATM) for wireless back-hauling, or optical networks OTN and WSON).

VPNs offer a scalable tunnel solution for customer traffic; However, they are wholly dependent on the Service Provider to setup and manage the VPNs, lacking customer-initiated service programmability: creation, resizing, and deletion.

2.2. Overlay Networks

An overlay network [RFC4208] provides an enhanced network

virtualization technique, with the overlay network providing a topology comprised of virtual or logical links and nodes, which are built on top of physical nodes and links, providing a topology in which some of the links and nodes are virtual or logical and are built from multiple nodes or links in a server network.

Overlay networks are typically used in the multi-layer context,

In which the packet layer is a client to the server transport layer. The scope of network virtualization in overlay networks is somewhat limited. Customers and applications which need visibility or programmability, and the ability to resize or add resources, may find that overlay network technologies do meet their requirements.

2.3. Other Industry Initiatives

ONF SDN Architecture (https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf) describes various arrangements of SDN controllers.

TM Forum's TR 215/TR225 addresses a common information model that can be applied to transport network in particular.

ITU-T Y.1312 and Y.1313 are a good reference to review for Layer 1 VPN in terms of terminology and architecture.

3. Motivations for Additional Functionality

3.1. Business Objectives

The traditional VPN and overlay network (ON) models are built on the premise that one single Network Provider provides all virtual private or overlay networks to its customers. This model is simple to operate but has some disadvantages in accommodating the increasing need for flexible and dynamic network virtualization capabilities.

A Network Provider may provide traditional end-to-end services And content (i.e., web and email) to its customers. Emerging services, applications and content are typically provided via Service Providers and Over the Top (OTT) (i.e., Video-on-demand, Social Media) providers. We can further categorize Service Providers as:

- A fixed or mobile Internet Service Providers (ISPs) which provide Internet connectivity and bandwidth to users;

- o A service provider that leases network resources from one or more network providers to create virtual network services between ISPs and the core Internet.

- o Data Center (DC)/content Network Provider and Service Providers who provide connectivity and bandwidth to content servers and application servers.

Network Providers and Service Providers of every type, all share The common business and revenue objectives:

- o Minimize time to plan and deploy new services;

- o Reduce the reliance on highly skilled personnel to operate their network;

- o Reduce time to react to changing business demands and customer applications;

- o Offer new, much more flexible services to their customers;

- o Maximize network resource usage and efficiency.

All aforementioned objectives have the capability to significant increase revenue and reduce operational costs.

Network and Service Providers require capabilities that extend the current landscape of network virtualization capabilities and overall business objectives of the Network Provider, Service Provider, and ultimately the Customer and their Applications.

3.2. Network Resource Recursiveness

A newly emerged network virtualization environment is a Collection of heterogeneous network architectures from different players. VPNs and overlay networks are somewhat limited in addressing programmable interfaces for application or customer layers as well as for the service layer. The model must be extended to address a recursive nature of layer interactions in

network virtualization across transport networks, service networks, and customers/applications.

3.3. Customer-Initiated Programmability

Network-driven technologies such as VPNs and overlay networks provide customers with a set of pre-defined programmatic parameters to enable virtual networks. However, this model is limited to only allow programmable interfaces in which customers initiate and define virtual network services. This model must be extended to allow customer-initiated network programmability.

3.4. Resource Partitioning

The ability to slice and allocate transport resources for Service Providers would be beneficial. It would improve transport network resource efficiency and provide a method for the transport Network Provider to offer resource flexibility and control to Service Providers and users.

3.5. Service Orchestration

Another dimension is diversity on the customer side. Customers in this newly emerged network virtualization environment bring different dynamics than the traditional VPNs or Overlay Networks. There may be a multiple virtual slices that need to be created, managed and deleted, each interfacing to a number of Service Providers and Network Providers as the end-points of the clients span across multiple network domains. Thus, multiple components will require automated co-ordination and management, this is known as service orchestration and is therefore one of the key capabilities that should be provided.

4. ACTN Objectives and Requirements

The overall goal of enabling network abstraction and multiple concurrent virtual networks to coexist together on a shared physical infrastructure, comprised on multiple physical layers,

and may be subdivided into several smaller objectives. These are outlined below and are required in order to fulfill the design goals of ACTN.

The ACTN effort should utilize existing physical layer monitoring capabilities, algorithmic representation and modelling of physical layer resources to consider appropriate transport metrics and constraints. Moreover, the model may want to support dynamic collection of the statistics (i.e., status and availability) of the underlying transport network infrastructure.

4.1. Capability and Resource Visibility

It may be necessary for the application or Customer to obtain available capabilities and available network resources, for example, abstracted resource view and control. The visibility of the capabilities and the resources can be obtained either by resource discovery or by resource publishing. In the former case, the customer performs resource collection directly from the provider network by using discovery mechanisms to get total information about the available resources to be consumed. In the latter case, the network provider exposes available resources to potential customers (e.g., through a resource catalog) reducing the amount of detail of the underlying network.

Furthermore, capabilities and resources will also include:

- Peering Points (may be based on business SLAs or policies);
- Transport Topology (i.e., transport switching type, topology and connection points);
- Transport Capacity (i.e., current bandwidth and maximum bandwidth).
- Policy Management (i.e., what resources and capabilities are available, and what may be requested and by whom).
- Information about the provider (i.e., informative data about the resource owner)

- Geographical information respect to the resources to be consumed (i.e., geolocation of the resources for preventing legal concerns that could appear in the provision of some final services).

- Information about resource cost, consumption, etc. (i.e., energy efficiency per transmitted bit, monetary cost of the resource usage per time unit, etc.).

- Information about achievable resiliency (i.e., protection/restoration capabilities, recover time, etc.).

4.2. Network Programmability

A programmable interface should provide customers with the capabilities to dynamically create, deploy, and operate services in response to customer and application demands. To enable the on-demand services, the separation of control and forwarding is a fundamental requirement. Once this separation is achieved the network layer may be programmed irrespective of the underlying forwarding mechanism.

The creation of a programmable abstraction layer for physical network devices would provide information models which would allow operators to manipulate the network resources. By utilizing open programmable north-bound network interfaces, it would enable access to virtual control layer by customer interfaces and applications.

4.3. Common Data Models

The abstraction of the underlay transport, and resource Information representation model should describe each technology type within the ACTN framework; they will all follow a uniform structure, which is extensible to support any future technologies.

Such models will represent the physical resources as a set of attributes, characteristics and functionality, while adaptively capturing the true real-time and dynamic (real-time) properties of underlying physical resources.

For future discussion, abstraction and the technology agnostic virtualization requirements may benefit from being split into new sub-sections, suggested below:

Attributes

- Metrics
- Control Actions
- Semantics
- Administrative information (resource ownership)

Resources will be described with semantic methods so that the resource description models can be exposed in a uniformly structured manner to the upper layers.

Virtual infrastructure requests from ACTN customers will be translated into network parameters according to aforementioned network abstraction model. Utilizing this mechanism, a request is translated into topology and multi-dimensional nodes, interfaces and spectrum space with specific attributes such as bandwidth, QoS, and node capability.

Apart from facilitating the request of resources, these data models could be used for other tasks like network operation (e.g., the management of the abstracted transport infrastructure by the customer), configuration (e.g., the control of the resources), monitoring (e.g., the uniform view of different infrastructures in use), KPI customization (e.g., the particularization of the collected metrics according to the customer interests), etc.

4.4. Scheduling

When requesting network slices it should be possible to request an immediate or scheduled service.

