

Network Working Group
Internet Draft
Intended status: Informational
Expires: December 10, 2015

Young Lee
Huawei
Daniel King
Lancaster University
M. Boucadair
France Telecom
R. Jing
China Telecom
L. Contreras Murillo
Telefonica
June 9, 2015

Problem Statement for Abstraction and Control of Transport Networks
draft-leeking-teas-actn-problem-statement-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire December 10, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

Internet-Draft

ACTN PS

June 2015

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Abstract

Transport networks that provide connectivity and bandwidth for customer services have typically been static, lacking flexibility, and requiring 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 to meet operators' requirements for virtual network operation.

Virtual network operation refers to the creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-administration, 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 the use of common core transport network resources 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, a scope of work, and outlines the core objectives and requirements to facilitate virtual network operation.

Table of Contents

| | | |
|----------------------|---|-------------------|
| 1. | Introduction..... | 4 |
| 1.1. | Terminology..... | 5 |
| 2. | Objectives and Functional Requirements..... | 7 |
| 2.1. | Use Cases..... | 7 |
| | 2.1.1 Packet Transport Networks (PTN) in Mobile Backhaul | |

| | |
|--|-------------------|
| Networks..... | 7 |
| 2.1.2 Packet Optical Integration (POI)..... | 7 |
| 2.1.3 Multi-domain Data Center Interconnect..... | 7 |
| 2.1.4 On-demand E2E Connectivity Services in Multiple Vendor Domain Transport Networks..... | 8 |
| 2.1.5 Multi Tenant Virtual Network Operators..... | 9 |

| | |
|--|--------------------|
| 2.1.6 Virtual Network Operation for Multiple Domains in a Single Operator Network..... | 10 |
| 2.1.7 Mobile Virtual Network Operation for Multiple Domains in a Single Operator Network..... | 10 |
| 2.1.8 Dynamic Service Control based on Performance Monitoring..... | 11 |
| 3. Relationship with Existing Technologies & Other Industry Initiatives..... | 11 |
| 3.1. Virtual Private Networks..... | 11 |
| 3.2. Overlay Networks..... | 12 |
| 3.3. Other Industry Initiatives..... | 12 |
| 4. Motivations for Additional Functionality..... | 13 |
| 4.1. Business Objectives..... | 13 |
| 4.2. Network Resource Recursiveness..... | 14 |
| 4.3. Customer-Initiated Programmability..... | 14 |
| 4.4. Resource Partitioning..... | 14 |
| 4.5. Service Orchestration..... | 14 |
| 5. ACTN Objectives and Requirements..... | 15 |
| 5.1. Capability and Resource Visibility..... | 15 |
| 5.2. Network Programmability..... | 16 |
| 5.3. Common Data Models..... | 16 |
| 5.4. Scheduling..... | 17 |
| 5.5. Slicing..... | 17 |
| 5.6. Adaptability..... | 17 |
| 5.7. Allocation..... | 17 |
| 5.8. Isolation..... | 18 |
| 5.9. Manageability..... | 18 |
| 5.10. Resilience..... | 19 |
| 5.11. Security..... | 19 |
| 5.12. Policy..... | 20 |
| 5.13. Technology Independence..... | 20 |
| 5.14. Optimization..... | 20 |
| 5.15. Multi-domain Support..... | 20 |
| 5.16. Architecture Principles..... | 20 |
| 5.16.1. Network Partitioning..... | 21 |
| 5.16.2. Orchestration..... | 21 |

| | | |
|------------------------|--|--------------------|
| 5.16.3 | Recursion..... | 21 |
| 5.16.4 | Legacy Support and Interoperability..... | 21 |
| 5.17 | Other Related Work..... | 21 |
| 5.17.1 | Requirements for Automated (Configuration) Management | 21 |
| 5.17.2 | Connectivity Provisioning Negotiation Protocol (CPNP) | 21 |
| 6 | References..... | 22 |
| 6.1 | Informative References..... | 22 |
| 7 | Acknowledgements..... | 24 |
| 8 | IANA Considerations..... | 24 |
| 9 | Authors' Addresses..... | 24 |

[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 existing network technologies and architectures limits network efficiency, scalability, and elasticity (i.e., they do not offer sufficient capability to adapt 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, facilitates 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.

