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..2
2. Operational Issues in Multi-domain Networks....................3
3. Virtual Network Operations for Multi-domain Networks..........6
   3.1. Responsibilities of Domain Control/Management Entities....7
   3.2. Responsibilities of the VNO Coordinator..................8
   3.3. Virtual Network Operations Interface (VNO-I).............9
4. References...9
Author's Addresses...10
Intellectual Property Statement..................................10
Disclaimer of Validity...10

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.

```
                                               +----------------------+
                                               |   +---+ DC Domain B  |
                                               |   |EP6|              |
                                               |   +---+              |
                                               |      |               |
                                               |      |--------       |
                                               |   ///         \\\    |
                           +----------------+  | //               \\  |
                           | TN Domain      |  ||                   | |
+------------------------+ |      ----     -|--||   Data Center B   | |
| DC Domain A            | |   //-    -\\ | |  ||                   | |
|        ---------       | |  /          \| |  | \\              //  |
|     ///         \\\    | | /            \ |  |   \\\        ///    |
|   //              \\  | ||              ||  |      ---------       |
|  |                   | | ||   Transport  ||  +----------------------+
|  |   Data Center A   |-|-||    Network   ||  +----------------------+
|  |                   | | ||              ||  |      ---------       |
|   \\              //  | | \            / |  |   ///        \\\    |
|     \\\         ///    | |  \          /| |  | //               \\  |
|     |  --------- |     | |   \\-    -// | |  ||                   | |
|     |            |     | |      ----    | |  ||   Data Center C   | |
|   +---+        +---+   | |       |       -|--||                   | |
|   |EP1|        |EP2|   | |       |        |  | \\              //  |
|   +---+        +---+   | |     +---+      |  |   \\\        ///    |
+------------------------+ |     |EP3|      |  |     |---------  |    |
                           |     +---+      |  |     |           |    |
                           |                |  |   +---+      +---+  |
                           +----------------+  |   |EP4|      |EP5|  |
                                               |   +---+      +---+  |
                                               |      DC Domain C     |
                                               +----------------------+
```

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.

```
                        +----------------------+
                        |    VNO Coordinator   |
                        +----------------------+
                                   |
                                   | VNO-I
              .-------------------------------------------.
              |             |             |             |
         +----------+  +----------+  +----------+  +----------+
         |    DCN   |  |    DCN   |  |    DCN   |  |          |
         | Domain A |  | Domain B |  | Domain C |  | TN Domain|
         | Control  |  | Control  |  | Control  |  | Control  |
         |          |  |          |  |          |  |          |
         +----------+  +----------+  +----------+  +----------+
               |             |             |             |
            /----\        /----\        /----\        /----\
          //      \\    //      \\    //      \\    //      \\
         |   DC A   |  |   DC B   |  |   DC C   |  | Transport|
          \\      //    \\      //    \\      //    \\Network/
            \----/        \----/        \----/        \----/
```

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