To enable such on-demand consumption of resources, the Network Providers must employ appropriate scheduling algorithms in all of the network elements.

4.5. Allocation

When establishing a network slice, a customer may require specific guarantees for the virtual node and link attributes. This might include a request that guarantees minimum packet processing on a virtual node, and fixed loss and delay characteristics on the virtual links. This should be governed by Service Level Agreements (SLAs) and can have implications in the supportive transport technologies, and in the properties of the service to be offered to the customer (e.g., protected versus non-protected).

To provide such guarantees and to create an illusion of an Isolated and dedicated network slice to each customer, the Network Providers must employ appropriate scheduling algorithms in all of the network elements.

4.6. Adaptability

Adaptability of services would allow the Service Provider, user, and application to request modification of exist network resource that has been assigned. This may include resizing of bandwidth, modification of the topology, and adding/removing connectivity points.

4.7. Slicing

It should be possible for transport network infrastructure to be partitioned into multiple independent virtual networks known as "slicing", based on provider service types, customers and application requirements.

4.8. Isolation

Isolation, both of physical underlay infrastructure and of co-existing virtual networks, and ensure no leakage of traffic. Furthermore, there must be mechanisms that ensure that once network slices are assigned Customer and Application services are not competing for transport resources.

Each customer or application should be able to use arbitrary network topology, routing, or forwarding functions as well as customized control mechanisms independent of the underlying physical network and other coexisting virtual networks.

It must also be possible for many virtual networks to share the underlying infrastructure, without significantly impacting the performance of applications utilizing the virtual networks.

4.9. Manageability

A broad range of capabilities, including: request, control, provisioning, monitoring, resilience, adaptation and re-optimization of end-to-end services will need to be provided through a set of well-defined interfaces, specifically it should be possible to provide:

- Control of virtual network resources, capable of delivering end-to-end services optimisation of connectivity and virtual infrastructure based on client interface and application demands, technology constraints (bandwidth, latency, jitter, function, etc.) and commercial constraints (energy, customer SLA, etc.).

- Automation of virtual service and function requests and objectives, and providing on-demand and self-service network

slicing.

- o Infrastructure elasticity to allow rapid provisioning, automatic scaling out, or in, of virtual resources.

- o Virtual resource monitoring [Editor's Note: Control of bandwidth, energy consumption and quality of service/packet scheduling.]

[Editor's Note: The requirements on the technology driver from both sides need to be analysed, e.g. the information update frequency.]

4.10. Resilience

The resilience of the transport service provided to the customer will depend on the requirements expressed by the customer. Two different resilience scenarios may be considered: (i) the resilience as observed from the point of view of the customer; and (ii) the resilience as observed from the point of view of the provider.

The former case refers to the situation in which the customer request for specific resilience requirements on the offered transport service. For instance, the customer can request transport protection on the disjoint paths for connecting service end-points. This specific requirement forces the provider to explicitly assign transport resources to a customer.

However there are other situations in which the provider has to allocate resources for implicit resilience. For instance, the customer could request a service with certain QoS or availability for a single connection between service end-points according to an SLA. In that case, the provider could trigger recovery actions in the network, e.g. during a network outage, and according to the conditions of the SLA. These measures may not be perceived by the customer.

4.11. Security

Network programmability may introduce new security and misconfiguration vulnerabilities. These must be investigated and discussed, and then solved with suitable solutions. ACTN-based networks must be resilient to existing, and new, faults and attacks.

Failure or security breach in one ACTN slice should not impact another virtual network. It must also be possible for separation of untrusted services and applications, along with confidential services and applications that must be secured.

Some other aspects are relevant to security within the context of ACTN:

- Security aspects from the service point of view. For instance, encryption capabilities as part of the service capabilities that could be requested by the customer.
- Security aspects from the customer/provider relationship point of view. For instance aspects like authentication, authorization, logging, etc.

4.12. Policy

[To be discussed.]

4.13. Technology Independence

ACTN must support a variety of underlay transport technologies, providing the flexibility to manage a variety of heterogeneous network technologies.

4.14. Optimization

It should be guaranteed the capability of the service provider to

optimize the provided transport infrastructure without impacting the customer services. As the resources become consumed some fragmentation in the usage of the underlying infrastructure could occur. The provider then can be interested in optimizing the usage of its resources for several reasons (e.g., energy consumption, reutilization of vacant resources, etc.).

4.15. Multi-domain Support

A given customer could required to compose an end-to-end transport service by using network capabilities from different service providers that may be internal organizations or external entity. Reasons for that could be geographical coverage of the service (not fully served by a unique provider), resource availability (not enough resources from a given provider) or simply resiliency (provider diversity). ACTN should allow the multi domain approach for giving the customer the possibility of composing multi-provider transport services.

4.16. Architecture Principles

4.16.1. Network Partitioning

Coexistence of multiple network slices will need to be supported. It should also be possible for multiple network slices used by different customers to coexist together, spanning over part or full of the underlying physical networks.

4.16.2. Orchestration

ACTN should allow orchestration (automated co-ordination of functions) for managing and controlling virtual network services that may span multiple Service Providers and Network Providers.

4.16.3. Recursion

It should be possible for a network slice to be segmented to allow a slicing hierarchy with parent child relationships. Allowing a customer to become a virtual provider, this is known as recursion as well as nesting of network slices.

4.16.4. Legacy Support and Interoperability

Capability to deploy ACTN should be transparent to existing Physical network control and management mechanisms and protocols. Additionally, interoperability with non-ACTN based (i.e., conventional) networks should be guaranteed, thus allowing for the coexistence of both kinds of network solutions from the perspective of either the customer or the provider.

4.17. Other Related Work

4.17.1. Requirements for Automated (Configuration) Management

Given the ever-increasing complexity of the configuration tasks required for the dynamic provisioning of IP networks and services, [I-D.boucadair-network-automation-requirements] aims at listing the requirements to drive the specification of an automated configuration management framework, including the requirements for a protocol to convey configuration information towards the managed entities.

4.17.2. Connectivity Provisioning Negotiation Protocol (CPNP)

[I-D.boucadair-connectivity-provisioning-protocol] specifies the Connectivity Provisioning Negotiation Protocol (CPNP) which is used to facilitate the dynamic negotiation of service parameters between a Customer and a Provider. As such, CPNP is a generic protocol that can be used for various negotiation purposes that include (but are not necessarily limited to) connectivity provisioning services, storage facilities, CDN (Content Delivery Networks) footprint, etc.

The generic CPP template allows for:

- Automating the process of service negotiation and activation, thus accelerating service provisioning;
- Setting the (traffic) objectives of Traffic Engineering functions and service management functions.
- Enriching service and network management systems with 'decision-making' capabilities based on negotiated/offered CPPs.

5. References

5.1. Informative References

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and 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.

[RFC4110] R. Callon and M. Suzuki, "A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4110, July 2005.

[RFC4847] T. Takeda, Ed., "Framework and Requirements for Layer 1 Virtual Private Networks", RFC 4847, April 2007.

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

[RFC4664] L. Andersson, and E. Rosen, Eds., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, Sep 2006.

[RFC5440] JP. Vasseur, Ed. And JL. Le Roux, Ed. "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440,

March 2009.

[I-D.boucadair-connectivity-provisioning-protocol]
Boucadair, M. and C. Jacquenet, "Connectivity Provisioning Negotiation Protocol (CPNP)", draft-boucadair-connectivity-provisioning-protocol-01 (work in progress), October 2013.