Transport networks that provide connectivity and bandwidth for customer services have typically been static, lacking flexibility, and requiring 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 to meet operators' requirements for virtual network operation.

Virtual network operation refers to the creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-administration, 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 the use of common core transport network resources 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 follows.

- o 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.
- o Multi-domain virtual network operation that facilitates multi-administration, multi-vendor, and multi-technology networks as a single virtualized network.
- o 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.
- o 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, themselves, be service providers.

This document first presents the summary of ACTN use-cases, then provides an ACTN problem description and scope of work, and outlines the core objectives and requirements to facilitate virtual network operation.

1.1. Terminology

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

o Customers:

Customers are users of virtual network services. They are provided with an abstract 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 enable multiple types of users and applications. Customers may also be considered to be trusted parties with respect to the provider wholesale service department. A trust model will be required and is discussed further later in this document.

o 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 one or more Network Provider to create virtual network

services or offer end-to-end services to their customers. A Service Provider may be a Network Provider such that some or all of the resources used are owned by the Service Provider. A Virtual Network Service Provider is a special type of Service Provider in that they might own no physical equipment or infrastructure, or might have only limited physical infrastructure and require virtual resources to be supplied to them by another Service Provider to offer the final service. A Virtual Network Service Provider only provide services built upon a virtual network infrastructure. The rest of this document does not distinguish between a Virtual Network Service Provider and Service Provider.

o 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.

- o Network Virtualization:

Network virtualization, refers to allowing the customers to utilize certain network resources as if they owned them, and thus allows the customers to control their allocated resources in a way most optimal for 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.

- o 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 resources providing connectivity bandwidth and traffic engineering for client layer services, such that resource guarantees may be provided to customers. Transport networks discussed in this document different types of connection-oriented networks including both 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/WSO), MPLS-TP, MPLS-TE, as well as other emerging network technologies with connection-oriented behavior.

[2. Objectives and Functional Requirements](#)

[2.1 Use Cases](#)

A group of Service Providers and Network Providers have identified a number of key use cases that identify key application scenarios for how ACTN may be used.

[2.1.1](#) Packet Transport Networks (PTN) in Mobile Backhaul Networks

The Packet Transport Networks (PTN) Network Provider may use ACTN to improve efficiency of provision and operation, optimize the resources utilization, and promote the customer's experiences. The Internet-Draft [[CHENG](#)] discusses the key requirements for ACTN in a PTN environment, these include:

- o Faster End-to-End Enterprise services Provisioning
- o Multi-layer coordination in L2/L3 Packet Transport Networks
- o Optimizing the network resources utilization (supporting various performances monitoring matrix, such as traffic flow statistics, packet delay, delay variation, throughput and packet-loss rate)
- o Virtual Networks Operations for Multi-domain Packet Transport Networks

[2.1.2](#) Packet Optical Integration (POI)

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. The Internet-Draft [[DHODY](#)] outlines the Packet Optical Integration (POI) use case for ACTN,

The Internet-Draft [[DHODY](#)] discusses the key requirements for ACTN for the Packet Optical Integration (POI) environment, requirements include:

- o Packet Optical Integration to support Traffic Planning, performance Monitoring, automated congestion management and Automatic Network Adjustments.
- o Protection and Restoration Synergy in Packet Optical Multi-layer network.

- o Service Awareness and Coordination between Multiple Network Domains.

[2.1.3](#) Multi-domain Data Center Interconnect

Data center operators 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 for dynamic and flexible applications and services.

The Internet-Draft [[FANG](#)] discusses the key requirements for ACTN for the data center interconnect environment, requirements include:

- o Multi-domain Data Center Interconnection to support VM Migration, Global Load Balancing, Disaster Recovery, On-demand Virtual Connection/Circuit Services.
- o The interfaces between the Data Center Operation and each transport network domain should support standards-based abstraction with a common information/data model to support the following:
 - 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.
 - Network Path Computation Request from the Data Center Operation to each transport network domain to estimate the path availability.
 - Network Virtual Connections/Circuits Request from the Data Center Operation to each transport domain to establish end-to-end virtual connections/circuits (with type, concurrency, duration, SLA.QoS parameters, protection.reroute policy options, policy constraints such as peering preference, etc.).
 - Network Virtual Connections/Circuits Modification Request.

[2.1.4](#) On-demand E2E Connectivity Services in Multiple Vendor Domain Transport Networks

There is a need for creation and operation of a virtualized environment supporting the viewing and controlling different vendor domains, including on-demand network connectivity

Internet-Draft

ACTN PS

June 2015

service across a single operator environment. 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.

The Internet-Draft [[KLEE](#)] highlights on-demand edge-to-edge (E2E) connectivity service requirements in multiple vendor domain transport networks, which include:

- o Two-stage path computation capability in a hierarchical control architecture (MDSC-PNC) and a hierarchical composition of integrated network views.
- o Coordination of signal flow for E2E connections.
- o Abstraction of:
 - Inter-connection data between domains
 - Customer Endpoint data
 - The multiple levels/granularities of the abstraction of network resource (which is subject to policy and service need).
 - 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).

[2.1.5](#) Multi-Tenant Virtual Network Operators

Creation and operation of multi-tenant virtual networks that use the common core network resources is important to facilitate rapid deployment of new services, including more dynamic and elastic services, and improve overall network operations and scaling of existing services.

The Internet-Draft [[KUMAKI](#)] discusses multi-tenant virtual networks that use the common core network resources, requirements include:

- o On-demand Virtual Network Service Creation
- o Domain Control Plane/Routing Layer Separation
- o Independent service Operation for Virtual Services from control of other domains
- o Multiple service level support for each VN (e.g., bandwidth and latency for each VN service).

- o VN diversity/survivability should be met in physical network mapping.
- o VN confidentiality and sharing constraint should be supported.

[2.1.6](#) Virtual Network Operation for Multiple Domains in a Single Operator Network

Virtual network operation for multiple domains in a single operator network is required. This would facilitate the application of virtual network abstractions to network operations. These abstractions will create a virtualized environment supporting the viewing and controlling different domains as a single virtualized network.

This use case is discussed in more detail in [[LOPEZ](#)], requirements include:

- o 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.
- o End-to-end connection lifecycle management.
- o Invocation of path provisioning request to each domain (including optimization requests).
- o Invocation of path protection/reroute to the affected domain(s).
- o End-to-end network monitoring and fault management. This could imply potential KPIs and alarm correlation capabilities.
- o End-to-end accounting and generation of detailed records for resource usage.

- o End-to-end policy enforcement

[2.1.7](#) Mobile Virtual Network Operation for Multiple Domains in a Single Operator Network

The use-case for mobile virtual networks with single operator Networks is discussed in [\[SHIN\]](#).

- o Resource abstraction: operational mechanisms in mobile backhaul network to give the current network usage information for dynamic and elastic applications be provisioned dynamically with QoS guarantee.

Lee & King

Expires December 10, 2015

[Page 10]

Internet-Draft

ACTN PS

June 2015

- o Load balancing or for recovery, the selection of core DC location from edge constitutes a data center selection problem.
- o Multi-layer routing and optimization, coordination between these two layers.

[2.1.8](#) Dynamic Service Control based on Performance Monitoring

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 may be used to support dynamic service control of network resources based on the aforementioned performance monitoring. This use case is discussed in [\[XU\]](#), requirements include:

- o Dynamic Service Control Policy enforcement and Traffic/SLA Monitoring:
 - 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.