[I-D.boucadair-network-automation-requirements]
Boucadair, M. and C. Jacquenet, "Requirements for Automated (Configuration) Management", draft-boucadair-network-automation-requirements-02 (work in progress), June 2013.

6. Acknowledgements

The authors wish to thank the contributions on the IETF ACTN mailing list.

7. IANA Considerations

Not Applicable.

8. Authors' Addresses

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

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

Mohamed Boucadair
France Telecom

Rennes 35000
France
Email: mohamed.boucadair@orange.com

Ruiquan Jing,
China Telecom Corporation Limited,
No. 118, Xizhimenneidajie, Xicheng District, Beijing, China
Email: jingrq@ctbri.com.cn

Luis Miguel Contreras Murillo
Telefonica I+D
Email: lmcm@tid.es

Intellectual Property Statement

The IETF Trust takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in any IETF Document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

Copies of Intellectual Property disclosures made to the IETF Secretariat and any assurances of licenses to be made available, Or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement any standard or specification contained in an IETF Document. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

All IETF Documents and the information contained therein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is currently provided by the

Internet Society.

Network Working Group
Diego Lopez (Ed.)
Telefonica

Internet Draft
Intended status: Informational

October 27, 2014

ACTN Use-case for Virtual Network Operation for Multiple Domains in a Single Operator Network

draft-lopez-actn-vno-multidomains-01.txt

Status of this Memo

Copyright Notice

Abstract

This document provides a use-case that addresses the need for facilitating the application of virtual network abstractions to network operation. These abstractions shall create a virtualized environment supporting operators in viewing and controlling different domains as a single virtualized network. Each domain can be created due to the applied technology, administrative zones, or vendor-specific technology islands).Such an approach will facilitate the deployment of NFV (Network Function Virtualization) mechanisms, and accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

This use-case considers the application of these abstractions within the network of a single operator.

Table of Contents

1. Introduction

Network operators build and operate their network using multiple domains in different dimensions. Domains may be defined by a collection of links and nodes (each of a different technology), administrative zones under the concern of a particular business entity, or vendor-specific "islands" where specific control mechanisms have to be applied. Establishing end-to-end connections spanning several of these domains is a perpetual problem for operators, which need to address both interoperability and operational concerns at the control and data planes. The introduction of new services often requiring connections that traverse multiple domains needs significant planning, the creation

of umbrella Network Management Systems (NMSs) or even several manual operations to interface different administrative zones, vendor equipment and technology. This problem becomes more relevant as the consolidation of virtualization technologies like Network Functions Virtualization (NFV) calls for a more elastic behavior of the transport network, able to support their requirements on dynamic infrastructure reconfiguration [NFV-UC].

This document provides a use-case that addresses the aforementioned need within a single operator network.

This use-case is a part of the overarching work, called Abstraction and Control of Transport Networks (ACTN). The goal of ACTN is to facilitate virtual network operation by:

- The creation of a virtualized environment allowing operators to view and work with the abstraction of the underlying multi-admin, multi-vendor, multi-technology networks and

- The operation and control/management of these multiple networks as a single virtualized network.

This will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

Related documents are the ACTN-framework [ACTN-Frame] and the problem statement [ACTN-PS].

2. Operational Issues in Multi-domain Networks

As an illustrative example, let’s consider a multi-domain network consisting of four administration zones: three Data Center Network zones, A, B and C; and one core Transport Network (TN) zone to which Data Center Network zones A, B and C are inter-connected. These zones are under a single operator’s administration, but there are organizational boundaries amongst them (being under the concern of different business units or technical departments, for example).

Figure 1 shows this multi-domain network example.

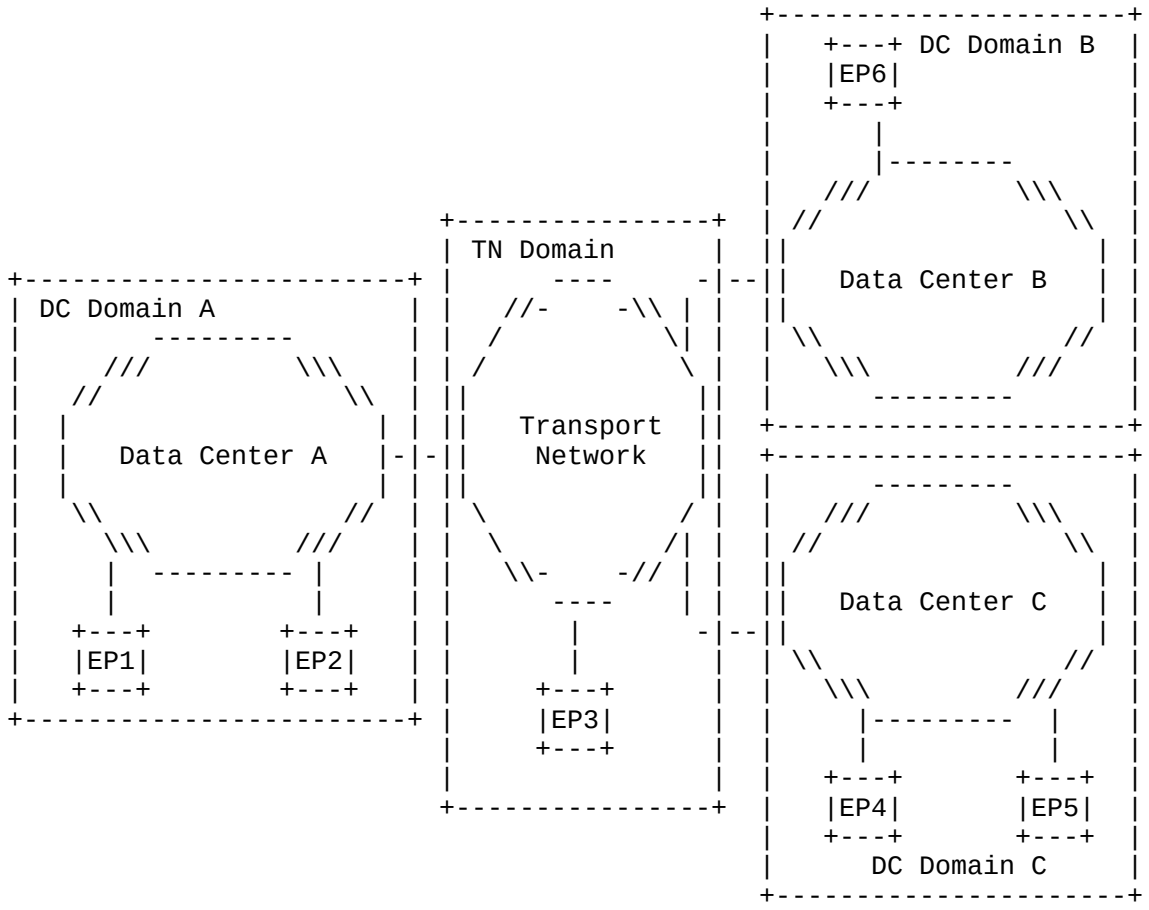


Figure 1. Multi-domain Network

Although the figure depicts a single operator’s network, there can be several partitions into sub-domains in which some connections may have to traverse several sub-domains to connect End Points (EPs). EPs are customer end-points such as enterprise gateway locations, some of which are directly homed on transport networks, while some

others are part of data center networks. EPs can also host physical or virtual network functions (PNFs/VNFs) or virtual machines (VMs). Connections between EPs in many cases have to traverse multiple technology and/or administrative domains. For instance, in Figure 1 if EP1 were to be connected to EP4, then the data path for this connection would have to traverse DC Domain A, TN Domain and DC Domain C where the destination of this connection resides. Another example of a multi-domain connection would be from EP3 in TN Domain to EP 6 in DC Domain B.