[3.](#) Relationship with Existing Technologies & Other Industry Initiatives

[3.1.](#) 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:

- o Protocol mechanisms used to tunnel the traffic;
- o Tunnel termination point and/or location;
- o Type of connectivity, site-to-site or remote-access;

- o 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.

[3.2.](#) 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.

[3.3.](#) Other Industry Initiatives

Lee & King

Expires December 10, 2015

[Page 12]

Internet-Draft

ACTN PS

June 2015

ONF Architecture [[ONF-SDN-ARCH](#)] describes various arrangements of SDN controllers.

TM Forum's [[TR215](#)] and [[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.

[4.](#) Motivations for Additional Functionality

[4.1.](#) Business Objectives

The 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 end-to-end services and content (i.e., web and email) to its customers. Other 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:

- o A fixed or mobile Internet Service Provider (ISP) which provides 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 significantly 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.

[4.2.](#) 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.

[4.3.](#) 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.

[4.4.](#) 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.

[4.5.](#) 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.

5. ACTN Objectives

The overall goal of enabling network abstraction and multiple concurrent virtual networks to coexist on a shared physical infrastructure comprised of multiple physical layers 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 transport metrics and constraints. Moreover, the model of the physical layer resources may need dynamic collection of the status and availability of the underlying transport network infrastructure.

5.1. Capability and Resource Visibility

It may be necessary for the application or Customer to obtain Information about available capabilities and available network resources, for example, a view and control of abstracted resource. 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:

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

- o Information about the provider (i.e., informative data about the resource owner)
- o Geographical information about the resources to be consumed (i.e., geolocation of the resources for preventing legal concerns that could appear in the provision of some services).
- o Information about resource cost, consumption, etc. (i.e., energy efficiency per transmitted bit, monetary cost of the resource usage per time unit, etc.).
- o Information about achievable resiliency (i.e., protection/restoration capabilities, recovery time, etc.).

[5.2.](#) Network Programmability

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.

A programmable interface should provide customers with the capabilities to dynamically create, deploy, and operate services in response to customer and application demands.

[5.3.](#) Common Data Models

The data model that describes the abstraction of the underlying transport network should be agnostic to each technology type within the ACTN framework. The model will provide a uniform structure which is extensible to support any future technologies.

The model 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.

The data model can be decomposed into the following elements.

- o Attributes
- o Metrics

o Semantics

o Administrative information (resource ownership)

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), Service Level Agreements (SLA) customization (e.g., the particularization of the collected metrics according to the customer interests), etc.

[5.4. 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 would be capable of employing appropriate scheduling algorithms in a centralized entity, or alternatively distributed across all of the network elements.

[5.5. Slicing](#)

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

[5.6. Adaptability](#)

Adaptability of services would allow the Service Provider, user, and application to request modification of existing virtual network resources that have been assigned. This may include resizing of bandwidth, modification of the underlying topology, and adding/removing connectivity points to modify the virtual network topology itself.

[5.7.](#) Allocation

Lee & King

Expires December 10, 2015

[Page 17]

Internet-Draft

ACTN PS

June 2015

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 times on a virtual node, and fixed loss and delay characteristics on the virtual links. This should be governed by 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 the necessary scheduling capability.

[5.8.](#) Isolation

Isolation, both of physical underlay infrastructure and of co-existing virtual networks, is required for management and confidentiality reasons. Additionally there must be no leakage of traffic between different customers. Furthermore, there must be mechanisms that ensure that once network slices are assigned, Customer and Application services do not compete for the transport resources that support their virtual networks.

Within their virtual networks, 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 of other coexisting virtual networks.

It must also be possible for many virtual networks to share the underlying infrastructure (multi-tenant), without impacting

the performance of applications utilizing the virtual networks.

5.9. Manageability

A broad range of capabilities will need to be provided through a set of well-defined interfaces. These capabilities apply to the management of end-to-end services and include the ability to request, control, provisioning, monitoring, resilience, adapt, and re-optimize those services. Specifically it should be possible to provide the following functions.

- o Control of virtual network resources. This control must be capable of delivering end-to-end services with optimization of connectivity and virtual infrastructure. Such optimization is based on client interface and application demands, technology constraints (bandwidth, latency, jitter, function, etc.), and commercial constraints (energy, customer

SLA, etc.).

- o Automation of virtual service and function requests and objectives, and providing on-demand and self-service network slicing subject to policy constraints set by the operators of the underlying physical networks, and under the control of commercial agreements between all parties.
- o Infrastructure elasticity to allow rapid provisioning, automatic scaling out, or in, of virtual resources.
- o Virtual resource monitoring
- o Control of bandwidth, energy consumption and quality of service/packet scheduling.

5.10. 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 requests specific resilience requirements on the offered transport service. For instance, the customer can request transport protection through the provision of disjoint paths 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.

[5.11.](#) Security

Network programmability may introduce new security and misconfiguration vulnerabilities. These must be investigated and discussed, and then solved. 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 to separate 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 are as follows.

- o 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.
- o Security aspects from the customer/provider relationship point of view. For instance aspects like authentication, authorization, logging, etc.

[5.12.](#) Policy

To be discussed.

[5.13. Technology Independence](#)

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

[5.14. Optimization](#)

The service provider must be able 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, re-utilization of vacant resources, etc.).

[5.15. Multi-domain Support](#)

A given customer could be required to compose an end-to-end transport service by using network capabilities from different service providers that may be internal organizations or external entities. 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 to give the customer the possibility of composing multi-provider transport services.

[5.16. Architectural Principles](#)

Lee & King

Expires December 10, 2015

[Page 20]

Internet-Draft

ACTN PS

June 2015

[5.16.1. 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, spanning part or all of the underlying physical networks.

[5.16.2. 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.

[5.16.3. 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 is known as "recursion" or "nesting" of network slices.

[5.16.4. Legacy Support and Interoperability](#)

The ability 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.

[5.17. Other Related Work](#)

[5.17.1. 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.

[5.17.2. Connectivity Provisioning Negotiation Protocol \(CPNP\)](#)

[[I-D.boucadair-connectivity-provisioning-protocol](#)] specifies the Connectivity Provisioning Negotiation Protocol (CPNP) which could be 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 Connectivity Provisioning Profile (CPP) template

allows for:

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

[6. References](#)

[6.1. 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-09](#) (work in progress), March 2015.

[I-D.boucadair-network-automation-requirements]

Boucadair, M. and C. Jacquenet, "Requirements for Automated (Configuration) Management", [draft-boucadair-network-automation-requirements-05](#) (work in progress), February 2015.

[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-lee-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.

Internet-Draft

ACTN PS

June 2015

Recommendation, September 2003, available from
<<http://www.itu.int>>.

[Y.1313] Y.1313 - Layer 1 Virtual Private Network service and network architectures, ITU-T Recommendation, July 2004, available from <<http://www.itu.int>>.

[TR215] TM Forum TR251, Logical Resource Network Model Advancements and Insights, August 2014, <<https://www.tmforum.org>>.

[TR225] TM Forum TR225, Logical Resource: Network Function Model, June 2015, <<https://www.tmforum.org>>.

[ONF-SDN-ARCH] Software Defined Network Architecture, ONF TR-502, June 2014, <<https://www.opennetworking.org/>>.

7. Acknowledgements

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

8. IANA Considerations

This problem statement document makes no requests for IANA action.

9. 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

Lee & King

Expires December 10, 2015

[Page 24]

Internet-Draft

ACTN PS

June 2015

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

Lee & King

Expires December 10, 2015

[Page 25]

Internet-Draft

ACTN PS

June 2015