There are also intra-domain connections; for instance, a connection from EP4 to EP5 would only constitute an intra-domain connection within DC Domain C. We can assume there are domain control entities of various types (e.g., SDN-controller, NMS/EMS, Control Plane, or a combination of these entities, etc.) responsible for domain-specific network operations such as connection operation and management (including creation/deletion of a connection, path computation and protections, etc.), and other functions related to operations such as configuration, monitor, fault management, etc. As different technologies have emerged in different points of time, there is a plethora of diverse domain control systems with their respective interfaces and protocols. To maximize capital investments, operators tend to keep the current legacy operation and management technology and to continue to offer network services from the technology deployed in their networks.

Due to these domain boundaries, facilitating connections that traverse multi-domains is not readily achieved. Each domain control establishing other domain control in a peer to peer level creates permutation issues for the end-to-end control. Besides, these domain controls are optimized for its local operation and in most cases not suited for controlling the end-to-end connectivity services. For instance, the discovery of the EPs that belong to other domains is hard to achieve partly because of the lack of the common API and its information model and control mechanisms thereof to disseminate the relevant information. Some scenarios would require a path computation service for each domain to carry out end-to-end path computation, but considering current status of the network.

Moreover, the path computation for any end-to-end connection would need abstraction of network resources and ways to find an optimal path that meets the connection’s service requirements. This would require knowledge of the inter-domain peering relationships and the local domain policy.

From a connection provisioning perspective, in order to facilitate a fast and reliable end-to-end signaling, each domain operation and management elements should ideally work with the same control protocols that its neighboring domains. At least each domain should

support a stitching mode, so the end-to-end connection can be created in a per domain basis.

From a network connectivity management perspective, it would require a mechanism to disseminate any connectivity issues from the local domain to the other domains whenever the local domain cannot resolve a connectivity issue. This connectivity issue can happen during the provisioning time or during the network operation, when there is a failure on a connection that cannot be restored or protected.

3. Virtual Network Operations for Multi-domain Networks

Based on the issues discussed in the previous section in regard to the operations for multi-domain networks, we propose the definition of a virtual network operations (VNO) infrastructure that helps operators to establish end-to-end connections spanning multiple domains and its related operation and management issues.

The VNO Coordinator facilitates virtual network operation, the creation of a virtualized environment allowing operators to view the underlying multi-admin, multi-vendor, multi-technology networks and their operation and management as a single, virtualized network.

The basic premise of VNO is to create a hierarchy of operations in which to separate virtual network operations from physical network operations. This helps operators build virtual network operations infrastructure on top of physical network operations. Figure 2 shows a hierarchical structure of operations.

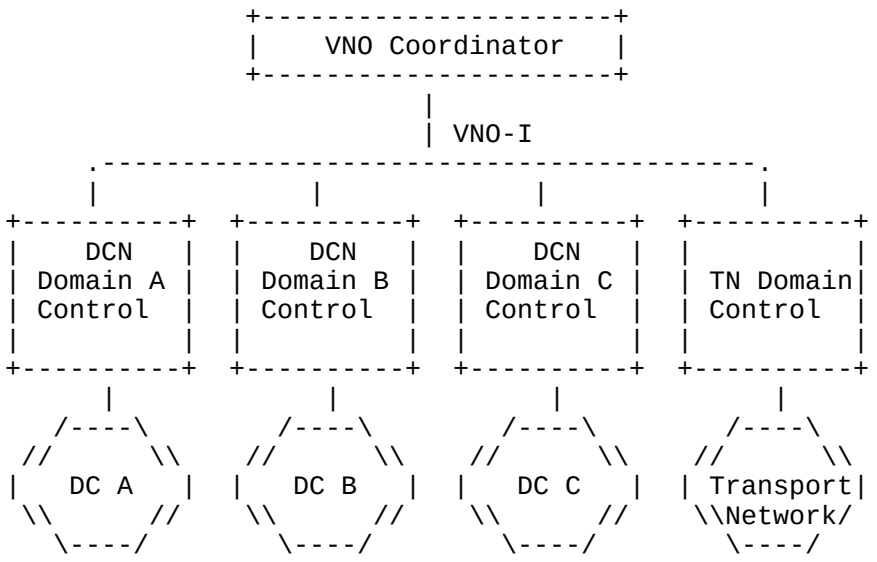


Figure 2. Operations Hierarchy

Figure 2 shows operations hierarchy based on Figure 1. The two main ideas are:

1. Domain control/management entities (e.g., DCN Domain Control A, B, C and TN Domain Control) are kept intact to continue its domain operations with its technology choice and policy, etc. As discussed before domain control/management entities can be a form of various types (e.g., SDN-controller, NMS/EMS, Control Plane, or a combination of these entities, etc.) that is responsible for domain-specific network operations.

2. The VNO Coordinator establishes a standard-based API (which is termed as the Virtual Network Operations Interface (VNO-I) in Figure 2) with each of the domain control/management entities. The VNO coordination takes place via the VNO-I's.

3.1. Responsibilities of Domain Control/Management Entities

. Creation of domain-level abstraction of network topology

It is the responsibility of domain control/management entity to create an abstraction of its network topology. The level of abstraction varies from one domain to another, subject to local domain policy. All EPs and gateway nodes to other domains need

to be represented at a minimum. The level of internal nodes and links may be abstracted according to its domain policy.

. Dissemination of abstraction of network topology to the VNO Coordinator (both Push and Pull models)

. VNO interface support (e.g., protocol, messages, etc.)

. Domain-level connection control/management that includes creation/deletion of a connection

. Domain-level path computation and optimization

. Domain-level protection and reroute

. Domain-lever policy enforcement

. Other functions related to operations such as monitor, fault management, accounting, etc.

3.2. Responsibilities of the VNO Coordinator

. Creation of a global abstraction of network topology.

The VNO Coordinator assembles each domain level abstraction of network topology into a global abstraction of the end-to-end network.

. VNO interface support (e.g., protocol, messages, etc.)

. End-to-end connection lifecycle management

. Invocation of path provisioning request to each domain (including optimization requests)

. Invocation of path protection/reroute to the affected domain(s)

. End-to-end network monitoring and fault management. This could imply potential KPIs and alarm correlation capabilities.

. End-to-end accounting and generation of detailed records for resource usage

. End-to-end policy enforcement

. OSS/BSS interface support for service management

3.3. Virtual Network Operations Interface (VNO-I)

VNO-I should support the transfer of information detailed above to perform the identified functionality. It should be based on open standard-based API.

[Editor's Note: the details of the supported functions of the VNO-I as well as the discussions pertaining to the info/data model requirements of the VNO-I will be supplied in the revision]

4. References

[ACTN-Frame] D. Ceccarelli, L. Fang, Y. Lee and D. Lopez, "Framework for Abstraction and Control of Transport Networks," draft-ceccarelli-actn-framework, work in progress.

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

[NFV-UC] NFV ETSI Industry Specification Group (ISG), "Network Functions Virtualisation (NFV); Use Cases", http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

Author's Addresses

Diego Lopez (Editor)
Telefonica
Email: diego@tid.es

Young Lee
Huawei
Email: leeyoung@huawei.com

LUIS MIGUEL CONTRERAS MURILLO
Telefonica
Email: luismiguel.contrerasmurillo@telefonica.com

Victor Lopez Alvarez
Telefonica
Email: victor.lopezalvarez@telefonica.com

Network Working Group J. Shin
R. Hwang
J. Lee
Internet Draft SK Telecom
Intended status: Informational

June 30, 2014

ACTN Use-case for Mobile Virtual Network Operation for Multiple Domains in a Single Operator Network

draft-shin-actn-mvno-multi-domain-00.txt

Status of this Memo

Copyright Notice

Abstract

This document provides a use-case that addresses the need for virtual network operation for mobile operators, which is facilitated by the application of network abstraction. These abstractions shall create a virtual network operation environment supporting mobile operators in viewing, managing and operating multi-domains of many dimensions (e.g., radio access, backhaul transport, mobile DC edge, mobile DC core, packet/optical transport for DC interconnect, etc.) as a single virtualized network.

This use-case considers the application of these abstractions and the need for the associated operational mechanisms within the network of a single operator.

Table of Contents

1. Introduction

Mobile network operators build and operate their network using multiple domains in different dimensions. From a network domain/technology point of view, mobile services/applications traverse many different domains such as radio access, backhaul transport, mobile DC edge, packet/optical backbone transport for DC interconnect, mobile DC core, etc. Due to this diversity of technology domains (e.g., radio, packet, optical, etc.) and the complex organizational boundaries for operations (e.g., access, backhaul, core transport, data center, etc.), the efficient operation of the services/applications spanning several of these domains has been a challenge for mobile operators.

In addition, multi-vendor issue adds another dimension of complexity. Both interoperability and operational concerns at the control and data planes have increased operational complexity and the OpEx.

Moreover, the widespread deployment of middle boxes (e.g. edge cache, firewall etc.) inside the DC edge and core edge will be achieved due to tightly-coupled interaction with higher layer protocols and transport control protocols (i.e. GMPLS, RSVP, etc.)

With the aforementioned situations, the introduction of new services and applications, often requiring connections that traverse multiple domains, necessitates significant planning, and several manual operations to interface different administrative zones, vendor equipment and transport technology.

This document provides a use-case that addresses the need for facilitating the application of virtual network abstractions to mobile network operators. These abstractions shall create a virtualized network operation environment supporting mobile operators in viewing and controlling multi-domains of many dimensions (e.g., radio access, backhaul transport, mobile DC edge, mobile DC core, packet/optical transport for DC interconnect, etc.) as a single virtualized network. This use-case considers the application of these abstractions within the network of a single operator.

This use-case is a part of the overarching work, called Abstraction and Control of Transport Networks (ACTN). The goal of ACTN is to facilitate virtual network operation by:

- The creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-admin, multi-vendor, multi-technology networks and

- The operation and control/management of these multiple networks as a single virtualized network.

This will accelerate rapid service deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

Related documents are the ACTN-framework [ACTN-Frame] and the problem statement [ACTN-PS].

2. Operational Challenges and Issues in Mobile Operator's Multi-domain Networks

Figure 1 depicts an illustrative example for mobile operator's multi-domain networks.

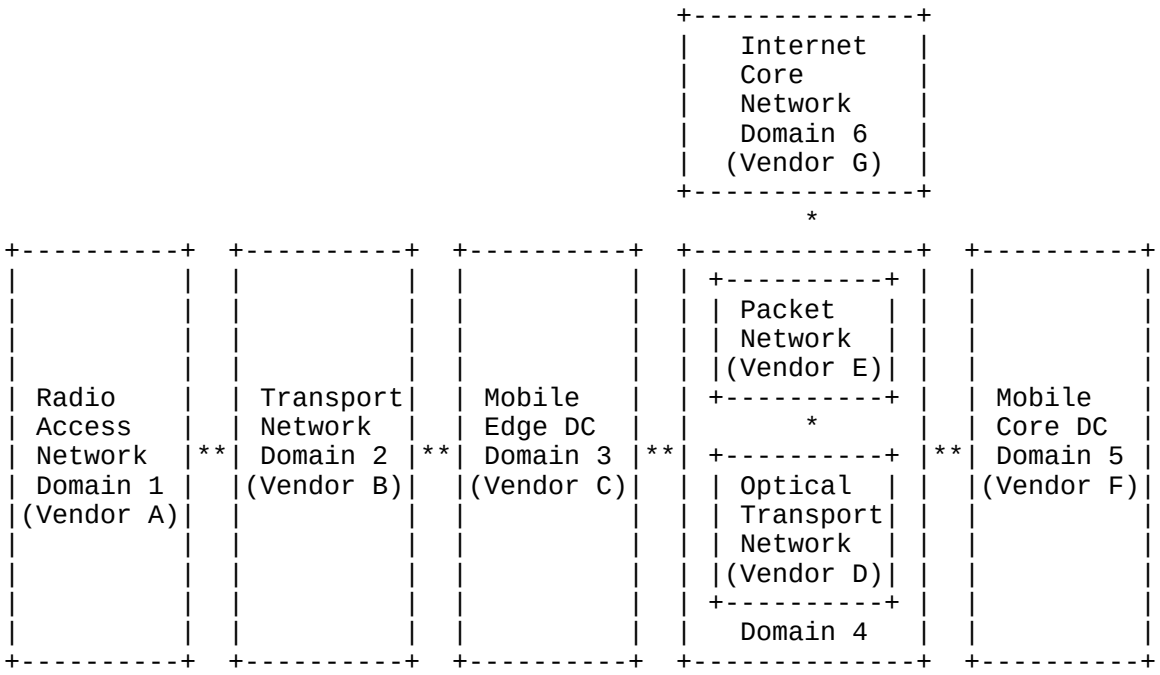


Figure 1: Multi-domains in Mobile Operator's Network

It consists of six domains:

1. Radio Access Network Domain
2. Mobile Backhaul Transport Network Domain
3. Mobile Edge Data Center Network Domain
4. Core Packet/Optical Transport Network Domain for Data Center interconnect (this domain typically consists of multi-layer)
5. Mobile Core Data Center Network Domain

6. Internet Core Network Domain

Mobile data application may find its servers hosted by the Mobile Edge DC (Domain 3) while some other applications hosted by servers in the Mobile Core DC (Domain 5). For the former case, the connectivity starts from a RAN edge and terminates at a Mobile Edge Data Center. For the latter case, the connectivity is extended beyond the Mobile Edge Data Center and traverses the Mobile Backhaul Transport Network domain and the Core Transport Network domain.

There are several issues that are relevant in the ACTN context:

1. Transport from RAN to Mobile Edge DC

From RAN to mobile edge DC, there is mobile backhaul transport network that provides connectivity between a client data device and one of the edge nodes in the Mobile Edge DC Domain. The backhaul transport networks provide tunnels for data transport for mobile applications. These tunnels are typically provisioned statically. This mobile backhaul transport network can be a resource bottle neck. Operators typically overprovision this backhaul network to accommodate unpredicted serge of data traffic.

Resource abstraction is one of the missing operational mechanisms in mobile backhaul network. Resource abstraction will give the current network usage information to the operators and will help dynamic and elastic applications be provisioned dynamically with QoS guarantee.

2. Transport from Mobile Edge DC to Mobile Core DC

From Mobile Edge DC domain to Mobile Core DC domain, there is core transport network that provides connectivity between edges to core. As Mobile Core DC servers may be geographically spread for load balancing or for recovery, the selection of core DC location from edge constitutes a data center selection problem.

To support dynamic and flexible connection setup for applications that are of dynamic nature with flexible bandwidth, network resource abstraction is needed to facilitate this operation.

3. Transport from Mobile Edge DC to Internet Core Network

From Mobile Edge DC domain to Internet Core Network, there is also core transport network that provides connectivity between edges to Internet core for Local traffic breakout (e.g. LIPA and SIPTO). As Mobile Edge DC servers may be geographically spread at the network edge side for load balancing, the selection of traffic from edge to Internet core is required to be controlled. See [3GPP TR 23.859] for related discussion.

4. Multi-layer Integration/Coordination (aka., POI)

Within the core transport network domain, there is also a multi-layer issue between packet networks and optical transport networks. To support multi-layer routing and optimization, coordination between these two layers are necessary. Network abstraction of both packet and optical networks will be very useful to support different applications flexibly and efficiently. See [ACTN-POI] for related discussion.

5. End-to-end tunnel/transport operations/management from RAN to Mobile Core DCN:

As there are multiple transport domains (namely, Mobile backhaul and Core transport networks) involved for an end-to-end connectivity within an operator’s network, the coordination between these domains are crucial for operation. Static provisioning with stitching tunnels are inadequate for many applications/services requiring strict QoS such as a guaranteed bandwidth and latency.

In the current network environments, these two domains are not well coordinated due to various reasons including the lack of a global resource view, a domain administrative boundary, and the differences in transport technology and vendor equipment.

In summary, due to complexity in mobile operator’s network in terms of heterogeneous transport technology, organizational boundaries between domains, multi-vendor issues and others, facilitating connectivity that traverse the aforementioned multi-domains is not readily achieved.

Each domain control establishing other domain control in a peer to peer level creates permutation issues for the end-to-end control. Besides, these domain controls are optimized for its local operation and in most cases not suited for controlling the end-to-end connectivity services.

Moreover, the path computation for any end-to-end connection would need abstraction of network resources and ways to find an optimal path that meets the connection’s service requirements. This would require knowledge of network abstraction and topology for all domains through which a connection traverses.

For mobile networks, signaling is a complex issue as it involves not only a session control but also a connection control. The coordination between the session control and the connection control has to be worked out for a seamless operation.

From a network connectivity management perspective, it would require a mechanism to disseminate any connectivity issues from the local domain to the other domains whenever the local domain cannot resolve a connectivity issues.

3. Virtual Network Operations for Mobile Operators' Networks

Based on the issues discussed in the previous section in regard to the operations for mobile multi-domain networks, there is a need to support a coordination that facilitates virtual network operation, the creation of a virtualized environment allowing operators to view the underlying radio access network, backhaul transport network, mobile DC edge, mobile DC core, packet/optical transport network for DC interconnect networks and their operation and management as a single, virtualized network.

The basic premise of this virtual network operation is to create a hierarchy of operations in which to separate virtual network operations from physical network operations. This helps operators build virtual network operations infrastructure on top of physical network operations. Figure 2 shows a hierarchical structure of operations.

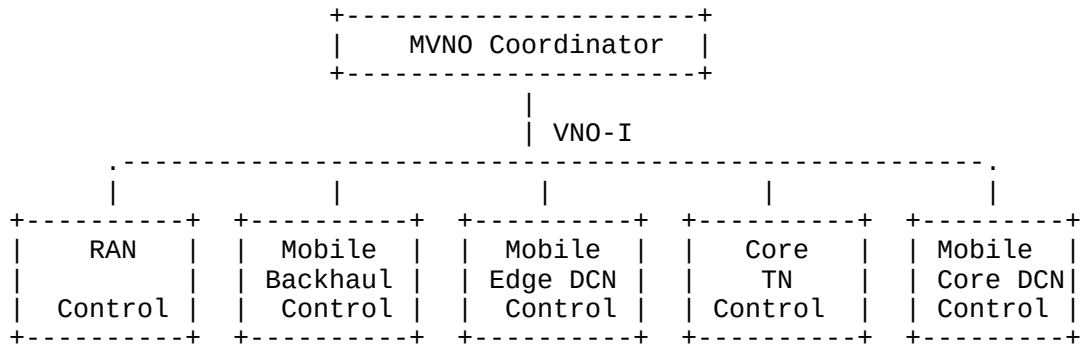


Figure 2. Mobile VN Operation Hierarchy

Figure 2 shows operations hierarchy based on Figure 1. The two main ideas are:

1. Domain control/management entities (e.g., RAN Control, Mobile Backhaul Network Control, Mobile Edge Data Center Network Control, Core Transport Network Control, Mobile Core Data Center Network Control) are kept intact to continue its domain operations with its technology choice and policy, etc. As discussed before domain

control/management entities can be a form of various types (e.g., SDN-controller, NMS/EMS, Control Plane, or a combination of these entities, etc.) that is responsible for domain-specific network operations.

2. The VNO Coordinator establishes a standard-based API (which is termed as the Virtual Network Operations Interface (VNO-I) in Figure 2) with each of the domain control/management entities. The VNO coordination takes place via the VNO-I's.

4. References

[ACTN-Frame] D. Ceccarelli, L. Fang, Y. Lee and D. Lopez, "Framework for Abstraction and Control of Transport Networks," draft-ceccarelli-actn-framework, work in progress.

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

[ACTN-POI] 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.

[3GPP TR 23.859] Local IP access (LIPA) mobility and Selected IP Traffic Offload (SIPTO) at the local network.

5. Contributors

Author's Addresses

Jongyoon Shin
SK Telecom
6 Hwangsaeul-ro, 258 beon-gil, Bundang-gu, Seongnam-si,
Gyeonggi-do, 463-784, Republic of Korea
Email : jongyoon.shin@sk.com

Rod Hwang
SK Telecom
6 Hwangsaeul-ro, 258 beon-gil, Bundang-gu, Seongnam-si,
Gyeonggi-do, 463-784, Republic of Korea
Email : rod.hwang@sk.com

Jongmin Lee
SK Telecom
6 Hwangsaeul-ro, 258 beon-gil, Bundang-gu, Seongnam-si,
Gyeonggi-do, 463-784, Republic of Korea

Email : jminlee@sk.com

Intellectual Property Statement

Disclaimer of Validity

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Network Working Group
Internet Draft
Intended status: Informational
Expires: October2015

Yunbin Xu
CATR

Guoying Zhang
CATR

Weiqiang Cheng
CMCC

Haomian zheng
Huawei

April 27, 2015

Use Cases and Requirements of Dynamic Service Control based on Performance Monitoring in ACTN Architecture
draft-xu-actn-perf-dynamic-service-control-03.txt

Status of this Memo

This Internet-Draft is submitted 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 October 27, 2015.

Copyright Notice

Abstract

This document introduces the dynamic creation, modification and optimization of services based on the performance monitoring in the Abstraction and Control of Transport Networks (ACTN) architecture.

Table of Contents

1. Introduction

The rapid growth of Internet traffic and the emerging applications such as cloud computing, datacenter interconnection, IP and optical integration, LTE backhauling, are driving the transport network to provide dynamic service provisioning based on the customer requirement and high quality services with guaranteed performance.

For datacenter interconnection services, IP network transit links, LTE backhauling services or some business customer services, the traffic vary over time. However, traditional optical network could only provide connection based on the maximum bandwidth needed. Based on flow traffic monitoring, it is possible to adjust the connection bandwidth according to the real bandwidth needed, create new connections or increase bandwidth when network traffic exceeds some certain threshold or reduce connection bandwidth when traffic drops down, thus helping the customers to save cost.

On the other hand, customers have different SLA requirements. Some customers such as financial service companies need ultra-low-latency transmission, some other customers has strict requirements on bit error rate (BER). In order to provide high quality services according to customer SLA, network provider needs to measure the service performance, and dynamically provision and optimize services based on the performance monitoring result.

The optical transport networks support various performance monitoring mechanisms, such as traffic flow statistics, packet delay, delay variation, throughput and packet-loss rate for MPLS-TP and packet OTN networks, BER, FEC error correction counters for OTN and DWDM networks, etc. These mechanisms can be used to support dynamic service control based on performance monitoring.

The Abstraction and Control of Transport Networks (ACTN) described in [ACTN-FWK] provides a centralized control architecture and open interfaces that can transmit the customer requirements and policies to the network, and provide customers with the network status to make a decision. This draft mainly discusses the use cases and requirements of dynamic service control based on performance monitoring in ACTN architecture, the requirements for southbound and northbound interface are also discussed.

2. Use Cases and Requirements for Dynamic Service Control based on Performance Monitoring

2.1. Dynamic Service Control based on Traffic Monitoring

For LTE backhauling based on MPLS-TP packet transport networks(PTN) or packet OTN, it is required that real time or semi-real time

traffic monitoring of the network should be conducted so as to resize or optimize traffic and do load balance. In IP and optical network integration scenario, the optical network can bypass IP transit traffic as far as the transit traffic bandwidth is large enough to occupy the granularity of an ODUk. Network traffic monitoring is important to facilitate automatic discovery of the imbalance of network traffic, and initiate the network optimization, thus helping the network operator or the virtual network service provider to use the network more efficiently and save CAPEX/OPEX.

For datacenter interconnection or enterprise leased line services, the traffic may vary over time and the customer want to pay for the bandwidth they really used. Therefore, it is important to provide some mechanism to monitor the network traffic, adjust and optimize the services dynamically to help the customers save expenses. In order to support these scenarios, the customers or client layer network controllers need to send traffic monitoring and control policies to the network, while the transport network should report the traffic monitoring results and dynamically control and adjust network connections based on the traffic optimization policy. The service adjustment or network optimization operations normally should be initiated with the decision of the customer.

2.2. Dynamic Service Control based on SLA monitoring

Customer services have various SLA requirements, such as service availability, latency, latency jitter, packet loss rate, BER, etc. The transport network can satisfy service availability and BER requirements by providing different protection and restoration mechanisms. However, for other performance parameters, there are no such mechanisms.

In order to provide high quality services according to customer SLA, one possible solution is to measure the service SLA related performance parameters, and dynamically provision and optimize services based on the performance monitoring results.

When the network performance deterioration that violates the SLA is detected, service optimization operations such as service rerouting, creation of new connections could be automatically started.

In order to support this requirement, the customer should be able to send its SLA information to the network, and the transport network should determine which performance parameters need to be monitored and the strategy of service optimization. When the service performance degradation is detected, the transport network can

notify the customer and immediately start the service optimization procedure, so as to reduce the impact on the service.

3. Workflows of ACTN Control Modules

In the ACTN architecture [ACTN-FWK], centralized controllers including Physical Network Controller (PNC), Multi Domain Service Coordinator (MDSC), Customer Network Controller(CNC), and the interfaces between them have been defined.

For different use cases and scenarios, the workflows across the customer controller, MDSC and PNC are different.

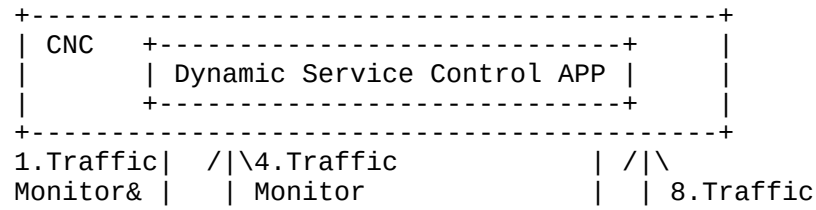
3.1. Workflows for Traffic Monitoring based Dynamic Service Control

Figure 1 shows the workflows for dynamic service control based on traffic monitoring.

In order to realize dynamic service creation, adjustment and optimization based on traffic monitoring, the customer controller should send traffic monitoring and traffic optimization strategies to MDSC. MDSC sends the corresponding path traffic monitoring request to PNC. Traffic monitoring parameters and monitoring cycle need to be carried in this request.

PNC gets the traffic monitoring results from the underlying physical networks, translates the monitoring results of the physical topology to the performance information of the abstract topology, and then reports to MDSC. According to the traffic optimization strategy obtained from the customer controller, MDSC determines whether the service needs to be adjusted, or a new connection should be created. If it needs to, then MDSC send the traffic monitoring results to the customer controller, indicating that the service needs adjustment.

Customer Network Controller confirms whether the service can be optimized then sends a service adjustment request to MDSC. MDSC will convert it into path modification or creation request, and send it to PNC to complete the service optimization. Then, PNC returns the optimization results to MDSC, and MDSC passes the results to the customer controller.



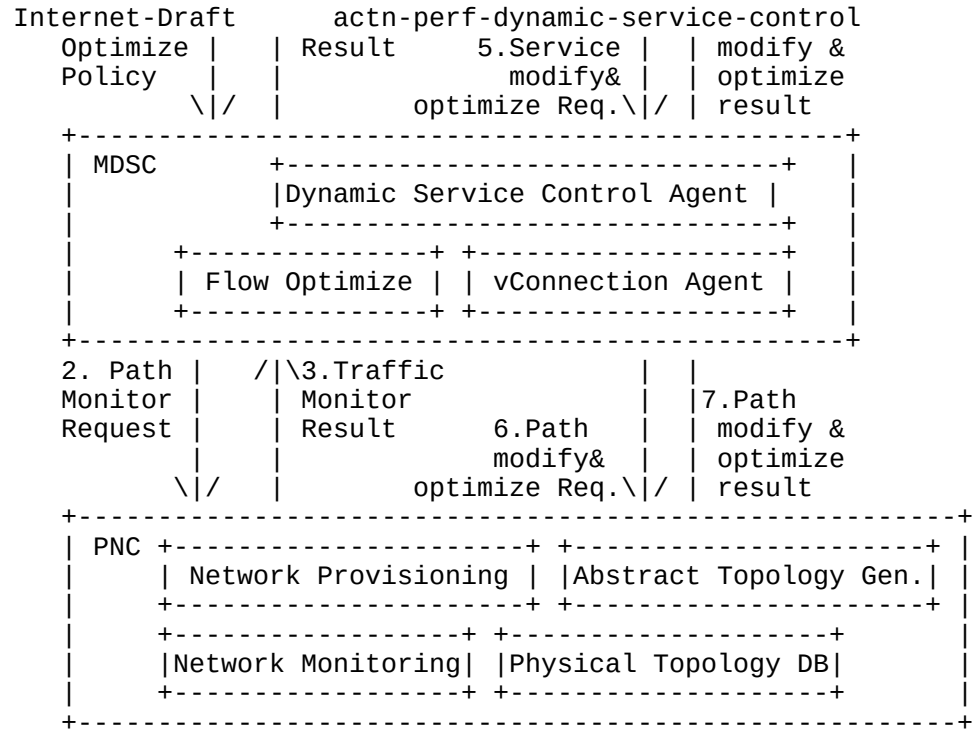


Figure 1 Workflows for dynamic service control based on traffic monitoring

3.2. Workflows for SLA monitoring based Dynamic Service control

Figure 2 shows the workflows for dynamic service control based on SLA related performance monitoring.

Customer controller sends the customer service SLA information and the performance based optimization strategy to MDSC.

MDSC will convert the SLA information to path performance monitoring request, which carries the performance monitoring parameters such as delay, jitter, packet loss, bit error rate and monitoring cycle, and then send it to the PNC.

PNC starts the performance monitoring in the underlying physical networks, collects the results of related path, translates the performance results of the physical topology to the performance information of the abstract topology, and reports to MDSC. MDSC

determines whether the relevant performance parameters can satisfy the SLA agreements. If the performance degradation seriously influences the service, such as service packet delay exceeds the performance threshold, MDSC will immediately start the optimization and adjustment. Then the performance monitoring results as well as the optimizing or adjusting results will be send to the Customer Network Controller.

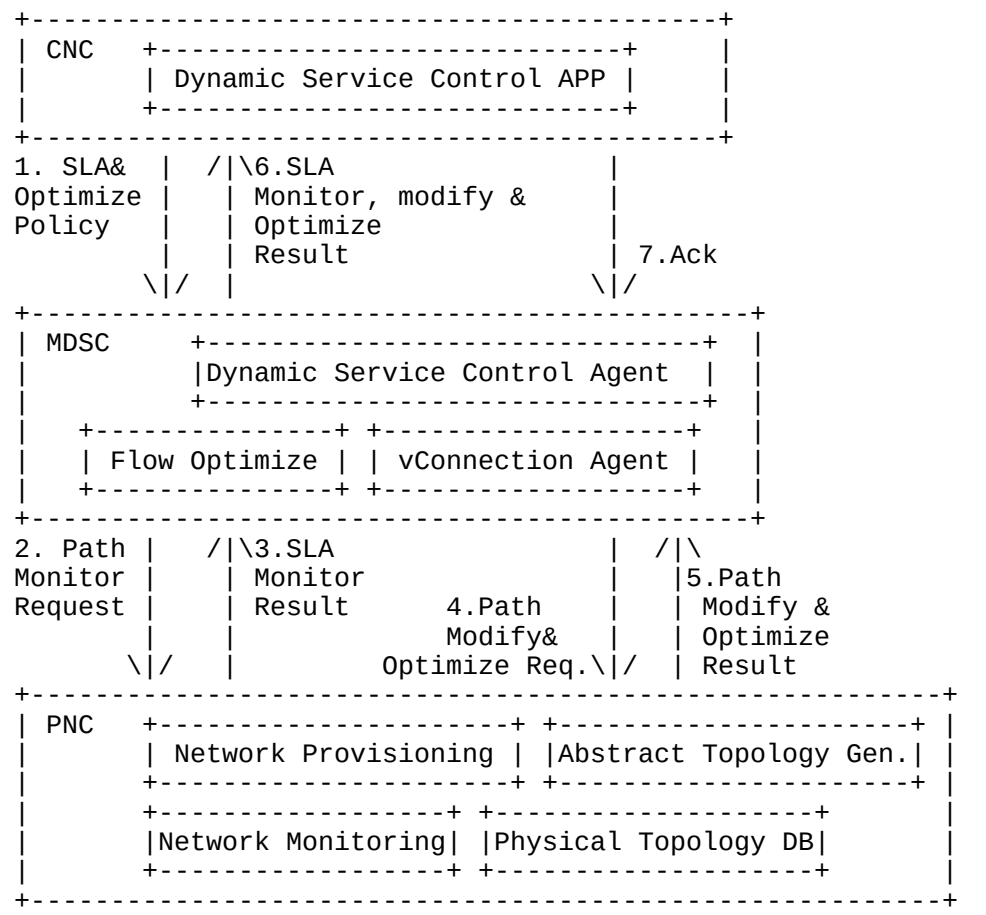


Figure 2 Workflows for dynamic service control based on SLA monitoring

4. Requirement for ACTN Interface

ACTN Interfaces defined [ACTN-FWK] includes the following:

- CNC-MDSC Interface (CMI): an interface between a Customer Network Controller and a Multi Service Domain Controller.

- MDSC-PNC Interface (MPI): an interface between a Multi Service Domain Controller and a physical network controller.

4.1. Interface Requirements for Dynamic Service Control Based on Traffic Monitoring

According to the work flow of dynamic service control based on performance monitoring, the information carried in CMI interface mainly relates to the traffic monitoring and control strategy, while the MPI interface mainly relates to transports path related traffic monitoring parameters and results.

1. CMI Interface

The following information is used by the customer network controller to send to MDSC through the CMI interface.

- Customer service performance monitoring strategy, including the traffic monitoring object (the service need to be monitored), monitoring parameters (e.g., transmitted and received bytes per unit time), traffic monitoring cycle (e.g., 15 minutes, 24 hours), threshold of traffic monitoring (e.g., high and low threshold), etc.

- Customer service optimization strategy, such as enabling service creation or modification when traffic exceeds the threshold.

The following information is used for MDSC to send to the customer network controller through MPI interface.

- Traffic monitoring results, to indicate if the traffic exceeds the bandwidth threshold.

2. MPI Interface

The following parameters are used for MDSC to send to PNC.

- Traffic monitoring parameters, monitoring object, monitoring cycle, performance threshold.

The following information is used for PNC to send to MDSC.

- o Traffic monitoring results. These results must be translated from the physical topology to abstract topology by the Abstract Topology Generalization module firstly.

4.2. Interface Requirements of Dynamic Service Control based on SLA monitoring

According to the work flow of dynamic service control based on SLA monitoring, the information in VCI interface mainly contains the SLA related information and measurement strategy, while the MPI interface mainly transports path related performance monitoring parameters and results.

1. CMI Interface

The following information is used by the customer network controller to send to the MDSC through CMI interface.

- o SLA related performance requirement information, including the required quality of service parameters (e.g., BER, delay, delay jitter, packet loss rate, throughput, etc.).

- o Service optimization strategy, including the service performance degradation thresholds and the consequent operations that are allowed (e.g., rerouting).

The following information is used by the customer network controller to send to MDSC.

- o Monitoring results of service performance, including performance monitoring parameters, and the services that have been influenced.

- o Service optimization results based on performance.

2. MPI Interface

The following information is used by MDSC to send to PNC.

- o The path performance monitoring request parameters, monitoring cycle and threshold.

The following information is used for PNC sending to MDSC.

- o Path performance monitoring results.

4.3. Discussion

Performance monitoring in a large scale network could generate a huge amount of performance information. Therefore, the appropriate

way to deliver the information in CMI and MPI interfaces should be carefully considered.

5. Security Considerations

This document raises no new security issues.

6. IANA Considerations

No new IANA considerations are raised by this document.

7. References

7.1. Informative References

[ACTN-FWK] Daniele C., Luyuan Fang, Yong Lee and Diego Lopez, "Framework for Abstraction and Control of Transport Networks",draft-ceccarelli-actn-framework-07.

Authors' Address

Yunbin Xu
China Academy of Telecom Research
NO.52 Huayuan Beilu, Haidian District, Beijing, China
Email: xuyunbin@catr.cn

Guoying Zhang
China Academy of Telecom Research
NO.52 Huayuan Beilu, Haidian District, Beijing, China
Email: zhangguoying@catr.cn

Weiqiang Cheng
China Mobile Communication Company

Email:chengweiqiang@chinamobile.com

Haomian Zheng
Huawei Technologies
F3-1-B R&D Center, Bantian, Longgang District Shenzhen, China
Email: zhenghaomian@huawei.com